Representation theory of finite groups
(UNPOLISHED DRAFT)

Alexander Yom Din

May 30, 2020

Contents

1 Introduction, conventions, notations, etc.

These notes are very preliminary, contain a lot of unfinished things, etc.! I don't claim originality etc.!

1.1 Sources

1. Serre, Linear Representations of Finite Groups
2. Etingof, `http://www-math.mit.edu/~etingof/replect.pdf`
3. Bernstein, lectures on representation theory of finite groups

1.2 Notations

Throughout the notes, G is a finite group and k a field.

Given $g \in G$, we denote by $C_g \subset G$ the conjugacy class containing g. We denote by $Conj(G)$ the set of conjugacy classes in G.

Given a set X and a ring A, we will denote by $Fun_A(X)$ the A-module of A-valued functions on X. We will simply write $Fun(X)$ for $Fun_k(X)$, where k is our habitual ground field. For $x \in X$, wel denote by $\delta_x \in Fun_A(X)$ the function which is equal to 1 at x and to 0 at all other points. More generally, for a subset $Y \subset X$, we denote by $\delta_Y \in Fun_A(X)$ the function which is equal to 1 at points of Y and to 0 at all other points. By $f_1 \cdot f_2$ we denote the pointwise multiplication (in the course, when X is a group, we will have another product, the convolution product $f_1 \star f_2$).

2 General theory

2.1 Definitions

Definition 2.1. Definition of **category**, of **k-linear category**.

Example 2.2. *Examples of categories - the category of sets, the category of finite groups. Examples of k-linear categories - the category $Vect_k$ of finite-dimensional vector spaces over k.*

Definition 2.3. A (finite) **G-set** is a pair (X, α), where X is a (finite) set and $\alpha : G \to S(X)$ is a homomorphism. A morphism between G-sets $(X, \alpha), (Y, \beta)$ is a map $\tau : X \to Y$ satisfying $\tau(\alpha(g)x) = \beta(g)\tau(x)$ for all $x \in X, g \in G$. We have the category of G-sets, denoted by $Set(G)$.

We will usually write just X instead of (X, α) and gx instead of $\alpha(g)x$.

Example 2.4. *We have the "trivial" G-set $*$ (one point), the "regular" G-set R (G with left action), the $S(X)$-set X.*

Definition 2.5. A (finite-dimensional) **representation of** G is a pair (V, ρ), where V is a finite-dimensional vector space over k and $\rho : G \to GL(V)$ is a homomorphism. A **morphism** between representations of G $(V, \rho), (W, \omega)$ is a k-linear map $T : V \to W$ satisfying $T(\rho(g)v) = \omega(g)T(v)$ for all $v \in V, g \in G$. We have the k-linear category of representations of G, denoted by $Rep(G)$. We denote by $Hom_G(V, W)$ for the vector space of morphisms.

We will usually write just V instead of (V, ρ) and gv instead of $\rho(g)v$.

Definition 2.6. Definition of a **functor** between categories, a **k-linear functor** between k-linear categories. Definition of a **contravariant functor**.

Definition 2.7. We define the ("fat") **linearization functor** $Lin : Set(G)^{op} \to Rep(G)$ as follows. $Lin(\alpha, X)$, as a vector space, is $Fun(X)$. The representation ρ is given by $(\rho(g)f)(x) = f(\alpha(g^{-1})x)$. Given a morphism $\tau : (X, \alpha) \to (Y, \beta)$, we define $Lin(\tau)(f) = f \circ \tau$.

We also have a "thin" linearization functor $lin : Set(G) \to Rep(G)$, defined by setting $lin(X, \alpha)$ to be the k-vector space with basis X, etc.

Remark 2.8. The procedures Lin, lin are somewhat reminiscent of "quantization".

Definition 2.9. We define the **trivial representation** $Triv \in Rep(G)$ as $Lin(pt)$, and the **regular representation** $Reg \in Rep(G)$ as $Lin(R)$. Concretely: ...

2.2 Constructions

Definition 2.10. Direct sum, Hom, dual, tensor product...

Definition 2.11. Subrepresentation, quotient representation.

Definition 2.12. Kernel, cokernel, image.

Remark 2.13. The k-linear category $Rep(G)$ is an **abelian category**.

2.3 Irreducible representations

Definition 2.14. A representation $E \in Rep(G)$ is called irreducible, if $E \neq 0$, and E contains no subrepresentations except 0 and E.

Definition 2.15. Denote by $Irr(G)$ the set of isomorphism classes of irreducible representations in $Rep(G)$.

Lemma 2.16 (Schur's lemma)**.** *Let $E \in Rep(G)$ be irreducible. Then $End_G(E)$ is a division algebra, i.e. every non-zero G-endomorphism of E is an automorphism.*

Proof. Let $T \in End_G(E)$. Since $Ker(T)$ is a subrepresentation of E, and E is irreducible, we get that $Ker(T) = 0$ or $Ker(T) = E$, so T is an automorphism or $T = 0$ respectively. □

Corollary 2.17. *Suppose that k is algebraically closed. Let $E \in Rep(G)$ be irreducible. Then $End_G(E) = k \cdot Id_E$.*

Proof. This follows from the fact that k is the only division algebra over k. Indeed, let D be a division algebra over k. For every $d \in D$, we claim that $d^{-1} \in k[d]$. This follows by considering the minimal polynomial of d acting on D by left multiplication.

Thus, we deduce that for every $d \in D$, $k[d]$ is a commutative division algebra, i.e. a field. Since k is algebraically closed, we obtain $k[d] = k$, i.e. $d \in k$. In other words, $D = k$. □

Lemma 2.18 (Schur's lemma, part 2)**.** *Let $E, F \in Rep(G)$ be irreducible representations. Then $Hom_G(E, F) = 0$ or else E and F are isomorphic.*

Proof. Let $T \in Hom_G(E, F)$. Then $Ker(T) = 0$, or $T = 0$, and also $Im(T) = F$ or $T = 0$. So, if $T \neq 0$, we get that T is an isomorphism. □

2.4 Decomposition into irreducible representations

Let $(V, \pi) \in Rep(G)$. We define $V^G := \{v \in V \mid \pi(g)v = v \ \forall g \in G\}$. Also, define $Av : V \to V$ by $Av := \frac{1}{|G|} \sum_{g \in G} \pi(g)$ (one can write Av_G^V or Av_G or Av^V instead of Av when one wants to emphasize V or G).

Lemma 2.19. *The operator Av is a projection operator with image V^G. Furthermore, given a G-morphism $\phi : V \to W$, we have $Av^W \circ \phi = \phi \circ Av^V$.*

Definition 2.20. The category $Rep(G)$ is called **semisimple**, if for every $V \in Rep(G)$ and a subrepresentation $W \subset V$, there exists a subrepresentation $U \subset V$, such that $V = W \oplus U$.

Theorem 2.21 (Maschke)**.** *The category $Rep(G)$ is semisimple (under our assumptions, where G is a finite group and k is of characteristic 0).*

Proof.

Proof 1: We know from linear algebra that there exists a complement U_0 to W, which is not necessarily a subrepresentation. We have the corresponding projection $P_0 : V \to V$ on W along U_0. We can consider P_0 as an element in the representation $Hom(V, V)$, and construct its average $P := Av(P_0)$. Concretely, $P := \frac{1}{|G|} \sum_{g \in G} \pi(g) P_0 \pi(g)^{-1}$. Then $P \in Hom(V, V)^G = Hom_G(V, V)$, i.e. P is a G-morphism, and it is immediate to check that P is again a projection operator with image W. This implies that $U := Ker(P)$ is a subrepresentation such that $V = W \oplus U$.

Proof 2: This proof works when $k = \mathbb{R}$ or $k = \mathbb{C}$. Let us consider any inner product Φ_0 on V. Let us average it: $\Phi(v_1, v_2) := \frac{1}{|G|} \sum_{g \in G} \Phi_0(\pi(g)v_1, \pi(g)v_2)$. Then Φ is still an inner product on V (here we use the interesting fact that the average of a positive form is clearly positive, although the average of a non-degenerate form is not necessarily non-degenerate). Moreover, the inner product Φ is G-invariant, i.e. $\Phi(\pi(g)v_1, \pi(g)v_2) = \Phi(v_1, v_2)$ for all $v_1, v_2 \in V$ and $g \in G$. Take now the orthogonal complement U to W in V, w.r.t. the form Φ.

Proof 3: Let us rephrase: We want to show that $V \to V/W$ admits a section as a morphism of representations, i.e. we want to show that there exists a G-morphism $V/W \to V$, such that the composition $V/W \to V \to V/W$ is the identity. We can make a more general formulation: Given a surjective G-morphism $V \to Z$ and a G-representation Y, we want to show that $Hom_G(Y, V) \to Hom_G(Y, Z)$ is surjective. Clearly, we have a surjective G-morphism $Hom(Y, V) \to Hom(Y, Z)$, and by applying the operation $(\cdot)^G$ to it we obtain our map. So, we can phrase the problem: Given a surjective G-morphism $\phi : V \to Z$, we want to show that $V^G \to Z^G$ is surjective as well. So, take $z \in Z^G$ and take any $v_0 \in V$ such that $\phi(v_0) = z$. Set $v := Av(v_0)$. Then one has $v \in V^G$ and $\phi(v) = \phi(Av(v_0)) = Av\phi(v_0) = Av(z) = z$.

□

Remark 2.22. We see from proofs 1 and 3 that the theorem holds also when the characteristic of k is positive, but does not divide $|G|$.

Exercise 2.1. *Show that $Rep_{\mathbb{C}}(\mathbb{Z})$ and $Rep_{\mathbb{F}_p}(\mathbb{F}_p)$ are not semisimple.*

Corollary 2.23. *Let $V \in Rep(G)$. Then we can find irreducible $E_1, \ldots, E_k \in Rep(G)$ such that $V \simeq E_1 \oplus \ldots \oplus E_k$.*

Notice that in the above corollary, the number of E_i's which are isomorphic to a given irreducible representation E does not depends on the choice of the decomposition; Indeed, this number is equal to $\frac{\dim Hom_G(E,V)}{\dim Hom_G(E,E)}$. So, we can define:

Definition 2.24. Let $V \in Rep(G)$ and $[E] \in Irr(G)$. Then we define the multiplicity with which $[E]$ appears in V as the number of E_i's isomorphic to E in a decomposition $V \simeq E_1 \oplus \ldots \oplus E_k$. We also write $[V : E]$ for that multiplicity. We say that E appears in V, if $[V : E] \neq 0$.

Remark 2.25. A better approach for defining multiplicites would be to invoke the Jordan-Holder theorem. That way it will be applicable also in positive characteristic.

Exercise 2.2. *Show that for $V \in Rep(G)$ and $X \in Set(G)$, one has (functorially) $Hom_G(lin(X), V) \cong Hom_G(X, delin(V))$, where $delin : Rep(G) \to Set(G)$ is the functor sending a representation to itself, viewed as a G-set (i.e. we forget the k-linear structure). In categorical language, lin is left adjoint to delin. Deduce from this that (assuming that k is algebraically closed) the number of times a given $[E] \in Irr(G)$ enters Reg is $\dim E$. As a consequence, deduce that $\sum_{[E] \in Irr(G)} (\dim E)^2 = |G|$.*

2.5 The group algebra

Let us denote by $\delta_g \in Fun(G)$ the function which equals to 1 on g and 0 on all the rest of the elements. The functions $(\delta_g)_{g \in G}$ form a basis of $Fun(G)$.

The vector space $Fun(G)$ admits the pointwise algebra structure

$$(f_1 \cdot f_2)(g) := f_1(g) f_2(g).$$

This structure has nothing to do with the multiplication in G. But $Fun(G)$ admits also another algebra structure:

Definition 2.26. Denote by $\star$ the algebra structure on $Fun(G)$ given by $\delta_g \star \delta_h = \delta_{gh}$ for $g, h \in G$. In a formula:

$$(f_1 \star f_2)(g) = \sum_{g_1 g_2 = g} f_1(g_1) f_2(g_2) = \sum_{h \in G} f_1(gh^{-1}) f_2(h).$$

Lemma 2.27. *Let $(V, \pi) \in Rep(G)$. Then there exists a unique algebra morphism $\widetilde{\pi} : (Fun(G), \star) \to End(V)$ such that $\widetilde{\pi}(\delta_g) = \pi(g)$.*

Remark 2.28. In what follows, we will denote $\widetilde{\pi}$ simply by π, by abuse of notation.

Denote by $Fun^{cent}(G)$ the center of the algebra $(Fun(G), \star)$. We have $Fun^{cent}(G) = \{f \in Fun(G) \mid f(ghg^{-1}) = f(h)\ \forall g, h \in G\}$. In other words, this is the subspace of functions constant on conjugacy classes.

Definition 2.29.

1. Define a symmetric bilinear form $(\cdot, \cdot)$ on $Fun(G)$ by:

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

2. For $f \in Fun(G)$, define $f^* \in Fun(G)$ by $f^*(g) = f(g^{-1})$.

3. For $f \in Fun(G)$, define $Av(f) = \frac{1}{|G|} \sum_{g \in G} f(g)$ (viewed as an element in k, but also commonly as a constant function in $Fun(G)$).

Lemma 2.30. *The form $(\cdot, \cdot)$ is non-degenerate, both on $Fun(G)$ and on $Fun^{cent}(G)$.*

Proof. For $Fun(G)$ this is clear, since $|G|(\delta_{g^{-1}}, f) = f(g)$. As for $Fun^{cent}(G)$, consider the operator $Ce : Fun(G) \to Fun^{cent}(G)$ given by

$$Ce(f)(g) := \frac{1}{|G|} \sum_{h \in G} f(h^{-1} g h).$$

For $f \in Fun^{cent}(G)$ and $f' \in Fun(G)$, we have $(Ce(f'), f) = (f', f)$. Hence, the non-degenerateness for $Fun^{cent}(G)$ follows from that for $Fun(G)$. □

3 Character theory

3.1 Definition

Definition 3.1. Let $(V, \pi) \in Rep(G)$. Define the character of V, $\chi_V \in Fun(G)$, to be the function

$$\chi_V(g) := Tr_V(\pi(g)).$$

Remark 3.2. The character generalizes the dimension. Indeed, $\chi_V(e) = \dim(V)$.

Exercise 3.1. *Let $V \in Vect$ and $T \in End(V)$. Define generating series*

$$A(x) = \sum_{k \geq 0} Tr(T^k) x^k.$$

Denote $n = \dim(V)$ and denote by p_T the characteristic polynomial of T. Show that

$$exp \int \frac{A(x) - n}{x} = \frac{1}{x^n p_T(x^{-1})}$$

or equivalently

$$\frac{d}{dx} log \frac{1}{x^n p_T(x^{-1})} = \frac{A(x) - n}{x}.$$

Thus, knowing the traces of all powers is equivalent to knowing the characteristic polynomial.

Exercise 3.2. *Let G act on a finite set X, and consider $Lin(X) \in Rep(G)$. Show that $\chi_{Lin(X)}(g)$ is equal to the number of fixed points of g acting on X.*

Lemma 3.3. *For every $V \in Rep(G)$, we have $\chi_V \in Fun^{cent}(G)$.*

Proof. This immediately follows from the property $Tr(TS) = Tr(ST)$ of the trace. □

Claim 3.4. *For $V, W \in Rep(G)$:*

1. $\chi_{V \oplus W} = \chi_V + \chi_W$.
2. $\chi_{V \otimes W} = \chi_V \cdot \chi_W$.
3. $\chi_{V^*} = \chi_V^*$.
4. $\chi_{Hom(V,W)} = \chi_V^* \cdot \chi_W$.
5. $\chi_{V^G} = Av(\chi_V)$.

Proof.

1. A simple computation.
2. A simple computation.
3. A simple computation.
4. We have an isomorphism of G-representations

$$Hom(V, W) \cong V^* \otimes W,$$

so this item can be deduced from items (2) and (3).

5. Write (V, π) for V. Notice that $\chi_{V^G} = \dim V^G$ (a constant function). On the other hand, we have the projection operator $\frac{1}{|G|} \sum_{g \in G} \pi(g)$, whose image is V^G, and thus its trace is equal to $\dim V^G$. Finally, notice that the trace of that operator is exactly $Av(\chi_V)$.

□

Exercise 3.3. *Let $V \in Rep(G)$. Consider the symmetric square and the alternating square $S^2V, \Lambda^2 V \in Rep(G)$. Show that*

$$\chi_{S^2V}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)), \quad \chi_{\Lambda^2 V}(g) = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2)).$$

Corollary 3.5. *For $V, W \in Rep(G)$, we have $\dim Hom_G(V,W) = (\chi_V, \chi_W)$ (as elements in k, and hence as integers since k has characteristic 0).*

Proof. Indeed,

$$\dim Hom_G(V,W) = \dim Hom(V,W)^G = Av(\chi_{Hom(V,W)}) = Av(\chi_V^* \cdot \chi_W) = (\chi_V, \chi_W).$$

□

Remark 3.6. In the context of categorification, one can interpret the last corollary as saying that $(\cdot,\cdot)$ is a decategorification of Hom_G.

Corollary 3.7. *The system $(\chi_E)_{[E]\in Irr(G)}$ is an orthogonal system in $Fun^{cent}(G)$ w.r.t. $(\cdot,\cdot)$. In particular, it is linearly independent.*

Lemma 3.8. *For $f \in Fun(G)$ and $(V,\pi) \in Rep(G)$, we have*

$$Tr_V(\pi(f)) = |G|(f^*, \chi_V).$$

Proof. Write $f = \sum_{g\in G} f(g)\delta_g$. Then

$$Tr_V(\pi(f)) = Tr_V(\sum_{g\in G} f(g)\pi(g)) = \sum_{g\in G} f(g) Tr_V(\pi(g)) = \sum_{g\in G} f(g)\chi_V(g) = |G|(f^*, \chi_V).$$

□

Corollary 3.9. *Suppose that k is algebraically closed. Then For $f \in Fun^{cent}(G)$ and irreducible $(V,\pi) \in Rep(G)$, we have*

$$\pi(f) = \frac{|G|}{\dim(V)}(f^*, \chi_V) \cdot Id_V.$$

Proof. The operator $\pi(f)$ acts by a scalar on the irreducible V, by Schur's lemma. The previous lemma allows to find that scalar. □

Claim 3.10. *Suppose that k is algebraically closed. Then the system $(\chi_E)_{[E]\in Irr(G)}$ spans $Fun^{cent}(G)$.*

Proof. Let $f \in Fun^{cent}(G)$, and suppose that $(f, \chi_E) = 0$ for every irreducible E. We want to show that $f = 0$. By claim 3.9, we see that f^* acts by zero on every irreducible representation. But then f^* acts by zero on every representation (since every representation can be written as a direct sum of irreducible representations). In particular, f^* acts by zero on the regular representation, which clearly implies that $f^* = 0$ and so $f = 0$. □

Corollary 3.11. *Suppose that k is algebraically closed. Then the number of isomorphism classes of irreducible representations is equal to the number of conjugacy classes in G.*

Remark 3.12. We now know that $\sum_{[E]\in Irr(G)} \dim(E)^s$ is equal to the number of conjugacy classes in G when $s = 0$, and to $|G|$ when $s = 2$. One can wonder about other values of s. There is a formula of Frobenius for $s = 2, 0, -2, -4, \ldots$: Fix $n \geq 0$. Then

$$\sum_{[E]\in Irr(G)} \dim(E)^{2-2n} = \frac{1}{|G|^{2n-1}} |c_n^{-1}(e)|,$$

where $c_n : G^{2n} \to G$ is given by $c_n(x_1, y_1, \ldots, x_n, y_n) = [x_1, y_1] \cdots [x_n, y_n]$.

3.2 The Fourier transform

In this subsection, we assume that k is algebraically closed.

Let us define a linear map

$$\mathcal{F} : Fun^{cent}(G) \to Fun(Irr(G))$$

by declaring $\mathcal{F}(f)([E])$ to be the scalar by which f acts on E.

Proposition 3.13. *The map $\mathcal{F} : (Fun^{cent}(G), \star) \to (Fun(Irr(G)), \cdot)$ is an isomorphism of algebras.*

Proof. It is clear that $\mathcal{F}$ is a homomorphism of algebras. To show that it is bijective, recall that $\mathcal{F}(f)([E]) = \frac{|G|}{\dim(E)}(f^*, \chi_E)$, and recall that the χ_E's form an orthogonal basis for $Fun^{cent}(G)$. □

Claim 3.14. *For irreducible $E \in Rep(G)$, we have*

$$\mathcal{F}(\chi_E)([F]) = \begin{cases} \frac{|G|}{dim(E)} \text{ if } [F] = [E^*] \\ 0 \text{ if } [F] \neq [E^*] \end{cases}.$$

Proof. Follows from the formula $\mathcal{F}(f)([F]) = \frac{|G|}{\dim(F)}(f^*, \chi_F)$. □

Corollary 3.15. *For irreducible $E, F \in Rep(G)$, we have*

$$\chi_E \star \chi_F = \begin{cases} \frac{|G|}{dim(E)} \cdot \chi_E \text{ if } [F] = [E] \\ 0 \text{ if } [F] \neq [E] \end{cases}.$$

Proof. Since $\mathcal{F}$ is an algebra isomorphism, we can check these formulas after application of $\mathcal{F}$, which is done using the previous corollary. □

In other words, up to a scalar normalization, the system $(\chi_E)_{[E]\in Irr(G)}$ forms a complete system of orthogonal idempotents in $Fun^{cent}(G)$.

3.3 Noncommutative Fourier transform

Let us note that for two isomorphic irreducible $E, E' \in Rep(G)$, one has a canonical identification of algebras $End(E) \simeq End(E')$, given by choosing any G-isomorphism between E and E' (this is because, by Schur's lemma, any two such G-isomorphisms differe by a scalar). Let us hence write $End_{[E]} := End(E)$. Let us also define $Fun^{nc}(Irr(G)) := \oplus_{[E]\in Irr(G)} End_{[E]}$. It is an (non-commutative) algebra.

Let us define a linear map $\mathcal{F}^{nc} : Fun(G) \to Fun^{nc}(Irr(G))$, by declaring $\mathcal{F}^{nc}(f)([E,\pi])$ to be the linear map $\pi(f)$.

Proposition 3.16. *The map $\mathcal{F}^{nc}$ is an isomorphism of algebras, and of $(G\times G)$-representations.*

Proof. That $\mathcal{F}^{nc}$ is a homomorphism of algebras and representations is clear. To show that it is injective, notice that if $\mathcal{F}^{nc}(f) = 0$, then f acts by zero on every irreducible representation, and hence on every representation. In particular, f acts by zero on the regular representation, which clearly implies that $f = 0$.

To show that $\mathcal{F}^{nc}$ is surjective, it is enough to see that $\sum_{[E]\in Irr(G)} \dim End(E) = |G|$, which is done in exercise 2.2.

Alternatively, claim 3.19 below will establish that $\mathcal{F}^{nc}$ is surjective or, yet alternatively, it will be shown in the section on matrix coefficients (which will construct a right inverse for $\mathcal{F}^{nc}$). □

Lemma 3.17. *Let H_1, H_2 be finite groups, $E_1 \in Rep(H_1), E_2 \in Rep(H_2)$ irreducible representations. Then $E_1 \otimes E_2 \in Rep(H_1 \times H_2)$ is irreducible.*

Lemma 3.18. *Let $(E,\pi) \in Rep(G)$ be irreducible. Then the map $\pi : Fun(G) \to End(E)$ is surjective.*

Proof. Notice that we can view π as a morphism of $(G \times G)$-representations, and $End(E) \simeq E^* \otimes E$ as $(G\times G)$-representations (it is an exercise to spell out all the $(G \times G)$-actions). From the previous lemma, we obtain that $End(E)$ is an irreducible $(G \times G)$-representation. Since π is non-zero, it is surjective. □

Claim 3.19. *Let $(E_1, \pi_1), \ldots, (E_r, \pi_r) \in Rep(G)$ be pairwise non-isomorphic irreducible representations. Then the map*

$$\oplus\pi_i : Fun(G) \to \bigoplus_{1\le i\le r} End(E_i)$$

is surjective.

Proof. We use induction on r. The case $r = 1$ is dealt with in the previous lemma. Using the induction hypothesis, we see that the cokernel of $\oplus\pi_i$ is a quotient of $End(E_j)$, for every j. Since the $End(E_j)$ are non-isomorphic irreducible $(G \times G)$-representations, we see that the cokernel must be zero. □

Exercise 3.4. *Using the fact that $\mathcal{F}^{nc}$ is an isomorphism of $(G\times G)$-representations, establish orthogonality relations of the type $\sum_{[E]\in Irr(G)} \chi_E(g)\chi_E(h^{-1}) =?$ for $g, h \in G$.*

3.4 Matrix coefficients

Let $(V, \pi) \in Rep(G)$. We define a map $MC_V : End(V) \to Fun(G)$ by $MC_V(T)(g) := Tr_V(\pi(g) \circ T)$. Notice that $MC(Id_V) = \chi_V$.

We have a claim analogous to one above:

Claim 3.20. *For $V, W \in Rep(G)$:*

1. $MC_{V \oplus W}(T \oplus S) = MC_V(T) + MC_W(S)$.
2. $MC_{V \otimes W}(T \otimes W) = MC_V(T) \cdot MC_W(S)$.
3. $MC_{V^*}(T^*) = MC_V(T)^*$.
4. $MC_{Hom(V,W)}(S \circ \cdot \circ T) = MC_V(T)^* \cdot MC_W(S)$.
5. $MC_{V^G}(Av^V \circ T) = Av(MC_V(T))$.

Proof.

1. A simple computation.
2. A simple computation.
3. A simple computation.
4. Left as an exercise.
5. Left as an exercise.

□

Let us now define a linear map

$$MC : Fun^{nc}(Irr(G)) \to Fun(G),$$

given on $End(E)$ by MC_E.

Claim 3.21. *The composition $\mathcal{F}^{nc} \circ * \circ MC$ is given by the scalar $\frac{|G|}{\dim(E)}$ on $End(E)$.*

Proof. Since $\mathcal{F}^{nc} \circ * \circ MC$ is $(G \times G)$-equivariant and $End(E)$ are non-isomorphic irreducible representations of $(G \times G)$, it is clear that the composition is given by a scalar on each $End(E)$. To find the scalar, we evaluate on Id_E. □

3.5 Application of Fourier theory - Dirichlet's theorem

Let $n \in \mathbb{Z}_{\geq 1}$ and $m \in \mathbb{Z}$, such that $(m,n) = 1$. Dirichlet's theorem states that in the set $m + \mathbb{Z}n$ there are infinitely many prime numbers.

Let $\chi \in Fun((\mathbb{Z}/n\mathbb{Z})^{\times})$. We then define a function $\widetilde{\chi}$ on $\mathbb{Z}$, by setting $\widetilde{\chi}(x) = \chi([x]_n)$ if $(x,n) = 1$ (here $[\cdot]_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is the projection), and $\widetilde{\chi}(x) = 0$ otherwise. We define

$$M_\chi(s) = \sum_{p \in \mathbb{Z}_{\geq 1} \text{ prime}} \frac{\widetilde{\chi}(p)}{p^s}.$$

The main analytic fact is:

Theorem 3.22. *$M_\chi(s)$ converges for $s > 1$. Suppose that χ is an irreducible character. Then if $\chi \neq 1$, $M_\chi(s)$ is bounded as $s \to 1^+$, while if $\chi = 1$, $|M_\chi(s)| \to \infty$ as $s \to 1^+$.*

Now, we write $\delta_m = \sum_\chi c_\chi \chi$. We have $c_\chi = (\delta_m, \chi)$, and so $c_1 = Av(\delta_m) \neq 0$. We now obtain

$$M_{\delta_m} = \sum_\chi c_\chi M_\chi,$$

and thus $|M_{\delta_m}(s)| \to \infty$ as $s \to 1^+$. This implies clearly that the sum defining M_{δ_m} is infinite, which says that in the set $m + \mathbb{Z}_{\geq 0} n$ there are infinitely many primes.

Let us how to start showing the analytic fact above. We assume from here that χ is an irreducible character. We define

$$\ell_\chi(s) = \sum_{p \in \mathbb{Z}_{\geq 1}} \sum_{r \geq 1} \frac{\widetilde{\chi}(p)^r}{p^{sr} r}.$$

Then

$$|\ell_\chi(s) - M_\chi(s)| \leq \sum_p \sum_{r \geq 2} \frac{1}{p^{sr} r} \leq \sum_p \sum_{r \geq 2} \frac{1}{p^r} = \sum_p p^{-2} \frac{p}{p-1} \leq \sum_p 2p^{-2} < \infty.$$

In other words, ℓ_χ converges for $s > 1$ and the difference $\ell_\chi - M_\chi$ bounded on $[1, \infty)$, so we can prove the above theorem for ℓ_χ instead of M_χ.

We have:

$$e^{\ell_\chi(s)} = \prod_p \frac{1}{1 - \widetilde{\chi}(p) p^s} = \sum_{r \in \mathbb{Z}_{\geq 1}} \frac{\widetilde{\chi}(r)}{r^s} =: L_\chi(s).$$

This passage, from the product over primes (a "difficult" set) to the sum over positive integers (an "easy" set), facilitated by the multiplicativity of χ, can be said to be the main idea; It is certainly not possible for δ_m.

4 Induction

We skip material about adjoint functors etc.

4.1 res^G_H, ind^G_H and Ind^G_H

Let $\iota : H \to G$ be a homomorphism of groups (typically for us, the embedding of a subgroup, but it is also convenient to look at the general case). We have the obvious forgetful functor $res^G_H : Rep(G) \to Rep(H)$. We define functors $ind^G_H, Ind^G_H : Rep(H) \to Rep(G)$ as the left and right adjoint of res^G_H. We next present their concrete description.

Let $(V, \pi) \in Rep(H)$. The functor ind^G_H is given by

$$ind^G_H(V) = Fun(G) \otimes_{Fun(H)} V.$$

Here, $Fun(G)$ is viewed as a $Fun(H)$-algebra, simply by sending δ_h to $\delta_{\iota(h)}$. More concretely yet, if $H \subset G$ and $x_1, \ldots, x_r \in G$ are representatives for G/H, then

$$ind^G_H(V) = \bigoplus_{1 \leq i \leq r} "x_i" V.$$

We multiply $g"x_i"v$ by writing $gx_i = x_j h$, and then $g"x_i"v = "x_j"\pi(h)v$.

The functor Ind^G_H is given, as a vector space, by

$$Ind^G_H(V) = \{f : G \to V \mid f(x\iota(h)) = \pi(h^{-1})f(x) \ \forall x \in G, h \in H\}.$$

The G-action is given by

$$(gf)(x) = f(g^{-1}x).$$

4.2 Coinvariants

For a representation $(V, \pi) \in Rep(G)$, except of the invariants

$$V^G = \{v \in V \mid \pi(g)v = v \ \forall g \in G\},$$

we also have the coinvariants $V_G = V/\langle \pi(g)v - v \rangle_{g \in G, v \in V}$. Using $\iota : G \to *$, we can interpret $V^G = Ind^*_G V$ and $V_G = ind^*_G V$. We have a map $V^G \to V \to V_G$. If the characteristic of k is prime to $|G|$, then we have a map inverse to the above one, induced by $Av : V \to V^G$. In other words, we have a functorial isomorphism $V^G \simeq V_G$.

4.3 $ind = Ind$

Let $\iota : H \to G$ be a homomorphism of groups, and $(V, \pi) \in Rep(H)$. Let us reinterpret the two functors ind^G_H and Ind^G_H as follows. We consider $Fun(G) \otimes V$. It has an action of G, via $g(f \otimes v) = (gf) \otimes v$, where $(gf)(x) = f(g^{-1}x)$. It also has an action of H, commuting with the G-action, given by $h(f \otimes v) = (fh^{-1}) \otimes \pi(h)v$, where $(fh)(x) = f(x\iota(h))$. Then we can interpret $ind^G_H(V) = (Fun(G) \otimes V)_H$ and $Ind^G_H(V) = (Fun(G) \otimes V)^H$. We thus deduce that we have a canonical isomorphism of functors $Ind^G_H \simeq ind^G_H$.

4.4 G-equivariant sheaves

Definition 4.1. Let $X \in Set$. A **sheaf** $\mathcal{V}$ on X is the data of a k-vector space $\mathcal{V}_x$ for every $x \in X$. Sheaves on X form a k-linear category $Sh(X)$.

If $\pi : X \to Y$ is a map, we have functors $\pi^* : Sh(Y) \to Sh(X)$ and $\pi_* : Sh(X) \to Sh(Y)$ described as follows. We have $\pi^*(\mathcal{V})_x = \mathcal{V}_{\pi(x)}$ and $\pi_*(\mathcal{W})_y = \prod_{\pi(x)=y} \mathcal{W}_x$ (we omit the standard details). The functor π^* is naturally left adjoint to π_*. In particular, for $\pi : X \to *$, we denote $\Gamma := \pi_*$ (**global sections** functor).

Definition 4.2. Let $X \in Set(G)$. A **G-equivariant sheaf** $(\mathcal{V}, \alpha)$ on X is the datum of a sheaf $\mathcal{V}$ on X, and an isomorphism $\alpha : p^*\mathcal{V} \cong a^*\mathcal{V}$, where $p, a : G \times X \to X$ are given by $p(g, x) = x, a(g, x) = gx$. Let us denote by $\alpha_{g,x} : \mathcal{V}_x \to \mathcal{V}_{gx}$ the isomorphism induced by α at the point (g, x). The data should satisfy the properties: $\alpha_{h,gx} \circ \alpha_{g,x} = \alpha_{hg,x}$ and $\alpha_{e,x} = id$.

G-equivariant sheaves on X form a k-linear category $Sh(X)^G$.

Definition 4.3. Definition of an equivalence of categories.

Example 4.4. *We have an equivalence of categories $Sh(*)^G \approx Rep(G)$.*

For a G-equivariant map $\pi : X \to Y$, the functors π^*, π_* naturally extend to functors $\pi^* : Sh(Y)^G \to Sh(X)^G, \pi_* : Sh(X)^G \to Sh(Y)^G$. In particular, we have $\Gamma : Sh(X)^G \to Sh(*)^G \approx Rep(G)$.

Claim 4.5. *Let X be a transitive G-set, $x \in X$, and $H := Stab_G(x)$. Then we have a natural equivalence of categories $Sh(X)^G \approx Rep(H)$.*

Proof. Given $\mathcal{V} \in Sh(X)^G$, we have $i^*\mathcal{V} \in Sh(\{x\})^H$, where $i : \{x\} \to X$ is the inclusion. This gives a functor in one direction. In the other direction, suppose that we have $V \in Rep(H) \approx Sh(\{x\})^H$. For $y \in X$, consider $T(x, y) = \{g \in G \mid gx = y\}$. We consider now

$$\mathcal{V}_y := \{(v_g) \in \oplus_{g \in T(x,y)} "g" V \mid v_{gh} = h^{-1} v_g \ \forall g \in T(x, y), h \in H\}.$$

Given $t \in G, y \in X$, one defines $\mathcal{V}_y \to \mathcal{V}_{ty}$ by sending $(v_g)_{g \in T(x,y)}$ to $(v_{t^{-1}g})_{g \in T(x,ty)}$. One obtains a functor in the other direction (after some routine checks). Then one constructs an isomorphism of the compositions of functors with identities... □

A similar claim in mathematics is:

Claim 4.6. *Let X be a nice connected topological space. Let $x \in X$. Then there is an equivalence of categories between $Cov(X)$ and $\pi_1(X, x) - sets$.*

Proof. Given a covering, its fiber over x gives a $\pi_1(X, x)$-set. Given a $\pi_1(X, x)$-set V and a point $y \in X$, we construct $\mathcal{V}_y$ similarly to above, considering $T(x, y)$, the set of connected components of the space of paths between x and y. □

The claim above can be generalized as follows.

Claim 4.7. *Let $H \subset G$ be a subgroup. Let Y be a H-set. Then we have a natural equivalence of categories $Sh(Y)^H \approx Sh(G \times_H Y)^G$.*

To prove this claim, we will use the following:

Claim 4.8. *Let $N \subset G$ be a normal subgroup, and X a G-set, on which N acts freely. Then we have a natural equivalence of categories $Sh(X)^G \approx Sh(N \backslash X)^{G/N}$.*

Proof. We claim that an equivalence is realized by $Sh(N \backslash X)^{G/N} \to Sh(X)^G$ given by pullback along the G-equivariant map $X \to N \backslash X$. The inverse equivalence is given by considering the N-invariants in the pushforward... □

Proof (of claim 4.7 given claim 4.8). We consider $G \times X$ as a $(G \times H)$-space, via $(g, h)(g_1, x) = (gg_1h^{-1}, hx)$. We have $Sh(G \times X)^{G \times H} \approx Sh(X)^H$ (since the G-action is free) and $Sh(G \times X)^{G \times H} \approx Sh(G \times_H X)^G$ (since the H-action is free). □

Definition 4.9. Definition of **groupoid**.

Example 4.10. *Given a G-set X, we construct the action groupoid $G \backslash\backslash X$, whose objects are elements of X and $Hom(x, y) = \{g \in G \mid gx = y\}$.*

Example 4.11. *Given a nice topological space X, we construct the fundamental groupoid $\pi_1(X)$.*

Remark 4.12. Given a G-set X, one has an equivalence of categories $Sh(X)^G \approx Funct(G \backslash\backslash X, Vect)$.

We can now prove claim 4.8 by constructing an equivalence of groupoids $G \backslash\backslash X \approx (G/N) \backslash\backslash (N \backslash X)$; We send $x \mapsto Nx$, and $g \cdot x = y$ to $gN \cdot Nx = Ny$.

Remark 4.13. Given a nice topological space X, we have an equivalence of categories $LocSys(X) \approx Funct(\pi_1(X), Vect)$. Here, $LocSys(X)$ is the category of local systems on X - those are sheaves of k-vector spaces on X, which are locally isomorphic to a constant sheaf.

Definition 4.14. Simplicial set, geometric realization of a simplicial set, Nerve of a category.

Claim 4.15. $\pi_1(|N(G \backslash\backslash X)|) \approx G \backslash\backslash X$. *Moreover,* $\pi_i(|N(G \backslash\backslash X)|) = 0$ *for* $i > 1$. *In particular,* $|N(G \backslash\backslash *)|$ *is BG, the classifying space.*

Corollary 4.16. $LocSys(|G \backslash\backslash X|) \approx Sh(X)^G$.

Remark 4.17. The "concrete" definition of a G-equivariant sheaf on X, can be restated as follows: We want a family $(\mathcal{F}_i)_{i \geq 0}$ of sheaves, $\mathcal{F}_i \in Sh(N(G \backslash\backslash X)_i)$, together with compatibilities along all maps between the sets $N(G \backslash\backslash X)_i$.

Let us illustrate this material. Let V be a finite-dimensinoal vector space over $\mathbb{R}$, and denote by X_V the space of inner products on V (this examples yields infinite sets, but we ignore this - we chose it for intuition reasons). Fix $B \in X_V$. Then $G := GL(V)$ acts transitively on X_V, and the stabilizer of B is O_B, the corresponding orthogonal group. Thus, $Rep(O_V) \approx Sh(X)^G$.

We have a natural equivalence of categories $Sh(X)^G \approx Funct(G\backslash\backslash X, Vect)$.

Now, in our case, let us also consider the groupoid $Euclid$, whose objects are $\mathbb{R}$-vector spaces of dimension $\dim V$ equipped with an inner product, and morphisms are isomorphisms of vector spaces preserving the inner product. We have an evident functor $G\backslash\backslash X \to Euclid$, which is an equivalence of categories. Thus, we obtain

$$Rep(O_V) \approx Sh(X)^G \approx Funct(G\backslash\backslash X, Vect) \approx Funct(Euclid, Vect).$$

The point is that $Funct(Euclid, Vect)$ is a very reasonable object of study - it consists of "universal" prescriptions of vector spaces to Euclidean vector spaces. One might argue that the motivation for $Rep(O_V)$ is less clear, but the statement above says that those are equivalent.

4.5 Case of $G = V \rtimes H$, where V is commutative

Claim 4.18. *Let X be a transitive G-set, $x \in X$, and $H := Stab_G(x)$. Then the functor*

$$Rep(H) \approx Sh(X)^G \xrightarrow{\Gamma} Sh(*)^G \approx Rep(G)$$

is isomorphic to Ind_H^G.

Let V be a commutative group, and H a group acting on V (by group automorphisms). We form the semidirect product $G := V \rtimes H$. Notice that H acts on $Irr(V)$. Given $E \in Rep(G)$, restricting it to V we obtain a decomposition $E = \oplus_{\omega \in Irr(V)} E_\omega$. Notice that $hE_\omega = E_{h*\omega}$. We can thus construct $\mathcal{F}_E \in Sh(Irr(V))^H$, for which $(\mathcal{F}_E)_\omega := E_\omega$... We obtain a functor $Rep(G) \to Sh(Irr(V))^H$.

Claim 4.19. *The above functor $Rep(G) \to Sh(Irr(V))^H$ is an equivalence.*

Proof. The inverse functor is constructed by sending $\mathcal{F} \in Sh(Irr(V))^H$ to $E := \oplus_{\omega \in Irr(V)} \mathcal{F}_\omega$, letting V act on the piece $\mathcal{F}_\omega$ via the character associated to ω, and letting H act naturally, since $\mathcal{F}$ is H-equivariant.

Put differently, given $\mathcal{F}$, by letting V act on $\mathcal{F}_\omega$ by the character associated to ω, we upgrade the H-equivariant structure on $\mathcal{F}$ to a G-equivariant structure. We obtain an equivalence of categories between $Sh(Irr(V))^H$ and $Sh(Irr(V))^G_\circ$ - the full subcategory of $Sh(Irr(V))^G$ consisting of sheaves for which V acts on the fiber over ω by the character associated to ω. Then we have an equivalence $Sh(Irr(V))^G_\circ \to Rep(G)$, by taking global sections. □

Corollary 4.20. *Let (ω_i) be representatives of the H-orbits on $Irr(V)$. Let $H_i := Stab_H(\omega_i)$. Then $Rep(G) \approx \oplus_i Rep(H_i)$.*

Concretely, the embedding $Rep(H_i) \to Rep(G)$ is given by first considering $E \in Rep(H_i)$ as a $(V \rtimes H_i)$-representation, by letting V act via ω_i, and then sending it to $ind^G_{V \rtimes H_i} E$.

Corollary 4.21. *We have a bijection between $Irr(G)$ and $\coprod_i Irr(H_i)$.*

Example 4.22. *Let $V = \mathbb{F}_q$, $H = \mathbb{F}_q^\times$. Then $G = V \rtimes H$ is the group of affine transformations of the field $\mathbb{F}_q$. We can identify $Irr(V)$ with $\mathbb{F}_q$, associating to $x \in \mathbb{F}_q$ the character $\psi_x(y) = \psi(xy) = e^{\frac{2\pi i}{q} xy}$. The H-action on $Irr(V) \cong \mathbb{F}_q$ is again by homotheties. We have two orbits, with representatives $0, 1$. We obtain $Rep(G) \approx Rep(H) \oplus Vect$. Concretely, given an H-representation E, we construct the G-representation $res^H_G(E)$ (where we restrict along the projection $G \to H$). Given a vector space E, we treat it as a V-representation by letting V act via ψ, and then construct the G-representation $ind^G_V E$.*

So, the irreducible representations of $\mathbb{F}_q \rtimes \mathbb{F}_q^\times$ are given by: $\mathbb{C}_\chi$, where χ is a character of $\mathbb{F}_q^\times$ and we pullback via $\mathbb{F}_q \rtimes \mathbb{F}_q^\times \to \mathbb{F}_q^\times$. Also, $ind_{\mathbb{F}_q}^{\mathbb{F}_q \rtimes \mathbb{F}_q^\times} \mathbb{C}_\psi$.

Let us write the character table:

type	$(0,1)$	$(1,1)$	$(0,c)$ $(c \neq 1)$
$\mathbb{C}_\chi$	1	1	$\chi(c)$
$ind_{\mathbb{F}_q}^{\mathbb{F}_q \rtimes \mathbb{F}_q^\times} \mathbb{C}_\psi$	$q-1$	-1	0

4.6 The Stone-von Neumann theorem and the oscillator representation

Let us now consider the groups of matrices

$$H := \{ \begin{pmatrix} 1 & e & c \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \}$$

over a finite field $\mathbb{F}_q$, and abbreviate (c, e, f) for a matrix as above. Then the multiplication law is

$$(c, e, f)(c', e', f') = (c + c' + ef', e + e', f + f').$$

Generalizing, let L be a finite-dimensional vector space over $\mathbb{F}_q$. Then we can consider the group whose underlying set is $\mathbb{F}_q \times L \times L^*$, and the product is

$$(c, e, f)(c', e', f') = (c + c' + f'(e'), e + e', f + f').$$

We can think of those as representing the operators on $Fun(L)$, given by

$$(T_{(0,e,0)}\phi)(x) = \phi(x - e),$$

$$(T_{(0,0,f)}\phi)(x) = \psi(f(x))\phi(x),$$

and

$$(T_{(c,0,0)}\phi)(x) = \psi(-c)\phi(x).$$

Here ψ is a fixed non-trivial character of $\mathbb{F}_q$. In other words, we cook up a group from the two natural families of operators on a commutative group - translation and multiplication by a character. Assuming that q is odd, we now pass to "polarized" coordinates, setting

$$(S_{(c,e,f)}\phi)(x) = \phi(-\frac{1}{2}f(e))T_{(c,e,f)}.$$

Then we have:

$$S_{(c,e,f)}S_{(c',e',f')} = S_{(c+c'+\frac{1}{2}(f'(e)-f(e')),e+e',f+f')}.$$

We can now generalize as follows. Let (V,ω) be a finite-dimensional symplectic vector space over $\mathbb{F}_q$. We define the Heisenberg group H_V by being $\mathbb{F}_q \times V$ as a set, and the multiplication is

$$(c,v)(c',v') = (c+c'+\frac{1}{2}\omega(v,v'), v+v').$$

Let $L \subset V$ be a Lagrangian. We have then an abelian subgroup

$$\widetilde{L} := \mathbb{F}_q \times L \subset H_V.$$

Let $M \subset V$ be a Lagrangian transversal to L. Then thinking of M as $\{0\} \times M \subset H_V$, we have $H_V = \widetilde{L} \rtimes M$. Now let us use $Rep(H_V) \approx Sh(Irr(\widetilde{L})^M)$ to see what irreducible representations H_V has. We can identify $\mathbb{F}_q \times M$ with $Irr(\widetilde{L})$, by sending (d,m) to the character $(c,\ell) \mapsto \psi(cd)\psi(\omega(\ell,m))$. Under this identification, M acts on $Irr(\widetilde{L})$ by

$$m' * (d,m) = (d, m-dm').$$

Thus, representatives for orbits are $(0,m)$ for $m \in M$ with stabiliser M, and $(d,0)$ for $d \in \mathbb{F}_q^\times$ with trivial stabiliser. Hence, the irreducible representations of H_V are as follows. We have a bunch of one-dimensional representations, factoring through the quotient $H_V/\mathbb{F}_q$ (where we identify $\mathbb{F}_q$ with $\mathbb{F}_q \times \{0\} = Z(H_V) \subset H_V$). On those the center acts trivially, Also, for every non-trivial central character $c \mapsto \psi(dc)$, we have the irreducible induced representation $ind_{\widetilde{L}}^{H_V}\mathbb{C}_{(d,0)}$ of dimension $\frac{1}{2}\dim V$. We obtain:

Theorem 4.23 (Stone-von Neumann)**.** *For a non-trivial central character of H_V, there exists a unique (up to isomorphism) irreducible representation of H_V with that central character.*

Let us consider now $Sp(V)$ acting on H_V by group automorphisms ($g(c,v) = (c,gv)$). Fix an irreducible representation $(\mathcal{H},\pi)$ of H_V with a non-trivial central character. Then for $g \in Sp(V)$, the representation $(\mathcal{H}, {}^g\pi)$ given by ${}^g\pi(h) = \pi(g^{-1} * h)$ is also an irreducible representation of H_V, with the same central character. By the Stone-von Neumann theorem, it follows that the representations $(\mathcal{H}, {}^g\pi)$ and $(\mathcal{H},\pi)$ are isomorphic. The isomorphism, by Schur's lemma, is unique up to a scalar. We thus obtain a well-defined element $T_g \in PGL(\mathcal{H}) := GL(\mathcal{H})/\mathbb{C}^\times$. We get a homomorphism $Sp(V) \to PGL(\mathcal{H})$. Such an homomorphism is called a **projective representation** (of $Sp(V)$ on $\mathcal{H}$, in this case). We can now ask whether we can lift this projective representation to a genuine one, and in how many ways. We can notice that the set of liftings is a torsor under $Hom(Sp(V), \mathbb{C}^\times)$.

Claim 4.24. *The group $Sp(V)$ is perfect, except for three cases of $(\dim V, q)$: $(2,2), (2,3), (4,2)$.*

Thus (omitting one case), if there exists a lift of our projective representation, it is unique.

Suppose that $\pi : G \to PGL(V)$ is a projective representation. We can choose arbitrary liftings $(T_g)_{g \in G} \in GL(V)$ of the $\pi(g)$'s. Then we have relations $T_g T_h = c_{g,h} T_{gh}$ for scalars $c_{g,h} \in \mathbb{C}^\times$. These scalars satisfy

$$c_{a,b} c_{ab,c} = c_{a,bc} c_{b,c}.$$

If we choose different liftings $(d_g T_g)$, then we obtain for the corresponding $(c'_{g,h})$ the relation

$$c'_{a,b} = \frac{d_a d_b}{d_{ab}} c_{a,b}.$$

Definition 4.25. The second cohomology of G with values in $\mathbb{C}^\times$ is defined as $Coker(\delta : C^1 \to B^2)$, where

$$C^1 = Fun(G, \mathbb{C}^\times),$$

$$B^2 = \{c \in Fun(G \times G, \mathbb{C}^\times) \mid c_{a,b} c_{ab,c} = c_{a,bc} c_{b,c}\},$$

and

$$\delta(d)_{a,b} = \frac{d_a d_b}{d_{ab}}.$$

Another approach to linearization would be as follows. For a Lagrangian $L \subset V$, consider $\mathcal{H}_L = ind_{\widetilde{L}}^{H_V} \mathbb{C}_\psi$. We can consider $\mathcal{H}_\bullet$ as a sheaf on $Lag(V)$, the set of Lagrangians.

We have an $Sp(V)$-equivariant structure $\beta_{L,g}$ on $\mathcal{H}_\bullet$ as follows. Define $\beta_{L,g} : \mathcal{H}_L \to \mathcal{H}_{gL}$ by $\beta_{L,g}(f)(h) = f(g^{-1} * h)$. Then $\beta_{L,g}(hf) = (g * h)\beta_{L,g}(f)$. So the identifications of fibers of this structure are not H_V-morphisms.

We would like to find "canonical intertwiners", i.e. for two $L, M \in Lag(V)$, an isomorphism $c_{L,M} : \mathcal{H}_L \to \mathcal{H}_M$ of H_V-representations, subject to

$$c_{M,N} \circ c_{L,M} = c_{L,N}$$

and also

$$c_{gL,gM} \circ \beta_{L,g} = \beta_{M,g} \circ c_{L,M}.$$

In fact, this is not quite possible, but if we consider things over the set $OLag(V)$ of oriented Lagrangians, i.e. Lagrangians together with a choice of a basis of the top power, then it is possible.

Given such a system of canonical intertwiners, and a fixed Lagrangian $L \in OLag(V)$, we define $T_g := c_{gL,L} \circ \beta_{L,g}$. Then T_g clearly is a lift as desired, and we have

$$T_g T_k = c_{gL,L} \circ \beta_{L,g} \circ c_{kL,L} \circ \beta_{L,k} = c_{gL,L} \circ c_{gkL,gL} \circ \beta_{kL,g} \circ \beta_{L,k} = c_{gkL,L} \circ \beta_{L,gk} = T_{gk}.$$

In fact, a more "canonical" approach then would be to define

$$\mathcal{H} = \{(f_L) \in \bigoplus_{L \in OLag(V)} \mathcal{H}_L \mid c_{L,M} f_L = f_M \ \forall L, M\},$$

and the action of $Sp(V)$ on $\mathcal{H}$ via $g(f_L) = (\beta_{g^{-1}L,g} f_{g^{-1}L})$. In this way we obtain a canonical Weil representation, built from (V, ω) with no extra choices (add reference to Gurevich-Hadani).

How to approach the construction of $c_{L,M}$? One first tries "naive" intertwiners $av_{L,M}$, given by

$$av_{L,M}(f)(x) = \frac{1}{|M|} \sum_{m \in M} f(xm).$$

One has $av_{gL,gM} \circ \beta_{L,g} = \beta_{M,g} \circ av_{L,M}$. But there is no reason for $av_{M,N} \circ av_{L,M} = av_{L,N}$. We are looking then for scalars $\gamma_{L,M}$ such that setting $c_{L,M} = \gamma_{L,M} av_{L,M}$ will work.

An idea is to find what we want for $(L, M) \in OLag(V)^2_\circ$, transversal Lagrangians. Then, for an arbitrary pair (L, M), we find a Lagrangian N transversal to both L and M, and set $c_{L,M} := c_{N,M} \circ c_{L,N}$.

Let us calculate an example. Write $V = L \oplus M$, a direct sum of Lagrangians. We can find bases $e_1, \ldots, e_n$ of L and $e_1^*, \ldots, e_n^*$ of M, such that $\omega(e_i, e_j^*) = \delta_{ij}$. Let $w \in Sp(V)$ be the element that sends $e_i \mapsto e_i^*$ and $e_i^* \mapsto -e_i$. We want to compute the operator $\pi(w)$ on $\mathcal{H}_M$, identifying $\mathcal{H}_M \cong Fun(L)$. We have $(\beta_{M,w} f)(h) = f(w^{-1}(h))$. Now,

$$(av_{L,M} \beta_{M,w} f)(\ell) = \frac{1}{q^n} \sum_{m \in M} f(w^{-1}(\ell m)) = \frac{1}{q^n} \sum_{\widetilde{\ell} \in L} f(w^{-1}(\ell) \widetilde{\ell}) =$$

$$= \frac{1}{q^n} \sum_{\widetilde{\ell} \in L} \psi(\omega(w^{-1}(\ell), \widetilde{\ell})) f(\widetilde{\ell}).$$

In coordinates, setting $\ell = \sum x_i e_i$, we obtain $w^{-1}\ell = \sum -x_i e_i^*$, and so

$$(\pi(w) f)(\sum x_i e_i) = \frac{1}{q^n} \sum_{(y_i)} \psi(\sum x_i y_i) f(\sum y_i e_i).$$

In other words, this is the Fourier transform.

4.7 Mackey formula

Given a subgroup $H \subset G$, a representation $(V, \pi) \in Rep(H)$, and an element $w \in G$, we will denote by $({}^wV, {}^w\pi)$ the representation of ${}^wH := wHw^{-1}$, which is V as a vector space, and the action is given by ${}^w\pi(g) := \pi(w^{-1}gw)$.

In terms of equivariant sheaves, ${}^wV$ has the following description. We consider the G-equivariant sheaf $\mathcal{V} \in Sh(G/H)^G$ corresponding to V. Then, considering the ${}^wH$-equivariant morphism $i : \{wH\} \to G/H$, we have $i^*\mathcal{V} \in Sh(\{wH\})^{{}^wH} \approx Rep({}^wH)$, and it is the desired representation.

Proposition 4.26 (Mackey formula)**.** *Let $H, K \subset G$ be two subgroups, and $V \in Rep(H)$. Then:*

$$res^G_K ind^G_H V \simeq \bigoplus_{w \in K\backslash G/H} ind^K_{K\cap {}^wH} res^{{}^wH}_{K\cap {}^wH} {}^wV.$$

Proof. Let us consider $\mathcal{V} \in Sh(G/H)^G$ corresponding to V under the equivalence $Sh(G/H)^G \approx Rep(H)$. Then $res^G_K ind^G_H V$ identifies with $\Gamma(res^G_K \mathcal{V})$ (where $res^G_K : Sh(G/H)^G \to Sh(G/H)^K$ is the obvious restriction functor). We decompose G/H into the disjoint union of K-orbits, and obtain

$$res^G_K \mathcal{V} \approx \oplus_{w\in K\backslash G/H} \Gamma(\mathcal{V}|_{KwH/H}).$$

Since the action of K on KwH/H is transitive, and the stabiliser of wH is $K \cap {}^wH$,

$$\Gamma(\mathcal{V}|_{KwH}) \cong ind^K_{K\cap {}^wH} \mathcal{V}|_{wH} \cong ind^K_{K\cap {}^wH} res^{{}^wH}_{K\cap {}^wH} {}^wV.$$

□

Corollary 4.27. *Let $H \subset G$ be a subgroup, and $V \in Rep(H)$ irreducible. Then $ind^G_H(V)$ is irreducible if and only if $res^H_{H\cap {}^wH} V$ and $res^{{}^wH}_{H\cap {}^wH}({}^wV)$ have no common irreducible components, for all $w \in H\backslash G/H - \{HeH\}$.*

Proof. Denote $H_w := H \cap {}^wH$ for simplicity. We have:

$$Hom_G(ind^G_H V, ind^G_H V) = Hom_H(V, res^G_H ind^G_H(V)) =$$

$$= \bigoplus_{w\in H\backslash G/H} Hom_H(V, ind^H_{H_w} res^{{}^wH}_{H_w}({}^wV)) = \bigoplus_{w\in H\backslash G/H} Hom_H(res^H_{H_w} V, res^{{}^wH}_{H_w}({}^wV)).$$

Comparing dimensions, we obtain the desired result. □

Corollary 4.28. *Let $H \subset G$ be a normal subgroup, and $V \in Rep(H)$ irreducible. Then $ind^G_H(V)$ is irreducible if and only if $V \not\simeq {}^wV$ for all $w \in G/H - \{eH\}$.*

Proof. We just specialize in the previous corollary. □

4.8 Projection formula

Let $V \in Rep(H)$, $W \in Rep(G)$. Then the projection formula states:

$$ind^G_H(V) \otimes W \simeq ind^G_H(V \otimes res^G_H W).$$

4.9 Induction of characters

Claim 4.29. *Let $V \in Rep(H)$. Then we have the following relation:*

$$\chi_{ind_H^G V}(g) = \sum_{x \in G/H \text{ s.t. } x^{-1}gx \in H} \chi_V(x^{-1}gx).$$

This leads us to define a linear map

$$ind_H^G : Fun^{cent}(H) \to Fun^{cent}(G)$$

by the formula

$$ind_H^G(f)(g) = \sum_{x \in G/H \text{ s.t. } x^{-1}gx \in H} f(x^{-1}gx).$$

Thus, for $W \in Rep(H)$, we have

$$\chi_{ind_H^G W} = ind_H^G \chi_W.$$

Lemma 4.30. *The following maps are adjoint:*

$$ind_H^G : Fun^{cent}(H) \rightleftarrows Fun^{cent}(G) : res_H^G$$

(w.r.t. our standard symmetric bilinear pairings $(\cdot,\cdot)$).

Proof.

Proof 1: Since characters span the space of central functions, it is enough to prove that for $V \in Rep(G)$ and $W \in Rep(H)$, we have

$$(ind_H^G \chi_W, \chi_V) = (\chi_W, res_H^G \chi_V).$$

Indeed, we have:

$$(ind_H^G \chi_W, \chi_V) = (\chi_{ind_H^G W}, \chi_V) = \dim Hom_G(ind_H^G W, V) =$$

$$= \dim Hom_H(W, res_H^G V) = (\chi_W, \chi_{res_H^G V}) = (\chi_W, res_H^G \chi_V).$$

Proof 2: We can just calculate, as if we don't know any representation theory: Let $f_1 \in Fun^{cent}(H)$ and $f_2 \in Fun^{cent}(G)$. Then

$$|G|(ind_H^G(f_1), f_2) = \sum_{g \in G} \sum_{x \in G/H \text{ s.t. } x^{-1}gx \in H} f_1(x^{-1}gx) f_2(g^{-1}) =$$

$$= \sum_{x \in G/H} \sum_{g \in xHx^{-1}} f_1(x^{-1}gx) f_2(g^{-1}) = \sum_{x \in G/H} \sum_{h \in H} f_1(h) f_2(h^{-1}) = |G/H| \cdot |H| \cdot (f_1, res_H^G f_2).$$

□

5 Artin's and Brauer's induction theorems

5.1 Artin's induction theorem

Theorem 5.1. *The morphism*

$$\oplus ind_H^G : \bigoplus_{H \subset G \ cyclic} R(H) \to R(G)$$

has a cofinite image; Equivalently, it is an epimorphism after tensoring with $\mathbb{Q}$ (equivalently still, with k).

Proof. Let $\chi \in R(G)$ be such that $(\chi, Ind_H^G \rho) = 0$ for every cyclic $H \subset G$ and $\rho \in R(H)$. By Frobenius reciprocity, this means $(Res_H^G \chi, \rho) = 0$ for all ρ and thus $Res_H^G \chi = 0$. Since the H's cover G, we obtain $\chi = 0$. □

5.2 Preparations for Brauer's induction theorem

Lemma 5.2. *Let $H \subset G$ be a normal subgroup, and $E \in Rep(G)$ an irreducible representation. Then there exists a subgroup $H \subset K \subset G$ and an irreducible representation $F \in Rep(K)$ such that $E \simeq Ind_K^G F$ and $Res_H^K F$ is isotypical.*

Proof. Since H is normal in G, the group G permutes the H-isotypical components in E, and since E is irreducible it does so transitively. Let $E_0 \subset E$ be one such isotypical component. Set $K = \{g \in G \mid gE_0 = E_0\}$. Then E_0 is a representation of K. It is easy to see that the natural map $ind_K^G E_0 \to E$ is an isomorphism. □

Definition 5.3. A group H is called supersolvable of length ≤ 0, if it is trivial. Recursively, H is called supersolvable of length $\leq n$, if there exists a normal cyclic subgroup $C \subset H$ such that H/C is supersolvable of length $\leq n-1$. The group H is called supersolvable if it is supersolvable of length $\leq n$ for some n.

Lemma 5.4. *Subgroups and quotient groups of supersolvable groups are supersolvable. The product of two supersolvable groups is supersolvable. p-groups are supersolvable.*

Lemma 5.5. *A non-abelian supersolvable group G has a normal abelian non-central subgroup.*

Proof. $G/Z(G)$ is a non-trivial supersolvable group, and hence we have a non-trivial cyclic normal subgroup $C \subset G/Z(G)$. Denote by $\widetilde{C}$ the preimage of C in G. Then $\widetilde{C}$ is a normal abelian non-central subgroup in G. □

Claim 5.6. *Let G be supersolvable, and $E \in Rep(G)$ an irreducible representation. Then there exists a subgroup $H \subset G$ and a character $\chi \in Hom(H, k^\times)$, such that $E = Ind_H^G k_\chi$.*

Proof. We prove the claim by induction on the order of G. If the representation E is not faithful, we can pass to the quotient of G by the kernel of the representation, and use induction. So let us suppose that E is faithful. If G is abelian, the claim is clear. So let us suppose also that G is not abelian. Then, by the previous lemma, we have a normal abelian non-central subgroup $H \subset G$. If $Res_H^G E$ would be isotypical, H would act on E by scalars. Since E is faithful, this would imply that H is central in G. Hence, $Res_H^G E$ is not isotypical. By a claim above, we can find a proper subgroup $K \subset G$ and a representation $F \in Rep(K)$ such that $E \simeq Ind_K^G(F)$. Now apply the induction hypothesis to $F \in Rep(K)$. □

5.3 Brauer's induction theorem - statement and corollaries

A finite group H is called p-elementary, if it is isomorphic to a product of a p-group and a cyclic group. It is called elementary if it is p-elementary for some p. Note that elementary groups are supersolvable (even nilpotent). Denote by $El(G)$ the set of elementary subgroups of G.

Theorem 5.7 (Brauer's induction theorem)**.** *The map*

$$\oplus ind_H^G : \bigoplus_{H \in El(G)} R(H) \to R(G)$$

is surjective.

Corollary 5.8. *Every $\chi \in R(G)$ can be written as a linear combination with integer coefficients of inductions of characters of one-dimensional representations.*

Proof. This follows by a combination of Brauer's induction theorem and claim 5.6. □

5.4 Brauer's induction theorem - proof

Definition 5.9. Let p be a prime number. An element $x \in G$ is called p-regular (resp. p-torsion), if $o(x)$ is prime to p (resp. a power of p).

Claim 5.10 ("Jordan decomposition")**.** *Let p be a prime number, and $x \in G$. Then there exists a unique pair $(y, z) \in G^2$ such that y is p-regular, z is p-torsion, y and z commute, and $x = yz$.*

Proof. Let us show uniqueness first. If $x = yz = y'z'$, then $x^{p^N} = y^{p^N} = (y')^{p^N}$ when N is large enough. Then $\langle y \rangle = \langle y^{p^N} \rangle = \langle (y')^{p^N} \rangle = \langle y' \rangle$. If r is the order of that group, then r is prime to p, and hence we can write $ar + bp^N = 1$. Then $y = (y^{p^N})^b = ((y')^{p^N})^b = y'$.

Let us show existence now. Let $p^N k$ be the order of x, where k is prime to p. Then we can write $ap^N + bk = 1$ and set $y = x^{ap^N}, z = x^{bk}$. Then the order of y divides k and so is prime to p, while the order of z divides p^N, so is a power of p.

□

Definition 5.11. In the notations of the above claim, we will write $y = x_{p\text{-reg}}$ and $z = x_{p\text{-tor}}$.

Remark 5.12. Notice that $G_{p\text{-reg}} \subset G$, the subset of p-regular elements, is stable under conjugation. It will play a role in the representation theory over a field of characteristic p.

Let us now prove Brauer's induction theorem. Let us denote by $I \subset R(G)$ the image of the map in the theorem. By the projection formula, I is an ideal in $R(G)$. Hence, in order to prove the theorem, it is enough to prove that $1 \in I$. For subrings $A, B \in k$, let us denote by $R_B^A(G) \subset Fun^{cent}(G)$ the subspace of $AR(G)$ consisting of functions all of whose values lie in B. Then $R_B^A(G)$ is a subring w.r.t. pointwise product, and is preserved under restriction and induction. We consider $R'(G) := R_{\mathbb{Z}}^{\mathbb{Z}[\sqrt[|G|]{1}]}(G)$, and denote by I' the image of the map analogous to the above

$$\oplus ind_H^G : \bigoplus_{H \in El(G)} R(H)' \to R(G)'.$$

Notice that I' is an ideal in $R(G)'$.

Now, we notice that it is enough to show that $1 \in I'$. This follows from $\mathbb{Z}$ being a direct summand in $\mathbb{Z}[\sqrt[|G|]{1}]$ (as opposed to merely an abelian subgroup).

Let us consider the group $Fun_{\mathbb{Z}}^{cent}(G)$ of integer-valued central functions on G. Then $Fun_{\mathbb{Z}}^{cent}(G)$ is a finitely-generated free abelian group, $1 \in Fun_{\mathbb{Z}}^{cent}(G)$ and $I' \subset Fun_{\mathbb{Z}}^{cent}(G)$. The following lemma shows that it is enough to show that $1 \in I' + p^k Fun_{\mathbb{Z}}^{cent}(G)$ for every prime p and $k \in \mathbb{Z}_{\geq 1}$.

Lemma 5.13. *Let A be a finitely generated free abelian group, $L \subset A$ a subgroup, and $a \in A$. Then $a \in L$ if and only if for every prime p and $k \in \mathbb{Z}_{\geq 1}$, one has $a \in L + p^k A$.*

Let us reduce the statement further to the following one:

Lemma 5.14. *Let p be a prime. There exists $f \in I'$ all of whose values are prime to p.*

Indeed, such an f will satisfy $1 - f^{\phi(p^k)} \in p^k Fun_{\mathbb{Z}}^{cent}(G)$ (and notice that $f^{\phi(p^k)} \in I'$ since I' is an ideal).

Next, we reduce from lemma 5.14 to the following one:

Lemma 5.15. *Let p be a prime, and $g \in G$ a p-regular element. Then there exists $f \in I'$ such that $f(x) = 0$ if $x_{p\text{-}reg}$ is not conjugate to g, and $f(x)$ is prime to p otherwise.*

Indeed, summing up functions as in lemma 5.14 when g runs over the conjugacy classes of p-regular elements will obviously be a function as desired in lemma 5.14.

To prove lemma 5.15, we consider a p-Sylow subgroup $S \subset Z_G(g)$, and then set $E := S \cdot \langle g \rangle \subset Z_G(g) \subset G$. Clearly, $E \in El_p(G)$.

We have $o(g) \cdot \delta_{\{g\}} \in R(\langle g \rangle)'$. By pulling back along the projection $E \to \langle g \rangle$, we see that $o(g) \cdot \delta_{Sg} \in R(E)'$. Thus, $f := ind_E^G(o(g) \cdot \delta_{Sg}) \in I'$. We claim that this f complies to the demands of lemma 5.15.

Indeed, we have:

$$ind_E^G(o(g)\delta_{Sg})(x) = o(g)\cdot|\{y \in G/E \mid y^{-1}xy \in Sg\}| = |\{y \in G/S \mid y^{-1}xy \in Sg\}|.$$

If $x_{p\text{-reg}}$ is not conjugate to g, then clearly the expression is equal to zero (because $y^{-1}xy$ can't land in Sg). If $x_{p\text{-reg}}$ is conjugate to g, then after applying a suitable conjugation, we can assume that $x \in Sg$, write $x = sg$. Now $y^{-1}xy \in Sg$ implies that $y^{-1}gy = y^{-1}x_{p\text{-reg}}y = (y^{-1}xy)_{p\text{-reg}} = g$, i.e. $y \in Z_G(g)$. So, we are left to show that

$$|\{y \in Z_G(g)/S \mid y^{-1}xy \in Sg\}|$$

is prime to p. Notice that:

$$|\{y \in Z_G(g)/S \mid y^{-1}xy \in Sg\}| = |\{y \in Z_G(g)/S \mid y^{-1}sy \in S\}| = |\{y \in Z_G(g)/S \mid syS \in yS\}|,$$

i.e. this is the number of fixed points of the left action of s on $Z_G(g)/S$. Since s is a p-torsion element, and $|Z_G(g)/S|$ is prime to p, the number of fixed points is prime to p. Done!

5.5 Artin L-functions

Interestingly, as far as I understand, Artin's induction theorem and Brauer's induction theorem where developed in order to study Artin L-functions (is it true for the latter?).

Let F/E be a finite Galois extension of number fields, with Galois group $G := Gal(F/E)$. For a number field K, let us denote by $Pr(K)$ the set of prime ideals in $\mathcal{O}_K$. We have a surjective map with finite fibers $Pr(F) \to Pr(E)$, given by $\pi_{F/E} : \mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{O}_E$. Given $\mathfrak{p} \in Pr(E)$, we have a decomposition $\mathfrak{p}\mathcal{O}_F = \prod_{\mathfrak{q}\in\pi^{-1}(\mathfrak{p})} \mathfrak{q}^{e_\mathfrak{p}}$, for some $e_\mathfrak{p} \in \mathbb{Z}_{\geq 1}$. We say that F/E is unramified over $\mathfrak{p}$, if $e_\mathfrak{p} = 1$. If F/E is unramified over $\mathfrak{p}$, and $\pi(\mathfrak{q}) = \mathfrak{p}$, then there exists a unique $Fr_\mathfrak{q} \in G$ such that $Fr_\mathfrak{q}x - x^{|\mathcal{O}_E/\mathfrak{p}|} \in \mathfrak{q}$ for all $x \in \mathcal{O}_F$. Moreover, for a different $\mathfrak{q}$, the resulting $Fr_\mathfrak{q}$ will be conjugate in G to the previous one. Hence, we have a well defined $Fr_\mathfrak{p} \in Conj(G)$. Given now a complex representation $V \in Rep(G)$, we define the (incomplete) Artin L-function

$$L_{F/E,V}(s) = \prod_{\mathfrak{p}\ \text{unr.}} \frac{1}{det(Id - |\mathcal{O}_E/\mathfrak{p}|^{-s}Fr_\mathfrak{p}; E)}.$$

It is easy to see that this function converges absolutely and represents a holomorphic function, for $Re(s)$ big enough. Does it have a meromorphic continuation to the whole complex s-plane?

Properties (everything up to a finite number of Euler factors):

1) $L_{F/E,Triv} = \zeta_E$.

2) $L_{F/E,V\oplus W} = L_{F/E,V} \cdot L_{F/E,W}$.

3) Let $K/F/E$, with K/E Galois (and F/E not necessarily so). Let $V \in Rep(G_{K/F})$. Then $L_{K/E,IndV} = L_{K/F,V}$.

4) Let $K/F/E$, with K/E and F/E Galois. Let $V \in Rep(G_{F/E})$. Then $L(K/E, infV) = L(F/E, V)$.

We in particular obtain

$$\zeta_F = L_{F/F,Triv} = L_{F/E,Reg} = \zeta_E \cdot \prod_{V \in Irr - \{Triv\}} L_{F/E,V}^{\dim V}.$$

Brauer's induction theorem implies that every Artin L-function can be expressed as a product of Artin L-functions and their inverses, for one-dimensional representations.

6 Representations of S_n

6.1 The representations $\Delta_\lambda, \nabla_\lambda, E_\lambda$

Fix a finite set X, and denote $n := |X|$. We have the group S_X of autobijections of X (so $|S_X| = n!$).

Recall that a partition of n is a sequence $\lambda = (\lambda_1, \lambda_2, \ldots)$ where $\lambda_k \in \mathbb{Z}_{\geq 0}$, $\lambda_k \geq \lambda_{k+1}$, and $\sum_k \lambda_k = n$ (so, in particular, the sequence has only finitely many non-zero entries). We denote by $Part(n)$ the set of partitions of n.

We have an involution $(\cdot)^t : Part(n) \to Part(n)$, given by associating to λ the partition λ^t where λ^t_k is equal to the number of λ_l's bigger or equal than k.

On $Part(n)$ we define the lexicographic linear order, by declaring $\lambda < \mu$ if for the first k for which $\lambda_k \neq \mu_k$, we have $\lambda_k < \mu_k$. Let us also define the order $<^t$ by $\lambda <^t \mu$ if $\lambda^t < \mu^t$.

We also have a partial order $\preceq$ on $Part(n)$, where $\lambda \preceq \mu$ if $\sum_{1 \leq i \leq k} \lambda_i \leq \sum_{1 \leq i \leq k} \mu_i$ for every $k \geq 1$. We define $\lambda \preceq^t \mu$ if $\lambda^t \preceq \mu^t$. Notice that $\lambda \preceq \mu$ implies $\lambda \leq \mu$ (and so $\lambda > \mu$ implies $\lambda \not\preceq \mu$).

Given a partition $\lambda \in Part(n)$, an ordered partition of X obeying λ is a sequence $\mathcal{P} = (\mathcal{P}_1, \mathcal{P}_2, \ldots)$, where $\mathcal{P}_i \subset X$, $|\mathcal{P}_i| = \lambda_i$, and the $\mathcal{P}_i$'s are disjoint (and so $\cup_{i \geq 1} \mathcal{P}_i = X$). Let us denote by X_λ the set of ordered partitions of X obeying λ. The group S_X acts on X_λ transitively.

Let us denote $\Delta_\lambda := Fun(X_\lambda)$ and $\nabla_\lambda := k_{sgn} \otimes Fun(X_{\lambda^t})$.

Claim 6.1. *The number* $\dim Hom_G(\Delta_\lambda, \nabla_\mu)$ *is equal to* 1 *if* $\mu = \lambda$ *and to* 0 *if* $\mu >^t \lambda$ *(in fact, if* $\mu \not\preceq^t \lambda$*).*

Proof. Let us interpret

$$Hom_G(\Delta_\lambda, \nabla_\mu) \simeq \left(k_{sgn} \otimes Fun(X_\lambda \times X_{\mu^t})\right)^G.$$

This is the space of functions on $X_\lambda \times X_{\mu^t}$ which are antisymmetric on G-orbits (where G acts on $X_\lambda \times X_{\mu^t}$ by the diagonal action) - meaning

$$f(g\mathcal{P}, g\mathcal{Q}) = sgn(g) f(\mathcal{P}, \mathcal{Q}).$$

Thus, $\dim Hom_G(\Delta_\lambda, \nabla_\mu)$ is equal to the number of G-orbits in $X_\lambda \times X_{\mu^t}$, the stabilizers of whose points are contained in A_X, the alternating group. Let us call such G-orbits good.

Suppose that $\mu^t > \lambda^t$. Then, for every $\mathcal{P} \in X_\lambda, \mathcal{Q} \in X_{\mu^t}$, we necessarily have two indices k, l for which $|\mathcal{P}_k \cap \mathcal{Q}_l| > 1$. Thus, if $x, y \in \mathcal{P}_k \cap \mathcal{Q}_l$ are two different points, the transposition $(x, y) \in S_X$ lies in the stabilizer of $(\mathcal{P}, \mathcal{Q})$. From this, we see that the number of good orbits is zero.

Suppose now that $\mu^t = \lambda^t$. Then there is exactly one good orbit (spelling this out left as an exercise?). □

Let $\lambda \in Part(n)$. Since $Hom_G(\Delta_\lambda, \nabla_\lambda)$ is one-dimensional, we have a well defined irreducible representation $E_\lambda := Im(\Delta_\lambda \to \nabla_\lambda)$ (where we take the image of any non-zero morphism).

Notice that E_λ appears in Δ_λ (with multiplicity 1) and does not appear in Δ_μ for $\mu <^t \lambda$. This shows that the E_λ's are pairwise non-isomorphic. Since $|Irr(S_X)| = |Conj(S_X)| = |Part(n)|$, this shows that the E_λ are exactly all the irreducible representations of S_X, up to isomorphism.

Let us write

$$\chi_{\Delta_\lambda} = \sum_\mu K_{\lambda\mu} \cdot \chi_{E_\mu}.$$

The non-negative integers $K_{\lambda\mu}$ are called Kostka numbers. As we mentioned, $K_{\lambda\mu} = 0$ if $\mu >^t \lambda$, and $K_{\lambda\lambda} = 1$.

Remark 6.2. The theme of "standard" objects Δ, "costandard" objects ∇, and triangular transition matrices as above, repeats itself a lot in representation theory. Also, usually the character of the Δ's and ∇'s is easy to describe, while that of the irreducible objects is hard (and basically encoded in the transition matrix as above or, rather, its inverse).

Corollary 6.3. *All the characters of S_n have values in $\mathbb{Z}$. This is clear for permutation representations Δ_λ, and since those form a $\mathbb{Z}$-basis for $R(S_n)$ by the above, the claim follows. Even better, we can say that all the representations of S_n are defined over $\mathbb{Q}$.*

Example 6.4. *Les us consider the two extreme examples. First, $\lambda = (n)$. Notice that $X_{(n)}$ has one element, so $\Delta_{(n)}$ is just the trivial representation. So obviously $E_{(n)}$ is also the trivial representation. Now, consider $\lambda = (1, \ldots, 1)$. Notice that $X_{(1,\ldots,1)}$ is a freely transitive S_X-set, so that $\Delta_{(1,\ldots,1)}$ is the regular representation. It contains all irreducible representations, but notice that $(1, \ldots, 1)^t = (n)$, so $\nabla_{(1,\ldots,1)}$ is the sign representation. Thus, $E_{(1,\ldots,1)}$ is the sign representation.*

Example 6.5. *Let us consider S_3. We have $Part(3) = \{(3) <^t (2,1) <^t (1,1,1)\}$. We have:*

$$\begin{pmatrix} \chi_{\Delta_{(3)}} \\ \chi_{\Delta_{(2,1)}} \\ \chi_{\Delta_{(1,1,1)}} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ ?_1 & 1 & 0 \\ ?_2 & ?_3 & 1 \end{pmatrix} \begin{pmatrix} \chi_{E_{(3)}} \\ \chi_{E_{(2,1)}} \\ \chi_{E_{(1,1,1)}} \end{pmatrix}$$

The dimensions in the vector on the right are $1, 2, 1$. The dimensions in the vector on the left are $1, 3, 6$. From this, $?_1 = 1$, and $?_2, ?_3$ are determined by the fact that an irreducible representation E appears in the regular representation $\dim E$ times. So, we get:

$$\begin{pmatrix} \chi_{\Delta_{(3)}} \\ \chi_{\Delta_{(2,1)}} \\ \chi_{\Delta_{(1,1,1)}} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} \chi_{E_{(3)}} \\ \chi_{E_{(2,1)}} \\ \chi_{E_{(1,1,1)}} \end{pmatrix}$$

or, inverting,

$$\begin{pmatrix} \chi_{E_{(3)}} \\ \chi_{E_{(2,1)}} \\ \chi_{E_{(1,1,1)}} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} \chi_{\Delta_{(3)}} \\ \chi_{\Delta_{(2,1)}} \\ \chi_{\Delta_{(1,1,1)}} \end{pmatrix}.$$

6.2 The character of Δ_λ

To handle characters of representations of S_X it is convenient, first, to interpret them as functions on $Part(n)$. Second, we consider expressions in the variables $x_1, x_2, \ldots$. Set $x^\lambda := \prod_{k\geq 1} x_k^{\lambda_k}$. Also, set $p_m := \sum_{k\geq 1} x_k^m$ (and $p_0 := 1$).

Let us give a formula for the character of Δ_λ.

Proposition 6.6. *The character of Δ_λ evaluated on $\mu \in Part(n)$ is the coefficient of x^λ in the polynomial $p_\mu := \prod_{k\geq 1} p_{\mu_k}$.*

Proof. Let $\mathcal{Q}$ be a partition of X obeying μ. Notice (by taking a permutation whose cycle structure is $\mathcal{Q}$) that the value $\chi_{\Delta_\lambda}(\mu)$ is equal to the number of partitions $\mathcal{P}$ obeying λ and coarsening $\mathcal{Q}$ (i.e. each element of $\mathcal{P}$ is a union of elements of $\mathcal{Q}$).

Let us consider functions $f : supp(\mu) \to \mathbb{Z}_{\geq 1}$. We set $(f_*\mu)_j = \sum_{f(i)=j} \mu_i$ (it is a partition). Then partitions $\mathcal{P}$ obeying λ and coarsening $\mathcal{Q}$ are in bijection with functions f such that $f_*\mu = \lambda$ (the relation is $\mathcal{P}_j = \cup_{f(i)=j} \mathcal{Q}_i$).

Notice that $p_\mu = \sum_f x^{f_*\mu}$, from which the desired relation follows.

□

Example 6.7. *Let us return to the example of S_3, and calculate the character χ_{Δ_λ}. We have:*

$$p_{(3)} = (x_1^3 + \ldots) = x_1^3 + \ldots,$$
$$p_{(2,1)} = (x_1^2 + \ldots)(x_1 + \ldots) = x_1^3 + x_1^2 x_2 + \ldots,$$
$$p_{(1,1,1)} = (x_1 + \ldots)(x_1 + \ldots)(x_1 + \ldots) = x_1^3 + 3x_1^2 x_2 + 6x_1x_2x_3 + \ldots.$$

Thus:

$$\chi_{\Delta_{(3)}} = x_1^3 + x_1^2 x_2 + x_1x_2x_3,$$
$$\chi_{\Delta_{(2,1)}} = x_1^2 x_2 + 3x_1x_2x_3,$$
$$\chi_{\Delta_{(1,1,1)}} = 6x_1x_2x_3.$$

So, by the matrix relation from the previous example, we get:

$$\chi_{E_{(3)}} = x_1^3 + x_1^2 x_2 + x_1x_2x_3,$$
$$\chi_{E_{(2,1)}} = -x_1^3 + 2x_1x_2x_3,$$
$$\chi_{E_{(1,1,1)}} = x_1^3 - x_1^2 x_2 + x_1x_2x_3.$$

6.3 The character of E_λ

Lemma 6.8. *Let $(\theta_\lambda)_{\lambda \in Part(n)} \subset R(S_X)$ be a family of virtual characters, and write*

$$\theta_\lambda = \sum_\mu L_{\lambda\mu} \cdot \chi_{\Delta_\mu}.$$

Suppose that the matrix $L_{\lambda\mu}$ is $<^t$-lower triangular, in the sense that

$$L_{\lambda\lambda} = 1, \quad L_{\lambda\mu} = 0 \ \forall \mu >^t \lambda$$

. Suppose in addition that $(\theta_\lambda, \theta_\lambda) = 1$. Then $\theta_\lambda = \chi_{E_\lambda}$.

Proof. The condition $(\theta_\lambda, \theta_\lambda) = 1$ means that θ_λ is either the character of an irreducible representation, or $-\theta_\lambda$ is.

We have a relation

$$\chi_{\Delta_\lambda} = \sum_\mu L^{-1}_{\lambda\mu} \theta_\mu$$

and $L^{-1}_{\lambda\mu}$ is also $<^t$-lower triangular. Thus, if by induction we already saw that $\theta_\mu = \chi_{E_\mu}$ for $\mu <^t \lambda$, then we see from the matrix relation above that the irreducibles that might appear in Δ_λ are those corresponding to θ_μ for $\mu <^t \lambda$, i.e. E_μ's with $\mu <^t \lambda$, and the irreducible corresponding to θ_λ. Since E_λ appears in Δ_λ, there is no choice but $\theta_\lambda = \chi_{E_\lambda}$. □

Theorem 6.9 (Frobenius character formula)**.** *The character of E_λ evaluated on $\mu \in Part(n)$ is the coefficient of x^λ in $s_\mu := p_\mu \prod_{j>i}(1 - \frac{x_j}{x_i})$.*

For an eventually-null sequence of integers $\lambda = (\lambda_1, \lambda_2, \ldots)$, let us define λ° to be illegal if λ has negative components, and otherwise we define λ° by reordering the entries in λ so as to become non-increasing. We define Δ_λ to be Δ_{λ°, where the latter is zero if λ° is illegal.

Let us denote by χ_λ the central function defined in the theorem (so that we want to show $\chi_{E_\lambda} = \chi_\lambda$).

Since the coefficient of x^λ in $p_\mu \frac{x_j}{x_i}$ is equal to the coefficient of $x^{\lambda + e_i - e_j}$ in p_μ (where e_i is the vector equal to 1 at i and to 0 elsewhere), and the p_μ are symmetric in the variables $x_1, x_2, \ldots$, we obtain

$$\chi_\lambda = \sum (-1)^{\cdots} \chi_{\Delta_{\lambda + \sum(e_i - e_j)}}.$$

Here, χ_{Δ_λ} enters with coefficient 1, and the rest of the $\chi_{\Delta_{\lambda'}}$ that enter satisfy $\lambda' <^t \lambda$ (incidentally, also $\lambda' > \lambda$).

Thus, it is enough to show that $(\chi_\lambda, \chi_\lambda) = 1$.

For a partition $\mu \in Part(n)$, let us denote by μ^i the number of $j \geq 1$ such that $\mu_j = i$. We have:

$$(\chi_\lambda, \chi_\lambda) = \frac{1}{n!} \sum_{\mu \in Part(n)} |C_\mu| \cdot |\chi_\lambda(\mu)|^2.$$

We can interpret $|\chi_\lambda(\mu)|^2$ as the coefficient of $x^\lambda y^\lambda$ in

$$p_\mu(x)p_\mu(y)\prod_{j>i}(1-\frac{x_j}{x_i})\prod_{j>i}(1-\frac{y_j}{y_i}).$$

Thus, $(\chi_\lambda,\chi_\lambda)$ is the coefficient of $x^\lambda y^\lambda$ in

$$\frac{1}{n!}\sum_{\mu\in Part(n)}|C_\mu|p_\mu(x)p_\mu(y)\prod_{j>i}(1-\frac{x_j}{x_i})\prod_{j>i}(1-\frac{y_j}{y_i}).$$

We have the formula

$$|C_\mu|=\frac{n!}{\prod_{m\geq 1}\mu^m!m^{\mu_m}}.$$

We now rewrite:

$$\frac{1}{n!}\sum_{\mu\in Part(n)}|C_\mu|p_\mu(x)p_\mu(y)=\sum_{\mu\in Part(n)}\prod_{m\geq 1}\frac{1}{\mu^m!}\left(\frac{1}{m}\sum_{i,j}(x_iy_j)^m\right)^{\mu^m}.$$

We can think of partitions of n as sequences $(\mu^1,\mu^2,\ldots)$ such that $\sum_{i\geq 1} i\cdot\mu^i=n$ (by the rule above - μ^k is the number of μ_i's equal to k). Denoting $Part(\infty)=\cup_{i\geq 1}Part(i)$, we see that

$$\sum_{\mu\in Part(n)}\prod_{m\geq 1}\frac{1}{\mu^m!}\left(\frac{1}{m}\sum_{i,j}(x_iy_j)^m\right)^{\mu^m}$$

is the n-homogeneous part of

$$\sum_{\mu\in Part(\infty)}\prod_{m\geq 1}\frac{1}{\mu^m!}\left(\frac{1}{m}\sum_{i,j}(x_iy_j)^m\right)^{\mu^m}.$$

Notice that for a function ϕ with domain $\mathbb{Z}_{\geq 0}\times\mathbb{Z}_{\geq 1}$ for which $\phi(0,m)=1$, we have

$$\sum_{\mu\in Part(\infty)}\prod_{m\geq 1}\phi(\mu^m,m)=\prod_{m\geq 1}\sum_{k\geq 0}\phi(k,m).$$

We apply this to

$$\phi(k,m)=\frac{1}{k!}\left(\frac{1}{m}\sum_{i,j}(x_iy_j)^m\right)^k,$$

and obtain

$$\sum_{\mu\in Part(\infty)}\prod_{m\geq 1}\frac{1}{\mu^m!}\left(\frac{1}{m}\sum_{i,j}(x_iy_j)^m\right)^{\mu^m}=\prod_{m\geq 1}\sum_{k\geq 0}\frac{1}{k!}\left(\frac{1}{m}\sum_{i,j}(x_iy_j)^m\right)^k=$$

$$= \prod_{m\geq 1} exp\left(\frac{1}{m}\sum_{i,j}(x_iy_j)^m\right) = exp\left(-\sum_{i,j} log(1-x_iy_j)\right) = \prod_{i,j}\frac{1}{1-x_iy_j}.$$

Thus, $(\chi_\lambda, \chi_\lambda)$ is the coefficient of $x^\lambda y^\lambda$ in

$$\frac{\prod_{j>i}(1-\frac{x_j}{x_i})(1-\frac{y_j}{y_i})}{\prod_{i,j}(1-x_iy_j)}. \tag{6.1}$$

Lemma 6.10.

$$\prod_{1\leq i<j\leq n}(x_i-x_j)(y_j-y_i) = det\left(\frac{1}{x_i-y_j}\right)\prod_{1\leq i,j\leq n}(x_i-y_j)$$

Proof. The right hand side is a polynomial of homogeneous degree n^2-n, which vanishes on the hyperplanes $x_i = x_j$ and $y_i = y_j$. Hence, it must be proportional to the left hand side. Let us now write this as

$$\frac{\prod_{1\leq i<j\leq n}(x_i-x_j)(y_j-y_i)}{\prod_{1\leq i,j\leq n}(x_i-y_j)} = C\cdot det\left(\frac{1}{x_i-y_j}\right).$$

Multiplying by $x_n - y_n$ both sides, we obtain the same equality but for $n-1$. This allows to show that $C = 1$ by induction. □

Setting x_i to be x_i^{-1} in the lemma, we obtain:

Corollary 6.11.

$$\prod_{1\leq i<j\leq n}(x_i-x_j)(y_i-y_j) = det\left(\frac{1}{1-x_iy_j}\right)\prod_{1\leq i,j\leq n}(1-x_iy_j)$$

Thus, our expression 6.1 is equal to:

$$det\left(\frac{1}{1-x_iy_j}\right)\prod_{j>i}\frac{1}{x_iy_i} = \left(\prod_{j>i}\frac{1}{x_iy_i}\right)\cdot\sum_{\sigma\in S_n} sgn(\sigma)\prod_{1\leq i\leq n}\frac{1}{1-x_iy_{\sigma(i)}}$$

For $\sigma \neq 1$, the corresponding summand can't contain $x^\lambda y^\lambda$. Indeed, denote $\rho = (n-1)e_1 + \ldots + (n-2)e_{n-2} + \ldots + e_{n-1}$. Notice that $\lambda + \rho$ has no repeated values, and thus x_i and y_j appear with different powers in $x^{\lambda+\rho}y^{\lambda+\rho}$ whenever $i \neq j$. Thus, $x^{\lambda+\rho}y^{\lambda+\rho}$ can not appear in $\prod_{1\leq i\leq n}\frac{1}{1-x_iy_{\sigma(i)}}$ for $\sigma \neq 1$, because in each monomial appearing in this product, x_i appears with the same power as $y_{\sigma(i)}$.

So, finally, the value of $(\chi_\lambda, \chi_\lambda)$ is equal to the coefficient of $x^\lambda y^\lambda$ in

$$\prod_{1\leq i\leq n}\sum_{m\geq 0} x_i^{m+i-n}y_i^{m+i-n},$$

which is 1.

6.4 Gelfand pairs

Definition 6.12. $K \subset G$ is called a **Gelfand pair**, if for every irreducible $E \in Rep(G)$, one has $[Res_K^G E : Triv] \leq 1$. It is called a **strong Gelfand pair**, if for every irreducible $E \in Rep(G)$ and irreducible $F \in Rep(K)$, one has $[Res_K^G E : F] \leq 1$.

Example 6.13. *We'll show later that $S_{n-1} \subset S_n$ is a strong Gelfand pair. Then one, by induction, obtains for every irreducible of S_n a decomposition into lines - the "Gelfand-Zeitlin basis".*

Definition 6.14. The **Hecke algebra** $\mathcal{H}(G, K)$ is defined as the subalgebra of $Fun(G)$, consisting of functions which are invariant under K both from left and from right.

Let us verify that it is indeed a subalgebra, with a unit. If $f_1, f_2 \in \mathcal{H}(G, K)$, then

$$(f_1 * f_2)(kg) = \sum_{g_1 g_2 = kg} f_1(g_1) f_2(g_2) = \sum_{g_1 g_2 = g} f_1(kg_1) f_2(g_2) = \sum_{g_1 g_2 = g} f_1(g_1) f_2(g_2) = (f_1 * f_2)(g)$$

and similarly for right multiplication.

The function $\delta_K := \frac{1}{|K|} \sum_{k \in K} \delta_k$ is a unit for $\mathcal{H}(G, K)$.

Notice that $\mathcal{H} := \mathcal{H}(G, \{e\}) = Fun(G)$.

Remark 6.15. Let $V \in Rep(G)$. Then $\mathcal{H}(G, K)$ leaves invariant V^K (in fact, maps the whole of V into V^K). We obtain a functor $(\cdot)^K : Rep(G) \to \mathcal{H}(G, K)$-mod.

Let us denote by $Irr^K(G) \subset Irr(G)$ the set of those $[E]$, for which $E^K \neq 0$ (call those the spherical irreducible representations).

Claim 6.16. *The functor $V \mapsto V^K$ induces a bijection between $Irr^K(G)$ and $Irr(\mathcal{H}(G, K))$. The inverse bijection is given by associating to E the unique spherical irreducible quotient module (in our semisimple realm, simply the unique spherical irreducible summand).*

To prove this claim, we study the adjunction

$$L := \mathcal{H} \otimes_{\mathcal{H}(G,K)} \cdot : \mathcal{H}(G, K)\text{-mod} \rightleftarrows Rep(G) : (\cdot)^K =: R.$$

More generally, let A be a finite-dimensional algebra over k, and $e \in A$ an idempotent (i.e. $e^2 = e$). Then we have a subalgebra $eAe \subset A$. It has a unit e, which is not the unit 1 of A, in general. Write $f = 1 - e$. We can consider the adjunction

$$L := A \otimes_{eAe} \cdot : eAe\text{-mod} \rightleftarrows A\text{-mod} : e \cdot =: R$$

(we consider categories of finite-dimensional modules).

The unit of this adjunction is an isomorphism: Notice that as a right eAe-module, A decomposes:

$$A = eAe \oplus fAe \oplus eAf \oplus fAf.$$

Thus $L(E) \cong E \oplus fAe \otimes_{eAe} E$ and we see that $E \to RL(E)$ is an isomorphism.

R is exact: We have $V = eV \oplus fV$, and R picks the first summand.

Given a spherical irreducible A-module V, we claim that $R(V)$ is irreducible. Indeed, if $E \subset R(V)$ is a non-zero submodule, then we obtain a non-zero map $L(E) \to V$, which is hence a surjection, and thus $E \cong R(L(E)) \to R(V)$ (which is simply the original inclusion) is also a surjection. Thus $E = R(V)$.

Given an irreducible eAe-module E, we have a unique spherical irreducible quotient of $L(E)$. Indeed, by considering a Jordan-Holder filtration of E, using the exactness of R, we deduce that there exists an irreducible subquotient V of $L(E)$, such that $R(V) \cong E$. But then we have a non-zero map $L(E) \to V$, so V can be realized as a quotient of E. Now, any map $L(E) \to V'$ to a spherical irreducible module must factor via $L(E) \to V$, because otherwise V' would be a quotient of $W := Ker(L(E) \to V)$, which is impossible since $R(V') \neq 0$ and $R(W) = 0$.

The above associations are mutually inverse: Given an irreducible spherical module V, the map $L(R(V)) \to V$ is non-zero, and hence V is an irreducible spherical quotient of $L(R(V))$. Conversely, given an irreducible E, from the analysis above it should be clear by this point that R applied to the spherical irreducible quotient of $L(E)$ is isomorphic to E.

Corollary 6.17. *Suppose that the Hekce algebra $\mathcal{H}(G, K)$ is commutative. Then $K \subset G$ is a Gelfand pair.*

Proof. IF $\mathcal{H}(G, K)$ is commutative, all its irreducible modules are one-dimensional. Hence $\dim V^K = [res_K^G V : Triv] \leq 1$ for all irreducible G-modules V. □

Lemma 6.18 (Gelfand's trick)**.** *Suppose that we have an anti-involution $t : G \to G$ (meaning $r(gh) = r(h)r(g)$ and $r \circ r = id$), which preserves all K-double cosets in G. Then $\mathcal{H}(G, K)$ is commutative.*

Proof. Notice that t induces an anti-involution of the group algebra $\mathcal{H}$, and since t preserves the K-double cosets, it acts as identity on $\mathcal{H}(G, K) \subset \mathcal{H}$. Thus, the identity automorphism of $\mathcal{H}(G, K)$ swaps order of multiplication, meaning that $\mathcal{H}(G, K)$ is commutative. □

Example 6.19. *Consider $S_{n-1} \subset S_n$. We consider the anti-involution $t(g) = g^{-1}$. It preserves the S_{n-1}-double cosets, because each double coset has a representative of order 2.*

Now we pass to strong Gelfand pairs.

Lemma 6.20. *A pair $K \subset G$ is a strong Gelfand pair if and only if the pair $K \subset G \times K$ (where K is embedded diagonally) is a Gelfand pair.*

Proof. The irreducible representations of $G \times K$ are of the form $V \otimes E^*$ where V is an irreducible representation of G and E is an irreducible representation of K. We have

$$[res_K^{G \times K}(V \otimes E^*) : Triv] = \dim Hom_K(E, V),$$

giving us the desired. □

Notice that $Fun(G)$ admits a subalgebra, $Fun(G//K)$, consisting of functions which are constant on K-conjugacy classes. We claim that the algebras $\mathcal{H}(G \times K, K)$ and $Fun(G//K)$ are isomorphic. Indeed, complete

As a corollary:

Corollary 6.21. *If $Fun(G//K)$ is commutative, then $K \subset G$ is a strong Gelfand pair.*

And:

Lemma 6.22 (Gelfand's trick)**.** *Suppose that we have an anti-involution $t : G \to G$ (meaning $r(gh) = r(h)r(g)$ and $r \circ r = id$), which preserves all K-conjugacy classes in G. Then $Fun(G//K)$ is commutative.*

Example 6.23. *Again we consider S_n with the anti-involution $t(g) = g^{-1}$. It is not hard to see that it preserves the S_{n-1}-conjugacy classes. Thus, $S_{n-1} \subset S_n$ is a strong Gelfand pair.*

6.5 A formula for the dimension of E_λ

7 Representations of $SL_2(\mathbb{F}_q)$

For simplicity, we assume that q is prime to 2. We set $G := SL_2(\mathbb{F}_q)$. For the record, $|G| = (q-1)q(q+1)$. We denote by $\mathbb{F}_{q^2}/\mathbb{F}_q$ a fixed quadratic extension, and $\mathbb{F}_{q^2}^{\times,1} := Ker(Nm : \mathbb{F}_{q^2}^\times \to \mathbb{F}_q^\times)$. We fix an element $\epsilon \in \mathbb{F}_q^\times$ which is not a square.

7.1 Some structure of G

7.1.1

We define

$$B := \{\begin{pmatrix} t & x \\ 0 & t^{-1} \end{pmatrix} \ : \ t \in \mathbb{F}_q^\times, x \in \mathbb{F}_q\} \subset G$$

and

$$T := \{\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \ : \ t \in \mathbb{F}_q^\times\} \subset G.$$

We denote

$$w := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in G.$$

The Bruhat decomposition states $G = B \cup BwB$. We have $N_G(B) = B$. The subgroup B is the stabilizer of the line $Sp\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\}$ in the standard action of G on $\mathbb{F}_q^2$. The subgroup $T = B \cap wBw^{-1}$ is the stabilizer of both $Sp\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\}$ and $Sp\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$ (i.e., the stabilizer of an ordered pair of distinct lines).

We also define a subgroup

$$O = \{\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \ : \ a, b \in \mathbb{F}_q, a^2 - \epsilon b^2 = 1\} \subset G.$$

The susbgroup O is the stabilizer of a line $(Sp\{\begin{pmatrix} \sqrt{\epsilon} \\ 1 \end{pmatrix}\})$ in the plane over $\mathbb{F}_{q^2}$, not defined over $\mathbb{F}_q$. Notice in addition that G acts transitively on such lines (in contrast to the case of $SL_2(\mathbb{R})$, where one has two orbits - the upper half plane and the lower half plane).

We will identify $\mathbb{F}_q^\times \simeq T$ via $t \mapsto \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$ and $\mathbb{F}_{q^2}^{\times,1} \simeq O$ via $a + \epsilon b \mapsto \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}$.

We will say that a multiplicative character λ of $T/O/\mathbb{F}_q^\times/\mathbb{F}_{q^2}^{\times,1}$ is regular, if $\lambda^2 \neq 1$. We will say that $\lambda_1 \sim \lambda_2$, if $\lambda_2 \in \{\lambda_1, \lambda_1^{-1}\}$.

7.1.2

We have four types of conjugacy classes, depending on the minimal polynomial. For most minimal polynomials, elements with the given minimal polynomial will constitute a single conjugacy class, but for one case (case 4), elements with the given minimal polynomial will constitute two conjugacy classes (reflecting the difference between conjugation in $SL_2(\mathbb{F}_q)$ and $GL_2(\mathbb{F}_q)$).

1. Split non-regular semisimple: $m = x - c$ for $c \in \mathbb{F}_q^\times$, $c^2 = 1$. Those are the elements that fix every line. There are 2 such conjugacy classes.

2. Split regular semisimple (a.k.a. hyperbolic): $m = (x - c)(x - c^{-1})$ for $c \in \mathbb{F}_q^\times$, $c^2 \neq 1$. Those are the elements which fix two lines. There are $\frac{q-3}{2}$ such conjugacy classes.

3. Non-split (regular) semisimple (a.k.a. elliptic): $m = (x - c)(x - c^{-1})$ for $c \in \mathbb{F}_{q^2}^{\times,1}$, $c^2 \neq 1$. Those are the elements that don't fix any line. There are $\frac{q-1}{2}$ such conjugacy classes.

4. Non-senismiple (a.k.a. parabolic): $m = (x-c)^2$ for $c \in \mathbb{F}_q^\times$, $c^2 = 1$. Those are the elements that fix one line. There are 4 such conjugacy classes. Here, as opposed to the previous cases, the elements with a given minimal polynomial constitute two conjugacy classes. We will denote by $(4a)$ (resp. $(4b)$) the conjugacy class of type $\begin{pmatrix} c & a \\ 0 & c \end{pmatrix}$, where a is a square (resp. not a square).

Summing up, we see that there are $q + 4$ conjugacy classes, and hence as many irreducible representation of G.

7.2 The principal series

Let $\lambda \in \hat{T}$. Using the morphism $B \to T$ given by $\begin{pmatrix} t & x \\ 0 & t^{-1} \end{pmatrix} \mapsto \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$, let us define $\widetilde{k}_\lambda := res_B^T k_\lambda$. We define $P_\lambda \in Rep(G)$ by

$$P_\lambda := ind_B^G \widetilde{k}_\lambda.$$

Claim 7.1. *The value of* $(\chi_{P_\lambda}, \chi_{P_{\lambda'}})$ *is* 0 *if* $\lambda' \not\sim \lambda$, 1 *if* $\lambda' \sim \lambda$ *and* λ *is regular, and* 2 *if* $\lambda' \sim \lambda$ *and* λ *is not regular.*

Proof. Using the Mackey formula, we calculate

$$Hom_G(P_\lambda, P_{\lambda'}) = Hom_T(k_\lambda, k_{\lambda'}) \oplus Hom_T(k_\lambda, k_{{}^w\lambda'}).$$

$\square$

Corollary 7.2. *If* λ *is regular,* P_λ *is irreducible. If* λ *is not regular, two irreducibles appear in* P_λ*, each exactly once. In addition,* P_λ *is has common irreducible summands with* $P_{\lambda'}$ *if and only if* $\lambda' \sim \lambda$.

All in all, we obtain $\frac{q-3}{2} + 4 = \frac{q+5}{2}$ irreducible representations coming from the principal series. Thus, $\frac{q+3}{2}$ are still missing.

7.3 A "canonical" view on the principal series

Claim 7.3. *Let* G *act on* X*, and let* $\mathcal{F} \in Sh(X)^G$*. Then*

$$\chi_{\Gamma\mathcal{F}}(g) = \sum_{x \in X,\ gx = x} Tr(g; \mathcal{F}_x).$$

Remark 7.4. Maybe, try to compare something like Lefschetz's fixed point formula to the above simple claim. (move the above claim to the general section about equivariant sheaves)

For a field F, let us denote by $Vect_F$ the category of finite-dimensional vector spaces over F and by $Line_F$ the category of one-dimensional vector spaces over F. For a group Σ, let us denote by $Tors_\Sigma$ the category of Σ-torsors (which means Σ-sets which on which Σ acts freely and transitively).

Given a homomorphism $\chi : \Sigma_1 \to \Sigma_2$, we have a functor $Tors_{\Sigma_1} \to Tors_{\Sigma_2}$, given by $Z \mapsto \Sigma_1 \backslash (\Sigma_2 \times Z)$, where the action is $\sigma(\tau, z) = (\tau\chi^{-1}(\sigma), \sigma z)$.

For a field F, we have an equivalence $Tors_{F^\times} \approx Vect_F$, given by $Z \mapsto F^\times \backslash (F \times Z)$, where the action is $c(a, z) = (ac^{-1}, cz)$.

Denote now by X the set of one-dimensional subspaces in $\mathbb{F}_q^2$. We have a transitive action of G on X, and the stabiliser of $x_0 := Sp\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\}$ is B. Now given $\lambda \in \hat{T}$, we can define a G-equivariant sheaf $\mathcal{F}_\lambda$ on X as follows:

$$G \backslash\backslash X \to Line_{\mathbb{F}_q} \approx Tors_{\mathbb{F}_q^\times} \xrightarrow{\lambda} Tors_{\mathbb{C}^\times} \approx Line_{\mathbb{C}} \subset Vect_{\mathbb{C}}.$$

Then it is immediate to verify that the action of B on $(\mathcal{F}_\lambda)_{x_0}$ is via $B \to T \xrightarrow{\lambda} \mathbb{C}^\times$, hence

$$\Gamma(\mathcal{F}_\lambda) \cong P_\lambda.$$

Thus, we obtained the principal series representations without choosing a Borel subgroup.

7.4 Characters of the principal series

Let us calculate the character of P_λ. We have

$$\chi_{P_\lambda}(g) = \sum_{\text{lines } L \text{ s.t. } gL=L} \lambda(g|_L).$$

Here, by $g|_L$ we mean the scalar by which g acts on L. We obtain:

type	(1)	(2)	(3)	(4)
χ_{P_λ}	$(q+1)\cdot\lambda(c)$	$\lambda(c)+\lambda(c^{-1})$	0	$\lambda(c)$

7.5 The reducible principal series

The representation P_1 obviously contains the trivial representation as a summand, and the remaining summand St is called the **Steinberg representation**.

For the non-trivial quadratic character ℓ (the **Legendre character**), we compute the characters of the irreducible summands of P_ℓ as follows. We consider $G \subset G' \subset G''$, where $G'' = GL_2(\mathbb{F}_q)$ and G' is the subgroup of matrices of square determinant (it is of index 2). Then the action of G on X comes from the action of G'' on X, which is also transitive. Taking $\lambda''(\begin{pmatrix} t & 0 \\ 0 & s \end{pmatrix}) = \lambda(t)$, we have the corresponding $P_{\lambda''}$), whose restrictions to G' and G are $P_{\lambda'}$ and P_λ. By the same calculations as above, P'' is irreducible, and P' is reducible with two different constituents. From this, we deduce that the characters of the two different constituents of P_λ are conjugate one to the other w.r.t. G''/G'. write this paragraph better. This will allow us easily to calculate the characters. We can already write:

type	(1)	(2)	(3)	(4a)	(4b)
$\chi_{P_\ell^+}$	$\frac{1}{2}(q+1)\cdot\ell(c)$	$\ell(c)$	0	$?_1(c)$	$?_2(c)$
$\chi_{P_\ell^-}$	$\frac{1}{2}(q+1)\cdot\ell(c)$	$\ell(c)$	0	$?_2(c)$	$?_1(c)$

Now, we have $?_1(c)+?_2(c) = \ell(c)$. Notice also that we have $?_i(-1) = \ell(-1)?_i(1)$ or $?_i(-1) = \ell(-1)?_{i^*}(1)$. The relation $(\chi_{P_\ell^+}, \chi_{P_\ell^+}) = 1$ gives

$$(q-1)q(q+1) = 2(\frac{1}{2}(q+1))^2+\frac{1}{2}(q-3)(q+1)q+2(q+1)\frac{1}{2}(q-1)(|?_1(1)|^2+|?_2(1)|^2),$$

which becomes after simplification

$$|?_1(1)|^2 + |?_2(1)|^2 = \frac{1}{2}(q+1).$$

If $\ell(-1) = 1$, then $?_1(1), ?_2(1)$ are real, and we obtain

$$?_1(1) = \frac{1}{2}(1 + \sqrt{q}), ?_2(1) = \frac{1}{2}(1 - \sqrt{q}).$$

If $\ell(-1) = -1$, then $?_2(1) = \overline{?_1(1)}$, and we obtain

$$?_1(1) = -\frac{1}{2}(1 + \sqrt{-q}), ?_2(1) = -\frac{1}{2}(1 - \sqrt{-q}).$$

7.6 Cuspidal representations

Let us say that an irreducible representation of G is **cuspidal**, if it does not appear in the principal series. An idea is that as we constructed the principal series using induction from the split torus T, we should construct the cuspidal representations using induction from the non-split torus O. But, in fact, we didn't induce from T, but rather lifted from T to B and then induced. The subgroup O is not contained in such a B, and the induction from it directly is "too big". We will now, nevertheless, tamper the induction from O, to obtain characters of cuspidal irreducible representations.

Let us first compute the character of $ind_O^G k_\theta$ for $\theta \in \hat{O}$. We have:

$$\chi_{ind_O^G k_\theta}(g) = \sum_{\text{lines } L \text{ in } \mathbb{F}_{q^2}^2 - \mathbb{F}_q^2 \text{ s.t. } gL = L} \theta(g|_L).$$

Thus, we calculate:

type	(1)	(2)	(3)	(4)
$\chi_{ind_O^G k_\theta}$	$(q-1)q \cdot \theta(c)$	0	$\theta(c) + \theta(c^{-1})$	0

Let us now consider

$$\widetilde{P}_\lambda := ind_T^G k_\lambda.$$

We have

$$\chi_{\widetilde{P}_\lambda}(g) = \sum_{\text{pairs of lines } (L_1, L_2) \text{ s.t. } L_1 \neq L_2,\ gL_1 = L_1,\ gL_2 = L_2} \lambda(g|_{L_1}).$$

Thus, we can compute:

type	(1)	(2)	(3)	(4)
$\chi_{\widetilde{P}_\lambda}$	$(q+1)q \cdot \lambda(c)$	$\lambda(c) + \lambda(c^{-1})$	0	0
$\chi_{\widetilde{P}_\lambda} - \chi_{P_\lambda}$	$(q+1)(q-1) \cdot \lambda(c)$	0	0	$-\lambda(c)$

We see that $\chi_{\widetilde{P}_\lambda} - \chi_{P_\lambda}$ only depends on $\lambda(-1)$! Let us denote this character by χ_1 if $\lambda(-1) = 1$ and χ_{-1} if $\lambda(-1) = -1$.

Since $O \cap Z(G) = T \cap Z(G) = \{\pm 1\}$, we will also think of $\hat{O}$ as divided into two families $\hat{O} = \hat{O}_+ \cup \hat{O}_-$ (according to whether $\theta(-1) = 1$ or $\theta(-1) = 1$).

So, if χ_1 and χ_{-1} are "locally constant", maybe they make sense for O as well. Thus, let us try to consider the following virtual characters:

$$\rho_\theta := ind_O^G k_\theta - \chi_{\theta(-1)}.$$

The values are:

type	(1)	(2)	(3)	(4)
ρ_θ	$-(q-1)\cdot\theta(c)$	0	$\theta(c)+\theta(c^{-1})$	$\theta(c)$

For some reason, we got $\rho_\theta(1) < 0$. But can still hope that $-\rho_\theta$ is the character of an irreducible representation. For this, it is enough to check that $(\rho_\theta, \rho_\theta) = 1$. Let us do a more general calculation:

Lemma 7.5. *The value of $(\rho_\theta, \rho_{\theta'})$ is 0 if $\theta' \not\sim \theta$, 1 if $\theta' \sim \theta$ and θ is regular, and 2 if $\theta' \sim \theta$ and θ is not regular.*

Proof.

$$|G|(\rho_\theta, \rho_{\theta'}) =$$

$$= (q-1)^2(1+\theta(-1)\theta'(-1)) + (q+1)(q-1)(1+\theta(-1)\theta'(-1)) + \frac{q(q-1)}{2} \sum_{c \in (\mathbb{F}_{q^2}^{\times,1})^{\mathrm{reg}}} (\theta(c)+\theta(\bar{c}))(\theta'(\bar{c})+\theta'(c)) =$$

$$= q(q-1) \sum_{c \in (\mathbb{F}_{q^2}^{\times,1})} \left((\theta\theta')(c) + (\theta^{-1}\theta')(c)\right).$$

In other words:

$$(\rho_\theta, \rho_{\theta'}) = Av(\theta\theta') + Av(\theta^{-1}\theta')$$

(where the average is over $\mathbb{F}_{q^2}^{\times,1}$). □

Corollary 7.6. *For regular $\theta \in \hat{O}$, $-\rho_\theta$ is the character of an irreducible representation C_θ.*

We notice easily that $-\rho_1 = \chi_{St} - \chi_{Triv}$, so it gives nothing interesting. On the other hand, $-\rho_\ell$ can't be the sum or difference of any two irreducible representations we have already found, either by comparing dimensions or by noticing that on type (3) conjugacy classes it is not constant. Hence, $-\rho_\ell$ must be the sum or difference of the two last missing irreducible representations. If we denote by n, m the dimensions of the two missing irreducible representations, we find

$$n^2 + m^2 = 2(\frac{q-1}{2})^2.$$

Thus, $-\rho_\ell$ can't be the difference of two representations (since then the sum of squares would be too big). Furthermore, notice that $-\rho_\ell$ is stable under conjugation in $GL_2(\mathbb{F}_q)$ by $\begin{pmatrix} 1 & 0 \\ 0 & \epsilon \end{pmatrix}$. It can't be that the two irreducible representations that enter in it are stable under conjugation, since then the character table would not be invertible. Hence, the two irreducible representations that enter $-\rho_\ell$ are conjugates each of the other.

7.6.1 Summing up

We having the following character table. Here,

$$L_{\pm}^{s} = \frac{s}{2}(1 \pm \sqrt{sq}),$$

and the divide in type (4) is according to types $(4a)$ and $(4b)$.

type	(1)	(2)	(3)	(4)
χ_{P_λ} $(\lambda \in \hat{T}/\sim$ regular)	$(q+1)\cdot\lambda(c)$	$\lambda(c)+\lambda(c^{-1})$	0	$\lambda(c)$
χ_{Triv}	1	1	1	1
χ_{St}	q	1	-1	0
$\chi_{P_\ell^+}$	$\frac{1}{2}(q+1)\cdot\ell(c)$	$\ell(c)$	0	$\ell(c)L_+^{\ell(-1)} \mid \ell(c)L_-^{\ell(-1)}$
$\chi_{P_\ell^-}$	$\frac{1}{2}(q+1)\cdot\ell(c)$	$\ell(c)$	0	$\ell(c)L_-^{\ell(-1)} \mid \ell(c)L_+^{\ell(-1)}$
χ_{C_θ} $(\theta \in \hat{O}/\sim$ regular)	$(q-1)\cdot\theta(c)$	0	$-\theta(c)-\theta(c^{-1})$	$-\theta(c)$
$\chi_{C_\ell^+}$	$\frac{1}{2}(q-1)\theta(c)$	0	$-\theta(c)$	$\mid$
$\chi_{C_\ell^-}$	$\frac{1}{2}(q-1)\theta(c)$	0	$-\theta(c)$	$\mid$

The missing values in the two last rows we can find similarly to those for $\chi_{P_\ell^{\pm}}$.

7.7 Construction of representations via etale cohomology

complete

7.8 Constructions of representations using the theta correspondence

complete

8 Rationality and integrality questions

Throughout this section, *all fields are of characteristic zero.*

Let L/K be a field extension. We say that $V \in Rep_L(G)$ is definable over K, if there exists $V_0 \in Rep_K(G)$ such that $V \simeq L \otimes_K V_0$ (as G-representations over L).

8.1 Rationality

8.1.1

Let L/K be a field extension. We have a map $c_{L/K} : Irr_L(G) \to Irr_K(G)$ defined as follows: To $E \in Irr_L(G)$, we attach $F \in Irr_K(G)$ such that E appears in F_L. There exists at most one such F, because for two non-isomorphic F, F', we have

$$Hom_G(F_L, F'_L) = L \otimes_K Hom_G(F, F') = 0,$$

so F_L, F'_L don't have common irreducible summands. There exists such F, because E appears in $Reg_L(G) = Reg_K(G)_L$.

Clearly, the map $c_{L/K}$ is surjective.

Lemma 8.1. *If $n := [L : K]$ is finite, then each fiber of $c_{L/K}$ has at most n elements. If moreover L/K is a Galois extension, then each fiber of $c_{L/K}$ is a Galois orbit.*

8.1.2

Claim 8.2. *Let L/K be a field extension. The following are equivalent:*

1. *For each irreducible $E \in Rep_K(G)$, $E_L \in Rep_L(G)$ is also irreducible.*
2. *Each irreducible $F \in Rep_L(G)$ is definable over K.*
3. *$R_K(G) = R_L(G)$.*
4. *$R_K(G)$ and $R_L(G)$ have the same $\mathbb{Z}$-rank.*
5. *$|Irr_K(G)| = |Irr_L(G)|$.*

Proof. (1) $\to$ (2): Let $E \in Rep_K(G)$ be irreducible and such that F enters E_L. Then since E_L is irreducible, F is isomorphic to E_L, and hence definable over K.

(2) $\to$ (3): We clearly always have $R_K(G) \subset R_L(G)$. Now, $R_L(G)$ is the $\mathbb{Z}$-span of characters of irreducible representations in $Rep_L(G)$, which are definable over K, hence these characters sit in $R_K(G)$.

(3) $\to$ (4): Clear.

(4) $\to$ (5): The number of irreducible representations over the field ? is equal to the $\mathbb{Z}$-rank of $R_?(G)$.

(5) $\to$ (1): If for some irreducible $E \in Rep_K(G)$ we have that E_L is not irreducible, we would obtain at least $|Irr_K(G)|$ different irreducible representations in $Rep_L(G)$, by counting the number of elements in the preimages under $c_{L/K}$. ☐

Definition 8.3. Given a field extension L/K, we will say that K **is big enough in** L **for** G, if the equivalent conditions of claim 8.2 are satisfied.

Claim 8.4. *The following conditions on the field K are equivalent:*

1. *For every field extension L/K, K is big enough in L for G.*
2. *For some algebraically closed L/K, K is big enough in L for G.*
3. *Each irreducible $E \in Rep_K(G)$ satisfies $\dim End_G(E) = 1$.*
4. *We have $|Irr_K(G)| = |Conj(G)|$.*

Proof. (1) → (2): Clear.

(2) → (3): Since E_L is irreducible, and since we have

$$L \otimes_K End_G(E) \cong End_G(E_L),$$

we get

$$\dim_K End_G(E) = \dim_L End_G(E_L) = 1.$$

(3) → (2): For each irreducible $E \in Rep_K(G)$, we have $\dim_L End_G(E_L) = \dim_K End_G(E) = 1$, hence E_L is irreducible.

(2) → (4): We have $|Conj(G)| = |Irr_L(G)| = |Irr_K(G)|$.

(4) → (1): Otherwise, we would have at least $|Irr_L(G)| > ||Conj(G)|$, which is impossible since the irreducibles form a linearly independent set in $Fun^{cent}(G)$. □

Definition 8.5. We will say that K **is big enough for** G, is the equivalent conditions of claim 8.4 are satisfied.

Claim 8.6. *Given a field K, there exists a finite field extension L/K such that L is big enough for G.*

Corollary 8.7. *For every finite group G, there exists a number field big enough for G.*

Proof (of claim 8.6). It is enough to show that if K is not big enough for G, then there exists an irreducible $E \in Rep_K(G)$ and a finite extension L/K, such that $E_L \in Rep_L(G)$ is not irreducible. Indeed, then $|Irr_L(G)| > |Irr_K(G)|$, and by inductively continuing like that, we will arrive to a big enough field for G, using characterization (2) in claim 8.4. By characterization (1), assuming that K is not big enough for G, we can find irreducible $E \in Rep_K(G)$ such that $\dim End_G(E) > 1$. Then $End_G(E)$, being a division algebra, contains a subfield $K \subset L \subset End_G(E)$ with $[L : K] > 1$ (just adjoint to K any element in $End_G(E) - K$). Notice now that E can be considered as a G-representation E' over L (clearly irreducible). Notice that we have a surjection $E_L \to E'$ in $Rep_L(G)$, which is not injective since the dimension of E' is less than that of E_L. Hence, E_L is not irreducible, as wanted.

□

8.1.3

Claim 8.8. *Let L/K be a field extension, and $V \in Rep_L(G)$. Then V is definable over K if and only if $\chi_V \in R_K(G)$.*

Proof. Suppose that $\chi_V \in R_K(G)$. We can thus write $\chi_V = \sum_i n_i \chi_{E_i}$ where the E_i's are pairwise non-isomorphic irreducible representations in $Rep_K(G)$. Notice that

$$n_i \cdot \dim End_G(E_i) = (\chi_V, \chi_{E_i}) = (\chi_V, \chi_{(E_i)_L}) \geq 0,$$

so $n_i \geq 0$. Thus, we can say that the character of V and $\oplus_i E_i^{\oplus n_i}$ are equal, so $V \simeq (\oplus_i E_i^{\oplus n_i})_L$, showing that V is definable over K. □

Let us denote by $R_L^K(G) \subset R_L(G)$ the subgroup consisting of functions all of whose values lie in K.

Claim 8.9. *Let L/K be a finite field extension. Then the group $R_L^K(G)/R_K(G)$ is finite.*

Proof. Given $V \in Rep_L(G)$, we can consider also V as a G-representation over K, call it $rs_K^L(V) \in Rep_K(G)$ ("restriction of scalars"). We have $\chi_{rs_K^L(V)} = Tr_K^L \circ \chi_V$. In particular, in case $\chi_V \in R_L^K(G)$, we have $\chi_{rs_K^L(V)} = [L:K] \cdot \chi_V$. This shows that

$$[L:K] \cdot R_L^K(G) \subset R_K(G).$$

□

Theorem 8.10. *Let m be a common multiple of all orders of elements in G. Then the field $\mathbb{Q}_m := \mathbb{Q}(\mu_m)$ is big enough for G.*

Proof. Let $L/\mathbb{Q}_m$ be a finite extension such that L is big enough for G. It is clear that $R_L^{\mathbb{Q}_m}(G) = R_L(G)$. By claim 8.9, this implies that

$$\mathrm{rk} R_{\mathbb{Q}_m}(G) = \mathrm{rk} R_L(G) = |Conj(G)|.$$

□

8.1.4

Let m be a common multiple of all the orders of elements of G. Let $L = K(\mu_m)$. Recall that by theorem 8.10, L is big enough for G. The extension L/K is a Galois extension, and we have an embedding

$$\iota : \Gamma_K := Gal(L/K) \to (\mathbb{Z}/m\mathbb{Z})^\times,$$

characterized by $\sigma(\zeta) = \zeta^{\iota(\sigma)}$ for all $\zeta \in \mu_m$.

We have an action of Γ_K on G as a set, given by $\sigma * g := g^{\iota(\sigma)}$. This action commutes with the conjugation action of G on itself. Let us consider the finest equivalence relation on G which is cruder than conjugacy and than being in the same Γ_K-orbit. In other words, $g_1 \sim g_2$ if there exists $\sigma \in \Gamma_K$ such that g_1 is conjugate to $\sigma * g_2$. We will call this equivalence relation **Γ_K-conjugacy**.

Proposition 8.11. *Let $f \in Fun_L^{cent}(G)$. Then $f \in K \cdot R_L(G)$ if and only if*

$$f(\sigma * g) = \sigma(f(g)), \quad \forall \sigma \in \Gamma_K, g \in G.$$

Proof. Let $(V, \pi) \in Rep_L(G)$. Let (λ_i) denote the eigenvalues of $\pi(g)$. Then $\lambda_i \in \mu_m$. Hence, for $\sigma \in \Gamma_K$:

$$\chi_V(\sigma * g) = \sum_i \lambda_i^{\iota(\sigma)} = \sigma(\sum_i \lambda_i) = \sigma(\chi_V(g)).$$

Conversely, suppose that $f \in Fun_L^{cent}(G)$ satisfies the condition as in the proposition. Since L is big enough for G, we can write $f = \sum_i m_i \cdot \chi_i$, where

$m_i \in L$ and χ_i characters of irreducible representations in $Rep_L(G)$. We have, for $\sigma \in \Gamma_K$:

$$\sum_i m_i \chi_i(\sigma * g) = f(\sigma * g) = \sigma(f(g)) = \sum_i \sigma(m_i)\sigma(\chi_i(g)) = \sum_i \sigma(m_i)\chi_i(\sigma * g).$$

Since the χ_i's are linearly independent, we obtain $m_i = \sigma(m_i)$ for every $\sigma \in \Gamma_K$, implying $m_i \in K$. □

Corollary 8.12. *Let $f \in Fun_K^{cent}(G)$. Then $f \in K \cdot R_K(G)$ if and only if f is constant on Γ_K-conjugacy classes.*

Proof. If $f \in K \cdot R_K(G)$, then $f \in K \cdot R_L^K(G)$, and thus f is clearly constant on Γ_K-conjugacy classes by the proposition. Conversely, suppose that $f \in Fun_K^{cent}(G)$ is constant on Γ_K-conjugacy classes. By the proposition, $f \in K \cdot R_L(G)$. Now, we have

$$[L:K] \cdot f = Tr_K^L \circ f \in K \cdot R_K(G),$$

so that $f \in K \cdot R_K(G)$. □

Corollary 8.13. *The characters of irreducible representations in $Rep_K(G)$ form a basis in the space of functions on G stable under Γ_K-conjugacy. In particular, $|Irr_K(G)|$ is equal to the number of Γ_K-conjugacy classes in G.*

Corollary 8.14. *The field K is big enough for G if and only if for every $\sigma \in \Gamma_K$ and $g \in G$, the elements g and $g^{\iota\sigma}$ are conjugate.*

Corollary 8.15. *The field $\mathbb{Q}$ is big enough for G if and only if for every integer c prime to $|G|$, and every $g \in G$, the elements g and g^c are conjugate.*

Example 8.16. *The field $\mathbb{Q}$ is big enough for S_n; This is easy to see using the cyclic decomposition of elements in S_n. In particular, all characters of S_n are $\mathbb{Z}$-valued.*

8.2 Representations over $\mathbb{R}$

8.2.1

Let $F \in Irr_{\mathbb{R}}(G)$. $End(F)$ is a division algebra. It is known that (finite dimensional) division algebras over $\mathbb{R}$ are isomorphic to exactly one of the following: $\mathbb{R}, \mathbb{C}, \mathbb{H}$ (the latter is the algebra of quaternions, of dimension 4 over $\mathbb{R}$). We thus can classify the irreps. in $Irr_{\mathbb{R}}(G)$ into 3 classes ("real", "complex", "quaternionic"). From this, we obtain a classification of irreps. in $Irr_{\mathbb{C}}(G)$ into 3 classes, via $c_{\mathbb{C}/\mathbb{R}}$.

Claim 8.17. *Let $F \in Irr_{\mathbb{R}}(G)$. If F is real, then $F_{\mathbb{C}}$ is irreducible. If F is complex, then $F_{\mathbb{C}} = E \oplus E^\sigma$, where E is irreducible and $E \not\simeq E^\sigma$. If F is quaternionic, then $F_{\mathbb{C}} = E \oplus E$, where E is irreducible (and $E \simeq E^\sigma$).*

Proof. □

Claim 8.18. *Let $E \in Irr_{\mathbb{C}}(G)$. Then E is real or quaternionic if and only if $E \simeq E^*$ if and only if χ_E takes real values.*

Proof. Notice that E is real or quaternionic if and only if $E \simeq E^\sigma$. On the other hand, $E \simeq E^\sigma$ if and only if $\chi_E = \chi_{E^\sigma} = \sigma \circ \chi_E$, which happens if and only if χ_E takes real values. Notice also that $E^\sigma \simeq E^*$. Indeed, denoting by $\lambda_1, \cdots, \lambda_n$ the eigenvalues of $\chi_E(g)$, we have

$$\chi_{E^\sigma}(g) = \sum_i \sigma(\lambda_i) = \sum_i \lambda_i^{-1} = \chi_{E^*}.$$

□

Claim 8.19. *Let $E \in Irr_{\mathbb{C}}(G)$. Then E is complex/real/quaternionic if and only if E admits no/symmetric/antisymmetric G-invariant non-degenerate bilinear form.*

Proof. Notice that the space of G-invariant non-degenerate bilinear forms is isomorphic to the space of isomorphisms of E and E^*. Thus there exists such a form if and only if E is real or quaternionic, by the previous claim. Notice further that the space of such forms is at most one-dimensional, and hence such a form must be either symmetric or antisymmetric. If E is real, then by complexifying a G-invariant inner product on F, we obtain a symmetric form as wanted. Conversely, suppose that E admits a symmetric G-invariant bilinear form $B(v, w)$. Let us also fix an Hermitian positive-definite G-invariant form $H(v, w)$. We have a unique anti-linear operator $T : V \to V$, such that

$$B(v, w) = H(Tv, w).$$

This T is bijective. The operator T^2 is a linear isomorphism, and we have that T^2 is positive-definite self-adjoint. Indeed:

$$H(T^2v, w) = B(Tv, w) = B(w, Tv) = H(Tw, Tv)$$

and the form $(v, w) \mapsto H(Tw, Tv)$ is clearly Hermitian and positive-definite. Hence, we have a unique positive-definite self-adjoint square root $S := \sqrt{T^2}$. Let us denote now $U := TS^{-1}$. Since T and S commute, $U^2 = Id$. Since U is anti-linear, $E^{U,-1} = iE^{U,1}$. Thus $E = E^{U,1} \oplus i \cdot E^{U,1}$. Finally, notice that T, and thus U, commutes with the G-action:

$$H(Tgv, w) = B(gv, w) = B(v, g^{-1}w) = H(Tv, g^{-1}w) = H(gTv, w).$$

Hence, $E^{U,1}$ is a real form of E as a G-representation. □

Claim 8.20. *Let $[E] \in Irr_{\mathbb{C}}(G)$. Then E is complex/real/quaternionic according to the value of*

$$\frac{1}{|G|} \sum_{g \in G} \chi_E(g^2)$$

being $0/1/-1$.

Proof. Let us write

$$a := \frac{1}{|G|}\sum_{g\in G}\chi_E(g)^2, b := \frac{1}{|G|}\sum_{g\in G}\chi_E(g^2).$$

Then a is equal to the dimension of the space of G-invariant bilinear forms on E, and using exercise 3.3 we see that $\frac{1}{2}(a+b)$ (resp. $\frac{1}{2}(a-b)$) is equal to the dimension of the space of symmetric (resp. antisymmetric) bilinear forms on E.

Thus, the claim easily follows from the previous one. □

9 Integrality

We assume that k is algebraically closed throughout.

9.1 Integral elements

Let A be a (associative, unital) k-algebra. An element $a \in A$ is called **integral**, if there exists a monic polynomial $p \in \mathbb{Z}[X]$ such that $p(a) = 0$.

Claim 9.1. *Let $a \in A$. Then a is integral if and only if $\mathbb{Z}[a]$ is finitely generated as a $\mathbb{Z}$-module.*

Proof. Suppose that a is integral. Then clearly powers $1, a, \ldots, a^{n-1}$ span $\mathbb{Z}[a]$, so it is finitely generated as a $\mathbb{Z}$-module.

Conversely, suppose that $\mathbb{Z}[a]$ is finitely generated as a $\mathbb{Z}$-module. Then considering the sub $\mathbb{Z}$-module P_n spanned by $1, a, \ldots, a^{n-1}$, by Noetherity one has $P_n = P_{n+1}$ for some n. Then clearly a satisfies a monic polynomial of degree n. □

Corollary 9.2. *Suppose that A is finitely generated as a $\mathbb{Z}$-module. Then all elements of A are integral.*

Claim 9.3. *Suppose that A is commutative. Then the subset of integral elements in A is a subring.*

Proof. Clearly $1, 0$ are integral. For two integral elements a, b, clearly $\mathbb{Z}[a, b]$ generated by finitely many elements of the form $a^n b^m$ (here we use the commutativity of A), and hence is finitely generated as a $\mathbb{Z}$-module. Hence, by the above, all its elements, and in particular $a + b, ab$, are integral. □

9.2 Integrality in the group algebra

Claim 9.4. *Consider $Fun(G)$ as an algebra under convolution.*

1. *The elements $\delta_g \in Fun(G)$ are integral.*

2. *For a conjugacy class $C \subset G$, the elements $\delta_C := \sum_{g\in C}\delta_g \in Fun(G)$ are integral.*

3. *If an element $f \in Fun(G)^{cent}$ has integral values, then it is integral.*

4. *Let $(V, \pi) \in Rep(G)$. Then χ_V has integral values.*

Proof.

1. This is clear since $\delta_g^{|G|} = \delta_e$.

2. Notice that the elements of the form δ_C form a basis for $Fun(G)^{cent}$, and that the convolution of two such elements is a (non-negative) rational integer combination of such elements. Hence, the $\mathbb{Z}$-span of such elements is a subalgebra of $Fun(G)^{cent}$ which is finitely generated as a $\mathbb{Z}$-module, and hence all elements in it are integral.

3. This is clear, since such an element is an integral combination of elements of the form δ_C.

4. This is clear, since $\chi_V(g)$ is a sum of eigenvalues of $\pi(g)$, which are roots of unity.

□

Claim 9.5. *Let $(V, \pi) \in Rep(G)$ and $f \in Fun(G)$.*

1. *If f is integral (as an element of the algebra $Fun(G)$ under convolution), then $|G|(f, \chi_V)$ is integral.*

2. *If f is integral and central, and V is irreducible, then $\frac{|G|}{\dim(V)}(f, \chi_V)$ is integral.*

Proof.

1. Since $f \in Fun(G)$ is integral, so is f^*, and thus so is $\pi(f^*) \in End(V)$. Thus so is $Tr_V(\pi(f^*)) = |G|(f, \chi_V) \in k$.

2. As in the previous item, $\pi(f^*) \in End(V)$ is integral. But $\pi(f^*)$ is scalar, and that scalar is $\frac{1}{\dim V} Tr_V(\pi(f^*)) = \frac{|G|}{\dim V}(f, \chi_V)$.

□

Claim 9.6. *Let $E \in Rep(G)$ be irreducible. Then* $\dim(E)$ *divides* $|G|$.

Proof. The element $\chi_E \in Fun(G)^{cent}$ has integral values, and hence is integral. Thus, $\frac{|G|}{\dim E}(\chi_E, \chi_E) = \frac{|G|}{\dim E}$ is integral, as desired. □

In fact a more refined statement is true:

Claim 9.7. *Let $E \in Rep(G)$ be irreducible, and $Z \subset G$ the center. Then* $\dim(E)$ *divides* $[G : Z]$.

Proof (Attributed by Serre to Tate). Let $m \geq 1$ and consider the representation $E^{\otimes m}$ of G^m. It is irreducible. Let $Z_m \subset Z^m$ be the subgroup consisting of vectors $(z_1, \ldots, z_m)$ satisfying $z_1 \cdots z_m = 1$. Since Z acts on E via some character, Z_m acts trivially on $Z^{\otimes m}$. Hence $E^{\otimes m}$ descends to an irreducible representation of G^m/Z_m, and thus by the previous claim we get that $dim(E^{\otimes m})$ divides $|G^m/Z_m|$. In other words, $dim(E)^m$ divides $|G|^m/|Z|^{m-1}$. Thus, we get for each prime p that $m \cdot v_p(dim(E)) \leq m \cdot v_p(|G|) - (m-1) \cdot v_p(|Z|)$, or $v_p(dim(E)) \leq v_p(|G|) - \frac{m-1}{m} v_p(|Z|)$. Taking the limit as $m \to \infty$ we obtain $v_p(dim(E)) \leq v_p(|G|) - v_p(|Z|) = v_p([G:Z])$. Thus $dim(E)$ divides $[G:Z]$. □

Claim 9.8. *Let $E \in Rep(G)$ be irreducible, and $g \in G$. Then $\frac{|C_g|}{\dim E}\chi_E(g)$ is integral.*

Proof. Since δ_{C_g} is integral, we obtain that $\frac{1}{\dim V}(\delta_{C_g}, \chi_E) = \frac{|C_g|}{\dim E}\chi_E(g)$ is integral. □

9.3 Burnside's theorem

Lemma 9.9. *Let $\zeta_1, \ldots, \zeta_d \in \mathbb{C}^\times$ be roots of unity. Then:*

1. *The average $\frac{\zeta_1 + \ldots + \zeta_d}{d}$ is of absolute value ≤ 1, and 1 is attained if and only if $\zeta_1 = \zeta_2 = \ldots = \zeta_d$.*
2. *The average $\frac{\zeta_1 + \ldots + \zeta_d}{d}$ is an algebraic integer if and only either it equals 0 or $\zeta_1 = \zeta_2 = \ldots = \zeta_d$.*

Proof. Point (1) is a simple exercise.

Let's prove (2). Notice that the norm-squared of an algebraic integer is an integer. Hence there are no algebraic integers c with $0 < |c| < 1$. Thus, (2) is clear by (1).

□

Claim 9.10. *Let $V \in Rep(G)$. Let $g \in G$ be an element for which $(|C_g|, \dim V) = 1$. Then either $\chi_V(g) = 0$, or g acts by scalar on V.*

Proof. By claim 9.8, the number $\frac{|C_g|}{\dim V}\chi_V(g)$ is integral. Since $(|C_g|, \dim V) = 1$ and $\chi_V(g)$ is integral, we obtain that easily that $\frac{1}{\dim V}\chi_V(g)$ is integral. Notice that $\chi_V(g)$ is the sum of $\dim(V)$ roots of unity (the eigenvalues of g acting on V). Hence by claim 9.9 either $\chi_V(g) = 0$ or all the eigenvalues of g acting on V are equal, meaning that g acts by a scalar on V. □

Claim 9.11. *Let G be a group, and $C \subset G$ a conjugacy class such that $|C|$ is a positive power of a prime number. Then G is not simple.*

Proof. Let us denote by p the prime whose power is $|C|$. It suffices to show that there exists a non-trivial irreducible $E \in Rep(G)$ on which elements in C act by scalar (then, taking two different $g, h \in C$, the element gh^{-1} acts as identity on E, and hence E is not faithful, showing that G is not simple). For that, using claim 9.10, it is enough to find a non-trivial irreducible E of dimension prime to p, such that $\chi_E(C) \neq 0$. An orthogonality relation (exercise 3.4) reads

$$\sum_{[E]\in Irr(G)} \dim E \cdot \chi_E(C) = 0.$$

Let us partition the sum as follows:

$$1+\sum_{[E]\in Irr(G),\ p|\dim E} \dim E\cdot\chi_E(C)+\sum_{[E]\in Irr(G),\ p\nmid\dim E,\ [E]\neq[Triv]} \dim E\cdot\chi_E(C) = 0.$$

Since p divides all the summands in the first sum (in the sense of algebraic integers), it must not divide all the elements in the second sum, so in particular $\chi_E(C) \neq 0$ for some irreducible $E \in Rep(G)$ whose dimension is not divisible by p. □

Theorem 9.12 (Burnside)**.** *Let G be a finite group whose order is divisible by at most two primes. Then G is solvable.*

Proof. It is known that groups of prime power order are solvable. The theorem is thus equivalent to showing that there are no simple groups G with $|supp|G|| = 2$ (where $supp(n)$ denotes the set of primes dividing n).

Suppose that G is a simple group with $supp(|G|) = \{p, q\}$ (and $p \neq q$). Then by the previous claim, each conjugacy class of G has either order 1, or order divisble by pq. We thus obtain that pq divides $|G| - |Z(G)|$. This implies that $|Z(G)| \neq 1$, contradicting the simplicity of G. □

10 Positive characteristic

In this section, the notation is as follows. A is a complete discrete valuation ring. K is the field of fractions of A, and $k = A/\mathfrak{m}$ is the residue field. We assume that K has characteristic 0, and k has positive characteristic p.

We fix a finite group G. We denote by m the lcm of the orders of elements of G, and assume?

10.1 Characters

We can define characters of representations as we did in characteristic zero. The following claim is still true:

Claim 10.1. *The system $(\chi_E)_{[E]\in Irr_k(G)} \subset Fun_k^{cent}(G)$ is linearly independent.*

Proof. Using claim 3.19, which is true in positive characteristic as well, we can find $f \in Fun_k(G)$ such that $Tr(\pi(f)) = 1$ for one of the irreducible representations (E, π), and $Tr(\sigma(f)) = 0$ for the rest of them (F, σ). Then $\sum_g f(g)\chi_E(g) = 1$ and $\sum_g f(g)\chi_F(g) = 0$. This implies what we want. □

We now notice that the characters will not generally span $Fun_k^{cent}(G)$:

Claim 10.2. *Let $V \in Rep_k(G)$. Then for every $g \in G$, we have $\chi_V(g) = \chi_V(g_{p\text{-}reg})$.*

Proof. Since $g_{p\text{-tor}}$ is acts unipotently and commutes with $g_{p\text{-reg}}$, this is an easy exercise. ☐

However, the following theorem is true:

Theorem 10.3 (Brauer)**.** *The system $(\chi_E)_{[E]\in Irr_k(G)}$ forms a basis of $Fun_k^{cent}(G^{p\text{-}reg})$.*

To prove it, we will study Brauer characters.

10.2 Grothendieck groups

It will be wiser to replace the character rings $R_k(G)$ by Grothendieck rings $\mathcal{K}_k(G)$. We recall the definition:...

Claim 10.4. *Let K be a field of characteristic zero. Then the map $\mathcal{K}_K(G) \to R_K(G)$ given by $[V] \mapsto \chi_V$ is an isomorphism of rings.*

10.3 The morphism $d : \mathcal{K}_K(G) \to \mathcal{K}_k(G)$

Let V be a finite-dimensional K-vector space. By a lattice in V we mean a finitely generated projective A-submodule $L \subset V$, such that $K \otimes_A L \to V$ is an isomorphism.

Lemma 10.5. *Let $L \subset V$ be a finitely generated A-submodule such that $KL = V$. Then L is a lattice in V.*

Proof. Since A is a principal ideal domain and L is a torsion-free finitely generated A-module, a well-known theorem says that L is a free A-module. Choosing an A-basis for L, we immediately see that $K \otimes_A L \to V$ is an isomorphism. ☐

Let now $V \in Rep_K(G)$. There always exist G-invariant lattices $L \subset V$. Indeed, we take any lattice $L_0 \subset V$, and then set $L := \sum_{g\in G} gL_0$. The previous lemma guarantees that L is a lattice in V.

For a G-invariant lattice $L \subset V$, we obtain $L/\mathfrak{m}L \in Rep_k(G)$. We define a homomorphism $d : \mathcal{K}_K(G) \to \mathcal{K}_k(G)$ by setting $d([V]) := [L/\mathfrak{m}L]$. Of course, we need:

Lemma 10.6. *$[L/\mathfrak{m}L] \in \mathcal{K}_k(G)$ from above does not depend on the choice of the G-invariant lattice L in V.*

Proof. Let us say, for two lattices $L, M \subset V$, that L is close to M (write $L(M$ for that relation) if $\pi M \subset L \subset M$. We first notice that the equivalence relation on G-invariant lattices generated by this closeness relation identifies any two G-invariant lattices. Indeed, let $L, M \subset V$ be two G-invariant lattices. Since $\pi L(L$ and $\pi^k L \subset M$ for big enough k, we can assume that $\pi^k M \subset L \subset M$ for some k. Now, $L(\pi^{k-1}M + L$ and $\pi^{k-1}M \subset \pi^{k-1}M + L \subset M$, so by reverse induction on k we are done.

Hence, it is enough to show that $[L/\pi L] = [M/\pi M]$ when $L(M$. For that, notice that we have an exact sequence in $Rep_k(G)$:

$$0 \to \pi M/\pi L \to L/\pi L \to M/\pi L \to M/L \to 0,$$

and that $\pi M/\pi L \simeq M/L$. □

10.4 The Brauer character

Let us recall Hensel's lemma:

Claim 10.7. *Let f...*

Using that lemma, we see that any root of unity in k of order prime to p, admits a unique lift to a root of unity in A. Let us denote this lifting procedure by $\bar{\cdot}$.

Let $(V, \pi) \in Rep_k(G)$. We define $\chi_V^{Br} \in Fun_A(G^{p\text{-reg}}) \subset Fun_K(G^{p\text{-reg}})$ as the function that associates to $g \in G^{p\text{-reg}}$ the sum $\sum_\lambda \bar{\lambda}$, where λ runs over the eigenvalues of $\pi(g)$.

Claim 10.8. *Let $V \in Rep_K(G)$. Then the restriction of χ_V to $G^{p\text{-reg}}$ is equal to $\chi_{d(V)}^{Br}$.*

Proof. By restricting to cyclic subgroups, we reduce to the case when G itself is cyclic, of order prime to p. In such a case, we can find an eigenbasis of V for G, and take its A-span as a G-invariant lattice. Then the claim becomes straightforward. □

The main theorem is:

Theorem 10.9. *The system $(\chi_E^{Br})_{[E] \in Irr_k(G)}$ forms a basis of $Fun_K^{cent}(G^{p\text{-reg}})$ (as a K-vector space).*

Proof. Let us prove that the Brauer characters span $Fun_K^{cent}(G^{p\text{-reg}})$. Let $f \in Fun_K^{cent}(G^{p\text{-reg}})$. We can extend f by zero to obtain a function $\widetilde{f} \in Fun_K^{cent}(G)$, and write it

$$\widetilde{f} = \sum_{[E] \in Irr_K(G)} n_{[E]} \chi_E,$$

where $n_{[E]} \in K$. Restricting to $G^{p\text{-reg}}$ and using claim 10.8, we obtain:

$$f = \sum_{[E] \in Irr_K(G)} n_{[E]} \chi_{d(E)}^{Br}.$$

Let us now prove linear independence. Suppose that we have a non-trivial relation

$$\sum_{[E] \in Irr_k(G)} n_{[E]} \chi_E^{Br} = 0,$$

where $n_{[E]} \in K$. By multiplying, we can assume that $n_{[E]} \in A$, and not all $n_{[E]} \in \mathfrak{m}$. Applying reduction, we obtain a non-trivial relation:

$$\sum_{[E]\in Irr_k(G)} \overline{n_{[E]}}\chi_E = 0 \quad \text{on } G^{p\text{-reg}}.$$

By claims 10.2 and 10.1 we obtain a contradiction. □

Proof (of theorem 10.3). We have already seen that the system is linearly independent. By theorem 10.9, the number of elements in the system matches the dimension of the vector space, so that it must span. □