Lecture notes for Ma120c (Caltech, Spring 2018 and Spring 2019) (UNPOLISHED DRAFT)

Alexander Yom Din

April 1, 2020

Contents

1 Introduction, conventions, etc.

If not specified otherwise, all rings and algebras are with unit. If not specified otherwise, by a module we mean a left module.

2 Some recollections on categories

Definition 2.1.

- categories, functors...
- functor categories, morphism between functors...
- products, coproduts, final objects, initial objects, limits, colimits...
- additive/k-linear categories, additive/k-linear functors...
- abelian categories, k-linear abelian categories...

Definition 2.2. An **adjunction** between two categories $(\mathcal{C}, \mathcal{D})$ is a pair of functors

$$F : \mathcal{C} \to \mathcal{D}, \quad \mathcal{C} \leftarrow \mathcal{D} : G,$$

together with one of the following equivalent pieces of data:

1. Morphisms $u : Id_{\mathcal{C}} \to G \circ F$ and $n : F \circ G \to Id_{\mathcal{D}}$ satisfying
$$F \xrightarrow{Fu} F \circ G \circ F \xrightarrow{nF} F \quad \text{is equal to } Id_F,$$
$$G \xrightarrow{uG} G \circ F \circ G \xrightarrow{Gn} G \quad \text{is equal to } Id_G.$$
2. An isomorphism of the functors
$$Hom(F\cdot, \cdot), Hom(\cdot, G\cdot) : \mathcal{C}^{op} \times \mathcal{D} \to Sets.$$

Definition 2.3. An **equivalence** between two categories $(\mathcal{C}, \mathcal{D})$ is one of the following (if one is careful, one should understand how they are exactly related):

1. An adjunction (F, G, u, n) between $\mathcal{C}, \mathcal{D}$ such that u and n are isomorphisms.
2. A pair of functors $F : \mathcal{C} \to \mathcal{D} \quad \mathcal{C} \leftarrow \mathcal{D} : G$ and isomorphisms $Id_{\mathcal{C}} \cong G \circ F,\ F \circ G \cong Id_{\mathcal{D}}$.
3. A pair of functors $F : \mathcal{C} \to \mathcal{D} \quad \mathcal{C} \leftarrow \mathcal{D} : G$ such that $G \circ F$ is isomorphic to $Id_{\mathcal{C}}$ and $F \circ G$ is isomorphic to $Id_{\mathcal{D}}$.
4. A functor $F : \mathcal{C} \to \mathcal{D}$ for which there exists $\mathcal{C} \leftarrow \mathcal{D} : G$ such that $G \circ F$ is isomorphic to $Id_{\mathcal{C}}$ and $F \circ G$ is isomorphic to $Id_{\mathcal{D}}$.
5. A functor $F : \mathcal{C} \to \mathcal{D}$ which is fully faithful and essentially surjective.

Remark 2.4. When dealing with additive categories, we will assume that all functors are additive, even if we don't mention this. Incidentally, let us remark that functors which are part of an adjunction between additive categories are automatically additive (in particular, equivalences of additive categories are automatically additive). When dealing with k-linear categories, we will assume that all functors are k-linear, even if we don't mention this.

3 Some properties in an abelian category

In this section, $\mathcal{A}$ is an abelian category. We will be interested in properties of objects in $\mathcal{A}$. We will say that a property of object in $\mathcal{A}$ is **Serre**, if 0 has this property, subobjects and quotient objects of objects having this property have this property, and if a subobject as well as the quotient by it have this property, then the object itself has this property.

3.1 Finiteness properties

3.1.1 Finite length

Definition 3.1. An object $M \in \mathcal{A}$ is said to be **simple**, or **irreducible**, if $M \neq 0$ and M contains no subobjects except 0 and M. We denote by $Irr(\mathcal{A})$ the "set"[1] of isomorphism classes of simple objects in $\mathcal{A}$.

Claim 3.2 (Schur's lemma)**.**

1. *Let $M \in \mathcal{A}$ be simple. Then $End(M)$ is a division ring.*

2. *Let $M, N \in \mathcal{A}$ be simple and non-isomorphic. Then $Hom(M, N) = 0$.*

Proof.

1. Let $T \in End(M)$, and suppose that $T \neq 0$. Then $Ker(T) \neq M$, and hence, by simplicity, we obtain $Ker(T) = 0$ (i.e. T is injective). Also, $Im(T) \neq 0$, and hence, by simplicity, we obtain $Im(T) = M$ (i.e. T is surjective). Thus, T is bijective, and so admits an inverse in $End(M)$.

2. Let $T \in Hom(M, N)$. If $Im(T) = N$ and $Ker(T) = 0$ then T is an isomorphism, contradicting the assumption. Hence either $Im(T) \neq N$ (in which case $Im(T) = 0$ so $T = 0$) or $Ker(T) \neq 0$ (in which case $Ker(T) = M$ so $T = 0$).

□

Definition 3.3. A **composition series** for an object $M \in \mathcal{A}$ is a sequence of submodules

$$0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$$

such that M_{i+1}/M_i is simple for every $0 \leq i \leq n-1$. An object $M \in \mathcal{A}$ is said to have **finite length** if it admits a composition series.

Lemma 3.4. *The property of being of finite length is Serre.*

[1] I am not very versed in foundations - for me it is a set in the sense that two elements in it are either equal or not; it is not a set in the sense that I don't a priory care about the ability to ask about its cardinality.

Definition-Claim 3.5 (Jordan-Holder theorem)**.** *Let $M \in \mathcal{A}$ be of finite length, and let*

$$0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$$

*be a composition series for M. For every $\pi \in Irr(\mathcal{A})$, let us denote by $[M : \pi] \in \mathbb{Z}_{\geq 0}$ the number of $0 \leq i \leq n-1$ such that M_{i+1}/M_i has isomorphism class π. Then $[M : \pi]$ does not depend on the choice of composition series. In particular, $\ell(M) := n$ does not depend on the choice of composition series. We call $([M : \pi])_{\pi \in Irr(\mathcal{A})}$ the **Jordan-Holder contents** of M, $\{\pi \in Irr(\mathcal{A}) : [M : \pi] \neq 0\}$ the **Jordan-Holder support** of M, and $\ell(M)$ the **length** of M.*

3.1.2 Noetherian and Aritnian properties

Definition 3.6.

1. An object $M \in \mathcal{A}$ is said to be **Noetherian**, if for every increasing sequence of subobjects $M_0 \subset M_1 \subset \ldots$ of M, there exists $K \in \mathbb{Z}_{\geq 0}$ such that $M_k = M_K$ for all $k \geq K$.

2. An object $M \in \mathcal{A}$ is said to be **Artinian**, if for every decreasing sequence of subobjects $M_0 \supset M_1 \supset \ldots$ of M, there exists $K \in \mathbb{Z}_{\geq 0}$ such that $M_k = M_K$ for all $k \geq K$.

Lemma 3.7. *The properties of being Noetherian/Artinian are Serre.*

Lemma 3.8. *An object $M \in \mathcal{A}$ is of finite length if and only if it is both Noetherian and Artinian.*

3.2 Semisimplicity

Definition 3.9. An object $M \in \mathcal{A}$ is said to be **semisimple**, if for every subobject $N \subset M$, there exists a subobject $L \subset M$ such that $M = N \oplus L$. The category $\mathcal{A}$ is said to be **semisimple**, if every object in it is semisimple.

Lemma 3.10. *Let us abbreviate "ss" for "semisimple".*

1. *0 is ss.*

2. *Simple objects are ss.*

3. *If an object is ss, then all of its subobjects and quotient objects are ss.*

4. *If two objects are ss, then their direct sum is ss.*

Example 3.11. *Let us consider $\mathcal{A} = Mod(\mathbb{C}[x])$. One has a full subcategory $Mod(\mathbb{C}[x])^{fd} \subset Mod(\mathbb{C}[x])$ consisting of modules which are finite-dimensional as $\mathbb{C}$-vector spaces. The study of $Mod(\mathbb{C}[x])^{fd}$ is, basically, linear algebra. We can use square matrices (up to similarity) to represent isomorphism classes of objects in $Mod(\mathbb{C}[x])^{fd}$. Then, one can check that $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ represents a* *semisimple object, while* $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *represents a non-semisimple object. More generally, a matrix will represent a semisimple object if and only if it is diagnolizable.*

Example 3.12. *The* $\mathbb{Z}$*-modules* $\mathbb{Z}/p\mathbb{Z}$*, where* p *is prime, are simple, hence semisimple. The* $\mathbb{Z}$*-module* $M := \mathbb{Z}/p^2\mathbb{Z}$*, where* p *is prime, is not semisimple. Indeed, consider* $pM \subset M$*. Since* $M/pM \cong \mathbb{Z}/p\mathbb{Z}$*, would* pM *have a complement in* M*, we would have an element in* M *of order* p*, which is not in* pM*, which we don't have.*

Remark 3.13. Let us recall that a short exact sequence

$$0 \to M_1 \xrightarrow{i} M_2 \xrightarrow{p} M_3 \to 0$$

is said to be **splittable**, if one of the following equivalent conditions is satisfied:

1. There exists $s : M_3 \to M_2$ such that $p \circ s = id$.
2. There exists $c : M_2 \to M_1$ such taht $c \circ i = id$.

In that case, M_2 is isomorphic to the direct sum of M_1 and M_3 (described naturally once s or c are fixed).

Remark 3.14. Let $N \subset M$. Then N admits a complement in M if and only if the short exact sequence

$$0 \to N \xrightarrow{\subset} M \to M/N \to 0$$

is splittable.

Remark 3.15. Let

$$0 \to M_1 \xrightarrow{i} M_2 \xrightarrow{p} M_3 \to 0$$

be a short exact sequence. If M_1 is injective, or M_3 is projective, then this short exact sequence is splittable.

Remark 3.16. Let us recall that an additive functor $F : \mathcal{A} \to \mathcal{B}$ (where $\mathcal{B}$ is another abelian category) transforms splittable short exact sequences into splittable short exact sequences.

Claim 3.17. *The following properties are equivalent:*

1. *The category* $\mathcal{A}$ *is semisimple.*
2. *Every short exact sequence in* $\mathcal{A}$ *is splittable.*
3. *Every object in* $\mathcal{A}$ *is projective.*
4. *Every object in* $\mathcal{A}$ *is injective.*

Proof. $(1) \iff (2)$: Follows from remark 3.14.

$(2) \implies (3), (4)$: The properties of being projective/injective are defined by some additive functors sending short exact sequences into short exact sequences. Since every short exact sequence in $\mathcal{A}$ is splittable, the properties follow from remark 3.16.

$(3) \implies (2), (4) \implies (2)$: Follows from remark 3.15. □

4 Semisimplicity

Throughout the seciton, let R be a ring. We denote by $Mod(R)$ the abelian category of R-modules, and $Irr(R) := Irr(Mod(R))$.

4.1 Semisimple modules

Lemma 4.1. *Let M be a non-zero R-module. Then M admits a simple subquotient.*

Proof. Replacing M by a non-zero finitely-generated submodule, we may assume that M is finitely-generated. We will show that in this case M admits a simple quotient. This follows from the fact that submodules of M, not equal to M, satisfy the conditions of Zorn's lemma (this follows by choosing a finite set of generators of M, and noticing that a submodule of M is equal to M if and only if it contains all these generators). □

Claim 4.2. *Let M be an R-module. The following are equivalent:*

1. *M is semisimple.*
2. *M can be written as a direct sum of simple submodules.*
3. *M can be written as a sum of simple submodules.*

Proof.

(1) $\implies$ (2): By Zorn's lemma, we can find a maximal family of simple submodules $I \subset Sub(M)$ such that the sum of submodules in I is direct. We claim that the sum of submodules in I is M. Indeed, let $N \subset M$ be a submodule complimentary to said sum. From the maximality of I, we deduce that N doesn't contain simple submodules. By semisimplicity, N can't contain then any simple subquotients. It then follows from lemma 4.1 that $N = 0$.

(2) $\implies$ (3): Clear.

(3) $\implies$ (1): Suppose that $M = \sum_{i \in I} M_i$, and let $N \subset M$ be a submodule. By Zorn's lemma, we can find maximal $J \subset I$ such that $\left(\sum_{i \in J} M_i\right) \cap N = 0$. We want to show that $\left(\sum_{i \in J} M_i\right) + N = M$. If that is not the case, then there exists $j \in I$ such that $M_j \not\subset \left(\sum_{i \in J} M_i\right) + N$. Since M_j is simple, this implies $M_j \cap \left(\left(\sum_{i \in J} M_i\right) + N\right) = 0$. Then $\left(\sum_{i \in J \cup \{j\}} M_i\right) \cap N = 0$, contradicting the maximality of J (notice that $j \notin J$).

□

Claim 4.3.

1. *Let $(M_i)_{i \in I}$ be a family of semisimple R-modules. Then $\oplus_{i \in I} M_i$ is semisimple.*
2. *Let M be an R-module, and $(M_i)_{i \in I}$ a family of semisimple submodules of M. Then $\sum_{i \in I} M_i$ is semisimple.*

Proof.

1. This clearly follows from the characterization of the previous claim.

2. Notice that $\sum_{i\in I} M_i$ is a quotient of $\oplus_{i\in I}M_i$, and hence the claim follows from the previous point and semisimplicity being a Serre property (alternatively, again directly from the previous claim).

□

4.2 Isotypic components

Definition 4.4. Let M be an R-module and $\pi \in Irr(R)$. We denote by M_π the sum of all submodules of M which are simple of isomorphism class π (it is called the **isotypic component** of M corresponding to π).

Lemma 4.5. *Let M be an R-module. One has $(M_\pi)_\pi = M_\pi$. The family $(M_\pi)_{\pi\in Irr(R)}$ is linearly independent, and $M = \oplus_{\pi\in Irr(R)}M_\pi$ if and only if M is semisimple.*

Proof. The only slightly non-trivial thing is to check that the family $(M_\pi)_{\pi\in Irr(R)}$ is linearly independent. For that, it is enough to show that if $E \subset M_{\pi_1} + \ldots + M_{\pi_n}$ is a simple submodule, then the isomorphism class of E is in $\{\pi_1, \ldots, \pi_n\}$. Indeed, since E is finitely generated we have $E \subset E_1 + \ldots + E_m$ where each E_i is a simple submodule whose isomorphism class is in $\{\pi_1, \ldots, \pi_n\}$. It is easy to see that the Jordan Holder support of $E_1 + \ldots + E_m$ is contained in the set of isomorphism classes of $E_1, \ldots, E_m$. Since it also contains the isomorphism class of E, by the Jordan Holder theorem we obtain that the isomorphism class of E is equal to the isomorphism class of one of $E_1, \ldots, E_m$. □

Lemma 4.6. *Let M, N be R-modules and $\phi : M \to N$ a morphism. Then for every $\pi \in Irr(R)$ we have $\phi(M_\pi) \subset N_\pi$.*

Proof. Clear. □

Definition 4.7. Let $S \subset Irr(R)$. For an R-module M, we define $M_S := \sum_{\pi\in S} M_\pi$.

Remark 4.8. Let $S \subset Irr(R)$. For an R-module M, one has $(M_S)_S = M_S$. If M is semisimple, then $M = M_S \oplus M_{c(S)}$, where we denote $c(S) := Irr(R) - S$.

4.3 Semisimple rings

Definition 4.9. The ring R is called **semisimple**, if the category $Mod(R)$ is semisimple (i.e. every R-module is semisimple).

Example 4.10. *A field is semisimple. More generally, a division ring is semisimple. Indeed, given a submodule $N \subset M$, we can choose a basis of N, and then completing it to a basis of M. The span of the complementing elements will be a submodule complementary to N.*

Claim 4.11. *The following are equivalent:*

1. *The ring R is semisimple.*
2. *The R-module R is semisimple.*

Proof.
(1) $\implies$ (2): Clear.
(2) $\implies$ (1): Every module is a quotient of a direct sum of copies of R. □

Recall, that R is called left Noetherian/left Artinian, if R as an (left) R-module is so.

Claim 4.12. *Suppose that R is semisimple. Then R is left Noetherian and left Artinian.*

Proof. The claim will follow if we show that R can be expressed as a finite direct sum of simple left ideals (because then R (as an R-module) will be of finite length, and hence Noetherian and Artinian). By semisimplicity, one can write $R = \oplus_{\sigma\in\Sigma} I_\sigma$ where $I_\sigma \subset R$ are simple left ideals. Decomposing 1 along this, we obtain $1 = \sum_{\sigma\in\Sigma'} f_\sigma$ where $\Sigma' \subset \Sigma$ is a finite subset. But then for $f \in I_\tau$, for $\tau \in \Sigma - \Sigma'$, one obtains

$$f = f \cdot 1 = \sum_{\sigma\in\Sigma'} f \cdot f_\sigma \in \sum_{\sigma\in\Sigma'} I_\sigma.$$

This forces $f = 0$, and thus one must have $\Sigma = \Sigma'$, i.e. Σ is finite. □

Corollary 4.13. *Suppose that R is semisimple. Then $Irr(R)$ is finite.*

Proof. Notice first that for every $\pi \in Irr(R)$ one has $R_\pi \neq 0$. Indeed, a simple R-module of isomorphism class π can be realized as a quotient R/I. By semisimplicity, this quotient module of R can be realized as a submodule of R.

Now, one has $R = \oplus_{\pi\in Irr(R)} R_\pi$. Since R is left Noetherian, this must be a finite sum. □

4.4 Two-sided ideals and splittings

Throughout this subsection, we assume that R is semisimple.

Lemma 4.14. *Let $E, F \subset R$ be two isomorphic simple submodules. Then there exists $r \in R$ such that $F = Er$.*

Proof. By semisimplicity, we can find a projection $R \to E$ which is left inverse to the inclusion $E \subset R$, compose it with an isomorphism of E with F, and then compose it with the embedding $F \subset R$ thus obtaining an R-module morphism $R \to R$ whose image when restricted to E is F. Such a morphism must be given by a multiplication on the right by an element $r \in R$. We thus obtain $F = Er$. □

Lemma 4.15.

1. *Let $S \subset Irr(R)$. The left ideal $R_S \subset R$ is a two-sided ideal.*
2. *Let $S, T \subset Irr(R)$, and suppose that $S \cap T = \emptyset$. Then $R_S R_T = 0$.*
3. *Let $I \subset R$ be a two-sided ideal. Then there exists a unique $S \subset Irr(R)$ such that $I = R_S$.*

Proof.

1. Let $r \in R$. Since $x \mapsto xr$ is a left R-module homomorphism, it preserves R_S.
2. Follows from R_S, R_T being two-sided ideals, and $R_S \cap R_T = 0$.
3. It is enough to show that if $E, F \subset R$ are two isomorphic simple submodules, and if $E \subset I$, then $F \subset I$. This follows at once from lemma 4.14.

□

Let $S \subset Irr(R)$. Recall that we denote $c(S) := Irr(R) - S$. Decomposing $1 \in R$ along $R = R_S \oplus R_{c(S)}$, we obtain an expression $1 = e_S + e_{c(S)}$. We have $e_S r = r e_S = r$ for $r \in R_S$ and $e_S r = r e_S = 0$ for $r \in R_{c(S)}$. We notice that R_S is itself a ring, with unit e_S. One has $R = R_S \times R_{c(S)}$, a direct product of rings.

Let us denote by $Mod(R)_S$ the full subcategory of $Mod(R)$ consisting of R-modules M for which $M_S = M$.

Lemma 4.16. *$Mod(R)_S \subset Mod(R)$ is a Serre subcategory, closed under infinite (small) direct sums. One has a canonical bijection $Irr(Mod(R)_S) \cong S$.*

Lemma 4.17. *Let E be a simple R-module. Then e_S acts as identity (resp. zero) on E if the isomorphism class of E is in S (resp. $c(S)$).*

Proof. Recall that R contains a submodule isomorphic to E. Such a submodule is contained in R_S or $R_{c(S)}$, according to the isomorphism class of E being in S or $c(S)$. Since $e_S r = r$ for $r \in R_S$ and $e_{c(S)} r = 0$ for $r \in R_{c(S)}$, the claim follows. □

Lemma 4.18. *Let $M \in Mod(R)$. The following are equivalent:*

1. *$M \in Mod(R)_S$.*
2. *$e_{c(S)} m = 0$ for every $m \in M$.*
3. *$e_S m = m$ for every $m \in M$.*

Proof. Follows from the previous lemma. □

Claim 4.19 (Localization)**.** *One has an equivalence of categories*

$$Mod(R)_S \rightleftarrows Mod(R_S).$$

The ring R_S is semisimple and one has a canonical bijection $Irr(R_S) \cong S$.

Proof. Let us describe what are the functors (leaving the verifcations as an exercise). Both functors act as identity on the underlying abelian groups. The functor from left to right is given by restricting along $R_S \to R$. The functor from right to left is given by letting $R_S \subset R$ act as it acts, and letting $R_{c(S)} \subset R$ act by zero.

That R_S is semisimple follows from $Mod(R_S) \approx Mod(R)_S$, and noting that $Mod(R)_S$ is semisimple as a Serre subcategory of $Mod(R)$.

Finally, notice that the equivalence yields $Irr(R_S) \cong Irr(Mod(R)_S) \cong S$. □

Definition 4.20. A ring R is called **simple**, if it is semisimple and $Irr(R)$ contains exactly one element.

Corollary 4.21 (From semisimple to simple)**.** *Let R be a semisimple ring. Then one has a canonical factorization $R = \prod_{\pi \in Irr(R)} R_\pi$, where R_π are simple rings.*

Remark 4.22. By claim 4.15, if R is a simple ring then the only two-sided ideals in R are 0 and R. A ring with such a property is called sometimes quasi-simple (or, non-compatibly with our terminology, simple). A quasi-simple ring might not be left Artinian, hence not semisimple (we will see later that a quasi-simple left Artinian ring is simple). As an example, one can check that $R = \mathbb{C}\{z, \partial_z\}/(\partial_z z - z\partial_z - 1)$ (the Weyl algebra, i.e. the algebra of differential operators with polynomial coefficients on the line) is quasi-simple and not left Artinian.

4.5 Jacobson's density theorem

Theorem 4.23. *Let M be a semisimple R-module. Let $S := End_R(M)$. Let $t \in End_S(M)$ and $v_1, \ldots, v_n \in M$. Then there exists $r \in R$ such that $tv_i = rv_i$ for $1 \leq i \leq n$.*

Proof. We first deal with the case $n = 1$. Since M is semisimple, we can write $M = Rv_1 \oplus M'$ for some R-submodule $M' \subset M$. One has the projection on Rv_1 along M', which is an element $s \in S$. Notice now that $stv_1 = tsv_1 = tv_1$, and thus $tv_1 \in Rv_1$. This means that there exists $r \in R$ such that $tv_1 = rv_1$.

For general n, let us consider the R-module M^n, and the vector $(v_1, \ldots, v_n) \in M^n$. Abusing notation, we denote by $t \in End(M^n)$ the diagonal operator $(t, t, \ldots, t)$. We now notice that t commutes with elements in $End_R(M^n)$ (by writing each element in $End_R(M^n)$ in matrix form). Using now the $n = 1$ case in this setting, gives us the desired claim. □

Corollary 4.24. *Let M be a semisimple R-module. Let $S := End_R(M)$. Suppose that M is finitely generated as an S-module. Then the morphism $R \to End_S(M)$ is surjective.*

Remark 4.25. On $End_S(M)$ we can define the "weak" topology, for which a subbasis of neighbourhoods of 0 consists of sets $U_v := \{t \in End_S(M) \mid tv = 0\}$ for $v \in M$. The one can state Jacobson's density theorem as follows: The image of the morphism $R \to End_S(M)$ is dense w.r.t. the weak topology.

4.6 Simple rings - the Artin-Wedderburn theorem

Proposition 4.26. *Assume that R is simple, and let E be a simple R-module. Denote $D := End_R(E)$ (recall that it is a division ring). Then E is finite-dimensional over D, and the natural morphism $R \to End_D(E)$ is an isomorphism.*

Proof. Notice that the morphism $R \to End_D(E)$ is injective; Indeed, if r maps to zero, then r acts by zero on every simple module, hence on every module (since every module is a sum of simple modules), and hence in particular on R, giving $r = 0$. Alternatively, injectivity is clear since R is quasi-simple.

If we will show that E is finite-dimensional over D, then the morphism $R \to End_D(E)$ will be surjective, by Jacobson's density theorem.

We have, for some $n \in \mathbb{Z}_{\geq 1}$, $R \cong E^n$. Let us notice that

$$E \cong Hom_R(R, E) \cong Hom_R(E^n, E) \cong Hom_R(E, E)^n,$$

where the D-module structure on each Hom-space is by postcomposing. Since $Hom_R(E, E)$ is a free D-module of rank 1, we see that E is of dimension n over D. □

Corollary 4.27. *Assume that R is semisimple. Then R is isomorphic to a finite direct product of rings of the form $End_D(E)$ where D is a division ring and E is a finite-dimensional vector space over D.*

4.7 Morita equivalence

Of course, in order for the previous subsection to be complete, we need also to check for ourselves that rings of the form $M_n(D)$, where D is a division ring, are simple. We will take the opportunity for a more general discussion.

Definition 4.28. Let R, S be rings. We say that A and B are **Morita equivalent**, if the categories $Mod(R)$ and $Mod(S)$ are equivalent.

Proposition 4.29. *Let $\mathcal{A}$ be an abelian category, admitting infinite direct sums[2]. Let $P \in \mathcal{A}$ be an object. Consider the functor*

$$G : \mathcal{A} \to Mod(End(P)^{op}) : \; M \mapsto Hom(P, M).$$

[2] In perhaps more modern terminology, "infinite direct sums" = "small coproducts".

Then G is an equivalence of categories if and only if P is a compact projective generator of $\mathcal{A}$, where:

- *P is projective means $Hom(P, \cdot) : \mathcal{A} \to Ab$ is exact.*
- *P is compact means $Hom(P, \cdot) : \mathcal{A} \to Ab$ commutes with infinite direct sums.*[3]*.*
- *P is a generator means that for every $M \in \mathcal{A}$, $Hom(P, M) = 0$ implies $M = 0$* [4]*.*

Proof. Let us abbreviate $R := End(P)^{op}$.

If G is an equivalence of categories, then to check the properties for $P \in \mathcal{A}$ is the same as to check the properties for $R \in Mod(R)$. This is left as an exercise.

Suppose now that P is a compact projective generator. We would like to verify that G is fully faithful and essentially surjective.

First, let us check that G is fully faithful, i.e. that for a pair $(N, M) \in \mathcal{A}^2$, the map $c_{N,M} : Hom(N, M) \to Hom(G(N), G(M))$ is a bijection. Let us fix M, and study for which N the map $c_{N,M}$ is a bijection. For $N = P$, that $c_{P,M}$ is a bijection is more-or-less a tautology. Both sides send infinite direct sums to infinite products (here we use P being compact). Also, both sides send cokernel diagrams to kernel diagrams (here we use P being projective). Hence, if an object N can be obtained from P by performing iteratively infinite direct sums and cokernels, $c_{N,M}$ will be a bijection. And indeed, we claim that every object $N \in \mathcal{A}$ is a cokernel of a morphism of the type $P^I \to P^J$. For this, it is enough to show that every object $N \in \mathcal{A}$ admits a surjection from some P^J. We have the universal try $\phi : P^{Hom(P,N)} \to N$. Every moprhism $P \to Coker(\phi)$ can be lifted to a morphism $P \to N$ since P is projective, and hence is zero. Since P is a generator, we obtain that $Coker(\phi) = 0$, i.e. ϕ is surjective.

Now, let us check that G is essentially surjective. We notice that G preserves infinite direct sums and cokernel diagrams. Hence, since we already know that G is fully faithful, the essential image of G is closed under infinite direct sums and cokernel diagrams. Since $R = G(P)$ is in the essential image and every R-module can be presetned as the cokernel of a morphism of type $R^I \to R^J$, we see that every R-module is in the essential image of G.

□

Example 4.30. *Let R be a ring. The object $R^n \in Mod(R)$ is a compact projective generator. Notice that $End(R^n)^{op} \cong M_n(R)$. Hence, the previous proposition gives us an equivalence of categories*

$$Mod(R) \approx Mod(M_n(R)).$$

Thus, $M_n(R)$ is Morita equivalent to R.

[3] the way we define compact is good only when P is projective, and we will use it only then.

[4] the way we define generator is good only when P is projective, and we will use it only then.

Example 4.31. *Notice that the properties of being semisimple/simple is stable under Morita equivalence. In particular, we obtain that for a division ring D, the ring $M_n(D)$ is simple.*

Claim 4.32. *Let R, S be simple rings. Then the following are equivalent:*

1. *R and S are Morita equivalent.*
2. *Given a simple R-module E and a simple S-module F, the division rings $End(E)$ and $End(F)$ are isomorphic.*
3. *There exists a division ring D and integers $n, m \in \mathbb{Z}_{\geq 1}$ such that $R \cong M_n(D)$ and $S \cong M_m(D)$.*

Proof.

(1) $\implies$ (2): This holds because the endomorphism ring of the (unique, up to isomoprhism) simple object is described category-theoretically.

(2) $\implies$ (3): By Artin-Wedderburn, R is isomoprhic to $M_n(D)$ for some $n \in \mathbb{Z}_{\geq 1}$, where D is the opposite of the endomorphism ring of a simple R-module.

(3) $\implies$ (1): We saw that $M_n(D)$ is Morita equivalent to D. □

The following claim we will need later, when discussing central simple algebras.

Claim 4.33. *Let R, S, T be rings, and assume that R and S are Morita equivalent. Then $R \otimes T$ and $S \otimes T$ are Morita equivalent.*

Proof. Given an abelian category $\mathcal{A}$, we can consider the category $\mathcal{A}^T$ of objects $M \in \mathcal{A}$ equipped with a morphism $T \to End(M)$. One easily shows that there is a natural equivalence of categories $Mod(R \otimes T) \approx Mod(R)^T$. Hence, if R and S are Morita equivalent, we obtain

$$Mod(R \otimes T) \approx Mod(R)^T \approx Mod(S)^T \approx Mod(S \otimes T).$$

□

Also, a nice feature is:

Exercise 4.34. *Let R be a ring. Then $Z(R)$ is isomorphic naturally to the endomorphism ring of the identity functor $Id_{Mod(R)}$.*

Corollary 4.35. *Let R, S be rings. If R and S are Morita equivalent, then $Z(R)$ and $Z(S)$ are isomorphic.*

Corollary 4.36. *Let R, S be commutative rings. If R and S are Morita equivalent, then R and S are isomorphic.*

Remark 4.37. All the above have variants, if we work with k-algebras instead of with rings. Then all morphisms/abelian categories/functors should be k-linear, all tensor products should be over k, etc.

4.8 The Jacobson radical

Definition 4.38. The **Jacobson radical** $J(R) \subset R$ is defined as the subset of all elements $r \in R$ such that $rE = 0$ for any simple R-module E.

Remark 4.39. Thus, in picturesque terms, the Jacosbon radical consists of operators which are immaterial on the irreducible spectrum.

Lemma 4.40.

1. *$J(R) \subset R$ is a two-sided ideal.*
2. *$J(R)$ is equal to the intersection of all maximal left ideals.*
3. *Let $r \in R$. Then $r \in J(R)$ if and only if $1 - sr$ is left-invertible for all $s \in R$.*

Proof.

1. Clear.
2. Notice that we can think of maximal left ideals as annihilators of non-zero elements in simple modules. From this, the claim is straightforward.
3. Suppose that $r \in J(R)$. Let $s \in R$. Then $1 - sr$ is not contained in any maximal left ideal. Hence, $R(1 - sr) = R$. Hence, $1 - sr$ is left-invertible. Conversely, suppose that $r \notin J(R)$. Then there exists a maximal left ideal $I \subset R$ such that $r \notin I$. Then $Rr + I = R$. Hence, there exist $s \in R, i \in I$ such that $sr + i = 1$. Then, $1 - sr \in I$ and so $1 - sr$ is not left-invertible.

□

Lemma 4.41 (Nakayama's lemma)**.** *Let M be a finitely-generated R-module. If $J(R)M = M$, then $M = 0$.*

Proof. Let $v_1, \dots, v_n \subset M$ be a set of generators of M. We can find elements $r_1, \dots, r_n \in J(R)$ such that $v_1 = r_1 v_1 + \dots + r_n v_n$. Then $(1 - r_1)v_1 \in Rv_2 + \dots + Rv_n$. Since $1 - r_1$ is left-invertible, we get $v_1 \in Rv_2 + \dots + Rv_n$. Thus, $v_2, \dots, v_n$ is also a set of generators of M. Continuing like this, we deduce that $M = 0$. □

Lemma 4.42.

1. *every nilpotent left ideal in R is contained in $J(R)$.*
2. *If R is left Artinian, $J(R)$ is nilpotent.*

Proof.

1. Let $I \subset R$ be a nilpotent left ideal, say $I^n = 0$, and let E be a simple R-module. Then if $IE \neq 0$, we have $IE = E$ and so, iterating, we obtain $0 = I^k E = E$ - a contradiction. Hence $IE = 0$.

2. The decreasing sequence $J(R)^n$ must stabilize - denote the common value $J(R)^\infty$. Then $J(R)^\infty J(R)^\infty = J(R)^\infty$. Consider the family of left ideals $I \subset J(R)^\infty$ which are finitely generated and for which $J(R)^\infty I \neq 0$. If $J(R)^\infty \neq 0$, this family is non-empty, and hence contains a minimal element I_0 (by the left Artinian property).

   Then $J(R)^\infty I_0 \neq 0$, and since $J(R)^\infty J(R)^\infty I_0 = J(R)^\infty I_0$, we can find $v \in J(R)^\infty I_0$ such that $J(R)^\infty v \neq 0$. Then Rv lies in our family, and hence by the minimality of I_0 we have $I_0 = Rv$. In particular, since $Rv \subset J(R)^\infty I_0 \subset I_0$, we obtain $I_0 = J(R)^\infty I_0$, and thus clearly also $J(R)I_0 = I_0$. Then, by Nakayama's lemma, we have $I_0 = 0$ - a contradiction. Hence $J(R)^\infty = 0$ or, in other words, $J(R)$ is nilpotent.

□

Claim 4.43. *Suppose that R is left Artinian. Then R is semisimple if and only if $J(R) = 0$.*

Proof. Suppose that R is semisimple. Then R is the sum of its simple submodules. Then, given $0 \neq r \in R$, since r doesn't act on R by zero, it must act not by zero on some simple submodule of R.

Conversely, suppose that $J(R) = 0$. Since $J(R)$ is the intersection of all maximal left ideals, and by the left Artinian property, we deduce that in fact we can find finitely many maximal left ideals $I_1, \ldots, I_n$ whose intersection is $J(R)$, i.e 0 by our assumption. This means that the natural R-module morphism

$$R \to R/I_1 \oplus \cdots \oplus R/I_n$$

is injective. This in turn shows that R is a semisimple R-module, since it can be embedded into a semisimple R-module. □

Example 4.44. *Consider the ring $\mathbb{Z}$. Then $J(\mathbb{Z}) = 0$, but $\mathbb{Z}$ is not semisimple.*

Claim 4.45. *Suppose that R is left Artinian, and let M be an R-module. Then M is semisimple if and only if $J(R)M = 0$.*

Proof. If M is semisimple, it is a direct sum of simple modules, and $J(R)$ annihilates every simple module, so the claim is clear in one direction.

Conversely, suppose that $J(R)M = 0$. Then we can consider M as an $R/J(R)$-module. Since $J(R/J(R)) = 0$ and $R/J(R)$ is left Artinian, we have that $R/J(R)$ is semisimple. Hence M is a semisimple $R/J(R)$-module, and thus clearly a semisimple R-module. □

Exercise 4.46. *Show that for a general R, the class of semisimple modules is not necessarily closed under infinite products. However, show that if R is left Artinian, the class of semisimple modules is closed under infinite products.*

For the next claim, let us recall that if R is a finite-dimensional algebra over a field k, then we have a functional $tr_R : R \to k$ given by sending $y \in R$ to the trace of the linear endomorphism of R given by $x \mapsto yx$.

Claim 4.47. *Let k be a field, and suppose that R is a finite-dimensional k-algebra. Then $J(R)$ is contained in the radical of the symmetric bilinear form $(x, y) \mapsto tr_R(xy)$. In particular, if $(x, y) \mapsto tr_R(xy)$ is non-degenerate, then R is semisimple.*

Proof. Let $r \in J(R)$ and $s \in R$. Since $J(R)$ is nilpotent, rs is nilpotent. Thus, the linear transformation $x \mapsto rsx$ is nilpotent, and so $tr(rs) = 0$. □

Example 4.48. *The converse of the claim is not true, due to inseparable field extensions, basically. Namely, if k is a field of characteristic p and $\alpha \in k$ has no p-th root in k, then we consider $R := k(\sqrt[p]{\alpha})$, which is a k-algebra of dimension p. Then it is easy to calculate that the trace functional is zero for the k-algebra R.*

5 Central simple algebras

Throughout this section, we fix a field k. By an algebra, we mean a k-algebra, by an abelian category/functor we mean a k-linear abelian category/functor, etc.

For a k-algebra A and a field extension K/k, we will denote $A_K := K \otimes_k A$ (it is a K-algebra).

5.1 Central simple algebras

Definition 5.1. A k-algebra A is called **central**, if $Z(A) = k$. We abbreviate "CSA" for "central f.d. simple algebra" and "CDA" for "central f.d. division algebra".

Recall that we say that a ring R is **quasi-simple**, if it has no two-sided ideals except 0 and R. Also, recall that we saw that a quasi-simple ring which is left Noetherian is simple.

Lemma 5.2. *Let A, B be quasi-simple k-algebras, and assume that A central. Then $A \otimes_k B$ is quasi-simple.*

Proof. Let $I \subset A \otimes_k B$ be a non-zero two-sided ideal. We can choose a non-zero element $c = \sum_{1 \le i \le n} a_i b_i \in I$, and also assume without loss of generality that $b_1, \ldots, b_n$ are linearly independent. We can also assume without loss of generality that $a_1 = 1$. Indeed, by reordering we can assume that $a_1 \neq 0$ and then, since A is quasi-simple, we can find $a_j^1, a_j^2 \in B$ such that $\sum_j a_j^1 a_1 a_j^2 = 1$. Then we replace c by $\sum_j (a_j^1 \otimes 1) c (a_j^2 \otimes 1)$, to obtain an element as desired.

Now we can prove by induction on n that $I = A \otimes_k B$ (i.e. $1 \otimes 1 \in I$). If $n = 1$, then we have $c = 1 \otimes b_1 \in I$, and since $b_1 \neq 0$ by an argument like above (using the quasi-simplicity of B) we see that $1 \otimes 1 \in I$. Next, if $a_i \in k$ for all i, then $c = 1 \otimes (\sum_i a_i b_i)$ so we reduce to the case $n = 1$. Otherwise, we take j such that $a_j \notin k$. Since A is central, there exists $a \in A$ such that $aa_j \neq a_j a$.

Then $(a \otimes 1)c - c(a \otimes 1)$ is equal to $1 \otimes b_1 + \sum_{i>1, i \neq j} (aa_i - a_i a) \otimes b_i$, so we can proceed by induction. □

Definition 5.3. A k-algebra A is called a **matrix algebra**, if A is isomorphic to $M_n(k)$ for some $n \in \mathbb{Z}_{\geq 1}$.

Exercise 5.4. *A matrix algebra is a CSA (can do this concretely, or notice that a matrix algebra is Morita equivalent to k, and being central and simple are stable under Morita equivalence).*

Lemma 5.5. *Let A, B be k-algebras. Then $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$.*

Proof. Let $c \in Z(A \otimes_k B)$. We can write $c = \sum_i a_i \otimes b_i$ with the a_i's linearly independent. Then $(1 \otimes b)c = c(1 \otimes b)$ for all $b \in B$ implies that $b_i \in Z(B)$ for all i. Now we can present $c = \sum_j a'_j \otimes b'_j$ with the b_j's linearly independent and every b'_j is equal to one of the b_i's. Then analogously to before we see that $a'_j \in Z(A)$ for all j. Therefore $c \in Z(A) \otimes_k Z(B)$. □

Lemma 5.6. *Let A be a k-algebra and K/k a field extension.*

1. *A is central if and only if A_K is central.*
2. *If A_K is quasi-simple then A is quasi-simple.*
3. *If A is a CSA then A_K is a quasi-simple.*
4. *A is a CSA if and only if A_K is a CSA.*

Proof.

1. One has $Z(A_K) = K \otimes_k Z(A)$. From this, the claim is clear.
2. If $I \subset A$ is a non-trivial two-sided ideal, then $K \otimes_k I \subset A_K$ is a non-trivial two-sided ideal.
3. This follows from lemma 5.2.
4. This follows from the previous items.

□

Claim 5.7. *The following are equivalent:*

1. *A is a central simple algebra.*
2. *For an algebraic closure K/k, A_K is a matrix algebra.*
3. *There exists a finite field extension K/k such that A_K is a matrix algebra.*

Proof. (1) $\implies$ (2): By lemma 5.6, A_K is a CSA. By Artin-Wedderburn, A_K is isomorphic to $M_n(D)$ where $n \in \mathbb{Z}_{\geq 1}$ and D is a division algebra over K. But K is the only such division algebra, hence A_K is a matrix algebra.

(2) $\implies$ (3): This is standard, from finite-dimensionality.

(3) $\implies$ (1): A matrix algebra is a CSA, hence A_K is a CSA, and hence, by lemma 5.6, A is a CSA. □

Lemma 5.8.

1. *Let A, B be CSA's. Then $A \otimes_k B$ is a CSA.*

2. *Let A be a CSA. Then A^{op} is a CSA.*

3. *Let A be a CSA. Then $A^{op} \otimes_k A$ is a matrix algebra.*

Proof.

1. By passing to a suitable finite algebraic extension, we reduce to A, B being matrix algebras. Then the claim follows from $M_n(k) \otimes_k M_m(k) \cong M_{nm}(k)$ (alternatively, this follows from lemmas above).

2. By passing to a suitable finite algebraic extension, we reduce to A being a matrix algebra. Then the claim follows from $M_n(k)^{op} \cong M_n(k)$.

3. One has a morphism of k-algebras $\phi : A^{op} \otimes_k A \to End_k(A)$, given by

$$a \otimes b \mapsto (c \mapsto bca).$$

Since $A^{op} \otimes A$ is simple by the already established part (1), ϕ is injective. By comparing dimensions, we deduce that ϕ is an isomorphism.

□

Definition 5.9. The **Brauer group** of k is defined as the group of isomorphism classes of CSA's up to Morita equivalence, with the tensor product as the group operation.

Remark 5.10. By claim 4.33 and lemma 5.8, the binary operation is well-defined. Clearly k defines the unit for this operation, and by lemma 5.7 inverses exist.

Remark 5.11. The elements of the Brauer group are in bijection with isomorphism classes of CDA's (because every CSA is Morita equivalent to a unique CDA, upt to isomorphism), but what should be the group operation is less clear if we would define it like this (because the tensor product of two CDA's might not be a CDA, but it is a CSA).

Remark 5.12. From all what was said above, we see that the elements of the Brauer group might be roughly considered as equivalence classes of k-linear categories $\mathcal{A}$ (maybe with some extra condition), such that for an algebraic closure K/K, one has $\mathcal{A}^K \approx Mod(K)$. In other words, the Brauer group classifies forms of the category of vector spaces, where "form" has the following sense: Suppose that for a field L, one has a world of entities $\mathcal{C}_L$. Suppose that for a field extension M/L, one has a transformation $\mathcal{C}_L \to \mathcal{C}_M$, with some expected properties (the "base change"). Suppose we pick an entity $F \in \mathcal{C}_M$. Then a standard question is to find all entities $f \in \mathcal{C}_L$ which become equivalent to F under the transformation above. Such f's are then called "L-forms" of F.

5.2 The centralizer theorem

Lemma 5.13. *Let A be a simple ring and V an A-module of finite length. Then $End_A(V)$ is also a simple ring.*

Proof. Since A is semismiple, the module V is projective. Since V is projective and finitely generated over A, it is compact. Since A is simple, V is a generator of $Mod(A)$. Therefore, $End_A(V)^{op}$ is Morita equivalent to A, so is simple. The opposite of a simple ring is simple. Therefore $End_A(V)$ is simple.

Alternatively, write $V \cong E^n$ where E is a simple A-module. Then denoting $D = End_A(E)$ (a division algebra) we have $End_A(V) \cong M_n(D)$ and hence it is simple. □

Lemma 5.14. *Let A be a simple ring and E a simple A-module. Denote $D = End_A(E)$. Then $\dim_D E = [A : [E]]$. In particular, if A is a k-algebra, we have $\dim_k A = (\dim_D E)^2 \cdot \dim_k D$.*

Proof. Writing $A \cong E^n$ (so $n = [A : [E]]$) we have (we already done this computation once before)

$$E \cong Hom_A(A, E) \cong Hom_A(E^n, E) \cong Hom_A(E, E)^n \cong D^n$$

and this is a D-module isomorphism. So $\dim_D E = n$, as desired. In the case that A is a k-algebra, we have

$$\dim_k A = [A : [E]] \cdot \dim_k E = [A : [E]] \cdot \dim_D E \cdot \dim_k D = n \cdot n \cdot \dim_k D.$$

□

Theorem 5.15 (Centralizer theorem)**.** *Let A be a CSA, and $B \subset A$ a simple subalgebra. Then:*

1. *$C_A(B) \subset A$ is simple.*
2. *$\dim_k A = \dim_k B \cdot \dim_k C_A(B)$.*
3. *$C_A(C_A(B)) = B$.*

Proof.

1. Let us consider A as an $(A^{op} \otimes_k B)$-module, via $(a, b) * x = bxa$. We notice that
$$C_A(B) \cong End_{A^{op} \otimes_k B}(A), \quad c \mapsto (x \mapsto cx).$$
Since $A^{op} \otimes B$ is simple, $End_{A^{op} \otimes_k B}(A)$ is also simple.

2. Denote by ℓ the length of A as a $(A^{op} \otimes_k B)$-module, by n the dimension of a simple $(A^{op} \otimes_k B)$-module over the division algebra of its endomorphisms, and by m the dimension over k of the division algebra of the endomorphism of a simple $(A^{op} \otimes_k B)$-module.

   Then $\dim_k A = \ell \cdot n \cdot m$, $\dim_k (A^{op} \otimes_k B) = n^2 \cdot m$ and $\dim_k C_A(B) = \ell^2 \cdot m$. Hence, $\dim_k B = \frac{\dim_k (A^{op} \otimes_k B)}{\dim_k A} = n/\ell$ and the desired relation is evident.

3. Since $B \subset C_A(C_A(B))$, the assertion follows by comparing dimensions, using the previous two assertions.

□

5.3 Maximal subfields

Claim 5.16. *Let D be a CDA, and $K \subset D$ a maximal subfield. Then* $\dim_k D = (\dim_k K)^2$.

Proof. Notice that $C_D(K) = K$. Hence, the assertion follows from the claim 5.15. □

Claim 5.17. *Let D be a CDA, and $K \subset D$ a maximal subfield. Then D_K is a matrix algebra.*

Proof. We consider D as a K-vector space, by right multiplication. Then we obtain a k-algebra homomorphism $D \to End_K(D)$, given by left multiplication. Extending scalars, we obtain a K-algebra homomorphism $\phi : D_K \to End_K(D)$. Since both are K-algebras of dimension $\dim_k D$ and D_K is simple, ϕ is an isomorphism. □

Lemma 5.18 (Noether, Jacobson)**.** *Let D be a CDA. If $D \neq k$, then there exists $d \in D - k$ such that $k(d)/k$ is separable.*

Proof. Omitted for now. □

Claim 5.19. *Let D be a CDA. Then there exists a maximal subfield $K \subset D$ such that K/k is separable.*

Proof. Let $K \subset D$ be maximal among subfields which are separable over k. We want to show that K is a maximal subfield in D. Consider $C_D(K)$. By the centralizer theorem, $C_D(K)$ is a CDA over K. If $C_D(K) = K$ then K has the correct dimension that by the centralizer theorem forces it to be a maximal subfield. Suppose by contradiction that $C_D(K) \neq K$. Then by lemma 4.1 there exists $d \in C_D(K) - K$ such that $K(d)/K$ is separable - which clearly contradicts the maximality of K. □

Corollary 5.20 (of claims 5.19 and 5.17)**.** *Let A be a CSA. Then there exists a separable finite extension K/k such that A_K is a matrix algebra.*

Remark 5.21. The last corollary says that CSA's always become matrix algebras over the separable closure (so it is not necessary to pass to the possibly bigger algebraic closure). This is important for the cohomological interpretation of the Brauer group.

5.4 The Noether-Skolem theorem

Lemma 5.22. *Let A, B be two k-algebras. Then $C_{A\otimes_k B}(A \otimes_k k) = Z(A) \otimes_k B$.*

Proof. Easy. □

Lemma 5.23. *Let A be a f.d. simple k-algebra, and M, N two f.d. A-modules. Then $M \cong N$ if and only if $\dim_k M = \dim_k N$.*

Proof. Clear, since every f.d. A-module is simply a direct sum of copies of the unique (up to isomorphism) simple A-module. □

Lemma 5.24. *Let A be a f.d. simple k-algebra, M a f.d. k-vector space, and $\theta_1, \theta_2 : A \to End_k(M)$ two k-algebra morphisms. Then there exists $U \in GL_k(M)$ such that $\theta_2(a) = U\theta_1(a)U^{-1}$ for all $a \in A$.*

Proof. The morphisms θ_1, θ_2 impose on M two A-module structures. By the previous lemma, the two resulting modules are isomorphic. An isomorphism between them is exactly U as wanted. □

Theorem 5.25 (Noether-Skolem)**.** *Let A be a CSA, B a simple algebra, and $\phi_1, \phi_2 : B \to A$ algebra morphisms. Then there exists $u \in A^\times$ such that $\phi_2(b) = u\phi_1(b)u^{-1}$ for all $b \in B$.*

Proof. Consider two $(A^{op} \otimes_k B)$-module structures on A given by $\iota_i : A^{op} \otimes_k B \to End_k(A)$ where $\iota_i(a \otimes b)(x) = \phi_i(b)xa$ (where $i = 1, 2$). Recalling that $A^{op} \otimes_k B$ is simple, we see by the previous lemma that there exists an invertible $U \in End_k(A)$ such that $U \circ \iota_1(a \otimes b) \circ U^{-1} = \iota_2(a \otimes b)$. Also, recall that $\iota : A^{op} \otimes_k A \to End_k(A)$ given by $\iota(a_1 \otimes a_2)(x) = a_2 x a_1$ is an isomorphism of algebras. Hence, setting $u_1 := \iota^{-1}(U)$, we have

$$u_1(a \otimes \phi_1(b))u_1^{-1} = a \otimes \phi_2(b).$$

Setting $b = 1$, we see that $u_1 \in C_{A^{op}\otimes_k A}(A^{op} \otimes_k k) = Z(A^{op}) \otimes_k A = k \otimes_k A$. Hence we can write $u_1 = 1 \otimes u$ for $u \in A$ (notice that $u \in A^\times$), and we get, substituting $a = 1$ this time,

$$u\phi_1(b)u^{-1} = \phi_2(b) \quad b \in B.$$

□

Corollary 5.26. *Let A be a CSA, and $B, C \subset A$ two simple subalgebras. Suppose given an isomorphism of algebras $\theta : B \to C$. Then there exists $u \in A^\times$ such that $ubu^{-1} = \theta(b)$ for all $b \in B$.*

Corollary 5.27. *Let A be a CSA, and $\theta : A \to A$ an automorphism of algebras. Then there exists $u \in A^\times$ such that $\theta(a) = uau^{-1}$ for all $a \in A$.*

5.5 Examples

5.5.1 Symbol algebras

Can we produce concrete examples of CSA's?

Let $n \in \mathbb{Z}_{\geq 2}$, assume that $n \neq 0$ in k, and assume that k contains all n-th roots of unity. Fix $\zeta \in k$, a primitive n-th root of unity.

Given $a, b \in k^{\times}$, define

$$C_{a,b} := C_{a,b}^{n,\zeta}(k) := k\langle x, y\rangle / \langle x^n = a, y^n = b, xy = \zeta yx\rangle.$$

Notice that it is not hard to understand that $C_{a,b}$ is an n^2-dimensional k-algebra, with basis $(x^i y^j)_{0 \leq i,j \leq n-1}$.

Here are some other properties which are not hard to establish:

Lemma 5.28.

1. *$C_{ac^n,b} \cong C_{a,bc^n} \cong C_{a,b}$ for $a, b, c, \in k^{\times}$.*
2. *$C_{a,b} \cong C_{b^{-1},a}$ for $a, b \in k^{\times}$.*
3. *$C_{a,b} \cong C_{b,a}^{op}$ for $a, b \in k^{\times}$.*

Lemma 5.29. *$C_{1,b}$ is a matrix algebra.*

Proof. Notice that an n^2-dimensional k-algebra A is a matrix algebra if and only if there exists a simple n-dimensional A-module E for which $End_A(E) = k$ (indeed, given such a module, the map $A \to End_k(E)$ is surjective by Jacobson's density theorem and therefore an isomorphism by comparing dimensions).

Therefore, let us try to construct an n-dimensional A-module E. Since $x^n = 1$, by diagnolization of the operator-to-be that x defines, it seems reasonable to fix a basis $(e_i)_{i \in \mathbb{Z}/n\mathbb{Z}}$ of E and set $xe_i = \zeta^i e_i$. Furthermore, $xy = \zeta yx$ shows that we must have $ye_i = c_i e_{i+1}$ for some $c_i \in k$. Then choosing arbitrarily (c_i)'s such that $\prod c_i = b$ gives as an $C_{a,b}$-module E. It is easy to see that E is simple (Since x is diagnolizable, every submodule is a direct sum of $k \cdot e_i$'s; Since y acts by translation, this must be the sum of all of them...). Then one can see that $End_{C_{a,b}}(E) = k$ either by easy direct computation, or by noticing that, fixing an algebraic closure K/k, one has $\dim End_{C_{a,b}}(E) = \dim End_{(C_{a,b})_K}(E_K)$, so that (since $(C_{a,b}(k))_K \cong C_{a,b}(K)$, and E_K is again a module of the same nature, so in particular simple by what we have already shown) it is easy to see that one can reduce to the case when k is algebraically closed, and then, since $End_{C_{a,b}}(E)$ is a division algebra, it must be k. □

Corollary 5.30. *Suppose that a admits an n-th root in k. Then $C_{a,b}$ is a matrix algebra.*

Proof. If a admits an n-th root in k, say $\alpha^n = a$, then $C_{a,b} \cong C_{\alpha^n,b} \cong C_{1,b}$ so by the above it is a matrix algebra. □

Claim 5.31. *$C_{a,b}$ is a CSA.*

Proof. We set $K = k(\sqrt[n]{a})$, and then $C_{a,b}(K)$ is a matrix algebra, so, since $C_{a,b}(k)_K \cong C_{a,b}(K)$, we see that $C_{a,b}(k)$ is a CSA. □

Claim 5.32. *We have $[C_{a,bc}] = [C_{a,b}] \cdot [C_{a,c}]$ (equality in the Brauer group).*

Proof (from Milnor's book on K-theory). Denote by x, y (resp. X, Y) the generators of $C_{a,b}$ (resp. $C_{a,c}$) as above and consider the algebra

$$C = C_{a,b} \otimes_k C_{a,c}.$$

Consider now the subalgebra B of C generated by $x \otimes 1$ and $y \otimes Y$, and the subalgebra B' of C generated by $x^{-1} \otimes X$ and $1 \otimes Y$. Then it is easy to see that $B \cong C_{a,bc}$ and $B' \cong C_{1,bc}$. Moreover, we see also that $C \cong B \otimes_k B'$. Therefore

$$C_{a,b} \otimes_k C_{a,c} \cong C_{a,bc} \otimes C_{1,bc}.$$

Since $C_{1,bc}$ is trivial in the Brauer group, we get the claimed. □

Proposition 5.33. *$[C_{a,b}] = 1$ whenever $a + b$ has an n-th root in k. In particular, we have the Steinberg relation $[C_{a,1-a}] = 1$ when $a \neq 1$ and the relation $[a, -a] = 1$.*

Proof (from Milnor's book on K-theory). We first compute that we have $(x + y)^n = x^n + y^n$, in general. Indeed, it is easy to see that the coefficient of $y^i x^{n-i}$ in the unfolding of the LHS is the coefficient of T^i in $(1+T\zeta^0) \cdot \ldots \cdot (1+T\zeta^{n-1})$. This polynomial is $(-T)^n - 1$ up to a constant.

Thus, if $a + b$ is an n-th root in k (write $a + b = c^n$) we see that $z := x + y$ is an element in $A := C_{a,b}$ which satisfies the polynomial equation $T^n - c^n = 0$ and no equation of lower degree. Therefore, since the polynomial $T^n - c^n$ splits completely over k, we see that $k[z]$ is isomorphic to the product of n copies of k. We can thus consider the corresponding orthogonal idempotents $e_1, \ldots, e_n \in k[z]$. One then sees that $A = Ae_1 \oplus Ae_2 \oplus \ldots \oplus Ae_n$. Therefore, A is an n^2-dimensional CSA admitting a simple module of k-dimension $\leq n$. It is easy to see from the Artin-Wedderburn theorem that A is then a matrix algebra. □

Remark 5.34. Thus, by the properties that we have seen, we obtain that $(a, b) \mapsto [C_{a,b}]$ defines a $\mathbb{Z}$-bilinear anti-symmetric map

$$(-,-)_n : k^\times/(k^\times)^n \times k^\times/(k^\times)^n \to Br(k)$$

which furthermore satisfies the Steinberg identity $(a, 1-a)_n = 1$ when $a \neq 1$.

Proposition 5.35. *The algebra $C_{a,b}$ is a matrix algebra (i.e. $(a, b)_n = 1$) if and only if b is in the image of the norm map from $k(\sqrt[n]{a})$ to k or equivalently from $k[T]/(T^n - a)$ to k.*

Proof (from Milnor's book on K-theory). The two criteria are equivalent because $k[T]/(T^n - a)$ is the product of several fields isomorphic to $k(\sqrt[n]{a})$. The rest of the proof is omitted for now (we will establish below the special case when $n = 2$). □

5.5.2 Quaternion algebras

Definition 5.36. A **quaternion algebra** is a CSA of dimension 4.

Notice that by dimension reasoning, a quaternion algebra is either a matrix algebra or a division algebra, and two Morita equivalent quaternion algebras are in fact isomorphic. The most famous quaternion algebra is $C^2_{-1,-1}$ in the case of $k := \mathbb{R}$ - the Hamilton quaternions. We will check below that it is a division algebra.

Claim 5.37. *Assume that $char(k) \neq 2$. Then every quaternion algebra is isomorphic to $C^2_{a,b}$ for some $a, b \in k^\times$.*

Proof. Let D be a quaternion algebra. If D is a matrix algebra, thne $D \cong C^2_{1,1}$ so that we are OK. Assume thus that D is a division algebra. A maximal subfield $K \subset D$ is of dimension 2, hence we can find an element $0 \neq x \in K$ such that $a := x^2 \in k$. By the Noether-Skolem theorem, we can find $0 \neq y \in D$ such that conjugation by y induces the non-trivial automorphism of K, i.e. $yxy^{-1} = -x$ (or $xy = -yx$). By dimension considerations, D has basis $1, x, y, xy$, in particular x, y generate D. Notice that $y^2xy^{-2} = x$, so y^2 centralizes both x and y, thus lies in the center of D, hence $b := y^2 \in k$. Now clearly $D \cong C^2_{a,b}$. □

Corollary 5.38. *For a quaternion algebra A, one has that $A \otimes_k A$ is a matrix algebra. In other words, elements in the Brauer group represented by quaternion algebras are 2-torsion.*

Proof. Writing $A \cong C^2_{a,b}$, we have

$$[A \otimes_k A] \cong [C^2_{a,b} \otimes_k C^2_{a,b}] = [C^2_{a,b^2}] = [C^2_{a,1}]$$

and the latter is trivial. □

Construction 5.39. *Let A be a CSA. Fix a field extension K/k such that A_K is a matrix algebra. Considering a simple A_K-module V, we define $RNm : A \to K$ by setting $RNm(a)$ to be the determinant of the endomorphism that a induces on the K-vector space V. Then, in fact the image of RNm lies in k, and the map RNm does not depend on the choice of K/k. One can see this easily if one knows that there always exist a separable splitting field, using Galois theory. The resulting map $RNm : A \to k$ is a multiplicative monoid morphism, and reflects invertibility (i.e. $a \in A$ is invertible if $RNm(a) \neq 0$).*

Claim 5.40. *Assume that $char(k) \neq 2$. Let $a, b \in k^\times$. Then $C^2_{a,b}$ is a matrix algebra (equivalently, not a division algebra) if and only if b lies in the image of $Nm : k(\sqrt{a})^\times \to k^\times$.*

Proof. If a has a square root in $k^\times$, then it is clearly a norm and also we already saw that $C^2_{a,b}$ is a matrix algebra, so everything is OK. Hence, we may assume that a has no square root in $k^\times$. Notice that $C^2_{a,b}$ is a matrix algebra if and only if there exists a non-zero element in $C^2_{a,b}$ which is non-invertible, and such an element is automatically a left and right zero-divisor.

Proof 1: One calculates

$$RNm(c_0 + c_1x + c_2y + c_3xy) = c_0^2 - ac_1^2 - bc_2^2 + abc_3^2.$$

Thus, $C^2_{a,b}$ is a matrix algebra if and only if there exists $z \in C^2_{a,b}$ such that $z \neq 0$ and $RNm(z) = 0$, or in other words if there exists $0 \neq (c_0, c_1, c_2, c_3) \in k^4$ such that

$$b = \frac{c_0^2 - ac_1^2}{c_2^2 - ac_3^2}$$

which is to say

$$b = Nm_k^{k(\sqrt{a})}(\frac{c_0 + \sqrt{a}c_1}{c_2 + \sqrt{a}c_3}).$$

This explains the claim.

Proof 2: Denote $K = k[x] \subset C^2_{a,b}$. One has $C^2_{a,b} = K \oplus K \cdot y$. Denote by $\theta : K \to K$ the non-trivial k-automorphism (i.e. $\theta(x) = -x$). Notice that $ry = y\theta(r)$ for $r \in K$. The existence of a zero-divisor is equivalent to the existence of $r, s \in K$ such that $(y + r)(y + s) = 0$ (because we will have some $(r_1y + r_2)(ys_1 + s_2) = 0$ but then we can multiply by r_1^{-1} on the left and by s_1^{-1} on the right). This equation unfolds to $y(\theta(r) + s) + (rs + b) = 0$, i.e. to $s = -\theta(r)$ and $b = -rs$. Therefore the existence of a zero-divisor is equivalent to the existence of $r \in K$ such that $b = r\theta(r) = Nm_k^K(r)$. □

We also have a reinterpretation of the condition we found:

Lemma 5.41. *Assume that $char(k) \neq 2$. Let $a, b \in k^\times$. Then b lies in the image of $Nm : k(\sqrt{a})^\times \to k^\times$ if and only if the equation $z^2 = ax^2 + by^2$ has a non-zero solution $(x, y, z) \in k^3$.*

Proof. If a is a square in k then the equation has a non-zero solution $(1, 0, \sqrt{a})$ and b lies in the image of the norm, so we are good. Suppose that a is not a square in k. Then b lies in the image of the norm if and only if there exists $(c, d) \in k^2$ such that $b = c^2 - ad^2$. In other words, if and only if the equation $z^2 = ax^2 + b$ has a solution. Since a is not a square in k, this equation has a solution if and only if the equation $z^2 = ax^2 + by^2$ has a non-zero solution. □

5.5.3 Algebraically closed fields

Let D be a f.d. division algebra over k, and let $d \in D - k$. Then $k[d] \subset D$ is a f.d. integral commutative k-algebra, hence a field. From this, we conclude:

Claim 5.42. *If k is algebraically closed, then $Br(k) = 1$.*

Proof. Indeed, there are no non-trivial f.d. division algebras over k. □

5.5.4 Finite fields

Claim 5.43. *If k is a finite field, then $Br(k) = 1$.*

Proof. Let D be a f.d. central division k-algebra; We want to show that $D = k$. For a maximal subfield $K \subset D$, we saw that $\dim K = \sqrt{\dim D}$. Hence, all maximal subfields are isomorphic in our case where k is finite. By the Noether-Skolem theorem, we get that every two maximal subfields are conjugate. Thus, fixing a maximal subfield $K \subset D$, we see in particular that $D^\times = \cup_{u \in D^\times} u K^\times u^{-1}$. A simple lemma about finite groups (see below) gives us $D^\times = K^\times$ and so $D = K$. Since D is central, we get $D = k$. □

We used the following lemma in the proof above:

Lemma 5.44. *Let G be a finite group, and $H \subset G$ a subgroup. If $\cup_{g \in G} g H g^{-1} = G$, then $H = G$.*

5.5.5 The field $\mathbb{R}$

Claim 5.45. *The only non-trivial CDA over $\mathbb{R}$ is the Hamilton quaternion algebra $C^2_{-1,-1}$.*

Proof. Let D be a CDA over $\mathbb{R}$. Since the only finite field extensions of $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$, by the results above on maximal subfields, if $D \neq \mathbb{R}$ then D must be four-dimensional. Hence, from what we saw above, $D \cong C^2_{a,b}$ for some $a, b \in \mathbb{R}^\times$. Since we can change a and b by squares, we can assume $a, b \in \{1, -1\}$. Since if either a or b are 1 then $C^2_{a,b}$ is a matrix algebra, we are only left with $C^2_{-1,-1}$, which is indeed a division algebra (for example, because -1 is not a norm from $\mathbb{C}$ to $\mathbb{R}$). □

Corollary 5.46. *$Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.*

We denote by $inv_\infty : Br(\mathbb{R}) \to \mathbb{Q}/\mathbb{Z}$ the unique embedding (i.e. the non-trivial element in $Br(\mathbb{R})$ goes to $1/2 + \mathbb{Z}$).

5.5.6 The fields $\mathbb{Q}_p$

We will not discuss too much, but just note the following theorem:

Theorem 5.47 (Part of local class field theory)**.** *One has a canonical isomorphism*

$$Br(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}.$$

In particular, there is, up to isomorphism, only one quaternion algebra over $\mathbb{Q}_p$ which is not a matrix algebra.

5.5.7 Local-to-Global stuff

Theorem 5.48 (Albert-Brauer-Hasse-Noether)**.** *Let D be a CSA over $\mathbb{Q}$. Then D is a matrix algebra if and only if for every $v \in pl(\mathbb{Q})$, $D_{\mathbb{Q}_v}$ is a matrix algebra.*

Lemma 5.49. *Let D be a CSA over $\mathbb{Q}$. Then, for almost all $v \in pl(\mathbb{Q})$, the CSA $D_{\mathbb{Q}_v}$ is a matrix algebra.*

Thus, we can rephrase the theorem by saying that

$$Br(\mathbb{Q}) \to \bigoplus_{v \in pl(\mathbb{Q})} Br(\mathbb{Q}_v)$$

is injective.

Recall that we have a canonical homomorphism $inv_v : Br(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z}$ which is an isomorphism when v is non-archimedean.

Theorem 5.50 (Part of global class field theory)**.** *The sequence*

$$0 \to Br(\mathbb{Q}) \to \bigoplus_{v \in pl(\mathbb{Q})} Br(\mathbb{Q}_v) \xrightarrow{\sum_v inv_v} \mathbb{Q}/\mathbb{Z} \to 0.$$

is exact.

Corollary 5.51. *Let A be a quaternion algebra over $\mathbb{Q}$. Then the number of $v \in pl(\mathbb{Q})$ for which $A_{\mathbb{Q}_v}$ is not a matrix algebra is even.*

Example 5.52. *In particular, consider the CSA $C_{p,q}(\mathbb{Q})$ where p and q are odd primes. By the corollary, the number of $v \in pl(\mathbb{Q})$ for which $z^2 = px^2 + qy^2$ has no solution in $\mathbb{Q}_v$ is even. For $v = \infty$ there clearly is a solution. Using Hensel's lemma etc., it is quite easy to see the following. For $v = p$ (resp. $v = q$) there is a solution if and only if q (resp. p) is a square modulo p (resp. q). For an odd prime $\ell \notin \{p, q\}$, there is always a solution. For $v = 2$, there is a solution if and only if at least one of the number p, q is equal to 1 modulo 4, i.e. if and only if $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even. Therefore we see that*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = 1.$$

.

5.6 The Brauer group as a cohomology group

To be added later, perhaps

6 Representations and characters

In this section, we fix a field k, and all vector spaces, algebras etc. are over k. By G we denote a finite group and by A we denote a f.d. algebra.

6.1 Group algebras and group representations

Definition 6.1. A **representation** of G is a pair (V, ρ) consisting of a vector space V and group morphism $\rho : G \to GL(V)$. A morphism of representations $(V, \rho), (W, \theta)$ is a linear transformation $T : V \to W$ such that $T \circ \rho(g) = \theta(g) \circ T$ for all $g \in G$. The category of representations we denote $Rep_k(G)$. The morphism spaces in this category we denote $Hom_G(\cdot, \cdot)$. The category $Rep_k(G)$ is an abelian category. We also denote $Irr_k(G) := Irr(Rep_k(G))$ (the set of isomorphism classes of irreducible representations).

Remark 6.2. Sometimes, given a group representation (V, ρ), we simply write gv instead of $\rho(g)(v)$. We might also simply say that V is a representation of G, omitting ρ all together (in the same way as when referring to an A-module M, one does not keep the structurual $A \to End(M)$ or $A \times M \to M$ in the notation).

Remark 6.3. We said that $Rep_k(G)$ is an abelian category. The reader should decipher for himself, what are subrepresentations, quotient representations, direct sums of representations, etc. Also, decipher what does it mean concretely for $Rep_k(G)$ to be semisimple.

Example 6.4. *The* ***trivial representation*** $k \in Rep_k(G)$ *is the one-dimensional vector space k, together with the trivial G-action, that is the corresponding $\rho : G \to GL(k)$ is given by $\rho(g) = id_k$ for all $g \in G$. More generally, given a group homomorphism $\theta : G \to k^\times$, one can consider the one-dimensional representation $k_\theta \in Rep_k(G)$, which is the vector space k with the $\rho : G \to GL(k)$ given by $\rho(g) = \theta(g) \cdot id_k$. Note that one-dimensional representations are always irreducible. Check that this construction yields an bijection between the set of group homomorphisms $Hom(G, k^\times)$ and the set of isomorphism classes of one-dimensional representations in $Rep_k(G)$.*

Definition 6.5. The **group algebra** of G, denoted $k[G]$, is the algebra with basis G and the product extending the one of G by bilinearity. Thus, concretely, elements of the group algebra are formal expressions $\sum_{g \in G} a_g g$, and the product is

$$\sum_{g \in G} a_g g \cdot \sum_{g \in G} b_g g = \sum_{g \in G} \left(\sum_{h \in G} a_{gh^{-1}} b_h \right) g.$$

Remark 6.6. Given an algebra A, the set of algebra morphisms $k[G] \to A$ is in bijection with the set of group morphisms $G \to A^\times$. In particular, given a vector space V, the structure of a module over $k[G]$ on V, i.e. an algebra morphism $k[G] \to End(V)$, is the same as the structure of a representation of G on V, i.e. a group morphism $G \to GL(V)$. We obtain in this way a natural equivalence of categories between $Rep_k(G)$ and $Mod(k[G])$ which we will use extensively.

6.2 Maschke's theorem and examples of non-semisimplicity

Claim 6.7. *Suppose that $char(k)$ does not divide $|G|$. Then $k[G]$ is semisimple (in other words, $Rep_k(G)$ is a semisimple category).*

Proof. Proof 1: Let us notice that for $g_1, g_2 \in G \subset k[G]$, one has $tr(g_1 g_2) = |G| \cdot \delta_{g_1, g_2^{-1}}$. Thus, the symmetric bilinear form $(x, y) \mapsto tr(xy)$ on $k[G]$ is nondegenerate. Thus, as we saw, $J(k[G]) = 0$ and so $k[G]$ is semisimple.

Proof 2: Let $M \in Mod(k[G])$ and $N \subset M$ a submodule. Let $p : M \to M$ be a projection operator with image N. Define $p_1 := \frac{1}{|G|} \sum_{g \in G} gpg^{-1}$. Then one checks that p_1 is again a projection operator with image N, and that p_1 is a $k[G]$-module morphism. Hence, $Ker(p_1)$ is a $k[G]$-submodule complimentary to N. □

Claim 6.8. *Suppose that $char(k) = p > 0$ and that p divides $|G|$. Then $k[G]$ is not semisimple.*

Proof. Consider $r := \sum_{g \in G} g \in k[G]$. Notice that $gr = r$ for $g \in G$ and $r^2 = 0$. Hence, the left ideal generated by r is nilpotent. Thus $r \in J(k[G])$, so $J(k[G]) \neq 0$ and so $k[G]$ is not semisimple. □

Let us illustrate an extreme:

Claim 6.9. *Suppose that $char(k) = p > 0$ and that G is a p-group. Then the trivial representation defines the only element in $Irr(G)$.*

Proof. Let E be an irreducible G-representaiton, and let us write $\rho : G \to GL(E)$ for the corresponding morphism. Notice that for every $g \in G$, one has $g^{p^r} = 1$ for some $r \in \mathbb{Z}_{\geq 1}$, and thus (recall that in char. p one has $(T+S)^{p^r} = T^{p^r} + S^{p^r}$) $(\rho(g) - id_E)^{p^r} = 0$ and thus in particular $\rho(g) - id_E$ is nilpotent, and hence not invertible. Now, suppose in addition that $g \in Z(G)$. Then $\rho(g) - id_E \in End_G(E)$. Recall that since E is irreducible, by Schur's lemma $End_G(E)$ is a division algebra. Hence $\rho(g) - id$, being non-invertible, must be zero. Thus we obtain $\rho(g) = id_E$ for all $g \in Z(G)$. This allows to think about E as a representation of $G/Z(G)$, which again is irreducible. Recall now that for a non-trivial p-group, the center is non-trivial. This allows to assume inductively that we already know the claim for $G/Z(G)$. We obtain that E is the trivial representation of $G/Z(G)$, and hence obviously the trivial representation of G. □

6.3 Character theory - 1

Throughout this subsection, we assume that k is algebraically closed. We fix a f.d. algebra A, and denote by $E_1, \ldots, E_n$ representatives of isomorphism classes of simple A-modules (recall that $Irr(A)$ is finite).

Remark 6.10. Let us recall that by the material we saw (Schur's lemma, Jacobson density theorem, Artin-Wedderburn theorem, etc.), we have $End_A(E_i) = k$

(because k is algebraically closed and $End_A(E_i)$ is a division k-algebra), the natural algebra morphism

$$A \to End_k(E_1) \times \ldots \times End_k(E_n)$$

is surjective, and it is injective if and only if A is semisimple (the kernel of this morphism is the Jacobson radical $J(A)$). In case A is indeed semisimple, the two-sided ideal $A_{[E_i]} \subset A$ corresponds under the above isomorphism to $End(E_i)$.

Definition 6.11. The **cocenter** of A is the vector space

$$cc(A) := A/\langle ab - ba : \ a, b \in A\rangle.$$

We also call $cc(A)^*$ the space of **trace functionals** on A.

Example 6.12. *Suppose $A = k[G]$. Then $Z(k[G])$ is the subspace of elements $\sum_{g \in G} a_g g$ such that $a_{hgh^{-1}} = a_g$ for all $h, g \in G$. The space $k[G]^*$ can be identified with the space of functions from G to k, and the space $cc(k[G])^*$ consists of the functions $\alpha : G \to k$ for which $\alpha(hgh^{-1}) = \alpha(g)$ for all $h, g \in G$. Let us denote by $Fun^{cl}(G, k) \subset Fun(G, k)$ the subspace of such functions; it is called the space of* ***class functions*** *on G.*

Definition 6.13. Let E be a f.d. A-module. Define the **character** of E, $\chi_E \in cc(A)^*$, by

$$\chi_E(a) := tr(a; E).$$

Remark 6.14. Given a short exact sequence of f.d. A-modules

$$0 \to E_1 \to E_2 \to E_3 \to 0,$$

one has $\chi_{E_2} = \chi_{E_1} + \chi_{E_3}$.

Theorem 6.15. *The characters $\chi_{E_1}, \ldots, \chi_{E_n} \in cc(A)^*$ are linearly independent. If A is semisimple, these are moreover a basis of $cc(A)^*$.*

Proof. By remark 6.10, for $1 \leq i \leq n$, we can find an element $a_i \in A$ such that a_i acts on E_j by zero if $j \neq i$ and by a linear transformation with trace 1 if $j = i$. Then $\chi_j(a_i) = \delta_{i,j}$, so that the first claim follows. Let us assume now that A is semisimple. Then to show that $\dim cc(A) = n$, by remark 6.10 it is enough to show that $\dim cc(M_m(k)) = 1$ for $m \in \mathbb{Z}_{\geq 1}$. This we will do below. □

Definition 6.16. The algebra A, equipped with a trace functional $\delta \in cc(A)^*$, is called a **symmetric Frobenius algebra**, if the symmetric bilinear form on A given by $\langle a_1, a_2\rangle := \delta(a_1 a_2)$ is non-degenerate. We refer to δ as a **non-degenerate trace functional**. We denote by $\delta_a \in A^*$ the functional given by $\delta_a(b) := \delta(ab)$. We also denote by $\langle \cdot, \cdot \rangle$ the induced non-degenerate symmetric bilinear form on A^*, i.e. $\langle \delta_a, \delta_b \rangle := \langle a, b\rangle$.

Example 6.17. *The usual trace functional $tr : M_m(k) \to k$ is a non-degenerate trace functional, so that $(M_m(k), tr)$ is a symmetric Frobenius algebra. We then see that if A is semisimple then it admits a structure of a symmetric Frobenius algebra, by using the decomposition in remark 6.10.*

Example 6.18. *Let G be a finite group, and assume that $char(k)$ does not divide $|G|$. Then the functional $\delta := \chi_{k[G]}$ is more concretely given by $\delta(\sum_{g \in G} a_g g) = |G| \cdot a_1$, and is easily seen to be non-degenerate, so that $(k[G], \delta)$ is a symmetric Frobenius algebra. The from $\langle \cdot, \cdot \rangle$ on $k[G]^*$ is given concretely by*

$$\langle \alpha, \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha(g) \beta(g^{-1}).$$

Indeed, $\langle g, h \rangle = |G| \cdot \delta_{h, g^{-1}}$. Therefore $\delta_g = |G| \cdot \mathbb{1}_{g^{-1}}$. Therefore

$$\langle \mathbb{1}_g, \mathbb{1}_h \rangle = \langle \frac{1}{|G|} \delta_{g^{-1}}, \frac{1}{|G|} \delta_{h^{-1}} \rangle = \frac{1}{|G|^2} \langle g^{-1}, h^{-1} \rangle = \frac{1}{|G|} \delta_{h^{-1}, g}$$

from which the formula follows easily by bilinearity.

Claim 6.19. *Let (A, δ) be a symmetric Frobenius algebra. Then there are natural isomorphisms*

$$\begin{tikzcd} A \arrow[r, "a \mapsto \delta_a", "\sim"'] & A^* \\ Z(A) \arrow[u, hook] \arrow[r, "\sim"] & cc(A)^* \arrow[u, hook] \end{tikzcd} .$$

Proof. The map $A \to A^*$ given by $a \mapsto \delta_a$ is an isomorphism because δ is a non-degenerate trace functional. We check now that δ_a sits in $cc(A)^*$ if and only if $a \in Z(A)$. Indeed, $\delta_a(bc) = \delta_a(cb)$ means $\delta(abc) = \delta(acb)$ or equivalently $\delta(abc) = \delta(bac)$ or yet equivalently $\delta((ab - ba)c) = 0$ and by non-degeneracy this holds for all $b, c \in A$ if and only if $a \in Z(A)$. □

Corollary 6.20. *One has* $\dim cc(M_m(k)) = 1$.

Proof. Since $(M_m(k), tr)$ is a symmetric Frobenius algebra, and is also central, one has $\dim cc(M_m(k)) = \dim Z(M_m(k)) = \dim k = 1$. □

Let us now provide the two most basic numerical relations.

Claim 6.21. *Suppose that A is semisimple (we do not assume that it is a symmetric Frobenius algebra here).*

1. *One has*

$$\dim A = \sum_{1 \le i \le n} (\dim E_i)^2.$$

In particular, for $A = k[G]$, we obtain

$$|G| = \sum_{1 \le i \le n} (\dim E_i)^2.$$

2. *One has*
$$\dim Z(A) = \dim cc(A) = n(= |Irr(A)|).$$
In particular, for $A = k[G]$, we get that the number of irreducible representations of G is equal to the number of conjugacy classes in G.

Proof.

1. Clear from remark 6.10.
2. From theorem 6.15 we have that $n = \dim cc(A)$. We also notice that $\dim Z(A) = n$, as is clear from the decomposition of remark 6.10.

□

Remark 6.22. Suppose that A is semisimple. Then $A \cong \oplus_{1 \le i \le n} E_i^{\dim E_i}$ as A-modules (although not canonically so). For example, notice that in terms of the decomposition of remark 6.10, one has $End_k(E_i) = A_{[E_i]}$ (the corresponding isotypic component), so $End_k(E_i)$ is a direct sum of copies of E_i, and from observing the dimensions it is clear how many.

Remark 6.23. For a finite group G in the semisimple setting, define the "zeta function"
$$\zeta_G(s) := \sum_{[E] \in Irr_k(G)} \dim(E)^{-s}.$$
Then we saw that $\zeta_G(0)$ is equal to the number of conjgacy classes in G, while $\zeta_G(-2)$ is equal to the number of elements in G. There is a formula of Frobenius generalizing this:
$$\zeta_G(-2+2n) = \frac{1}{|G|^{2n-1}} |c_n^{-1}(1)|$$
for $n \in \mathbb{Z}_{\ge 0}$, where $c_n : G^{2n} \to G$ is given by
$$c_n(x_1, y_1, \ldots, x_n, y_n) := [x_1, y_1] \cdot \ldots \cdot [x_n, y_n].$$

Example 6.24. *Consider $G = S_3$ and $k = \mathbb{C}$. The character table is the following:*

	(•)(•)(•)	(••)(•)	(• • •)
	1	1	1
	1	−1	1
	2	0	−1

Example 6.25. *Suppose that G is abelian. Then every irreducible representation is one-dimensional (This is because the center $Z(G)$ must act by scalars on an irreducible representation by Schur's lemma), and one gets $Irr(G) \cong Hom(G, k^\times)$. Then $\chi_{E_1}, \ldots, \chi_{E_n} = \chi_1, \ldots, \chi_n$ are simply the elements of $Hom(G, k^\times)$. One obtains now two natural bases of $Fun(G, k)$ - the basis of delta functions $(\mathbb{1}_g)_{g \in G}$ and the basis $\chi_1, \ldots, \chi_n$. The first basis diagnolizes the operators M_f of pointwise multiplication by a function $f \in Fun(G, k)$, while the second basis diagnolizes the operators S_g of shift by $g \in G$.*

6.4 Character theory - 2

We continue with the notations of the previous subsection, but furthermore assume that A is semisimple, and $\delta \in cc(A)^*$ is a non-degenerate trace functional (so that (A, δ) is a symmetric Frobenius algebra). Thus, when we concentrate on the case $A = k[G]$, we assume that $char(k)$ does not divide $|G|$, and we take $\delta = \chi_{k[G]}$.

Recalling remark 6.10, we denote by $e_i \in Z(A)$ the unique element that acts on E_j by $\delta_{i,j}$. Then $e_1, \ldots, e_n$ is a basis of $Z(A)$ and we have the relations $e_i e_i = e_i$, $e_i e_j = 0$ when $i \neq j$ and $e_1 + \ldots + e_n = 1$.

Claim 6.26. *The following are equivalent:*

1. $\delta(e_i) \neq 0$ *for all* $1 \leq i \leq n$.
2. $\dim E_i \neq 0$ *in* k, *for all* $1 \leq i \leq n$.
3. *The restriction of* $\langle \cdot, \cdot \rangle$ *to* $Z(A)$ *is non-degenerate.*

If these conditions are satisfied, then one has

$$\chi_{E_i} = \frac{\dim E_i}{\delta(e_i)} \cdot \delta_{e_i}.$$

Proof. Recall the isomorphism $Z(A) \cong cc(A)^*$, and let us denote by $z_i \in Z(A)$ the element corresponding to χ_{E_i} (in other words, $\delta_{z_i} = \chi_{E_i}$). Thus, we have to bases for $Z(A)$, the basis $e_1, \ldots, e_n$ and the basis $z_1, \ldots, z_n$. Notice that we have:

$$\langle e_i, e_j \rangle = \delta(e_i e_j) = \delta(e_i) \cdot \delta_{i,j}$$

and

$$\langle e_i, z_j \rangle = \chi_{E_j}(e_i) = \dim E_i \cdot \delta_{i,j}.$$

From this, the claim is clear. □

Exercise 6.27. *Show that the conditions of the previous claim are also equivalent to the following one: The composition $Z(A) \to A \to cc(A)$ of the natural inclusion followed by th enatural projection, is an isomorphism.*

Corollary 6.28. *[Orthogonality relations] Suppose that the conditions of claim 6.26 are satisfied for A. Then*

$$\langle \chi_{E_i}, \chi_{E_j} \rangle = \frac{(\dim E_i)^2}{\delta(e_i)} \cdot \delta_{i,j}.$$

Proof. We have

$$\langle \chi_{E_i}, \chi_{E_j} \rangle = \langle \frac{\dim E_i}{\delta(e_i)} e_i, \frac{\dim E_j}{\delta(e_j)} e_j \rangle = \frac{(\dim E_i)^2}{\delta(e_i)} \cdot \delta_{i,j}.$$

□

Example 6.29. *Suppose that $char(k) = p > 0$. Then $(M_p(k), tr)$ fails to satisfy the conditions in claim 6.26.*

Claim 6.30. *In the case $A = k[G]$, the conditions of claim 6.26 are satisfied.*

Proof. We would like to check that the restriction of $\langle \cdot, \cdot \rangle$ to $Z(k[G])$ is non-degenerate.

Let us consider the linear operator $av : k[G] \to k[G]$ given by $av(D) := \frac{1}{|G|} \sum_{g \in G} g \cdot D \cdot g^{-1}$. Then it is easy to check that av is a projection operator, with image $Z(k[G])$. Furthermore, it is easy to check the adjunction formula

$$\langle D_1, av(D_2) \rangle = \langle av(D_1), D_2 \rangle, \quad D_1, D_2 \in k[G]$$

and therefore in particular

$$\langle D_1, av(D_2) \rangle = \langle D_1, D_2 \rangle, \quad D_1 \in Z(k[G]), D_2 \in k[G].$$

Thus, if for $D_1 \in Z(k[G])$ one has $\langle D_1, D_2 \rangle = 0$ for all $D_2 \in Z(k[G])$ then one also has $\langle D_1, D_2 \rangle = 0$ for all $D_2 \in k[G]$ so that $D_1 = 0$. □

Remark 6.31. Thus, our non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$ on $Fun(G, k)$ restricts to a non-degenerate form on $Fun^{cl}(G, k)$.

Claim 6.32. *In the case $A = k[G]$, one has $\delta(e_i) = (\dim E_i)^2$.*

Proof. Let us notice that

$$\delta(e_i) = \chi_A(e_i) = \sum_{1 \leq j \leq n} \dim E_j \cdot \chi_{E_j}(e_i) = (\dim E_i)^2.$$

□

Corollary 6.33. *[Orthogonality relations for groups] In the case $A = k[G]$, one has:*

$$\langle \chi_{E_i}, \chi_{E_j} \rangle = \delta_{i,j}.$$

More concretely:

$$\frac{1}{|G|} \sum_{g \in G} \chi_{E_i}(g) \chi_{E_j}(g^{-1}) = \delta_{i,j}.$$

Proof. We just plug the result of claim 6.32 in the relation of 6.28. □

Corollary 6.34. *In the case $A = k[G]$, one has:*

$$e_i = \frac{\dim E_i}{|G|} \sum_{g \in G} \chi_{E_i}(g^{-1}) \cdot g.$$

Proof. First, let $D \in k[G]$. Write $D = \sum_{g \in G} c_g \cdot g$. Then

$$c_g = \frac{1}{|G|}\langle D, g^{-1}\rangle = \frac{1}{|G|}\delta_D(g^{-1}).$$

In other words, we have

$$D = \frac{1}{|G|}\sum_{g \in G} \delta_D(g^{-1}) \cdot g.$$

We saw that

$$\delta_{e_i} = \dim E_i \cdot \chi_{E_i}.$$

Therefore

$$e_i = \frac{\dim E_i}{|G|}\sum_{g \in G} \chi_{E_i}(g^{-1}) \cdot g.$$

□

Remark 6.35. Let us describe a second approach to orthogonality relations in the case of a group.

For a f.d. representaiton $M \in Rep_k(G)$, we can construct the contragradient, or dual, representation M^*, which is the dual vector space, with G-action $(g\alpha)(m) = \alpha(g^{-1}m)$. For two f.d. representations $M, N \in Rep_k(G)$, we can construct the tensor product representation $M \otimes_k N$, which is the tensor product of vector spaces, with G-action $g(m \otimes n) = gm \otimes gn$. Given a f.d. representaiton $M \in Rep_k(G)$, we can construct a vector space M^G, given by: $M^G = \{m \in M \ : \ gm = m \ \forall g \in G\}$.

Alongside, for a function $f \in Fun(G,k)$ let us define $f^*(g) := f(g^{-1})$. For functions $f_1, f_2 \in Fun(G,k)$, let us define $(f_1 \cdot f_2)(g) := f_1(g)f_2(g)$. Let us also define a linear functional $\int : Fun(G,k) \to k$ by $\int f := \frac{1}{|G|}\sum_{g \in G} f(g)$.

One can check now that $\chi_{M^*} = \chi_M^*$, $\chi_{M \otimes_k N} = \chi_M \cdot \chi_N$ and $\dim M^G = \int \chi_M$. Finally, one can check that one has a natural isomorphism of vector space $(M^* \otimes_k N)^G \cong Hom_G(M, M)$ and also that one has an equality $\int (f_1^* \cdot f_2) = \langle f_1, f_2\rangle$. Aggregating all this, one obtains:

$$\dim Hom_G(M, N) = \langle \chi_M, \chi_N\rangle.$$

Now, if M and N are irreducible, by Schur's lemma the number $\dim Hom_G(M, N)$ is equal to 0 if M and N are non-isomorphic, and to 1 otherwise. Hence we obtain the orthogonality relations.

The next claim describes how the symmetric bilinear form $\langle \cdot, \cdot \rangle$ on $Fun^{cl}(G, k)$ is a "decategorification" of the Hom-spaces in $Rep_k^{f.d.}(G)$.

Claim 6.36. *Let $M_1, M_2 \in Rep_k(G)$ be f.d. representations. Then*

$$\dim Hom_G(M_1, M_2) = \langle \chi_{M_1}, \chi_{M_2}\rangle.$$

Proof.

Option 1: Both sides are biadditive in short exact sequences, and hence we reduce to the case when M_1, M_2 are irreducible. Then the left-hand side is 0 if M_1, M_2 are not isomorphic and 1 otherwise, by Schur's lemma. The right-hand side is 0 if M_1, M_2 are not isomorphic and 1 otherwise, by orthogonality relations. Hence, both sides are equal.

Option 2: As in remark 6.35 above. □

Example 6.37. *Consider $G = S_3$ and $k = \mathbb{C}$. The inner product is:*

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{6}\left(\chi_1((\bullet)(\bullet)(\bullet))\chi_2((\bullet)(\bullet)(\bullet)) + 3\cdot\chi_1((\bullet\bullet)(\bullet))\chi_2((\bullet\bullet)(\bullet)) + 2\cdot\chi_1((\bullet\bullet\bullet))\chi_2((\bullet\bullet\bullet))\right).$$

One can check the orthogonality relations in the the table in example 6.24.

Remark 6.38. Let E be a f.d. representation of G. Then one has a non-canonical isomorphism $E \cong \oplus_{1\leq i\leq n} E_i^{\oplus m_i}$ for some uniquely defined vector $(m_1, \ldots, m_n) \in \mathbb{Z}^n_{\geq 0}$. Then, using the orthogonality relations, one calculates:

$$\langle \chi_E, \chi_E \rangle = \sum_{1\leq i\leq n} m_i^2.$$

In particular, we see that E is irreducible if and only if the "length squared" of its character, $\langle \chi_E, \chi_E \rangle$, is equal to 1.

Remark 6.39. Let us sum up. Let k be an algebraically closed field, and G a finite group. Assume that the characteristic of k does not divide the order of G. Then the category $Rep_k^{fd}(G)$ of representations of G on finite-dimensional vector spaces over k is a semisimple abelian category, with finitely many irreducible objects up to isomorphism, which for convenience of notation we list $E_1, \ldots, E_n$. In the space of functions $Fun(G, k)$ one has a subspace $Fun^{cl}(G, k)$ of class functions, which are those functions f which satisfy $f(ghg^{-1}) = f(h)$ for all $g, h \in G$. One has a symmetric bilinear form $\langle \cdot, \cdot \rangle$ on $Fun(G, k)$, given by $\langle f_1, f_2 \rangle = \frac{1}{|G|}\sum_{g\in G} f_1(g)f_2(g^{-1})$. This form is non-degenerate, and moreover its restriction to the subspace of class functions $Fun^{cl}(G, k)$ is again non-degenerate. To each $E \in Rep_k^{fd}(G)$ one assigns a class function $\chi_E \in Fun^{cl}(G, k)$ (its character). For a short exact sequence $0 \to E' \to E \to E'' \to 0$ one has $\chi_E = \chi_{E'} + \chi_{E''}$. One has that $\chi_{E_1}, \ldots, \chi_{E_n}$ are a basis of the space of class functions $Fun^{cl}(G, k)$, which moreover satisfy the orthogonality relations $\langle \chi_{E_i}, \chi_{E_j} \rangle = \delta_{i,j}$. The number of irreducible representation, $n = |Irr_k(G)|$, is equal to the number of conjugacy classes in G. The sum $\sum_{1\leq i\leq n} \dim E_i^2$ is equal to $|G|$.

7 Induction

In this section, we fix a field k, and all vector spaces, algebras etc. are over k. By G we denote a finite group. We assume that k is algebraically closed, and that $char(k)$ does not divide $|G|$ (i.e. $k[G]$ is semisimple).

7.1 Restriction and induction

Let $\phi : B \to A$ be a morphism of algebras. We have a functor $res_B^A : Mod(A) \to Mod(B)$ simply given by restriction of the action along ϕ. It has a left adjoint $ind_A^B : Mod(B) \to Mod(A)$ and a right adjoint $Ind_A^B : Mod(B) \to Mod(A)$. They are described as follows:

$$ind_A^B(M) := A \otimes_B M,$$

$$Ind_A^B(M) := Hom_B(A, M)$$

(in the last expression, the space $Hom_B(A, M)$ is a left A-module via $(a\phi)(a') = \phi(aa')$).

Exercise 7.1. *Recall what are adjoint functors, write explicitly what the adjunction means in the above two cases, and verify the above adjunctions.*

7.2 0-th Hochchild homology and cohomology

Definition 7.2. Let A be a k-algebra and M an A-bimodule. We define the vector spaces:

$$HH^0(A; M) := \{m \in M \mid am = ma \ \forall a \in A\}$$

and

$$HH_0(A; M) := M/\text{Span}\{am - ma\}_{a \in A, m \in M}.$$

Example 7.3. *Let M be A itself as an A-bimodule in the standard way. Then $HH^0(A; A) = Z(A)$ and $HH_0(A; A) = cc(A)$.*

Notice that we have an obvious linear map

$$HH^0(A; M) \to HH_0(A; M)$$

(by the inclusion into M followed by the projection).

Claim 7.4. *Let $A = k[G]$, where G is a finite group and $char(k) \not| |G|$. Then $HH^0(A; M) \to HH_0(A; M)$ is an isomorphism for any A-bimodule M.*

Proof. We define $av : M \ toM$ by

$$m \mapsto \frac{1}{|G|} \sum_{g \in G} gmg^{-1}.$$

On element of the form $gm - mg$ this map vanishes, and so it induces a map $HH_0(A; M) \to HH^0(A; M)$. One now easily checks that it is inverse to our map $HH^0(A; M) \to HH_0(A; M)$. □

Remark 7.5. I could not figure out whether the last Claim still holds when A is a symmetric Frobenius algebra with the extra condition we had above (equivalent to $Z(A) \to cc(A)$ being an isomorphism).

7.3 The coincidence of the left and right adjoints

Let A, B be finite-dimensional algebras, and let $\phi : B \to A$.

We have

$$ind_B^A(M) = A \otimes_B M \cong HH_0(B; A \otimes_k M).$$

Here B acts on $A \otimes_k M$ on the left by $b(a \otimes m) = a \otimes bm$ and on the right by $(a \otimes m)b = a\phi(b) \otimes m$. These actions commute with the left action of A (by $a'(a \otimes m) = a'a \otimes m$) and therefore $HH_0(B; A \otimes_k M)$ is a quotient A-module of $A \otimes_k M$, and the above stated isomorphism is an isomorphism of A-modules.

We have

$$Ind_B^A(M) = Hom_B(A, M) \cong HH^0(B; Hom_k(A, M)) \cong HH^0(B; A^* \otimes_k M).$$

Here B acts on $Hom_k(A, M)$ on the left by $(b\theta)(a) = b\theta(a)$ and on the right by $(\theta b)(a) = \theta(\phi(b)a)$. These actions commute with the left action of A (by $(a'\theta)(a) = \theta(aa')$) and therefore $HH^0(B; Hom_k(A, M))$ is a sub A-module of $Hom_k(A, M)$, and the first above stated isomorphism is an isomorphism of A-modules. The second stated isomorphism is given by the standard isomorphism $Hom_k(A, M) \cong A^* \otimes_k M$. In the second description, the left action of B is by $b(\ell \otimes m) = \ell \otimes bm$, the rigt action of B is by $(\ell \otimes m)b = \ell b \otimes m$ and the left action of A is by $a(\ell \otimes m) = a\ell \otimes m$.

Remark 7.6. Let A be a finite-dimensional algebra. Then A is an A-bimodule naturally. Also, A^* is an A-bimodule naturally. Suppose that δ is a non-degenerate trace functional on A. It induces an isomorphism of vector spaces $A \cong A^*$. We then easily check that this is in fact an isomorphism of A-bimodules.

If A is a symmetric Frobenius algebra, then by the Remark, we can identify $A^* \otimes_k M$ with $A \otimes_k M$, and this identification preserves the left A-module structure and the left and right B-module structures. We thus identify

$$Ind_B^A(M) \cong HH^0(B; A^* \otimes_k M) \cong HH^0(B; A \otimes_k M).$$

Therefore, we obtain a morphism

$$ind_B^A(M) \cong HH_0(B; A \otimes_k M) \to HH^0(B; A \otimes_k M) \cong Ind_B^A(M).$$

If $B = k[H]$ (when $char(k) \not| |H|$), by the above we obtain that this morphism is an isomorphism.

Therefore, we have obtained:

Corollary 7.7. *Let $H \to G$ be a morphism of finite groups. Assume that $char(k) \not| |G|$. Then one has a canonical isomorphism*

$$ind_H^G \to Ind_H^G.$$

7.4 Concrete descriptions in the case of group algebras

Let us describe Ind_G^H more concretely. One has:

$$Ind_G^H(M) = Hom_{k[H]}(k[G], M) \cong \{f : G \to M \mid f(hg) = hf(g) \ \forall h \in H, g \in G\}$$

with G-action

$$(g'f)(g) = f(gg').$$

Let us also describe $ind_G^H(M)$ more concretely. Choosing representatives $g_1, \ldots, g_r \in G$ for the cosets G/H, One can describe $Ind_G^H(M)$ as $"g_1"M \oplus \ldots \oplus "g_r"M$ (where $"g_i"$ are formal placeholders, so that we are dealing with a direct sum of several copies of M), and the G-action is $g \cdot "g_i"m = "g_j"(hm)$ where we should write $gg_i = g_j h$ for some (uniquely defined) $1 \leq j \leq r$ and $h \in H$.

7.5 Characters and induction

Let again $H \subset G$ be a subgroup. Let $M \in Rep_k(G)$ be a f.d. representation. We would like to calculate $\chi_{ind_G^H M} \in Fun^{cl}(G, k)$ in terms of $\chi_M \in Fun^{cl}(H, k)$.

Claim 7.8. *One has*

$$\chi_{ind_G^H(M)}(g) = \sum_{x \in G/H \ s.t. \ x^{-1}gx \in H} \chi_M(x^{-1}gx)$$

(here the meaning of the expression $x^{-1}gx$ is that we first should replace x with an actual representative of it in G, and the answer doesn't depend on this choice).

Proof. We will use the last description of induction above. We fix $g \in G$, and count what contributes to the trace of g acting on $"g_1"M \oplus \ldots \oplus "g_r"M$. First, only $1 \leq i \leq r$ for which $gg_i \in g_i H$, i.e. $g_i^{-1}gg_i \in H$, contribute. For such i, writing $gg_i = g_i h$ with $h \in H$, one has a commutative diagram

$$\begin{tikzcd}
"g_i"M \arrow[r, "g"] & "g_i"M \\
M \arrow[u] \arrow[r, "h"] & M \arrow[u]
\end{tikzcd}$$

where the vertical arrows are simply the isomorphisms of appending the placeholder. Hence, the trace of g on $"g_i"M$ is equal to the trace of h on M, i.e. to $\chi_M(h) = \chi_M(g_i^{-1}gg_i)$. □

Next, let us see how the adjunction between induction and restriction reflects in terms of characters.

Claim 7.9 (Frobenius reciprocity)**.** *Let $M \in Rep_k(H)$ and $N \in Rep_k(G)$ be f.d. representations. Then one has*

$$\langle \chi_{ind_G^H M}, \chi_N \rangle = \langle \chi_M, \chi_{res_H^G N} \rangle$$

(here the first inner product is of functions on G, and the second one of functions on H).

Proof. One has:

$$\langle \chi_{ind_G^H M}, \chi_N \rangle = \dim Hom_G(ind_G^H M, N) = \dim Hom_H(M, res_H^G N) = \langle \chi_M, \chi_{res_H^G N} \rangle.$$

□

Remark 7.10. We can define $ind_G^H : Fun^{cl}(H,k) \to Fun^{cl}(G,k)$ by the same formula as above:

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

Of course, we also have a natural operation $res_G^H : Fun^{cl}(G,k) \to Fun^{cl}(H,k)$ given by simply restricting the function. Then one has:

$$\langle f_1, ind_G^H f_2 \rangle = \langle res_H^G f_1, f_2 \rangle$$

for all $f_1 \in Fun^{cl}(G,k), f_2 \in Fun^{cl}(H,k)$. Either one checks that independently (which is more natural, since we don't want to know representation theory to check such a simple claim), or one reduces to Frobenius reciprocity above thanks to characters spanning the space of class functions.

As a simple application, let us show:

Theorem 7.11 (Artin)**.** *Let $M \in Rep_{\mathbb{C}}(G)$ be a f.d. representation. χ_M can be written as a linear combination with rational coefficients of characters of the form $\chi_{ind_G^H \mathbb{C}_\theta}$ where $H \subset G$ is a cyclic subgroup, $\theta \in H \to \mathbb{C}^\times$ a homomorphism, and $\mathbb{C}_\theta$ the corresponding one-dimensional representation of H.*

Proof. Let us first notice that it is enough to show that the characters of the peculiar form span the space of class functions on G. Indeed, this would mean that χ_M can be written as a linear combination with complex coefficients of such characters, and since all characters reside in the $\mathbb{Z}$-lattice spanned by the basis $\chi_{E_1}, \ldots, \chi_{E_n}$, the claim then follows from linear algebra.

Next, in order to show that the characters of the peculiar form span the space of class functions on G, it is enough to show that if a class function $f \in Fun^{cl}(G,k)$ is orthogonal to all such characters, then it is 0. But

$$\langle f, \chi_{ind_G^H \mathbb{C}_\theta} \rangle = \langle res_H^G f, \chi_{\mathbb{C}_\theta} \rangle,$$

so we obtain that $res_H^G f$ is orthogonal to all $\chi_{\mathbb{C}_\theta}$'s. Since the $\mathbb{C}_\theta$'s are all the irreducible representations, their characters span $Fun^{cl}(H,k)$, and hence we get $res_H^G f = 0$. In other words, f is zero on every cyclic subgroup, and hence clearly f is zero. □

Remark 7.12. Artin used the above theorem to deduce some information about Artin L-functions. Better information would be granted if one knows Brauer's theorem, which replaces the rational coefficients in Artin's theorem with integer coefficients.

7.6 A geometric interpretation of induction of class functions

By a *finite groupoid* we mean a category $\mathcal{G}$ all the arrow in which are isomorphism, for which the set $\pi_0(\mathcal{G})$ of isomorphism classes of objects is finite, and for which every $Isom_{\mathcal{G}}(x_1, x_2)$ is finite for all objects $x_1, x_2 \in \mathcal{G}$.

Every finite set we consider a finite groupoid with only identity isomorphisms.

The basic example of finite groupoids: Let G be a finite group acting on a finite set X. Then we define a finite groupoid $G\backslash X$, whose objects are elements of X, and

$$Isom_{G\backslash X}(x_1, x_2) := \{g \in G \mid gx_1 = x_2\}.$$

It is straight-forward to define composition.

Given functors between finite groupoids $F_1 : \mathcal{H}_1 \to \mathcal{G}$ and $F_2 : \mathcal{H}_2 \to \mathcal{G}$, the *fiber product* $\mathcal{H}_1 \underset{\mathcal{G}}{\times} \mathcal{H}_2$ is defined by the relevant universal property in the 2-category of finite groupoids. Let us describe it concretely. An object of $\mathcal{H}_1 \underset{\mathcal{G}}{\times} \mathcal{H}_2$ is a triple (x_1, x_2, α) consisting of an object x_1 of $\mathcal{H}_1$, an object x_2 of $\mathcal{H}_2$, and an isomorphism $\alpha : F_1(x_1) \cong F_2(x_2)$ in $\mathcal{G}$. One defines isomorphisms in an evident way (we skip the explication for now).

For a finite groupoid $\mathcal{G}$, we denote

$$Fun(\mathcal{G}, k) := Fun(\pi_0(\mathcal{G}), k).$$

We define an inner product on $Fun(\mathcal{G}, k)$ by

$$\langle f_1, f_2 \rangle_{\mathcal{G}} := \sum_{[x] \in \pi_0(\mathcal{G})} \frac{f_1(x) \cdot f_2(x)}{|Aut_{\mathcal{G}}(x)|}.$$

For example, allowing ourself the frivolity of an infinite finite groupoid, we will find that $\langle 1, 1 \rangle_{\mathbb{N}} = e$ where $\mathbb{N}$ denotes the groupoid of finite sets and e is Euler's constant (base of natural logarithm).

Let $F : \mathcal{H} \to \mathcal{G}$ be a functor between finite groupoids. We want to define linear maps

$$F^* : Fun(\mathcal{G}, k) \rightleftarrows Fun(\mathcal{H}, k) : F_*.$$

We define F^* simply by $F^*(f)(x) := f(F(x))$. We then define F_* as adjoint to F^* (with respect to the inner products defined above). Concretely,

$$(F_*)(f)(x) = \sum_{y \in \bullet \underset{\mathcal{G}}{\times} \mathcal{H}} \frac{f(pr_2(y))}{|Aut(y)|}$$

where the map $\bullet \to \mathcal{G}$ is by x.

Notice that for a finite group G we have $\pi_0(G\backslash G) \cong Conj(G)$ where here the action of G on G is by conjugation. Correspondingly, we have

$$Fun(G\backslash G, k) \cong Fun^{cl}(G, k).$$

Now, consider an injective morphism of finite groups $\phi : H \to G$. It induces a functor between finite groupoids $F_\phi : H\backslash H \to G\backslash G$. We then claim that

$$(F_\phi)_* : Fun(H\backslash H, k) \to Fun(G\backslash G, k)$$

is precisely

$$ind_G^H : Fun^{cl}(H, k) \to Fun^{cl}(G, k)$$

(under our identification of the space of class functions with the space of functions on the corresponding finite groupoid). Indeed, first denote

$$Fix(G, G/H) := \{(g, g'H) \in G \times G/H \mid gg'H = g'H\}$$

and define an action of G on $Fix(G, G/H)$ by

$$\widetilde{g}(g, g'H) := (\widetilde{g}g\widetilde{g}^{-1}, \widetilde{g}g'H).$$

Then it is easy to construct an equivalence of finite groupoids

$$H\backslash H \approx G\backslash Fix(G, G/H).$$

From this we obtain a fiber product diagram

$$\begin{tikzcd}
\{g'H \in G/H \mid gg'H = g'H\} \arrow[r] \arrow[d] & Fix(G, G/H) \arrow[r] \arrow[d] & H\backslash H . \arrow[d] \\
\{g\} \arrow[r] & G \arrow[r] & G\backslash G
\end{tikzcd}$$

Therefore,

$$(F_\phi)_*(f)(g) = \sum_{g'H \in G/H \text{ s.t. } gg'H = g'H} f((g')^{-1}gg').$$

(requires a bit of work to explain things in a clearer way)

7.7 Mackey stuff

Let $H, K \subset G$ be two subgroups. For $g \in G$ and $(M, \rho) \in Rep_k(H)$, let us denote by $(T_gM, T_g\rho) \in Rep_k(g^{-1}Hg)$ the representation which is M as a vector space, and the action given by $(T_g\rho)(x)(m) = \rho(gxg^{-1})(m)$.

Claim 7.13. *Let $g_1, \ldots, g_r \in G$ be representatives for the double cosets $H \backslash G / K$. Then one has an isomorphism of functors $Rep_k(H) \to Rep_k(K)$:*

$$res_K^G \circ Ind_G^H \cong \bigoplus_{1 \le i \le r} Ind_K^{K \cap g_i^{-1} H g_i} \circ res_{K \cap g_i^{-1} H g_i}^{g_i^{-1} H g_i} \circ T_{g_i}.$$

Proof. We can obviously decompose $res_K^G(Ind_G^H(M))$ into the direct sum of subspace $V_i(M)$, where $V_i(M)$ consists of functions $f : G \to M$ which are zero outside of $H g_i K$. Notice that each $V_i(M)$ us a subrepresentation of $res_K^G(Ind_G^H(M))$. Let us write concretely:

$$V_i(M) = \{ f : H g_i K \to M \mid f(hx) = hf(x) \ \forall h \in H, x \in H g_i K. \},$$

and the action of K on $V_i(M)$ is by $(kf)(x) = f(xk)$.

Now, it is easy to see that there is an isomorphism of vector spaces between the above

$$\{ f : H g_i K \to M \mid f(hx) = hf(x) \ \forall h \in H, x \in H g_i K. \}$$

and

$$\{ \widetilde{f} : K \to M \mid \widetilde{f}(rx) = (g_i r g_i^{-1}) \widetilde{f}(x) \ \forall r \in K \cap g_i^{-1} H g_i, x \in K \}$$

given by sending f in the former to $\widetilde{f}(x) := f(g_i x)$ in the latter. This isomorphism respects the action of K on both vector spaces by appending on the right. For the former, this results in the K-representation $res_K^G(Ind_G^H(M))$. For the latter, this results in the K-representation

$$Ind_K^{K \cap g_i^{-1} H g_i} \left(res_{K \cap g_i^{-1} H g_i}^{g_i^{-1} H g_i} (T_{g_i}(M)) \right).$$

□

Corollary 7.14 (Irreducibility criterion)**.** *Suppose that H is normal in G. Let $g_1 = 1, \ldots, g_r$ be representatives for the cosets G/H. Let $E, F \in Rep_k(H)$ be two irreducible representations. Then $\dim_k Hom_G(Ind_G^H E, Ind_G^H F)$ is equal to the number of $1 \le i \le r$ for which $T_{g_i} E$ is isomorphic to F. In particular, $Ind_G^H E$ is irreducible if and only if $T_{g_i} E$ is not isomorphic to E for all $2 \le i \le r$.*

Proof. One has

$$Hom_G(Ind_G^H E, Ind_G^H F) \cong Hom_H(res_H^G Ind_G^H E, F) \cong$$

$$\cong \bigoplus_{1 \le i \le r} Hom_H(Ind_H^{H \cap g_i^{-1} H g_i} res_{H \cap g_i^{-1} H g_i}^{g_i^{-1} H g_i} T_{g_i} E, F) \cong$$

$$\cong \bigoplus_{1 \le i \le r} Hom_H(T_{g_i} E, F)$$

and from this the claim is clear. □

Remark 7.15. Let $H \subset G$ be a subgroup. Notice that every irreducible representation of G is isomorphic to a subrepresentation of the induction from H to G of an irreducible representation. Indeed, for irreducible $E \in Rep_k(G)$, one has $res^G_H E \neq 0$, and hence one can find an irreducible quotient representation $res^G_H E \to L$. But then by adjunction one obtains a non-zero morphism $E \to Ind^H_G L$, which is therefore an injection since E is irreducible. Hence, by decomposing into irreducibles the inductions to G of irreducible representations of H, we will find all irreducible representations of G, up to isomorphism.

8 Example: The dihedral group

Let

$$G = D_{2n} = \langle r, s : \; r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$$

be the dihedral group. We would like to compute the character table of G.

G has a normal subgroup of index 2, namely $H = \langle r \rangle$. We will follow the strategy of Remark 7.15.

Denote by $\mu_n \subset k^\times$ the group of n-th roots of unity (it is a cyclic group with n elements, since $char(k) \not| |G| = 2n$). Then we have an isomorphism of groups $\mu_n \cong Hom(H, k^\times)$, given by sending ζ to the homomorphism $\chi_\zeta : r^i \mapsto \zeta^i$. Thus, the irreducible representations of H are given, up to isomorphism, by k_{χ_ζ}, for $\zeta \in \mu_n$.

Notice that the non-trivial element in G/H, represented by s, sends (by the action T_s as above) k_χ to $k_{\chi^{-1}}$. Therefore, by the criterion above, the dimension of $Hom_G(Ind^H_G k_{\chi_\zeta}, Ind^H_G k_{\chi_\eta})$ is equal to the number of elements in $\{\zeta, \zeta^{-1}\}$ which are equal to η. Thus, fixing for simplicity of notation a primitive root of unity $\zeta_1 \in \mu_n$ and writing $\chi_i := \chi_{\zeta^i}$, we see that an exhaustive and non-repetitive list of irreducible representations of G is given by:

- $E_i := Ind^H_G k_{\chi_i}$ for $0 < i < n/2$.
- Two irreducible constituents of $Ind^H_G k_{\chi_0}$.
- If n is even, two irreducible constituents of $Ind^H_G k_{\chi_{n/2}}$.

Notice that $Ind^H_G k_{\chi_i}$ is two-dimensional, and hence when it is reducible, its irreducible constituents are simply one-dimensional representations of G whose restriction to H maps non-trivially into k_{χ_i} (again by adjunction), so they simply correspond to $\theta \in Hom(G, k^\times)$ such that $\theta|_H = \chi_i$. It is simple to observe that such exist exactly whenever $\chi_i(r) = \pm 1$, and then there are exactly two such (differentiated by $\theta(s) = 1$ and $\theta(s) = -1$). This, incidentally, recovers the above without need for the irreducibility criterion.

Using the formula for the character of induction, one easily now writes the character table of G (the first row is a general expression for the character of $Ind^H_G \chi_i$, but we consider it for $0 < i < n/2$; The second and third rows are the two irreducible constituents of $Ind_G^H k_{\chi_0}$, and the fourth and fifth rows are the two irreducible constituents of $Ind_G^H k_{\chi_{n/2}}$ (exist only if n is even):

	r^j	sr^j
$ind_G^H k_{\chi_\zeta} \quad (\zeta = \zeta_1^i (0 < i < n/2))$	$\zeta^j + \zeta^{-j}$	0
E_0^+	1	1
E_0^+	1	-1
$E_{n/2}^+$	$(-1)^j$	$(-1)^j$
$E_{n/2}^-$	$(-1)^j$	$-(-1)^j$

9 Example: $SL_2(\mathbb{F}_q)$

Let is consider the group $G = SL_2(\mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field with q elements. Let us consider the Borel subgroup $B \subset G$, which consists of the upper-triangular matrices. It is convenient also to denote by U the subgroup of unipotent upper-triangular matrices, by B^- the subgroup of lower-triangular matrices, and by T the subgroup of diagonal matrices.

For $\chi \in Hom(T, \mathbb{C}^\times)$, let us denote by $\widetilde{\chi} \in Hom(B, \mathbb{C}^\times)$ the composition $B \to T \to \mathbb{C}^\times$ where $B \to T$ sends a matrix to its diagonal part. The **principal series** of representations of G are given by

$$P_\chi := Ind_G^B \mathbb{C}_{\widetilde{\chi}}.$$

To analyze the reducibility of the principal series, we first notice $G = B \coprod BwB$ where $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. We now have as in the irreducibility criterion:

$$Hom_G(P_\chi, P_{\chi'}) \cong Hom_B(res_B^G Ind_G^B \mathbb{C}_{\widetilde{\chi}}, \mathbb{C}_{\widetilde{\chi'}}) \cong$$

$$\cong Hom_B(\mathbb{C}_{\widetilde{\chi}}, \mathbb{C}_{\widetilde{\chi'}}) \oplus Hom_B(Ind_B^T res_T^{B^-} T_w \mathbb{C}_{\widetilde{\chi}}, \mathbb{C}_{\widetilde{\chi'}}) \cong$$

$$\cong Hom_B(\mathbb{C}_{\widetilde{\chi}}, \mathbb{C}_{\widetilde{\chi'}}) \oplus Hom_B(Ind_B^T \mathbb{C}_{^w\chi}, \mathbb{C}_{\widetilde{\chi'}}) \cong$$

$$\cong Hom_B(\mathbb{C}_{\widetilde{\chi}}, \mathbb{C}_{\widetilde{\chi'}}) \oplus Hom_T(\mathbb{C}_{^w\chi}, \mathbb{C}_{\chi'}) \cong$$

$$\cong Hom_T(\mathbb{C}_\chi, \mathbb{C}_{\chi'}) \oplus Hom_T(\mathbb{C}_{^w\chi}, \mathbb{C}_{\chi'}).$$

Here ${}^w\chi(\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}) = \chi(\begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix})$. Let us say that χ is regular, if $\chi \neq {}^w\chi$, and singular otherwise. Then we see that P_χ is irreducible if and only if χ is regular, and has length two (with two different irreducible constituents) otherwise.

Let us parametrize $\chi(\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}) = \alpha(t)$ where $\alpha \in Hom(\mathbb{F}_q^\times, \mathbb{C}^\times)$. We notice that there are exactly two singular χ's - the trivial χ and that $lgndr$ corresponding to α being the Legendre symbol. The representation P_1 consists of functions on G/B, has the trivial representation as a subrepresentation, and the complementary representation is an irreducible representation called the Steinberg representation - denote it by St.

Let us calculate characters of the irreducible representations entering the principal series. First, we will simply calculate the characters of the principal series themselves. We have:

$$\chi_{P_\chi}(g) = \sum_{x \in G/B \text{ s.t. } gxB = xB} \chi(x^{-1}gx).$$

But what is $\chi(x^{-1}gx)$? First, let us interpret G/B as the set $\mathbb{P}(\mathbb{F}_q^2)$ of one-dimensional subspaces of $\mathbb{F}_q^2$, by sending gB to gL_0 where $L_0 := Span\{(1,0)^t\}$. For g fixing L_0, i.e. sitting in B, we notice that $\chi(g)$ is equal to $\alpha(g|_{L_0})$ where we abuse notation and denote by $g|_{L_0}$ the scalar in $\mathbb{F}_q^\times$ by which g acts on L_0. Then, for g which fixes xL_0, we see that $\chi(x^{-1}gx) = \alpha((x^{-1}gx)|_{L_0}) = \alpha(g|_{xL_0})$. Therefore, we can rewrite

$$\chi_{P_\chi}(g) = \sum_{L \in \mathbb{P}(\mathbb{F}_q^2) \text{ s.t. } gL = L} \alpha(g|_L).$$

In other words, to compute the character of P_χ on an element g, we need to sum the eigenvalues of g, running over all possible eigen-lines. We therefore calculate (the last column is for matrices which have no eigenvalues over $\mathbb{F}_q$):

	$\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} (t \in \{\pm 1\})$	$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} (t \notin \{\pm 1\})$	$\begin{pmatrix} t & a \\ 0 & t \end{pmatrix} (t \in \{\pm 1\},\, a \in \mathbb{F}_q^\times)$	$\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} (b \neq 0)$
P_χ	$(q+1) \cdot \alpha(t)$	$\alpha(t) + \alpha(t^{-1})$	$\alpha(t)$	0
$\mathbb{C}$	1	1	1	1
St	q	1	0	-1

It is left to calcaulte the characters of the two irreducible representations appearing in P_{lgndr}. For this, we consider $G \subset G' \subset G''$ where $G'' = GL_2(\mathbb{F}_q)$ and G' is the subgroup of matrices with the determinant being a square in $\mathbb{F}_q^\times$. We define principal series representations for G'' and G' exactly in the same way as for G (and all the T, B, etc.). We see easily (using Mackey theory or directly) that, since $G'B'' = G''$, one has

$$res_{G'}^{G''}(P''_{\chi''}) \cong P'_{\chi''|_{T'}}, \quad res_G^{G'}(P'_{\chi'}) \cong P_{\chi'|_T}.$$

Let us now set $\alpha : \mathbb{F}_q^\times \to \mathbb{C}^\times$ to be the Legendre character, and let us consider $\chi''(\begin{pmatrix} t & 0 \\ 0 & s \end{pmatrix}) = \alpha(t)$. Then using Mackey theory as above, we see that $P''_{\chi''}$ is irreducible, but $P'_{\chi'}$ is reducible, decomposing into two non-isomorphic irreducible representations

$$P'_{\chi'} = E \oplus F.$$

Denoting by $h \in G''$ some element with non-square determinant, we notice that hE is a subrepresentation of $P'_{\chi'}$, which is not E (since $P''_{\chi''}$ is irreducible), so has no intersection with E, and therefore we must in fact have $hE = F$. Thus, the characters of E and F simply differ by conjugation by h. We can now try to complete our table (where we now restrict E and F further to G):

	$\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}$ $(t \in \{\pm 1\})$	$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$ $(t \notin \{\pm 1\})$	$\begin{pmatrix} t & a \\ 0 & t \end{pmatrix}$ $(t \in \{\pm 1\},\, a \in \mathbb{F}_q^\times)$	$\begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}$ $(b \neq$
P_{lgndr}	$(q+1) \cdot \alpha(t)$	$\alpha(t) + \alpha(t^{-1})$	$\alpha(t)$	0
E	$\frac{q+1}{2} \cdot \alpha(t)$	$\alpha(t)$	?	0
F	$\frac{q+1}{2} \cdot \alpha(t)$	$\alpha(t)$	?	0

Here, the problem is that for $t \in \{\pm 1\}$ the matrices conjugate to those of the form

$$\begin{pmatrix} t & a \\ 0 & t \end{pmatrix}$$

fall into two conjugacy classes in $SL_2(\mathbb{F}_q)$ - depending on whether a is a square or a non-square, and conjugation by h swaps them - let $g_{t,a}$ denote an element in one of those four conjugacy classes. We want to compute $\chi_E(g_{t,a})$ and $\chi_F(g_{t,a})$. We know that

$$\chi_E(g_{1,a}) + \chi_F(g_{1,a}) = 1.$$

Also, we know that

$$\chi_E(g_{-1,a}) = \chi_E(-1 \cdot g_{1,-a}) = \alpha(-1) \cdot \chi_E(g_{1,-a})$$

and similarly for F. Then we use the relation $\langle \chi_E, \chi_E \rangle = 1$ to compute (complete this sometime - can copy from my finite group representation notes).

10 Groups and group actions

10.1 G-sets

We fix a group G.

Definition 10.1. A (left) **G-set** is a pair (X, a) consisting of a set X and a map $a : G \times X \to X$ such that $a(g_1, a(g_2, x)) = a(g_1 g_2, x)$ for all $g_1, g_2 \in G$ and $x \in X$, and such that $a(1, x) = x$ for all $x \in X$. A morphism between two G-sets (X, a) and (Y, b) is a map $f : X \to Y$ which satisfies $f(a(g, x)) = b(g, f(x))$ for all $g \in G$ and $x \in X$. We denote by $Set(G)$ the category of G-sets.

Remark 10.2. We usually omit a from the notation, and write gx, or $g * x$, for $a(g, x)$.

Example 10.3. *Let $H \subset G$ be a subgroup. Then we can consider the G-set G/H, where the G-action is $g * (g'H) := gg'H$. The resulting G-set when $H = 1$*

we can call the regular G-set - let us denote it by G (meaning that if not said otherwise, this is the G-set structure on G that we consider).

Notice that one has a unique G-set morphism $G \to G/H$ which sends 1 *to* $1H$.

Example 10.4. *The set G has also two other G-set structures, except the one from the previous example. One is $g * g' := g'g^{-1}$ and another is $g * g' := gg'g^{-1}$.*

Definition 10.5. Let X be a G-set.

1. We define an equivalence relation on X, by declaring $x_1, x_2 \in X$ to be equivalent if there exists $g \in G$ such that $gx_1 = x_2$. We call the equivalence classes G-**orbits**. We denote the equivalence class passing x by $\mathcal{O}_G(x)$.

2. X is called **transitive** (one also says that the G-action on X is transitive) if the number of G-orbits on X is 1.

3. Given $x \in X$, we define the **stabilizer** of x in G to be the subgroup $St_G(x) \subset G$ given by $\{g \in G \mid gx = x\}$.

Lemma 10.6. *Let X be a G-set, and let $x \in X$. Then there exists a unique isomorphism of G-sets $G/St_G(x) \to \mathcal{O}(x)$ mapping $1 \cdot St_G(x)$ to x.*

10.2 p-stuff

Fix a prime number p.

Definition 10.7. A p-**group** is a finite group whose order is a power of p.

Lemma 10.8. *Let P be a p-group and let X be a P-set. Denote by $Fix_P(X) \subset X$ the subset $\{x \in X \mid px = x \mid \forall p \in P\}$. Then $|Fix_P(X)|$ is congruent to $|X|$ modulo p. In particular, if $|X|$ is prime to p, then $|Fix_P(X)| \neq 0$ (i.e. there exists a fixed point).*

Proof. Notice that $|X|$ is equal to $|Fix_P(X)|$ plus a sum of sizes of G-orbits in X which are not singletons. Each such G-orbit is isomorphic to G/H for some subgroup $H \neq G$. Thus the size of each such G-orbit is a positive power of p. From this the claim is clear. □

Claim 10.9. *Let P be a p-group. If $P \neq 1$, then $Z(P) \neq 1$.*

Proof. Consider the action of P on itself by conjugation. Then the set of fixed points is equal to $Z(P)$. By lemma 10.8, we get that $|Z(P)|$ is congruent to $|P|$ modulo p, so p divides $|Z(P)|$. Since $|Z(P)| \geq 1$ (since $1 \in Z(P)$), we obtain $|Z(P)| \geq p$, and so $Z(P) \neq 1$. □

Another claim, which we will use to show that Sylow subgroups exist, is as follows:

Claim 10.10. *Let G be a finite group, and $P \subset G$ a p-subgroup. Suppose that $[G : P]$ is divisible by p. Then $N_G(P) \neq P$.*

Proof. Consider the P-action on G/P. The set of fixed points is $N_G(P)/P$. By lemma 10.8, we see that $[N_G(P) : P]$ is congruent to $[G : P]$ modulo p, so $[N_G(P) : P]$ is divisible by p, so $[N_G(P) : P] \neq 1$ and thus $N_G(P) \neq P$. □

Claim 10.11 (Cauchy's theorem). *Let G be a finite group, whose order $|G|$ is divisible by p. Then there exists $g \in G$ of order p (i.e. $g \neq 1$ and $g^p = 1$).*

Proof. Consider the subset $X \subset Fun(\mathbb{Z}/p\mathbb{Z}, G)$ consisting of functions f for which $\prod_{i \in \mathbb{Z}/p\mathbb{Z}} f(i) = 1$. The subset X is stable under the $\mathbb{Z}/p\mathbb{Z}$-action on $Fun(\mathbb{Z}/p\mathbb{Z}, G)$ given by $(i * f)(j) = f(i - j)$. The fixed points of this action on X are in correspondence with element $g \in G$ for which $g^p = 1$. The number of fixed points, by lemma 10.8, is congruent to $|G|^{p-1}$ modulo p, i.e. is divisible by p. Hence, since it is ≥ 1, it is $\geq p$. □

10.3 Sylow subgroups

In this subsection, G denotes a finite group.

Definition 10.12. Let p be a prime number. Denote by $k \in \mathbb{Z}_{\geq 0}$ the largest integer for which $p^k \mid |G|$. A p-**Sylow** subgroup of G is a subgroup of order p^k.

Theorem 10.13 (Sylow). *Let p be a prime number.*

1. *There exists a p-Sylow subgroup in of G.*

2. *Let $P \subset G$ be a p-Sylow subgroup and $Q \subset G$ a p-subgroup. Then there exists $g \in G$ such that $gQg^{-1} \subset P$.*

3. *Let $P \subset G$ be a a p-subgroup. Then P is contained in some p-Sylow subgroup of G.*

4. *Let $P, Q \subset G$ be two p-Sylow subgroups. Then P, Q are conjugate, i.e. there exists $g \in G$ such that $gPg^{-1} = Q$.*

5. *Denote by $n_p(G)$ The number of p-Sylow subgroups of G. Then $n_p(G)$ is congruent to 1 modulo p, and $n_p(G)$ divides $|G|/p^k$, where $k \in \mathbb{Z}_{\geq 0}$ is the largest integer for which $p^k \mid |G|$.*

Proof.

1. Let us denote by $k \in \mathbb{Z}_{\geq 1}$ the largest integer for which $p^k \mid |G|$. It is enough to show that if G contains a subgroup H of order p^i, for some $0 \leq i < k$, then G contains a subgroup of order p^{i+1}. Indeed, by claim 10.10, $N_G(H) \neq H$, and by Cauchy's theorem we can find an element $xH \in N_G(H)/H$ of order p. Then $\langle H, x \rangle$ is a subgroup of G of order p^{i+1}.

2. Let $P \subset G$ be a p-Sylow subgroup and $Q \subset G$ a p-subgroup. Consider the action of Q on G/P. From lemma 10.8 we deduce that this action admits a fixed point xP. We then have $qxP = xP$ for all $q \in Q$, which gives $x^{-1}Qx \subset P$.

3. Clear from item (2).

4. Clear from item (2).

5. Denote by $Syl_p(G)$ the set of p-Sylow subgroups of G. We have a natural action of G on $Syl_p(G)$, by conjugation. By the above, this action is transitive and hence, fixing some $P \in Syl_p(G)$, we have $|G|/|St_G(P)| = |Syl_p(G)|$. Notice that $P \subset St_G(P)$, and hence $|G|/|St_G(P)| \mid |G|/p^k$, showing that $|Syl_p(G)|$ divides $|G|/p^k$.

   Also, consider the restriction of this action of G on $Syl_p(G)$ to P. We have then that $|Syl_P(G)|$ is congruent to $|Fix_P(Syl_p(G))|$ modulo p, so it is enough to show that P is the only fixed point of the P-action on $Syl_p(G)$. In other words, we want to show that if for a p-Sylow subgroup $Q \subset G$ one has $pQp^{-1} = Q$ for all $p \in P$, then $Q = P$. Let us consider $N_G(Q) = \{g \in G \mid gQg^{-1} = Q\}$. We see that $P, Q \subset N_G(Q)$. Since P and Q are clearly p-Sylow subgroups of $N_G(Q)$, we obtain that P and Q are conjugate in $N_G(Q)$. But Q is normal in $N_G(Q)$, so that only it is conjugate to itself. We obtain $Q = P$.

□

11 Integrality and Burnside's theorem

We assume that k is algebraically closed of characteristic 0 throughout.

11.1 Integral elements

Let A be a k-algebra.

Definition 11.1. An element $a \in A$ is called **integral**, if there exists a monic polynomial $p \in \mathbb{Z}[X]$ such that $p(a) = 0$.

Lemma 11.2. *An element of $\mathbb{Q}$ is integral if and only if it is an integer.*

Proof. An exercise. □

Claim 11.3. *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 11.4. *Suppose that A is finitely generated as a $\mathbb{Z}$-module. Then all elements of A are integral.*

Claim 11.5. *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. □

11.2 Integrality in the group algebra

Claim 11.6. *Let G be a finite group and consider the group algebra $k[G]$.*

1. *The elements $\mathbb{1}_g \in k[G]$ are integral.*
2. *For a conjugacy class $C \subset G$, the elements $\mathbb{1}_C := \sum_{g \in C} \mathbb{1}_g \in k[G]$ are integral.*
3. *If for an element $D = \sum_{g \in G} d_g \cdot \mathbb{1}_g \in Z(k[G])$ all d_g are integral, then D is integral.*
4. *Let $V \in Rep_k^{fd}(G)$. Then χ_V has integral values.*

Proof.

1. This is clear since $\mathbb{1}_g^{|G|} = 1$.
2. The $\mathbb{Z}$-span of the elements $\mathbb{1}_C$ is a commutative subalgebra , and it is finitely generated as a $\mathbb{Z}$-module. Hence all its elements are integral.
3. This is clear, because we can write $D = \sum_{C \in Conj(G)} d_{g_C} \cdot \mathbb{1}_C$ where $g_C \in C$, and thus D is the sum of products of integral elements in a commutative algebra, hence integral.
4. Since each g acts on V by a transformation whose some integer power is 1, and so which is integral, this follows from Lemma 11.7 that follows.

□

Lemma 11.7. *Let V be a finite-dimensional vector space over k, and let T : $End_k(V)$ be integral. Then $tr(T; V) \in k$ is integral.*

Proof. We can base change to an algebraic closure, in which case the trace is a sum of eigenvalues. Since the transformation is integral, it is clear that all its eigenvalues are integral as well, and thus also their sum. □

Claim 11.8. *Let $V \in Rep_k^{fd}(G)$ and $D \in k[G]$.*

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

Proof. Denote by $\pi : k[G] \to End_k(V)$ the action.

1. Since D is integral, so is $\pi(D)$. Hence $tr(\pi(D);V) = \chi_V(D)$ is integral, by Lemma 11.7.
2. Since V is irreducible, $\pi(D)$ is a scalar multiple $\pi(D) = c \cdot Id_V$. Thus, since c is integral since it is the eigenvalue of the integral $\pi(D)$. Finally, notice that $c = \frac{\chi_V(D)}{\dim V}$.

□

Claim 11.9. *Let $E \in Rep_k^{fd}(G)$ be irreducible. Then $\dim E$ divides $|G|$.*

Proof. Consider $e \in k[G]$ - the central idempotent corresponding to E (i.e. acting as identity on E and as zero on all irreducible representations not isomorphic to E). By Corollary 6.34, we have

$$e = \frac{\dim E}{|G|} \sum_{g \in G} \chi_E(g^{-1}) \cdot g.$$

Notice therefore that $\frac{|G|}{\dim E} \cdot e$ is integral element of $Z(k[G])$, by parts 3 and 4 of Claim 11.6. Therefore, by the previous Claim, we have that

$$\frac{\chi_E(\frac{|G|}{\dim E} e)}{\dim E} = \frac{|G|}{\dim E} \cdot \frac{\dim E}{\dim E} = \frac{|G|}{\dim E}$$

is integral. Therefore, $\dim E$ divides $|G|$. □

In fact a more refined statement is true:

Claim 11.10. *Let $E \in Rep_k^{fd}(G)$ 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 $[G : Z]$. □

An even more refined statement is true, for which we will have a Lemma first.

Lemma 11.11. *Let $H \subset G$ be a normal subgroup, and $E \in Rep_k(G)$ an irreducible representation. Then either $res_H^G(E)$ is isotypical, or there exists $H \subset K \subset G$ and irreducible $F \in Rep_k(K)$ such that $K \neq G$ and $Ind_G^K(F) \cong E$.*

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 $K = \{g \in G \mid gE_0 = E_0\}$. Clearly $H \subset K$ and 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. The case $K = G$ corresponds to $E_0 = E$, meaning $res_H^G(E)$ is isotypical. □

Proposition 11.12. *Let $E \in Rep_k^{fd}(G)$ be irreducible, and $A \subset G$ be a normal abelian subgroup. Then* $\dim(E)$ *divides* $[G : A]$.

Proof. We proceed by induction on $|G|$. If $res_A^G(E)$ is isotypical, then A acts on E via a character; Denoting by $\rho : G \to GL_k(E)$ the relevant morphism, we see that $\rho(A)$ sits in the center of $\rho(G)$ (consisting of scalars), hence by Claim 11.10 we see that $\dim(E)$ divides $[\rho(G) : \rho(A)]$ which devides $[G : A]$. Otherwise, by the previous Lemma there exists $A \subset H \subset G$ and an irreducible $F \in Rep_k^{fd}(H)$ such that $Ind_G^H(F) \cong E$ and $H \neq G$. By induction, $dim(F)$ divides $[H : A]$. So $dimE = [G : H] \cdot \dim(F)$ divides $[G : H] \cdot [H : A] = [G : A]$. □

We will need the following Claim in the next subsection.

Claim 11.13. *Let $E \in Rep_k^{fd}(G)$ be irreducible, and $g \in G$. Denote by $C_g \subset G$ the conjugacy class containing g. Then $\frac{|C_g|}{\dim E}\chi_E(g)$ is integral.*

Proof. Since $\mathbb{1}_{C_g}$ is integral by part 2 of Claim 11.6, we obtain by Claim 11.8 that

$$\frac{\chi_E(\mathbb{1}_{C_g})}{\dim E} = \frac{|C_g|}{\dim E}\chi_E(g)$$

is integral. □

11.3 Burnside's theorem

An integral complex number is said to be an algebraic integer.

Lemma 11.14. *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 (say, imagine the orthogonal projection to the line passing through 0 and the average...).

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 11.15. *Let $E \in Rep^{fd}_{\mathbb{C}}(G)$ be irreducible. Let $g \in G$ be an element for which*

$$gcd(|C_g|, \dim E) = 1.$$

Then either $\chi_E(g) = 0$, or g acts on E by a scalar.

Proof. By Claim 11.13, the number $\frac{|C_g|}{\dim E}\chi_E(g)$ is integral. Since $gcd(|C_g|, \dim E) = 1$ and $\chi_E(g)$ is integral, we obtain easily that $\frac{1}{\dim E}\chi_E(g)$ is integral. Notice that $\chi_E(g)$ is the sum of $\dim E$ roots of unity (the eigenvalues of g acting on E). Hence by claim 11.14 either $\chi_E(g) = 0$ or all the eigenvalues of g acting on E are equal, meaning that g acts by a scalar on E. □

Claim 11.16. *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 $E \in Rep^{fd}_{\mathbb{C}}(G)$ 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 11.15, it is enough to find a non-trivial irreducible E of dimension prime to p, such that $\chi_E(C) \neq 0$. Computing the trace of the action of an $g \in C$ on $k[G]$, we obtain

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

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. □

Corollary 11.17. *Let G be a finite group such that $|G|$ is divided by exactly two different primes. Then G is not simple.*

Proof. It is enough, by the previous Claim, to see that there exists a conjugacy class C in G such that $|C|$ is a positive prime power. If there is no such conjugacy class, then every conjugacy class either has 1 element or its size is divisible by pq (where p and q are the two primes dividing $|G|$). Therefore, we would get that $|G| - |Z(G)|$ is divisible by pq. Since $|G|$ is divisible by pq, this would imply that $|Z(G)|$ is divisible by pq. In particular, $Z(G) \neq 1$, and therefore G is not simple (because then either $Z(G)$ is a non-trivial normal subgroup, or $Z(G) = G$, and the only abelian finite groups which are simple are the cyclic groups, so their order has only one prime divisor). □

Theorem 11.18 (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. Hence we can deduce the claim from the previous Corollary, by induction (our group is not simple, so has a proper normal subgroup, and both the normal subgroup and the quotient by it are solvable by induction, so the group itself is solvable). □

12 Equivariant sheaves and induction

12.1 G-equivariant sheaves

Definition 12.1. Let $X \in \mathit{Sets}$. 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 naturally a k-linear category $\mathit{Sh}(X)$.

If $\pi : X \to Y$ is a map, we have functors $\pi^* : \mathit{Sh}(Y) \to \mathit{Sh}(X)$ and $\pi_* : \mathit{Sh}(X) \to \mathit{Sh}(Y)$ 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 12.2. Let $X \in \mathit{Set}(G)$. A G**-equivariant sheaf** $(\mathcal{V}, \alpha)$ on X is the datum of a sheaf $\mathcal{V}$ on X, and an isomorphism $\alpha_{g,x} : \mathcal{V}_x \xrightarrow{\sim} \mathcal{V}_{gx}$ for all $g \in G$ and $x \in X$, with the conditions $\alpha_{h,gx} \circ \alpha_{g,x} = \alpha_{hg,x}$ and $\alpha_{1,x} = \mathit{id}$. G-equivariant sheaves on X form a k-linear category $\mathit{Sh}(X)^G$.

Example 12.3. *We have an equivalence of categories* $\mathit{Sh}(*)^G \approx \mathit{Rep}(G)$.

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

Definition 12.4. A **groupoid** is a category in which every morphism is an isomorphism.

Example 12.5. *Given a G-set X, we construct the action groupoid* $G\backslash\backslash X$*, whose objects are elements of* X *and* $Hom(x, y) = \{g \in G \mid gx = y\}$.

Claim 12.6. *Given a G-set X, one has an equivalence of categories* $\mathit{Sh}(X)^G \approx \mathit{Funct}(G\backslash\backslash X, \mathit{Vect})$.

Claim 12.7. *Let X be a transitive G-set,* $x \in X$*, and* $H := \mathit{Stab}_G(x)$*. Then we have a natural equivalence of categories* $\mathit{Sh}(X)^G \approx \mathit{Rep}(H)$.

Proof. We have an equivalence of groupoids $H\backslash\backslash * \to G\backslash\backslash X$ given by sending $*$ to x. Therefore we have

$$\mathit{Sh}(X)^G \approx \mathit{Funct}(G\backslash\backslash X, \mathit{Vect}) \approx \mathit{Funct}(H\backslash\backslash *, \mathit{Vect}) \approx \mathit{Sh}(*)^H \approx \mathit{Rep}(H).$$

□

Remark 12.8. Let us illustrate. Let V be a finite-dimensinoal vector space over $\mathbb{R}$, and denote by X_V the space of inner products on V. 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.

The relation of equivariant sheaves to induction is as follows:

Claim 12.9. *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.

The character formula for induction reads using this language as follows:

Claim 12.10. *Let G act on a finite X, and let $\mathcal{F} \in Sh(X)^G$. Consider $\Gamma(\mathcal{F})$ as a G-representation via $Sh(\bullet)^G \approx Rep(G)$. Then*

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

12.2 Mackey's theorem revisited

Let us see how Mackey theorem's proof is interpreted in terms of equivariant sheaves.

Thus, let G be a finite group and $H, K \subset G$ two subgroups. We want first to interpret the functor

$$res_K^G Ind_G^H : Rep(H) \to Rep(K)$$

in terms of equivariant sheaves. We interpret $Ind_G^H(M)$ as $\Gamma(\mathcal{F})$ where $\mathcal{F} \in Sh(G/H)^G$ is the corresponding G-equivariant sheaf. Then $res_K^G(Ind_G^H(M)) = res_K^G(\Gamma(\mathcal{F}))$ can be rewritten as $\Gamma(res_K^G(\mathcal{F}))$. Now, G/H as a K-set breaks down into the disjoint union of transitive K-sets $X_1, \ldots, X_r$ passing through points g_1H , ..., g_rH (where $g_1, \ldots, g_r$ are representatives for double cosets $K\backslash G/H$). Therefore

$$\Gamma(res^G_K(\mathcal{F})) \cong \bigoplus_{1\le i\le r} \Gamma\bigg(res^G_K(\mathcal{F})|_{X_i}\bigg).$$

Now, $\mathcal{F}$ can be described as the G-equivariant sheaf on G/H corresponding to the $Stab_G(g_iH) = g_iHg_i^{-1}$-representation $T_{g_i^{-1}}M$. Therefore, clearly $(res^G_K\mathcal{F})|_{X_i}$ can be described as the K-equivariant sheaf corresponding to the $(g_iHg_i^{-1} \cap K)$-representation $res^{g_iHg_i^{-1}}_{g_iHg_i^{-1}\cap K}(T_{g_i^{-1}}M)$. Therefore $\Gamma((res^G_K\mathcal{F})|_{X_i})$ can be described as

$$Ind_K^{g_iHg_i^{-1}\cap K}(res^{g_iHg_i^{-1}}_{g_iHg_i^{-1}\cap K}(T_{g_i^{-1}}M)).$$

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

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 12.11. *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 12.12. *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 12.13. *We have a bijection between $Irr(G)$ and $\coprod_i Irr(H_i)$.*

Example 12.14. *Let $V = \langle r : r^n = 1\rangle$, $H = \langle s : s^2 = 1\rangle$ where the action of s sends r to r^{-1}. Thus, $G = V \rtimes H$ is the dihedral group D_{2n} again. We can identify $Irr(V)$ with μ_n, where $\zeta \in \mu_n$ corresponds to $\omega_\zeta(r^i) = \zeta^i$. The* *resulting action of H on μ_n is by $s * \zeta = \zeta^{-1}$. The stabilizers are trivial for all $\zeta \in \mu_n$ except $\zeta = 1$ and, when n is even, $\zeta = -1$. Therefore, the irreducible representations of G are $Ind_V^G(\mathbb{C}_{\omega_\zeta})$ for $\zeta \notin \{1, -1\}$ and also two or four one-dimensional representations, given by the multiplicative characters which are equal to a quadratic character on V and one of the two multiplicative characters on H.*

Example 12.15. *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 $res_G^H(E)$ (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 $ind_V^G E$.*

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, $ind_{\mathbb{F}_q}^{\mathbb{F}_q \rtimes \mathbb{F}_q^{\rtimes}} \mathbb{C}_\psi$.

Let us write the character table:

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

13 Brief remarks on characteristic p

We fix a finite group G and an algebraically closed field k.

13.1 p-Regular and p-torsion elements

Definition 13.1. 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 13.2 ("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 13.3. In the notations of the above claim, we will write $y = x_{p\text{-reg}}$ and $z = x_{p\text{-tor}}$.

Remark 13.4. 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.

13.2 Characters

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

Claim 13.5. *The system $(\chi_E)_{[E]\in Irr_k(G)} \subset Fun(G;k)^{cl}$ is linearly independent.*

Proof. Recall that we have still an isomorphism of $k[G]/J(k[G])$ with

$$End_k(E_1) \times \ldots \times End_k(E_n)$$

(where $E_1, \ldots, E_n$ are representatives for isomorphism classes in $Irr_k(G)$). Therefore, we still can find $D \in k[G]$ such that $\chi_{E_i}(D) = Tr(D; E_i) = 1$ for some $1 \leq i \leq n$ and $\chi_{E_j}(D) = Tr(D; E_j) = 0$ for $j \neq i$. □

We now notice that the characters will not generally span $Fun(G,k)^{cl}$:

Claim 13.6. *Let $V \in Rep_k^{fd}(G)$. 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 13.7 (Brauer)**.** *The system $(\chi_E)_{[E]\in Irr_k(G)}$ forms a basis of $Fun(G^{p\text{-}reg}, k)^{cl}$.*