Contents

Lecture 1 - Wednesday, December 11

1.1 General comments and reference material. The first two of the three sections in these notes cover two hour-and-a-half-long lectures on modular representations of finite groups - finite dimensional representations of finite groups over (mostly algebraically closed) fields of 'bad' characteristic - that were given at IISER Tirupati on December 11 and 13 of 2019, as part of an NCM workshop on Modular Forms and Galois Representations, organized by Professors Shalini Bhattacharya and Eknath Ghate. Section 3 contains the example of representations of S_4 in characteristic 3, that was worked out by Anand Chitrao in the tutorial on December 13.

1.1.1 References. Here are some references that I have used (all of which cover much more than the material here):

- Daniel Bump's notes, at: http://sporadic.stanford.edu/modrep/

- Tony Feng's version of Daniel Bump's notes, available as of now at: https://www.mit.edu/ fengt/mod_rep_theory.pdf
- Alperin's book 'Local Representation Theory' - this is what was followed for much of Lecture 2.

One topic I regret not being able to discuss is a comparison of the representation theories of $SL_2(\mathbb{F}_p)$ in characteristic 0, in positive characteristic different from p, and in characteristic p - especially the computations concerning reduction from characteristic zero to characteristic p. This and a lot of other very interesting material on mod p representations of various groups can be found in an article of Professor Dipendra Prasad available at:

http://www.math.iitb.ac.in/∼dprasad/dp-mod-p-2010.pdf

1.1.2 Comments on these notes. These notes are mostly just a catalogue of some of the basic, standard results in the subject. Proofs are mostly omitted, but some verbal commentary/heuristics has been indulged in to help informally relate to the results. Some easy examples have been discussed too - the cases of S_3, S_4 and $SL_2(\mathbb{F}_p)$, of course with most justifications suppressed in the case of $SL_2(\mathbb{F}_p)$.

These notes cover lesser material than what the number of pages might indicate - I erred on the side of overexplaining. After all, apart from small additions (such as the statements of the first two of the three main theorems on the Brauer correspondence) this consists entirely of material that was covered in a total of three hours. The references above are all more efficient.

This subject is not what I do for a living, and errors are bound to be there: use at your own risk (or use this to get a flavour of the subject and then move to one of the standard references such as the ones given above).

1.1.3 Acknowledgements. I thank Professors Eknath Ghate and Shalini Bhattacharya for the kind invitation to the NCM Workshop, and Anand Chitrao for going through a good part of the following notes and pointing out a large number of inaccuracies and typos.

1.2 Some notation and conventions. Let G be a finite group, k a field, and p a prime number. For most of these notes - i.e., except in some examples where we state explicitly otherwise - we will assume that the characteristic of k is p. Our rings A will be associative and with a multiplicative identity, but their multiplications will not be assumed to be commutative.

A representation $\rho : G \to GL_k(E)$ may be written variously as (ρ, E), or ρ, or E, or $g \mapsto (v \mapsto g \cdot v)$, by abuse of notation.

Recall the group algebra $k[G] := \left\{\sum_{g\in G} a_g g \mid a_g \in k \,\forall\, g \in G\right\}$, whose multiplication is given by

$$\left(\sum a_h h\right)\left(\sum b_g g\right) = \sum_{h,g\in G} a_h b_g hg = \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g.$$

Throughout, we will use the 'correspondence' (which is more precisely an equivalence categories in particular) between representations of G and modules over $k[G]$. To recall this correspondence, let E be a k-vector space. Then:

- Any representation of G on E, written as $g \mapsto (v \mapsto g \cdot v)$, upgrades the k-vector space E into a $k[G]$-module via $\left(\sum_{g\in G} a_g g\right) \cdot v = \sum_{g\in G} a_g(g \cdot v)$; and
- If a $k[G]$-module structure on E is given, which is compatible with the k-vector space structure on E, it defines a representation of G on E by $g_0 \mapsto (v \mapsto \delta_{g_0} \cdot v)$, where $\delta_{g_0} \in k[G]$ is the element $1 \cdot g_0$.

This dictionary respects the notion of a map of G-representations, in the following sense. Suppose E_1 and E_2 are G-representations, and hence also thought of as $k[G]$-modules. Then, given a k-linear transformation $T : E_1 \to E_2$, T is a map of G-representations if and only if it is a homomorphism of $k[G]$-modules (this makes the above correspondence 'functorial', where the functor is described by the above bullet points at the level of objects, and is the 'identity' at the level of morphisms).

Under this dictionary, a representation of G is irreducible if and only if the corresponding $k[G]$-module is simple, i.e., has no proper nonzero submodule.

A representation of G is completely reducible (i.e., is a direct sum of irreducible representations) if and only if the corresponding $k[G]$-module is semisimple, i.e., is a direct sum of simple submodules.

Note: All modules over $k[G]$ considered in this lecture will be assumed to be finite dimensional as vector spaces over k.

1.3 Failure of complete reducibility in bad characteristic. Throughout, $\#S$ will denote the cardinality of a set S.

Recall that if k had characteristic 0, then every finite dimensional representation of G would be completely reducible. Usually two proofs are given for this fact - either using a G-invariant inner product, or 'taking a vector space section and averaging over G'. The latter proof continues to apply if $(p, \#G) = 1$, but the proof as well as the result fails when $(p, \#G) > 1$ (that is to say, when p divides the cardinality of G). The following exercise gives a simple but instructive counterexample.

Exercise 1.3.1. Suppose $G = \mathbb{Z}/p\mathbb{Z}$. Since char $k = p$, k contains a copy of $\mathbb{Z}/p\mathbb{Z}$ (note that this is used in stating (i) below).

(i) Check that the following homomorphism $G \to GL_2(k) = GL_k(k^2)$ is a representation of G:

$$\mathbb{Z}/p\mathbb{Z} \ni x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in GL_2(k).$$

(ii) Let $e_1 = (1, 0)$ be the first standard basis vector of k^2. Show that the only proper nonzero G-invariant subspace of k^2 is ke_1, which is the span of e_1. (Thus, this representation cannot be completely reducible, because proper G-invariant subspaces of k^2 do not span it).

(iii) Since each element of G leaves ke_1 invariant and hence has an induced action on k^2/ke_1, we get a quotient representation $G \to GL_k(k^2/ke_1)$. Show that both the subrepresentation of G on ke_1 and the quotient representation of G on k^2/ke_1 are trivial, even though the representation of G on k^2 is not.

Let us now generalize part of the above exercise to all p-groups.

Lemma 1.3.2. *Suppose G is a p-group. Then every irreducible representation (ρ, V) of G on a k-vector space is trivial.*

Note that the above lemma is implied by the following lemma (Lemma 1.3.3), which is what we will prove:

Lemma 1.3.3. *Suppose G is a p-group. Then every representation (ρ, V) of G in a k-vector space contains a nonzero vector fixed by G.*

Proof. Reduction to the case where $k = \mathbb{F}_p$ and V is of finite dimension. (Ignore this if you are willing to assume that k equals $\mathbb{F}_p$ and that V is of finite dimension over k). Let (ρ, V) be a representation of G, which we wish to show to have a nonzero G-fixed vector. Choose any $0 \neq v \in V$, and recall that k being of characteristic p contains $\mathbb{F}_p$. Then the $\mathbb{F}_p$-span of $\{\rho(g)v \mid g \in G\}$, call it V_0, is a nonzero $\mathbb{F}_p$-linear subspace of V (i.e., it is not a k-vector subspace of V but only a subspace of V viewed as an $\mathbb{F}_p$-vector space). Being spanned by $\#G$ elements, V_0 has dimension at most $\#G$ as a vector space over $\mathbb{F}_p$. Clearly, V_0 is invariant under the action of $\rho(g)$, for each $g \in G$. Since $\rho(g) : V \to V$ is k-linear, the restriction of $\rho(g)$ to V_0 is $\mathbb{F}_p$-linear.

Hence it is enough to show that V_0 has a nonzero G-fixed vector. We can therefore replace (ρ, V) with $(g \mapsto \rho(g)|_{V_0}, V_0)$ to assume that $k = \mathbb{F}_p$ and that V is a finite dimensional vector space over $k = \mathbb{F}_p$.

Proof when $k = \mathbb{F}_q$ for some power q of p, and V is of finite dimension. Let us assume that (ρ, V) is a representation of G on an n-dimensional $\mathbb{F}_q$-vector space $V = \mathbb{F}_q^n$, where q is a power of p (we just showed that we could assume $q = p$, but keeping this slightly more general q with us does not hurt).

Since G is a p-group, so is $\rho(G) \subset GL_n(\mathbb{F}_q)$. Therefore, $\rho(G)$ is contained in a p-Sylow subgroup of $GL_n(\mathbb{F}_q)$. We claim that one of the p-Sylow subgroups of $GL_n(\mathbb{F}_q)$ is given by the group $U_n(\mathbb{F}_q)$ of upper triangular matrices with 1's on all diagonal entries. For this, note that $\#U_n(\mathbb{F}_q) = q^{n(n-1)/2}$, while

$$\#GL_n(\mathbb{F}_q) = (q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}) = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \ldots (q - 1),$$

so that $\#U_n(\mathbb{F}_q)$ is the largest power of p dividing $\#GL_n(\mathbb{F}_q)$. Therefore, $U_n(\mathbb{F}_q) \subset GL_n(\mathbb{F}_q)$ is a p-Sylow subgroup.

Thus, by one of the Sylow theorems, there exists $T \in GL_n(\mathbb{F}_q)$ such that $T\rho(G)T^{-1}$ is contained in $U_n(\mathbb{F}_q)$, and hence fixes the basis vector $e_1 = (1, 0, \ldots, 0) \in k^n$ (as every element of $U_n(\mathbb{F}_q)$ does).

Since $T\rho(G)T^{-1}$ fixes e_1, it follows that $\rho(G)$ fixes $T^{-1}e_1$ (I wrongly wrote Te_1 in the lecture, and this was pointed out to me after the lecture). Thus, there exists a nonzero vector (namely $T^{-1}e_1$) in V fixed by the action of G, as desired. □

Remark 1.3.4. An alternate proof - after reducing to the finite dimensional case where $k = \mathbb{F}_q$ - involves noting that the G-orbits that are not given by G-fixed points, i.e., the non-singleton orbits, all have cardinalities that are multiples of p. Since the cardinality of $\mathbb{F}_q^n$ is a multiple of p, it follows that the number of G-fixed points in $\mathbb{F}_q^n$ is a multiple of p. This multiple is nonzero since $0 \in \mathbb{F}_q^n$ is G-fixed, so there should be at least $p-1$ nonzero G-fixed points in $\mathbb{F}_q^n$.

Corollary 1.3.5. *If G is a p-group with $\#G > 1$, then not all representations of G are completely reducible.*

Proof. Since all irreducible representations of G are trivial by the above lemma, G acts trivially on completely reducible representations, but there exist representations on which G acts nontrivially (e.g., the regular representation of G, which corresponds to $k[G]$ viewed as a left module over itself by left multiplication), which therefore cannot be completely reducible. □

1.4 Review of semisimplicity for rings and modules.

Recall the following basic theorem about semisimple modules, where the main example to keep in mind will be the case of the ring $A = k[G]$:

Proposition 1.4.1. *Let A be a ring and M an A-module. The following are equivalent:*

(i) M is the sum of its simple submodules;

(ii) M is the direct sum of some of its simple submodules;

(iii) Every submodule $N \subset M$ is a direct summand (i.e., there exists a submodule $N' \subset M$ such that $M = N \oplus N'$, that is to say, $M = N + N'$ and that $N \cap N' = \{0\}$).

Recall that a semisimple module is by definition a direct sum of a family of simple modules, so a semisimple module can be actually defined by any of the criteria (i)-(iii) of the above proposition.

The following is an easy corollary:

Corollary 1.4.2. *Every submodule of a semisimple module is semisimple. Every quotient module of a semisimple module is semisimple. A direct sum of a collection of semisimple modules is semisimple.*

Definition 1.4.3. A ring A is said to be semisimple if A, viewed as a left module over itself by left multiplication, is a semisimple module.

Since every left A-module is a quotient of a free left A-module, the corollary above gives:

Corollary 1.4.4. *A is a semisimple ring if and only if every left A-module is a semisimple left A-module.*

Remark 1.4.5. • Since all representations of G are completely reducible when $(\#G, p) = 1$, it follows that the ring $k[G]$ is semisimple whenever $(\#G, p) = 1$.

• If $(\#G, p) \neq 1$, it is not hard to prove that not all representations of G are completely reducible (we have already seen this when G is a p-group), though we skip a proof.

1.5 The radical and semisimplicity.

One tool to understand the failure of semisimplicity of $k[G]$ when $(\#G, p) = 1$ is the (Jacobson) radical of $k[G]$, a notion we now proceed to define.

Definition 1.5.1. (i) Let M be a left module over $A = k[G]$. Then its *radical* is defined to be the intersection of the maximal left submodules (i.e., maximal proper left submodules) of M:

$$\mathrm{rad}(M) = \bigcap_{\substack{M' \subset M \\ M' \text{ maximal} \\ \text{(proper) submodule}}} M'.$$

It is clearly a left A-submodule of M.

(ii) The *(Jacobson) radical* of A is defined to be the intersection of all maximal left ideals of A:

$$\mathrm{rad}(A) = \bigcap_{\substack{\mathfrak{m} \subset A \\ \mathfrak{m} \text{ maximal left ideal}}} \mathfrak{m}.$$

We will not prove the following proposition, which summarizes some basic results concerning the Jacobson radical, but merely give some ideas on how to think of them:

Proposition 1.5.2. *Let A be a k-algebra (i.e., a ring containing k in its center), and assume that A is finite dimensional as a k-vector space, i.e., $\dim_k A < \infty$ (think of $A = k[G]$). Let M be a left A-module with $\dim_k M < \infty$*

(i) The left ideal rad(A) of A is in fact a two-sided ideal.

(ii) M is semisimple if and only if rad$(M) = 0$.

(iii) If $M'' = M/M'$ for a left A-submodule M' of M, then M'' is semisimple if and only if $M' \supset$ rad(M) - i.e., semisimple quotients (M'') of M are precisely those that factor through $M \to M/$rad(M).

(iv) rad$(M) =$ rad$(A) \cdot M$ (where rad$(A) \cdot M$ is the submodule of M consisting of the set of finite linear combinations $\sum a_i m_i$, where each a_i belongs to rad(A) and each m_i to M).

(v) A is semisimple (as a ring) if and only if rad$(A) = \{0\}$.

Now let us indicate some informal ideas related to its proof, just to make it believable that radicals can be related to semisimplicity.

Some ideas 'in one direction': It is easy to see (from one of the three isomorphism theorems for modules) that M/M' is simple if and only if M' is a maximal submodule of M, so $\mathrm{rad}(M)$ is in the kernel of every simple quotient of M, and hence in the kernel of every semisimple quotient of M. Note also that simple left A-modules N are precisely of the form $A/\mathfrak{m}$ as $\mathfrak{m}$ varies over maximal left ideals of A: if $0 \neq x \in N$, then $a \mapsto ax$ defines a left A-module surjection $A \to N$, quotienting to an isomorphism $A/\mathrm{ann}(x) \xrightarrow{\cong} N$, and then the simplicity of N forces the annihilator $\mathrm{ann}(x)$ of x to be a maximal left ideal of A. Since $\mathrm{rad}(A)$ is contained in every maximal left ideal, $\mathrm{rad}(A)$ annihilates x (for every $0 \neq x \in N$). Thus, $\mathrm{rad}(A)$ annihilates every simple left A-module, and hence also every semisimple left A-module.

Now some ideas 'in the other direction'. We have an injection of left A-modules

$$A/\mathrm{rad}(A) \hookrightarrow \prod A/\mathfrak{m},$$

where $\mathfrak{m}$ runs over the maximal left ieals of A. But since A is finite dimensional, one can restrict to finitely many maximal ideals and still get an injection of left A-modules:

$$A/\mathrm{rad}(A) \hookrightarrow \prod_{i=1}^{n} A/\mathfrak{m}_i = \bigoplus_{i=1}^{n} A/\mathfrak{m}_i$$

(for finitely many modules, the direct sum is the same as the direct product). Thus, $A/\mathrm{rad}(A)$ is a semisimple left A-module. If you believe that $\mathrm{rad}(A)$ is a two-sided ideal of A, so that the quotient $A/\mathrm{rad}(A)$ is actually a ring, this shows that $A/\mathrm{rad}(A)$ is a semisimple left module over itself, and hence a semisimple ring. Thus, any left A-module annihilated by $\mathrm{rad}(A)$, being a module over $A/\mathrm{rad}(A)$, is semisimple (see Corollary 1.4.4).

Note: I think there were some stupid errors I made on the board that I unfortunately cannot recall or find in my notes; perhaps I wrongly wrote a maximal submodule of M as $\mathfrak{m} \cdot M$ or that $\mathfrak{m}$ annihilates a simple quotient of M or something of this sort, because at some point I mixed up left and right multiplication on the spot; please correct them if at all you are using notes that you wrote from the lecture.

The above proposition allows us to write down informally:

Corollary 1.5.3. *$M/rad(M)$ is the 'maximal semisimple quotient' of M.*

1.6 The Jordan-Holder series, the radical and socle series. Once the ring A is not semisimple, how does one think of left A-modules as built up from simple left A-modules?

Definition 1.6.1. A left A-module M is said to be of *finite length* if there exists a chain $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ of left A-submodules of M such that for $1 \leqslant i \leqslant n$, M_i/M_{i-1} is a simple left A-module. Such a chain is called a *composition series* for M, n is called the *length* of this composition series, and the (multi)set [1] $\{M_1/M_0, M_2/M_1, \ldots, M_n/M_{n-1}\}$ of simple modules (understood to be taken up to isomorphism) is called the (multi)set of *Jordan-Holder factors* of this composition series.

[1] A multiset is like a set but in which elements are allowed to occur more than once; e.g., $\{0, 1, 1\}$ and $\{0, 1\}$ are the same as sets but not as multisets.

We will keep using the following obvious fact without further mention: if A contains k and is finite dimensional as a k-vector space, then finite length A-modules are precisely those A-modules which are finite dimensional as k-vector spaces.

The following lemma is the Jordan-Holder theorem in this setting:

Lemma 1.6.2. *Suppose a left A-module M has finite length. Any two Jordan-Holder series for M have the same length and the same multiset of Jordan-Holder factors, and hence we may define these to be the* length of M *and the* (multi)set of Jordan-Holder factors of M*, respectively.*

The idea is that one can think of M as being built up of the simple left A-modules $M_1/M_0, M_2/M_1, \ldots, M_n/M_{n-1}$: after all, in the case where $M = N_1 \oplus \cdots \oplus N_n$ is a sum of simple left A-modules, setting $M_i := N_1 + \cdots + N_i$ for $1 \leqslant i \leqslant n$ (and $M_0 = 0$), it is easy to check that $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ is a composition series for M and the corresponding Jordan-Holder factors are $N_1, \ldots, N_n$, which are precisely the simple modules $N_1, \ldots, N_n$ that sum to N.

The above lemma also allows us to talk of the Jordan-Holder multiplicity of a simple left A-module N in a left A-module M - the number of times N occurs in the multiset of Jordan-Holder factors of M.

Exercise 1.6.3. But this conception of thinking of M as built up out of its Jordan-Holder factors does not describe M completely. To illustrate this in the case where $A = \mathbb{Z}$, check that both $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ have the same Jordan-Holder factors, namely the (multi)set $\{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\}$, though they are of course non-isomorphic $\mathbb{Z}$-modules. To illustrate this in a case where A is of the form $k[G]$, note that when $G = \mathbb{Z}/p\mathbb{Z}$, the module k^2 of Exercise 1.3.1 has Jordan-Holder factors $\{k, k\}$ by (iii) of that exercise (where k is viewed as the $k[G]$-module corresponding to the trivial representation of G), i.e., the same as for a direct sum of two copies of the trivial representation, but that module is not isomorphic to a direct sum of two copies of the trivial representation.

Another problem with this description is that a module can have many composition series (though all of them will give the same Jordan-Holder factors), so there is something noncanonical about this description.

Two ways to make 'part' of this canonical are given by the *radical series* and the *socle series* of M.

For this, let us first define the socle of M:

Definition 1.6.4. The *socle* of M is its left A-submodule $\mathrm{soc}(M)$ given by:

$$\{x \in M \mid (\mathrm{rad}A) \cdot x = \{0\}\}.$$

It is easy to see that $\mathrm{soc}(M)$ is the maximal semisimple left A-submodule of M, because semisimple left A-modules are precisely those that are annihilated by $\mathrm{rad}(A)$.

Definition 1.6.5. Let A be a k-algebra (i.e., a ring containing k in its center) which is finite dimensional as a k-vector space. Let M be a left A-module which is of finite length, or equivalently $\dim_k M < \infty$.

(i) The *radical series* of M is the chain of left A-submodules of M given by:

$$M \supset \text{rad}(M) \overset{\text{Proposition 1.5.2(iv)}}{=} \text{rad}(A) \cdot M \supset \text{rad}(\text{rad}M) = (\text{rad}A)^2 M \supset \cdots \supset (\text{rad}A)^r M = 0$$

(that this filtration is strictly decreasing and hence eventually zero follows from the fact that for each left A-submodule $0 \neq M' \subset M$, the quotient left A-module $M'/\text{rad}(M')$, being the maximal semisimple quotient of M', is nonzero: this follows from the fact that, M' being finite dimensional, among the nonzero quotient left A-modules of M', we can choose one whose dimension over k is the smallest possible; this quotient is necessarily simple and hence semisimple).

(ii) The *socle series* of M is the series of left A-submodules of M given by

$$N_0 = 0 \subset N_1 \subset N_2 \subset \cdots \subset N_r = M,$$

where $N_1 = \text{soc}(M)$ is the maximal semisimple left A-submodule of M, and inductively, for $1 \leqslant i \leqslant r$, once N_{i-1} is defined, N_i is the pre-image of $\text{soc}(M/N_{i-1})$ under the quotient map $M \to M/N_{i-1}$.

Remark 1.6.6. (a) In (ii) of the above definition, note that $N_i/N_{i-1} \cong \text{soc}(M/N_{i-1})$ is semisimple, and N_i is in fact maximal among the left A-submodules of M that contain N_{i-1} and satisfy that their quotient by N_{i-1} is semisimple. Thus, N_1 being maximal semisimple in M, one cannot get a larger semisimple left A-submodule of M, one takes the next in the series to be the maximal left A-submodule N_2 containing N_1 such that N_2/N_1 is semisimple, and so on.

(b) There is clearly a similar interpretation with radical series involving maximal semisimple quotients. And there is, as with the radical series, a justification for why, in the case of the socle series, N_r has to be the whole of M for some r.

The radical series and the socle series are canonically defined, though they are not composition series (the successive quotients are only semisimple, not simple).

1.7 The number of irreducible representations of G up to isomorphism. Let $\hat{G}$ be the set of (isomorphism classes of) irreducible representations of G. So far we know the following about the number of irreducible representations of G up to isomorphism, i.e., about $\#\hat{G}$:

(i) If G is a p-group, we have seen that any irreducible representation of G is trivial, so this number equals one.

(ii) In the characteristic zero case, it is well known that, if $k = \bar{k}$, then this number equals the number of conjugacy classes of G.

(ii) above continues to be true if $(\#G, p) = 1$, but as (i) shows, not otherwise.

Yet, (i) and (ii) happen to have a common generalization to all (finite) G, assuming $k = \bar{k}$, to state which we will use the following definition.

Definition 1.7.1. A conjugacy class $C \subset G$ is said to be *p-regular* if any $g \in C$ has order prime to p (this needs to be checked only for one $g \in C$ as all elements in a conjugacy class have the same order).

Then (ii) above generalizes nicely, as follows:

Theorem 1.7.2 (Brauer, Nesbitt)**.** *Assume $k = \bar{k}$. Then the number $\#\hat{G}$ of irreducible representations of G up to isomorphism equals the number of p-regular conjugacy classes in G.*

The above theorem is one of several theorems due to Brauer and Nesbitt, so it cannot be called 'the' Brauer-Nesbitt theorem. As an easy exercise, check that the above theorem generalizes both (i) and (ii) (under the assumption $k = \bar{k}$).

We will not discuss the proof of the above theorem, but here is an idea. First, let us discuss the proof of (ii) above considering the characteristic zero case, or the case where $(\#G, p) = 1$. One shows that both $\#\hat{G}$ and the number of conjugacy classes in G equal $\dim_k k[G]/[k[G], k[G]]$. This uses an isomorphism of k-algebras:

$$k[G] \cong \prod_{(\pi,V)\in\hat{G}} \operatorname{End}_k(V). \tag{1}$$

Thus, at the level of k-vector spaces, we have:

$$k[G]/[k[G], k[G]] \cong \prod_{(\pi,V)\in\hat{G}} \operatorname{End}_k(V)/[\operatorname{End}_k(V), \operatorname{End}_k(V)] \cong \prod_{(\pi,V)\in\hat{G}} k$$

(this does not make sense at the level of rings, because $[k[G], k[G]]$ is not a left ideal in $k[G]$). Hence $\#\hat{G}$ equals $\dim_k k[G]/[k[G], k[G]]$, and to complete the proof, one shows that $[k[G], k[G]]$ is the set of elements $\sum_{g\in G} a_g g \in k[G]$ with the property that for each conjugacy class $C \subset G$, $\sum_{g\in C} a_g = 0$ - note that this forces $\#\hat{G} = \dim_k(k[G]/[k[G], k[G]])$ to be the number of conjugacy classes in G.

Of course, this proof does not work when $(\#G, p) \neq 1$. For instance, (1) above is no longer true, though it becomes true if on the left-hand side we replace $k[G]$ with $k[G]/\operatorname{rad}(k[G])$.

Thus, $\#\hat{G}$ is actually the dimension of the k-vector space $\dfrac{k[G]}{(\operatorname{rad}(k[G])) + [k[G], k[G]]}$ (I may have carelessly omitted the '+' on the board). One has to then show that this dimension equals the number of p-regular conjugacy classes. We will not prove this result, but merely remark that the presence of the radical brings in conditions that involve raising elements of G to large p-powers, and raising elements of a conjugacy class of G to a large p-power takes it to a p-regular conjugacy class.

Example 1.7.3. The group S_3 consisting of the permutations of $\{1, 2, 3\}$ has three conjugacy classes - the singleton conjugacy class containing just the identity element, the three-element conjugacy class consisting of the transpositions each of which has order (exactly) 2, and the two-element conjugacy class consisting of the three cycles each of which has order (exactly) 3.

So, while there are three conjugacy classes (and hence S_3 has exactly three irreducible representations up to isomorphism in characteristic zero), only two of these conjugacy classes are 3-regular, so the above theorem tells us that S_3 has exactly two irreducible representations over $\bar{\mathbb{F}}_3$, up to isomorphism, so let us see this explicitly.

First, there are two 'obvious' irreducible representations of S_3 over $\bar{\mathbb{F}}_3$: the trivial representation, and the 'sign representation' or the 'sign character', which is by definition the composite:

$$S_3 \to S_3/A_3 \stackrel{\cong}{\to} \{\pm 1\} \hookrightarrow \bar{\mathbb{F}}_3 = GL_1(\bar{\mathbb{F}}_3),$$

where $A_3 \subset S_3$ is the alternating group consisting of the three cycles and the identity element, which is a normal subgroup of S_3. Thus, we need to see that every irreducible representation of S_3 is isomorphic to one of these. These are clearly the only irreducible representations (up to isomorphism) that factor through the two-element group S_3/A_3, so it is enough to show that any irreducible representation $\rho : S_3 \to \mathrm{GL}_{\bar{\mathbb{F}}_3}(V)$, where V is a finite dimensional vector space over $\bar{\mathbb{F}}_3$, is trivial on A_3. The subspace of V consisting of A_3-fixed vectors is S_3-invariant (by the normality of A_3 in S_3), and nonzero (by Lemma 1.3.3), and hence equals V by the irreducibility of ρ, forcing ρ to be trivial on $A_3 \subset S_3$, as desired.

1.8 Indecomposable modules and the Krull-Schmidt theorem. As we said earlier, a left $k[G]$-module is not in general the direct sum of its Jordan-Holder factors, and hence cannot be reconstructed from them. One therefore also tries to study left $k[G]$-modules in terms of modules which may not be simple, but are 'indecomposable' in the following sense:

Definition 1.8.1. A left A-module M is said to be *indecomposable* if M cannot be written as the direct sum of two proper left A-submodules of M.

So another approach to studying left $k[G]$-modules could be to write a left $k[G]$-module as a direct sum of indecomposable modules, and then study the indecomposable left $k[G]$-modules. But this immediately begs the question of whether there is a well-defined notion of 'indecomposable components' of a left $k[G]$-module, and the famous Krull-Schmidt theorem asserts that this is the case for left modules of finite length over $k[G]$ (i.e., for finite dimensional representations):

Theorem 1.8.2 (The Krull-Schmidt Theorem)**.** *Let E be a left module of finite length over a k-algebra A that is finite dimensional as a k-vector space. Then:*

(i) E has a decomposition $E = M_1 \oplus \cdots \oplus M_n$ into indecomposable left modules.

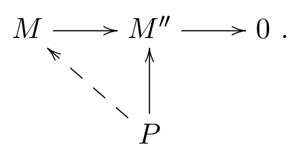
(ii) The multiset $\{M_1, \ldots, M_n\}$ (its elements considered up to isomorphism) is unique. In other words, if $E = M_1 \oplus \cdots \oplus M_n = M_1' \oplus \cdots \oplus M_r'$, where each M_i and each M_j' are indecomposable, then $n = r$, and there exists a permutation $\sigma \in S_n$ such that $M_i \cong M_{\sigma(i)}'$ for each i.

Of course, in the above theorem, M_i will in general be only isomorphic to $M_{\sigma(i)}'$ - M_i and $M_{\sigma(i)}'$ will not be the same left A-submodule of M, but only be two possibly distinct left A-submodules of M isomorphic to each other - this is already the case for $A = k[G]$ when G is the trivial group.

When we decompose a representation E of G in characteristic zero into irreducible subrepresentations, the decomposition is not canonical on the nose, but the sum of all subrepresentations of E isomorphic to a given representation σ is canonical - it is called the σ-isotypic component of E. But an analogous assertion is not true for decomposition into indecomposable left $k[G]$-modules: in the situation of the above theorem, the subspace of E given as $\bigoplus_{\{1\leqslant i\leqslant n|M_i\cong\sigma\}} M_i$ will not in general be equal (but only be isomorphic) to $\bigoplus_{\{1\leqslant j\leqslant n|M'_j\cong\sigma\}} M'_j$. For instance, this is the case with $G = \mathbb{Z}/2\mathbb{Z}$ when $p = 2$, since the left $k[G]$-module $k[G]\oplus k$ (the factor k being the trivial representation of G considered as a left $k[G]$-module) can also be decomposed as $\iota(k[G]) \oplus k$, with $\iota : k[G] \hookrightarrow k[G] \oplus k$ being defined by $a \mapsto (a, a \cdot 1)$.

1.9 Projective indecomposable modules and projective covers. Note: For the rest of this lecture, we will often simply say an 'A-module' or an 'A-submodule' to mean a left A-module or a left A-submodule, etc.

Recall that an A-module P is called *projective* if for any surjection $\lambda : M \twoheadrightarrow M''$ of A-modules, the map $\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, M'')$ given by $\varphi \mapsto \lambda \circ \varphi$ surjective, i.e., if the dotted arrow in the following diagram necessarily exists:



The projective indecomposable $k[G]$-modules play an important role in studying the representation theory of G. They also happen to have many nice properties, as we shortly state.

First, using that $\dim_k k[G] < \infty$, one can prove:

Lemma 1.9.1. *Suppose M is a $k[G]$-module of finite length. Then:*

(i) There exists a projective $k[G]$-module P and a surjection $\varphi : P \to M$ of $k[G]$-modules which is 'essential' in the sense that $\varphi|_N$ is not surjective for any proper $k[G]$-submodule $N \subset P$.

(ii) The $k[G]$-module P in (i) above is unique up to (a non-unique) isomorphism (though the map φ is not).

Definition 1.9.2. Such a P or a (P, φ) as in the above lemma is called a *projective cover* of M.

Here is one reason why the above lemma is nice. Recall that every module is the quotient of a free module (which is automatically projective). But such a free/projective module quotienting to a given module is highly non-unique. The above lemma says that there is a 'good' way of choosing a projective module with M as a quotient, which is in some sense minimal (projective covers don't exist in the kind of generality that injective envelopes to, but the fact that $k[G]$ is Artinian and that M is of finite length ensures the existence of a projective cover). An equivalent characterization of a projective cover $P \to M$ of M in our situation is that the resulting map

$$P/\mathrm{rad}(P) \cong P/\mathrm{rad}(A)P \to M/\mathrm{rad}(A)M \cong M/\mathrm{rad}(M)$$

should be an isomorphism (so that P is minimal enough to ensure that its maximal semisimple quotient $P/\mathrm{rad}(P)$ is no bigger than $M/\mathrm{rad}(M)$).

Example 1.9.3. As Anand Chitrao pointed out in response to a question, although G is finite, $k[G]$ can have infinitely many indecomposable modules up to isomophism - e.g., this is the case with $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. This example is worked out towards the end of Section 4 (in Chapter II) of Alperin's 'Local Representation Theory'.

Assume that $k = \bar{k}$. The infiniteness in the above exercise goes away if we restrict to projective indecomposable modules:

Theorem 1.9.4. *Assume that $k = \bar{k}$. Then exists a bijection between the set of isomorphism classes of simple $k[G]$-modules and the set of isomorphism classes of indecomposable projective $k[G]$-modules, that takes any simple $k[G]$-module S to a projective cover of S. The inverse of this isomorphism takes a projective indecomposable module P to the module $P/rad(P)$ (in particular, for any indecomposable projective $k[G]$-module P, the semisimple module $P/rad(P)$ is actually simple).*

The proof of this theorem is not difficult; apart from playing with projectivity in standard ways, e.g., as indicated by the following commutative diagram

$$\begin{array}{ccc} P & \longrightarrow & P/\mathrm{rad}(P) \\ \downarrow & & \downarrow \cong \\ Q & \longrightarrow & Q/\mathrm{rad}(Q) \end{array},$$

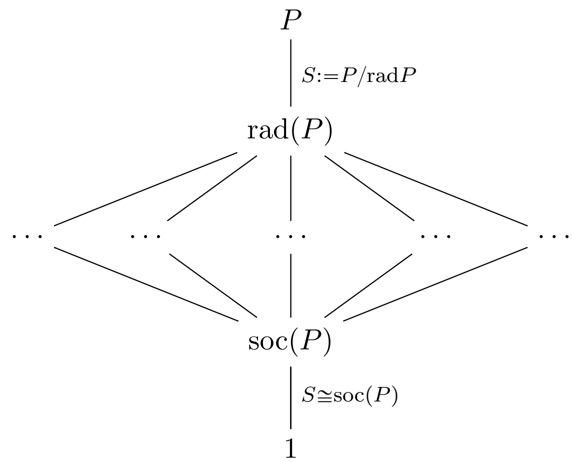
one uses a crucial property that holds in the category of $k[G]$-modules, that a $k[G]$-module turns out to be indecomposable if and only if its endomorphism ring is a local ring (where the assumption that $k = \bar{k}$ is used). I think I missed stating this assumption $k = \bar{k}$ in the lecture, and I certainly missed it in the earlier crude draft of these notes. The standard references use $k = \bar{k}$, but I haven't checked if this assumption can be removed.

1.10 Three more properties of projective indecomposable modules. Suppose P is a projective indecomposable $k[G]$-module. Then there are two obvious semisimple modules one can associate to P - the maximal semisimple submodule $\mathrm{soc}(P)$ and the maximal semisimple quotient $P/\mathrm{rad}(P)$.

If we know that P corresponds to a simple $k[G]$-module S as per Theorem 1.9.4, then $P/\mathrm{rad}(P) \cong S$. The following non-obvious theorem says that $\mathrm{soc}(P)$ is isomorphic to S too.

Theorem 1.10.1. *If P is a projective indecomposable $k[G]$-module, then $P/rad(P) \cong \mathrm{soc}(P)$.*

In other words, informally speaking, the structure of the 'submodule lattice' of P can be pictorially represented as follows:



(unlike the theorem, the above informal diagram only represents a very typical case, and is not meant to imply that $\mathrm{soc}(P)$ is always contained in $\mathrm{rad}(P)$, which may not be the case, e.g., it is not the case if P is simple).

The next property concerns the multiplicity of a projective indecomposable $k[G]$-module P in the regular representation (i.e., $k[G]$ viewed as a module over itself), in the sense of Theorem 1.8.2:

Theorem 1.10.2. *Assume that $k = \bar{k}$. Let S be a simple $k[G]$ module and P the corresponding projective indecomposable module. The multiplicity of P in $k[G]$ (in the sense of the decomposition of Theorem 1.8.2) equals the dimension $\dim_k S$ of S as a k-vector space.*

Note that in the case where k has characteristic zero, or where $(\#G, p) = 1$, any simple $k[G]$-module S is also projective (so $P = S$), and its multiplicity in the regular representation $k[G]$ equals $\dim_k S$. Thus, when we generalize from characteristic zero to characteristic p, the '$\dim_k S$' term no longer remains equal to the Jordan-Holder multiplicity of S in $k[G]$ (as defined in Subsection 1.6) , but rather equal to the Krull-Schmidt multiplicity of P in $k[G]$. In other words, the same S of characteristic zero has two different analogues in characteristic p, namely S and P, and in generalizing the theorem on multiplicities in the regular representation from characteristic 0 to characteristic p, one of the S's remains S while the other becomes P.

The proof of the above theorem is actually easy, and here is a sketch (a proof if you know the identifications mentioned in it). If $k[G] = \bigoplus_i c_i P_i$, with c_i the multiplicity of the projective indecomposable module P_i corresponding to the simple module $S_i = P_i/\mathrm{rad}(P_i)$, then

$$k[G]/(\mathrm{rad}k[G]) \cong \bigoplus_i c_i(P_i/(\mathrm{rad}k[G] \cdot P_i)) = \bigoplus_i c_i(P_i/\mathrm{rad}(P_i)) = \bigoplus_i c_i S_i.$$

Now $k[G]/(\mathrm{rad}k[G])$ can be identified with $\prod_i \mathrm{End}_k(S_i)$ (thanks to the assumption $k = \bar{k}$) as a map of $G \times G$-representations, and then the equality $k[G]/(\mathrm{rad}k[G]) \cong \bigoplus_i c_i S_i$ forces $c_i = \dim_k S_i$.

Example 1.10.3. Let us see how Theorem 1.10.2 works out when $G = S_3$ and $k = \bar{\mathbb{F}}_3$. We saw in Example 1.7.3 that S_3 has exactly two simple modules up to isomorphism, the trivial representation and the sign character. So we would like to see that S_3 has exactly two indecomposable projective modules, each occurring in $k[S_3]$ with multiplicity one. I leave the following for you to check. Thinking of S_3 as the dihedral group generated by elements x, y with $x^3 = y^2 = 1$ and $yxy^{-1} = x^{-1}$, check that we have a decomposition of $k[S_3]$ into a direct sum of two left ideals:

$$k[S_3] = k[S_3](1 - y) \oplus k[S_3](1 + y)$$

(I wrote a more complicated expression in the lecture, which is not necessary for our purposes).

Thus, $k[S_3](1 - y)$ and $k[S_3](1 + y)$ are projective $k[S_3]$-modules. Their indecomposability follows by Lemma 1.3.3 once you check that the subgroup $A_3 \subset S_3$ of order 3 (which equals $\{1, x, x^2\}$) has exactly one fixed vector up to scaling, namely of the form $(1 + x + x^2)(1 \pm y)$, in each of $k[S_3](1 - y)$ and $k[S_3](1 + y)$.

Check that the Jordan-Holder factors of $k[S_3](1 - y)$ are the sign character, the trivial character and the sign character necessarily in that order, making it a projective cover of the sign character, and that the Jordan-Holder factors of $k[S_3](1 + y)$ are the trivial character, the sign character and the trivial character necessarily in that order, making it a projective cover of the trivial representation.

A third property of projective indecomposable modules is the 'symmetry of the Cartan matrix', where the Cartan matrix of G is defined as follows:

Definition 1.10.4. Let $S_1, \ldots, S_n$ be the set of simple $k[G]$-modules up to isomorphism, and $P_1, \ldots, P_n$ the corresponding projective indecomposable modules. Then the Cartan matrix of G (for the field k) is defined to be the $n \times n$ matrix $[c_{ij}]$, where for $1 \leqslant i, j \leqslant n$, c_{ij} is the Jordan-Holder multiplicity of S_i in P_j (as defined in Subsection 1.6).

Proposition 1.10.5. *Suppose $k = \bar{k}$. Then the Cartan matrix C is symmetric, i.e., $c_{ij} = c_{ji}$ for all $1 \leqslant i, j \leqslant n$, with notation as in the above definition.*

The above 'surprising' result has a beautiful explanation and proof in terms of 'characteristic zero' theory: Brauer and Nesbitt related the characteristic zero and characteristic p representation theories of G, to get a beautiful factorization of C as a product ${}^tDD$ of matrices, where D is a (not necessarily $n \times n$) matrix called the 'decomposition matrix' of G, and where ${}^tD$ denotes the transpose of D. This forces C to be symmetric, since ${}^t({}^tDD) = {}^tD\,{}^t{}^tD = {}^tDD$.

Here are some more indulgently informal ideas regarding this approach. First (at least when $k = \bar{\mathbb{F}}_p$), one can pass from the algebraically closed field k to a finite extension $\mathbb{F}_q$ of $\mathbb{F}_p$ that is 'large enough' (depending on G). One can choose a finite extension K of $\mathbb{Q}_p$ such that $k = \mathbb{F}_q$ is the residue field of the ring O_K of integers of K. Then one proves the existence of a triangle of the following form, whose arrows we will not define precisely, the so called CDE triangle:

$$\begin{array}{ccc} P_k(G) & \xrightarrow{\quad c \quad} & R_k(G) \ . \\ & {\scriptstyle e}\searrow \qquad \nearrow{\scriptstyle d} & \\ & R_K[G] & \end{array}$$

Here $P_k(G)$ is the set of finite $\mathbb{Z}$-linear combinations of (isomorphism classes of) indecomposable projective $k[G]$-modules, while $R_K(G)$ is the set of finite $\mathbb{Z}$-linear combinations of (isomorphism classes of) simple $K[G]$-modules, and the definition of $R_k(G)$ is obtained by replacing 'K' with 'k' in that of $R_K(G)$.

The horizontal arrow 'c' of the above diagram is what captures the matrix C. The downward (and rightward) arrow 'e' involves lifting projective $k[G]$-modules first to projective $O_K[G]$-modules, which give elements of $R_K(G)$, while the upward (and rightward) arrow 'd' involves choosing G-invariant lattices in $K[G]$-modules and reducing from O_K to k.

The arrows 'e' and 'd' give us matrices D_1 and D_2 respectively with respect to obvious bases on their sources and targets, resulting in a factorization $C = D_1 D_2$. One then shows that the above maps satisfy a certain 'adjointness' relation that allows one to show that $D_1 = {}^tD_2$, so that C is a product of the form ${}^tDD$ (with $D = D_2$), and hence symmetric.

1.11 Example: mod-p-representations of $SL_2(\mathbb{F}_p)$.

Exercise 1.11.1. Show that the number of p-regular conjugacy classes in $SL_2(\mathbb{F}_p)$ is exactly p.
Hint: Think in terms of eigenvalues; how many conjugacy classes can correspond to a given pair (λ, λ^{-1}) of eigenvalues?

Therefore, we should have p irreducible representations of $SL_2(\mathbb{F}_p)$ up to isomorphism (by Theorem 1.7.2), if $k = \bar{k}$. Even without assuming $k = \bar{k}$, these turn out to be given by $V_1, \ldots, V_p$, where for $1 \leqslant i \leqslant p$, V_i is a certain i-dimensional irreducible representation of $SL_2(\mathbb{F}_p)$ described as follows.

V_i can be described as the i-dimensional vector space consisting of homogeneous polynomials in $k[x, y]$ of degree $i - 1$, where $g \in SL_2(\mathbb{F}_p)$ acts on a polynomial function f by:

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f\right)(x, y) = f(ax + cy, bx + dy).$$

For those who know what symmetric powers are, here is another description. V_1 is the space k^2, thought of as 2×1 column matrices, on which $SL_2(\mathbb{F}_p)$ acts by matrix multiplication from the left (this makes sense because $\mathbb{F}_p \subset k$). This representation is called the standard representation of $SL_2(\mathbb{F}_p)$. For $1 \leqslant i \leqslant p$, the representation V_i is then the $(i - 1)$-st symmetric power of V_1 (the action of each $g \in SL_2(\mathbb{F}_p)$ on V_1 also induces an action of g on each symmetric power of V_1).

Proving that $V_1, \dots, V_p$ are irreducible is not difficult, but it is not 'obvious' either. The proof of this irreducibility may be said to involve an adapation of considerations from 'highest weight theory' for finite dimensional lie algebras over, say, $\mathbb{C}$. Of the representations $V_1, \dots, V_p$, one can show that only one is projective, namely, V_p. One knows a description of projective indecomposable covers for each V_i, $1 \leqslant i \leqslant p-1$, but we will not go into it; a reference is Alperin's 'Local Representation Theory'.

Lecture 2 - Friday, December 13

2.1 Product decompositions of rings and central idempotents. We would like to discuss the notion of blocks for the representations of G, or equivalently for modules over $k[G]$.

This basically amounts to the following: if $A = A_1 \times A_2 \times \cdots \times A_n$ is a product of rings, we can study A-modules by separately studying modules over $A_1, \dots, A_n$ (as we will see below). Much of this subsection will be discussed using very simple exercises - please read through them even if you do not work out every detail, since we will need them in the subsequent sections.

Let A be a ring. Suppose we know that A decomposes as a product $A_1 \times A_2$ of rings A_1 and A_2 (where the addition and multiplication in $A_1 \times A_2$ are defined component-wise).

Let $e_1 = (1,0) \in A_1 \times A_2 = A$ and $e_2 = (0,1) \in A_1 \times A_2 = A$.

Exercise 2.1.1. Note/prove the following:

- e_1, e_2 are central idempotents in A, and thanks to this centrality, $I_1 := Ae_1$ and $I_2 := Ae_2$ are two-sided ideals of A. Further, we have an isomorphism $A \cong Ae_1 \oplus Ae_2$ (isomorphism as left A-modules).
- We have isomorphisms of rings $A/I_2 \cong A_1$ and $A/I_1 \cong A_2$, given by the 'projection' maps $(x,y)+I_2 \mapsto x$ and $(x,y)+I_1 \mapsto y$, respectively.

Exercise 2.1.2. (i) Conversely, given central idempotents $e_1, e_2 \in A$ with $e_1 + e_2 = 1$, show that the addition and multiplication inherited by $A_1 := Ae_1$ and $A_2 := Ae_2$ from A make them into rings with multiplicative identities e_1 and e_2 respectively, and that the map $A \to A_1 \times A_2$ given by $a \mapsto (ae_1, ae_2)$ is an isomorphism of rings.

(ii) Given a decomposition $A = I_1 \oplus I_2$ of the left A-module A as a direct sum of two left A-submodules, where $I_1, I_2 \subset A$ are left ideals (equivalently, left A-submodules of A), write $1 = e_1 + e_2$ according to this decomposition. Assume further that I_1 and I_2 are two-sided ideals of A, and not just left ideals. Show that e_1 and e_2 are central idempotent elements of A, so that by (i) we have a decomposition $A \cong A_1 \times A_2$ of A as a product of rings.
Hint: $(e_1+e_2)^2 = e_1^2 + e_2^2 + e_1e_2 + e_2e_1$. Note that $e_1e_2, e_2e_1 \in I_1 \cap I_2 = \{0\}$, so $1 = e_1^2 + e_2^2$ is again a decomposition of 1 according to $A = I_1 \oplus I_2$, forcing $e_1^2 = e_1$ and $e_2^2 = e_2$.

Note: Henceforth, we will often drop 'left' for simplicity: an 'A-module' will mean a left A-module, an 'ideal' of A will mean a left ideal of A, a two-sided ideal of A will be qualified with 'two-sided' etc.

Exercise 2.1.3. Prove the following:

(i) Any A_1-module M_1 can be thought of as an A-module annihilated by I_2, because $A_1 \cong A/I_2$ is a quotient of A. This way, A_1 modules can be thought of as precisely the A-modules annihilated by I_2. Similarly, A_2-modules are precisely the A-modules annihilated by I_1.

(ii) Given an A-module M, we can uniquely write $M = M_1 \oplus M_2$, where $M_1 \subset M$ is an A-submodule annihilated by I_2, and $M_2 \subset M$ is an A-submodule annihilated by I_1 (take M_i to be the A-submodule of M consisting of all elements annihilated by I_{3-i}). Thus, M_1 is an A_1-module thought of as an A-module, and M_2 is an A_2-module thought of as an A-module.

(iii) Every map $\varphi : M \to N$ of A-modules respects the decomposition of (ii) - i.e., if we write $M = M_1 \oplus M_2$ and $N = N_1 \oplus N_2$ as above, then $\varphi(M_1) \subset N_1$, and $\varphi(M_2) \subset N_2$.

(iv) A module M of finite length over A is annihilated by I_2 (i.e., is an A_1-module thought of as an A-module) if and only if every composition factor of M is annihilated by I_2, and a similar statement applies to I_1 and A_2 in place of I_2 and A_1.

For those who are familiar with the language of categories and functors, the upshot is that the category of A-modules can be thought of as a product of the category of A_1-modules and the category of A_2-modules. Thus, to study A-modules, it is enough to separately study A_1-modules and A_2-modules.

Now the same could be done with decompositions of A into a product of n rings as opposed to two rings:

Exercise 2.1.4. Let $n \in \mathbb{N}$. Generalize and extend the considerations of and preceding Exercise 2.1.2 by establishing bijections between the following three kinds of objects:

(i) Decompositions $A = I_1 \oplus \cdots \oplus I_n$ of A into a direct sum of n two-sided ideals;

(ii) Expressions $1 = e_1 + \cdots + e_n$ of $1 \in A$ into a sum of n central idemopotents $e_1, \ldots, e_n$; and

(iii) Expressions $A \cong A_1 \times \cdots \times A_n$ of the ring A as a product of n rings (up to a suitable notion of equivalence).

In each case, be clear on up to what equivalence you are considering the decompositions.

Exercise 2.1.5. Generalize the considerations of Exercise 2.1.3 to the case of decompositions $A = A_1 \times \cdots \times A_n$ of A into a product of n rings, so that studying left modules over A reduces to separately studying left modules over the possibly much smaller rings $A_1, \ldots, A_n$.

2.2 The definition and some first properties of blocks. How do we apply this to the ring $A := k[G]$? First, there may be several decompositions of $k[G]$ into a product of rings (or equivalently a direct sum of two-sided ideals), so we need to find a 'canonical' choice of decomposition (else different people will work with different decompositions and that will result in confusion). In other words, we want a unique decomposition instead of an arbitrary decomposition.

This is done by the following easy exercise, which says that one gets such a decomposition by decomposing A into 'as many factors as possible', or even by 'keeping on decomposing A into a product of factors until one cannot go any further':

Exercise 2.2.1. Let $A = k[G]$. If $A = I_1 \oplus \cdots \oplus I_n$ and $A = I'_1 \oplus \cdots \oplus I'_r$ are two decompositions of A into two-sided ideals, such that no I_i or I'_j is a direct sum of smaller two-sided ideals of A, then show that $n = r$, and that the multi-sets $\{I_1, \ldots, I_n\}$ and $\{I'_1, \ldots, I'_r\}$ are equal (i.e., $\exists$ a permutation $\sigma \in S_n = S_r$ such that $I_i = I'_{\sigma(i)}$ inside A for each i).

By applying Exercise 2.1.4 together with the above exercise, one gets a suitably canonical decomposition of $k[G]$ into a product $A_1 \times \cdots \times A_n$ of rings, such that none of the rings $A_1, \ldots, A_n$ can be decomposed into a product of smaller rings.

By Exercise 2.1.5, studying modules over $k[G]$ is equivalent to separately studying modules over $A_1, \ldots, A_n$.

The term 'block' or a 'block of A' is used for either of the following two things (and informally also for related constructs):

- Any one A_i from among the factor rings $A_1, \ldots, A_n$ occurring in the above decomposition of $k[G]$ into a product of rings that cannot be decomposed any further; and
- For any fixed A_i as above, the collection of modules over A_i, thought of as modules over A via the surjection $A \to A_i$ arising as a projection from the product decomposition $A = A_1 \times \cdots \times A_n$. Any module belonging this collection will be referred to as 'belonging to this block'

Thus, to say that studying A-modules reduces to separately studying modules over the A_i, becomes in this language the assertion that to study modules over A, it is enough to separately study blocks of A.

For instance, to study how the indecomposable A-modules look like, one asks how indecomposable modules over or in any given block of A look like.

Remark 2.2.2. A decomposition $k[G] = \bigoplus c_i P_i$ of $k[G]$ into indecomposable projective modules is its decomposition into a direct sum of left ideals, where as the block decomposition involves decomposition into two-sided ideals. Thus, one would typically expect one block to contain multiple indecomposable projectives, as seen in the example of S_3 when $p = 3$, discussed below.

Example 2.2.3. In Examples 1.7.3 and 1.10.3 of Lecture 1, we saw that S_3 has two simple modules up to isomorphism, and hence two indecomposable projective modules up to isomorphism. But both these belong to the same block, as each indecomposable projective module was seen to have both the non-isomorphic simple modules as composition factors. Therefore, we conclude that S_3 has only one block.

One advantage of the notion of blocks - apart from that a block consists of modules over a smaller ring and hence is typically simper to describe (e.g., one can often find a concrete description of the collection of indecomposable modules over a given block) - is that often it is blocks that get transferred to a bigger group from a smaller group.

Thus, for instance, it turns out that $SL_2(\mathbb{F}_p)$ has three blocks (to be discussed later), and only two of these will be accounted for by a correspondence (called the Brauer correspondence) from blocks for the subgroup B of $\mathrm{SL}_2(\mathbb{F}_p)$ consisting of the upper triangular matrices of $SL_2(\mathbb{F}_p)$.

Remark 2.2.4. Another way to think of blocks involves thinking of $k[G]$ as a $k[G \times G]$-module. Recall the regular representation of $G \times G$ on $k[G]$ given by $(g_1, g_2)(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g \cdot (g_1 g g_2^{-1})$ (i.e., $(g_1, g_2) \in G \times G$ acts by left multiplication by g_1 together with right multiplication by g_2^{-1}). This being a representation of $G \times G$ turns $k[G]$ into a $k[G \times G]$-module. It is immediate that the two-sided ideals in $k[G]$ are precisely the $k[G \times G]$-submodules of $k[G]$. Thus, decompositions of $k[G]$ as direct sums of two-sided ideals which cannot be decomposed further are the same as the decompositions of $k[G]$ into indecomposable $k[G \times G]$-modules. In other words, blocks can also be thought of as the indecomposable components of the $k[G \times G]$-module $k[G]$ in the sense of Theorem 1.8.2 (though in this case they are defined on the nose and not just up to isomorphism).

When do two simple modules belong to the same block? The following remark gives a simple sufficient condition, explaining that any two Jordan-Holder factors of an indecomposable module belong to the same block.

Remark 2.2.5. Not every module belongs to a block, but every module is uniquely a direct sum of submodules each belonging to a block. It follows that every indecomposable module has to belong to some block. On the other hand, part of Exercise 2.1.5, namely the part that generalizes Exercise 2.1.3(iv), says in particular that a finitely generated $k[G]$-module M belongs to a particular block if and only each of its composition factors do. We conclude that any two composition factors of an indecomposable module belong to the same block.

Unfortunately, the converse is not true: ‘belonging to the same block’ is an equivalence relation, but it turns out that ‘being composition factors of a common indecomposable module’ is not - the latter relation is not transitive. The following proposition tells us how to ‘fix’ this (namely, by taking the transitive closure of the latter relation): while two simple modules belonging to the same block may not be composition factors of a common indecomposable module, one can pass from one of them to another through a chain of simple modules, any two successive elements of which are composition factors of a common indecomposable module (the proposition gives two stronger versions of this).

Proposition 2.2.6. *Let S, T be simple $k[G]$-modules. Then the following are equivalent:*

(i) S, T lie in the same block;

(ii) There exist simple modules $S = S_1, \ldots, S_m = T$ such that for each $1 \leqslant i \leqslant m-1$, there exists an indecomposable projective $k[G]$-module having both S_i and S_{i+1} as composition factors; and

(iii) There exist simple A-modules $S = T_1, \dots, T_n = T$ such that for $1 \leqslant i \leqslant n-1$, there exists a nonsplit extension between one of T_i, T_{i+1} and the other: in other words, there exists a module M, not isomorphic to $T_i \oplus T_{i+1}$ (this is the meaning of 'non-split') such that either $T_i \subset M$ and $M/T_i \cong T_{i+1}$, or $T_{i+1} \subset M$ and $M/T_{i+1} \cong T_i$.

For the proof of this proposition and that of various results that are going to be quoted, a reference is Chapter IV of the book 'Local Representation Theory' by Alperin.

Note that (ii) and (iii) are sufficient conditions by Remark 2.2.5, so the main difficulty, if it can be called so, is to show that they are also necessary, i.e., implied by (i).

2.3 Review of induced representations. (This subsection was assumed, and not discussed, in the lecture).

We would like to transfer representations between two groups, so let us review two 'standard' ways to do so. Let $H \subset G$ be a subgroup of our finite group G.

Given a $k[G]$-module V, there is an obvious way to get a $k[H]$-module - since H is a subgroup of G, we can restrict the action of G on V to H. In other words, $k[H]$ is naturally a subring of $k[G]$, and every $k[G]$-module V can be thought of as a module over the smaller ring $k[H]$. This representation is called the representation of H obtained from V by *restriction from G to H*, and will be denoted $V|_H$.

Given a $k[H]$-module U, there is a slightly less obvious way to get a $k[G]$-module from it. Namely, one can define the k-vector space:

$$U^G := \{f : G \to U \mid f(hg) = h \cdot f(g) \, \forall \, h \in H\}.$$

We can then upgrade U^G from a k-vector space to a $k[G]$-module, i.e., to a representation of G, by making $g_0 \in G$ act on $f \in U^G$ by requiring that for all $g \in G$:

$$(g_0 \cdot f)(g) = f(gg_0) \in U$$

- check that this indeed defines a representation of G.

The $k[G]$-module U^G is called the *representation of G or the $k[G]$-module obtained by inducing U from H to G*. This process of obtaining U^G from U is called *induction of representations*. Common sense modifications of this terminology will be resorted to: e.g., will refer to U^G as an 'induced module' etc.

(Alperin's book typically uses U for a module for a bigger group and V for a related module for a smaller group; I apologize for getting these switched, but hope these changed conventions hardly matter).

The above definition might look a bit artificial unlike the previous 'restriction' $V \mapsto V|_H$, and it is probably more natural to think of the $k[G]$-module U^G in terms of two of its properties that relate it to the restriction $V \mapsto V|_H$ discussed above, that we are going to recall.

To do this, first note that there are k-linear maps:

$$\epsilon : U \to U^G \qquad \text{and } \delta : U^G \to U,$$

where for all $u \in U$, $\epsilon(u) \in U^G$ is the map $G \to U$ given by:

$$\epsilon(u)(g) = \begin{cases} g \cdot u, & \text{if } g \in H, \text{ so that } g \cdot u \text{ is defined; and} \\ 0, & \text{otherwise} \end{cases},$$

and, for all $f \in U^G$, $\delta(f)$ is defined to be the element $f(1) \in U$.

Note that ϵ and δ are not just k-linear, but actually maps of $k[H]$-modules (where U^G is thought of as a $k[H]$-module via restriction), though of course they cannot be maps of $k[G]$-modules since U is only a $k[H]$-module and not a $k[G]$-module.

The following result, called Frobenius reciprocity, are the two properties referred to above as relating induction to restriction:

Proposition 2.3.1. *Let U be a $k[H]$-module, and V a $k[G]$-module.*

(i) The map

$$\text{Hom}_{k[G]}(U^G, V) \to Hom_{k[H]}(U, V|_H)$$

given by precomposition with ϵ (i.e., by the prescription $T \mapsto T \circ \epsilon$) is an isomorphism of k-vector spaces.

(ii) The map

$$\text{Hom}_{k[G]}(V, U^G) \to \text{Hom}_{k[H]}(V|_H, U)$$

given by post-composition with δ (i.e., by the prescription $T \mapsto \delta \circ T$) is an isomorphism of k-vector spaces.

For those who are familiar with the language of categories and functors, (i) of this proposition says that induction is a left-adjoint functor to restriction, and (ii) of this proposition says that restriction is a left-adjoint functor to induction.

2.4 The easy case of the Green correspondence. As mentioned in Lecture 1 (see Exercise 1.6.3), since we are working over 'bad characteristic', i.e., $(p, \#G) \neq 1$, just knowing the Jordan-Holder factors of a finite length $k[G]$-module M does not allow us to reconstruct M up to isomorphism.

However, we also know that a finite length $k[G]$-module M decomposes as a direct sum of indecomposable modules, so if we know how to describe all indecomposable modules over $k[G]$, then we can construct every finite length $k[G]$-module up to isomorphism. But this is much harder than describing all simple modules over $k[G]$ - for instance, as mentioned last time, even for an easy group like $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, there are infinitely many indecomposable $k[G]$-modules (i.e., indecomposable representations of G) up to isomorphism.

However, in many situations, it turns out to be possible to study some of the indecomposable representations of a group G in terms of indecomposable representations of a subgroup L. A result of this nature is the Green correspondence. In this subsection, we state the Green correspondence in an especially easy case: namely, in the case where, for a p-Sylow subgroup $P \subset G$, we have that for every $x \in G$, $xPx^{-1} \cap P$ equals either the whole of P or the trivial group. Note that this is equivalent to requiring that the intersection of any two distinct p-Sylow subgroups of G is the trivial group $\{1\}$.

(Warning: the next two paragraphs are redundant, and have been put in simply to explain the theorem using more 'English' rather than Mathematics).

Let L be the normalizer of the p-Sylow subgroup $P \subset G$. The Green correspondence then gives a bijection

$$\left\{ \begin{array}{c} \text{Isomorphism classes of} \\ \text{non-projective indecomposable} \\ k[G]\text{-modules} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Isomorphism classes of} \\ \text{non-projective indecomposable} \\ k[L]\text{-modules} \end{array} \right\} \tag{2}$$

- the forward direction (from G to L) is given by (i) of Theorem 2.4.1 below, the reverse direction from L to G is given by (ii) of the same theorem.

The idea behind defining such a correspondence is as follows:

- If V is an indecomposable $k[G]$-module, an obvious way to get a $k[L]$-module is to restrict the G-representation V to L to get a representation $V|_L$ of L. The problem is that $V|_L$ may not be indecomposable.
- If U is an indecomposable $k[L]$-module, an obvious way to get a $k[G]$-module is to induce the L-representation U to G to get a representation U^G of L. The problem is that U^G may not be indecomposable.

In the Green correspondence, one shows (in our easy case of trivial intersections of Sylow subgroups) that though $V|_L$ is not indecomposable, its 'Krull-Schmidt' decomposition into indecomposable $k[G]$-modules has a unique non-projective component, which may be taken to be the indecomposable $k[L]$-module $U(V)$ associated to V. A similar comment applied to the second bullet point above gives an indecomposable $k[G]$-module $V(U)$ associated to U.

So here is the formal statement of the Green correspondence in the easy case we are currently considering.

Theorem 2.4.1. *Assume that the intersection of any two distinct p-Sylow subgroups of G is the trivial group. Let $P \subset G$ be a p-Sylow subgroup, and L its normalizer. Then:*

(i) Given an indecomposable $k[G]$-module V, the $k[L]$-module $V|_L$ can be written as a direct sum $V|_L = U(V) \bigoplus X$, where $U(V)$ is a non-projective indecomposable $k[L]$-module and X is a projective (possibly decomposable) $k[L]$-module: note that $U(V)$ and X are unique up to isomorphism by the Krull-Schmidt theorem (Theorem 1.8.2).

(ii) Given an indecomposable $k[L]$-module U, the $k[G]$-module U^G obtained by inducing U from L to G can be written as a direct sum $U^G = V(U) \bigoplus Y$, where $V(U)$ is a non-projective indecomposable

$k[G]$-module, and Y is a projective (possibly decomposable) $k[G]$-module: note that $V(U)$ and Y are unique up to isomorphism by the Krull-Schmidt theorem.

(iii) There exists a bijection

$$\left\{ \begin{array}{c} \textit{Isomorphism classes of} \\ \textit{non-projective indecomposable} \\ k[G]\textit{-modules} \end{array} \right\} \to \left\{ \begin{array}{c} \textit{Isomorphism classes of} \\ \textit{non-projective indecomposable} \\ k[L]\textit{-modules} \end{array} \right\},$$

which takes a non-projective indecomposable $k[G]$-module V to the non-projective indecomposable $k[L]$-module $U(V)$ described in (i). Moreover, the inverse of this (obviously unique) bijection takes a non-projective indecomposable $k[L]$-module U to the non-projective indecomposable $k[G]$-module $V(U)$ described in (ii).

We will not comment on the proof of this theorem at all, except for remarking that it uses the theorem of Mackey on how the restriction of an induced representation decomposes - i.e., how the representation $(\sigma^{H_1})|_{H_2}$ of H_2 decomposes, where $H_1, H_2 \subset G$ are subgroups and σ is a representation of H_1.

Example 2.4.2. While the condition that the intersection of any two distinct p-Sylow subgroups of G be trivial is quite restrictive, there is a nice special case in which it is satisfied: namely, it is satisfied by $SL_2(\mathbb{F}_p)$, simply because every p-Sylow subgroup of that group has order p. Thus, in this case the Green correspondence gives a bijection between the isomorphism classes of non-projective indecomposable representations of $SL_2(\mathbb{F}_p)$ and those of the subgroup B of upper triangular matrices of $SL_2(\mathbb{F}_p)$ - it is left to the reader, if any, to check that B is indeed the normalizer of some p-Sylow subgroup of $SL_2(\mathbb{F}_p)$. Note that B is a semidirect product of $\mathbb{F}_p^\times$ with $\mathbb{F}_p$ and is solvable - barely a step away from being abelian - and is hence a much simpler group than $SL_2(\mathbb{F}_p)$. Thus, the set of indecomposable representations of B (up to isomorphism) is much easier to study.

For the general case of the Green correspondence (without requiring the intersection of distinct p-Sylow subgroups to be trivial), the statement of Theorem 2.4.1 needs to be modified: the bijection (2) needs to now take the form (informally speaking):

$$\left\{ \begin{array}{c} \text{Isomorphism classes of} \\ \text{`sufficiently non-projective'} \\ \text{indecomposable } k[G]\text{-modules} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Isomorphism classes of} \\ \text{`sufficiently non-projective'} \\ \text{indecomposable } k[L]\text{-modules} \end{array} \right\}. \tag{3}$$

But what does 'sufficiently non-projective' mean? To explain that, we need to introduce the notion of a 'vertex' for an indecomposable representation, which is a certain p-subgroup of G (or rather, a conjugacy class of p-subgroups of G) that gives an idea of how non-projective the representation is.

2.5 Relative projectivity, vertices and sources. In characteristic zero or when $(\#G, p) = 1$, it follows from the decomposition of the regular representation (the $k[G]$-module $k[G]$) that every simple $k[G]$-module is projective, so that by complete reducibility every $k[G]$-module of finite length is projective.

This is of course not true when $(\#G, p) \neq 1$, for otherwise every indecomposable module would be simple.

The non-projectivity of a $k[G]$-module W means, by definition, that a surjection $\varphi : V \twoheadrightarrow W$ of $k[G]$-modules may not have a $k[G]$-linear section, i.e., there may not exist a map $s : W \to V$ of $k[G]$-modules such that $\varphi \circ s$ equals the identity on W (of course, there will exist k-linear maps $s : W \to V$ such that $\varphi \circ s$ equals the identity on W, but one will in general not be able to choose such an s to be a map of $k[G]$-modules).

How do we measure this failure of projectivity? The failure of projectivity is due to $(\#G, p)$ being greater than one or equivalently, to G having a nontrivial p-Sylow subgroup P. Let us take a re-look at this:

If $\varphi : V \twoheadrightarrow W$ is a surjective map of $k[G]$-modules (in particular of $k[P]$-modules), then whenever φ has a $k[P]$-linear section $s' : W \to V$, we claim that it also has a $k[G]$-linear section $s : W \to V$. To see this, suppose that $s' : W \to V$ is $k[P]$-linear section, so that $s'(w) = p^{-1}(s'(p \cdot w))$ for all $w \in W$ and $p \in P$. Thus, if $g \in G$ and $w \in W$, $g^{-1}(s'(g \cdot w))$ depends only on the image $\dot{g}$ of g in $P\backslash G$, so we may denote it by $\dot{g}^{-1}s'\dot{g}(w)$. Now, define $s : W \to V$ by:

$$s(w) = \frac{1}{\#(G/P)} \sum_{\dot{g} \in P\backslash G} \dot{g}^{-1} s \dot{g}(w),$$

where this formula makes sense because $\#(P\backslash G)$ is relatively prime to p and hence invertible in k. I leave it to you to check that $s : W \to V$ is a section of $k[G]$-modules. Note that this argument is an adaptation of one of the two usual proofs of complete reducibility in characteristic zero.

The above paragraph can be informally summarized as saying that "any failure of projectivity already manifests at the level of a p-Sylow subgroup $P \subset G$". In other words, $k[G]$-modules may not be projective, but they are always 'relatively P-projective' in the sense of the following definition:

Definition 2.5.1. Let $H \subset G$ be a subgroup. Then a $k[G]$-module W is said to be *relatively H-projective* if any surjection $\varphi : V \twoheadrightarrow W$ that admits a $k[H]$-linear section, also admits a $k[G]$-linear section (i.e., "any obstruction to projectivity manifests at the level of the subgroup H").

Example 2.5.2. (i) If $H \subset G$ is a p-Sylow subgroup, we just saw that every $k[G]$-module is relatively H-projective (it is immediate that the same argument also works if H is only required to contain a p-Sylow subgroup).

(ii) On the other hand, if H is the trivial group, it follows from definition that a $k[G]$-module is relatively H-projective if and only if it is projective. Thus, the notion of projectivity is a special case of the notion of relative projectivity.

Just as with the usual notion of projectivity, there are many equivalent characterizations of relative H-projectivity. One of them is as follows:

Lemma 2.5.3. *A $k[G]$-module V is relatively H-projective if and only if it is a direct summand of a module of the form U^G, where U is an H-module.*

To see how this generalizes the usual notion of projectivity, we simply need to observe that when $H = \{1\}$ is the trivial group, U^G is isomorphic to the free module $k[G]^n$, where $n = \dim_k U$.

Note that, roughly speaking, 'the larger H is, the easier it is to be relatively H-projective'. For instance, clearly, a relatively H-projective module is also relatively H'-projective for any subgroup H' of G that contains H. In other words, we would like to think of a measure of the non-projectivity of an indecomposable representation of G as the 'smallest' p-group H contained in G such that the representation is relatively H-projective, assuming that such an H exists and is unique for that property (so that it is well-defined). But it is easy to see that such an H cannot possibly be unique: if H and H' are conjugate by an element of G, an indecomposable representation of G is relatively H-projective if and only if it is relatively H'-projective. But one might hope for such an H to exist and be well-defined up to conjugacy: the following theorem says that this can indeed be done.

Theorem 2.5.4. *Let V be an indecomposable $k[G]$-module. Then:*

(i) There exists a p-subgroup $Q \subset G$ (by this we mean that Q is a subgroup of G which is a p-group), unique up to conjugacy, such that given any subgroup $H \subset G$, V is relatively H-projective if and only if H contains a conjugate of Q.

(ii) Given a subgroup $Q \subset G$ as in (i), there exists an indecomposable representation U of Q, unique up to conjugacy by the normalizer $N_G(Q)$ of Q in G, such that V is a direct summand of U^G. [2]

Definition 2.5.5. Given any indecomposable $k[G]$-module V, a p-subgroup Q as in the above theorem, which is unique up to conjugacy, is called a *vertex of V*. A representation σ as in the above theorem is called a *source of V*.

It is this p-subgroup Q of G (well-defined up to conjugacy) that we would like to think of as a measure of the non-projectivity of the indecomposable $k[G]$-module V. The larger the vertex of an indecomposable module is, the less projective it is.

Thanks to this notion of vertex, we can now state the Green correspondence - please note how the statement of the following theorem generalizes (2) and makes (3) precise, and how it generalizes Theorem 2.4.1.

Theorem 2.5.6. *Let Q be a p-subgroup of G, and L a subgroup of G that contains the normalizer $N_G(Q)$ of Q in G. Then:*

(i) For any $k[G]$-module V, the $k[L]$-module $V|_L$ has a unique indecomposable summand $U(V)$ that has a vertex contained in Q [3] *but does not have a vertex contained in any $sQs^{-1} \cap Q$, $s \in G \backslash L$;*

---

[2] i.e., if the representation U is given as $\sigma : Q \to GL_k(U)$, and if the representation σ' of Q too satisfies the same property, then there exists $x \in N_G(Q)$ such that σ' is isomorphic to the representation $Q \to GL_k(U)$ defined by $g \mapsto \sigma(x^{-1}gx)$.

[3] One should either require this containment in Q and the analogous one in (ii), or assume that Q is p-Sylow; in the lecture I meant to do the latter, but might have the glaring omission of avoiding both in the lecture.

in fact, $V|_L = U(V) \bigoplus X$ *for a* $k[G]$*-module* X *each of whose indecomposable components has a vertex contained in* $sQs^{-1} \cap L$*, for some* $s \in G \backslash L$ *(*X *is 'relatively more projective than* $U(V)$*').* [4]

(ii) For any $k[L]$*-module* U*, the* $k[G]$*-module* U^G *has a unique indecomposable summand* $V(U)$ *that has a vertex contained in* Q *but does not have a vertex contained in any* $sQs^{-1} \cap Q$*,* $s \in G \backslash L$*; in fact,* $U^G = V(U) \bigoplus Y$ *for a* $k[G]$*-module* Y *each of whose indecomposable components has a vertex contained in* $sQs^{-1} \cap Q$ *for some* $s \in G \backslash L$ *(thus,* Y *is 'relatively more projective than* $V(U)$*').*

(iii) The map of (i) sending V *to* $U(V)$ *gives a bijection*

$$\left\{ \begin{array}{c} \textit{Isomorphism classes of indecomposable} \\ k[G]\textit{-modules with a vertex which is contained in } Q \\ \textit{but is not } G\textit{-conjugate to any } sQs^{-1} \cap Q,\ s \in G \backslash L \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \textit{Isomorphism classes of indecomposable} \\ k[L]\textit{-modules with a vertex which is contained in } Q \\ \textit{but is not } G\textit{-conjugate to any } sQs^{-1} \cap Q,\ s \in G \backslash L \end{array} \right\},$$

whose inverse is the map $U \mapsto V(U)$ *of (ii).*

(iv) The bijection of (iii) preserves vertices: i.e., V *and* $U(V)$ *have the same vertex for every* $k[G]$*-module* V *(and hence so also do* U *and* $V(U)$ *for every* $k[L]$*-module* U*).*

2.6 Defect groups. Thanks to the notion of vertices, we can now define the notion of a defect group of a block. Just as a vertex of an indecomposable module is a p-subgroup of G that measures its non-projectivity, the defect group of a block of G is a p-subgroup that measures how far non-projective the indecomposable modules belonging to the block can get. The formal definition will need the following theorem, where we denote by $\Delta : G \to G \times G$ the 'diagonal' map given by $g \mapsto (g, g)$:

Theorem 2.6.1. *If* B *is a block of* $k[G]$*, thought of as an indecomposable* $k[G \times G]$*-module as in Remark 2.2.4, then it has a vertex of the form* $\Delta(D) \subset G \times G$*, for a* p*-subgroup* D *of* G*.*

Definition 2.6.2. Given a block B of G, a subgroup D as in the above theorem is called a *defect group* of the block B. It is immediately verified that a defect group D of B is unique up to G-conjugacy, thanks to the uniqueness of $\Delta(D)$ up to $G \times G$-conjugacy. The cardinality of any defect group of B is called the *defect* of the block B (in the lecture, I erroneously used the term 'defect' for 'defect group').

Remark 2.6.3. The assertion that the $k[G \times G]$-module B has a vertex contained in $\Delta(G)$ follows once we show that B is relatively $\Delta(G)$-projective; this is an easy consequence of identifying $k[G]$ with $k[(G \times G)/\Delta(G)]$ as a $G \times G$-module - this identification can be done because $(G \times G)/\Delta(G)$ can be identified (as a set) with G by $(g, h) \mapsto gh^{-1}$, and with this, the left-multiplication action of $G \times G$ on $(G \times G)/\Delta(G)$ gets transferred to the regular action $(g_1, g_2) \cdot g = g_1 g g_2^{-1}$ of $G \times G$ on G.

Example 2.6.4. (i) If $(\#G, p) = 1$ (or when k has characteristic zero), we know that every simple $k[G]$-module is projective. It is easy to see that the block containing this module does not contain any other simple $k[G]$-module (where 'other' means 'non-isomorphic') - e.g., note that the isotypic subspace of $k[G]$ corresponding to any irreducible representation of G is a two-sided ideal in this case. Thus, in this situation, there are as many blocks as there are irreducible representations of

[4]To see why the set of conditions on the vertices of $U(V)$ and the set of conditions on the indecomposable components of X are mutually exclusive, see Lemma 2 in Section 11 of Alperin's 'Local Representation Theory'.

G up to isomorphism. Since every indecomposable $G \times G$-module is simple and projective in this case (note that $(\#(G \times G), p) = 1$ as well), it follows that each block of G has defect zero.

(ii) If G is a p-group, then the trivial representation of G is the only irreducible representation of G up to isomorphism, so by Remark 2.2.5, there is only one block of $k[G]$-modules. It is easy to see that the entire group G is a defect group of this block.

Here is a statement of a relation between vertices and defect groups, - crudely speaking, a defect group for a block tightly bounds from above our measure of non-projectivity of the indecomposable modules in the block:

Proposition 2.6.5. *Let B be a block of G with a defect group D.*

(i) For every indecomposable $k[G]$-module V belonging to B, D contains a vertex of V.

(ii) There exists an indecomposable module in the block B which has D as a vertex.

Remark 2.6.6. For S_3 when $p = 3$, we saw in Example 2.2.3 that we have only one block. Its defect group, being a 3-group, can only be the trivial group or the unique 3-Sylow subgroup $A_3 \subset S_3$. Since not every S_3-module is projective, Proposition 2.6.5 tells us that A_3 is a defect group for this block.

2.7 The Brauer correspondence. I did not get time to discuss the Brauer correspondence in the lectures. I will copy some results from Chapter IV of Alperin's book below. While the Green correspondence transfers indecomposable modules from a smaller group to a bigger group, the Brauer correspondence transfers blocks (as opposed to individual representations) from a smaller group to a bigger group. First, one has the following:

Definition 2.7.1. Let $H \subset G$ be a subgroup, and b a block of H. If B is a block of G such that:

(i) Viewing B and b respectively as a $k[G \times G]$-module and a $k[H \times H]$-module, b is a direct summand of the restriction $B|_{H \times H}$; and

(ii) B is the only block of G satisfying the property of (i);

then we say that B corresponds to b, and write $B = b^G$.

To be sure, there is an 'if' in the above definition: given a block b of H, a block $B = b^G$ as above may not exist. But there are many situations in which b^G exists, as in the following lemma:

Lemma 2.7.2. *Let b be a block of the subgroup H of G. Let D be a defect group of b. If H contains the centralizer $C_G(D)$ of D in G, then b^G is defined.*

Note that the larger D becomes, the smaller $C_G(D)$ becomes, and hence it gets easier for H to contain $C_G(D)$. Thus, the blocks containing 'sufficiently non-projective representations' are those that can be transferred to G.

Now the theorem below, called *Brauer's First Main Theorem*, says that if H contains the normalizer $N_G(D) \supset C_G(D)$ of D in G, then this correspondence works better:

Theorem 2.7.3. *If $D \subset G$ is a p-subgroup and H is a subgroup of G containing the normalizer $N_G(D)$ of D in G, then the assignment $b \mapsto b^G$ defines a bijection*

$$\left\{ \begin{matrix} \text{blocks of } H \\ \text{with defect group } D \end{matrix} \right\} \leftrightarrow \left\{ \begin{matrix} \text{blocks of } G \\ \text{with defect group } D \end{matrix} \right\}.$$

Given the definition of $b \mapsto b^G$, which looks similar to the Green correspondence, one would obviously ask what its relation with the Green correspondence is - rather, one can ask if the Green correspondence is compatible in the obvious way (as in the following theorem) with the Brauer correspondence. The following theorem, called *Brauer's Second Main Theorem*, gives a result in this spirit:

Theorem 2.7.4. *Let $H \subset G$ be a subgroup, V an indecomposable $k[H]$-module and U an indecomposable $k[G]$-module. Assume that:*

- *Some vertex Q of V satisfies $C_G(Q) \subset H$; and*
- *U is a direct summand of $V|_H$ (a condition one sees in the Green correspondence).*

Then, denoting by b the block of H containing U, then the block b^G of G is well-defined and contains V.

The *principal block* of G is the block containing the trivial representation. There is a *Brauer's Third Main Theorem*, asserting that under certain circumstances, only a principal block can transfer to a principal block. We will skip even a precise statement of this result.

2.8 Blocks of $SL_2(\mathbb{F}_p)$. Let us study the blocks of of $G = SL_2(\mathbb{F}_p)$, where we now assume that p is odd. Recall the simple $k[G]$-modules $V_1, \ldots, V_p$ from Subsection 1.11. Of these, one can show that the simple module V_p is projective, and that its block in $SL_2(\mathbb{F}_p)$ consists of those representations all of whose Jordan-Holder factors are isomorphic to V_p - since V_p is projective, these are just direct sums of finitely many copies of V_p (we are only considering finite length representations).

So there is at least one more block for $SL_2(\mathbb{F}_p)$, one that contains some of $V_1, \ldots, V_{p-1}$. We claim that in fact there are at least two more - namely, we claim that for $1 \leqslant i, j \leqslant p-1$, V_i and V_j belong to distinct blocks if $i \not\equiv j \pmod 2$. This uses the simple idea called the central character of a representation.

A representation $\rho : G \to GL_k(V)$ of G is said to have central character $\chi : Z(G) \to k^\times$, where $Z(G) \subset G$ is the center of G, if $\rho(zg) = \chi(z)\rho(g)$ for all $z \in Z(G), g \in G$ (where $\chi(z)\rho(g) \in GL_k(V)$ refers to the composite of $\rho(g) \in GL_k(V)$ with scalar multiplication by $\chi(z) \in k^\times$). Schur's lemma immediately implies that every irreducible representation of G has a central character, if $k = \bar{k}$.

For our $G = SL_2(\mathbb{F}_p)$, we have $Z(G) = \{\pm 1\}$ - the identity matrix and the negative of it (we will continue to denote these as ± 1 rather than as their matrix forms).

- For $1 \leqslant i \leqslant p-1$, V_i has a central character χ_i, characterized by $\chi_i(-1) = (-1)^i$ - in particular, the central characters of V_i and V_j are different if $1 \leqslant i, j \leqslant p-1$ and $i \not\equiv j \pmod 2$.

- If two simple $k[G]$-modules have different central characters, they belong to different blocks - this is an easy consequence of the fact that for each $z \in Z(G)$, the linear operator $\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g (zg)$ commutes with the action of $G \times G$ (or equivalently with both left and right mutiplication of $k[G]$ on itself), and hence taking the common generalized eigenspaces of these commuting operators gives a decomposition of any two-sided ideal in $k[G]$ into smaller two-sided ideals.

Thus, we now have shown that there are at least three different blocks for G - the one containing V_p, at least one each corresponding to the collection $\{V_i \mid 1 \leqslant i \leqslant p-1, i \text{ odd}\}$, and at least one corresponding to the collection $\{V_i \mid 1 \leqslant i \leqslant p-1,\ i \text{ even}\}$.

It so turns out that there are exactly three blocks for G: in other words, if $1 \leqslant i, j \leqslant p-1$ and i, j are of the same parity, then it so turns out that V_i and V_j belong to the same block. For this, one can produce (and I am skipping the details) a non-split extension between V_i and V_{p-1-i} for each $1 \leqslant i < p-1$, and one between V_i and V_{p+1-i} for each $1 < i \leqslant p-1$. If I correctly understood and remember a discussion with Professor Dipendra Prasad, the nonsplit extensions between V_i and V_{p-1-i} $(1 \leqslant i < p-1)$ can also be obtained by reducing suitable characteristic zero cuspidal representations of $SL_2(\mathbb{F}_p)$ (having dimension $p-1$) modulo p, and the nonsplit extensions between V_i and V_{p+1-i} $(1 < i \leqslant p-1)$ can also be obtained by reducing suitable characteristic zero principal series representations of $SL_2(\mathbb{F}_p)$ (having dimenion $p+1$) modulo p. Results in this spirit can be found in Section 4 of his article mentioned earlier, namely http://www.math.iitb.ac.in/∼dprasad/dp-mod-p-2010.pdf

In any case, the existence of these extensions means that V_i and V_{p-1-i} are in the same block for $1 \leqslant i < p-1$, while V_i and V_{p+1-i} are in the same block for $1 < i \leqslant p-1$. Using this, one can show that V_i and V_j are in the same block if $1 \leqslant i, j \leqslant p-1$ and i, j are of the same parity.

Moreover, one can show that V_i is not projective if $1 \leqslant i \leqslant p-1$, so that each of the two blocks of $SL_2(\mathbb{F}_p)$ that do not contain V_p has a p-Sylow subgroup of $SL_2(\mathbb{F}_p)$ as its defect group.

2.9 The Brauer Correspondence for $SL_2(\mathbb{F}_p)$. We saw that there are three blocks for $SL_2(\mathbb{F}_p)$, and that only two of them have a non-trivial defect group, which we may and do choose to be the subgroup U of upper triangular matrices in $SL_2(\mathbb{F}_p)$ with the diagonal entries 1. Thus, one would like to see how these two blocks arise via the Brauer correspondence. We continue to assume that $p > 2$.

Thus, we need subgroups of $SL_2(\mathbb{F}_p)$ that contain the normalizer of our chosen defect group U of these blocks, namely, those that contain the subgroup B of upper triangular matrices in $SL_2(\mathbb{F}_p)$ (now the letter B will no longer stand for a block for G).

Let us look at what the blocks of B are. What are the simple $k[B]$-modules? Since every simple $k[B]$-module has a U-fixed vector (U being a p-group), the normality of U in B forces (as we have seen earlier) each simple $k[B]$-module to consist entirely of U-fixed vectors.

In other words, every irreducible representation of B factors through the quotient $B \twoheadrightarrow B/U$, and it is easy to check that the map $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto a$ factors to an isomorphism of groups $B/U \to \mathbb{F}_p^\times$.

Thus, the irreducible representations of B are obtained by pull back via $B \to B/U \cong \mathbb{F}_p^\times$ from the irreducible representations of $\mathbb{F}_p^\times$, which being a cyclic group of order $p-1$ (which is prime to p) has exactly $p-1$ homomorphisms $\mathbb{F}_p^\times \to k^\times = GL_1(k)$ as its irreducible representations.

What are these characters? Since k has characteristic p, we have $\mathbb{F}_p \hookrightarrow k$ as fields, so $\mathbb{F}_p^\times \hookrightarrow k^\times$ as groups. This inclusion $\theta : \mathbb{F}_p^\times \hookrightarrow k^\times = GL_1(k)$ is one irreducible representation. The fact that $\mathbb{F}_p^\times$ is cyclic then implies that $1, \theta, \theta^2, \dots, \theta^{p-1}$ are distinct homomorphisms $\mathbb{F}_p^\times \to k^\times = GL_1(k)$, so the irreducible representations of B are obtained by pulling these back to B under $B \to B/U \cong \mathbb{F}_p^\times$. Let us, by abuse of notation, denote the resulting characters $B \to k^\times = GL_1(k)$ also by $1 = \theta^0, \theta, \dots, \theta^{p-1}$. Thus:

$$\theta^i \left(\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \right) = a^i.$$

These are the irreducible representations of B, i.e., the simple $k[B]$-modules.

When are θ^i and θ^j in the same block? First, the same argument as with $SL_2(\mathbb{F}_p)$ tells us that for $1 \leqslant i, j \leqslant p-1$, θ^i and θ^j belong to different blocks of i and j are of different parity. Namely, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is central in B, and θ^i and θ^j take different values on this central element unless $i \equiv j$ modulo 2.

Now let us see that θ^i and θ^j will belong to the same block if $i \equiv j$ modulo 2. This is easy: a non-split extension between θ^i and θ^{i+2} is easily checked to be given by the representation:

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto \theta^{i+1} \left(\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \right) \cdot \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} a^{i+2} & a^{i+1}b \\ 0 & a^i \end{pmatrix}.$$

(In other words, all we have done is to note that the 'standard' representation of B given by the inclusion $B \hookrightarrow G = SL_2(\mathbb{F}_p) \hookrightarrow GL_2(k)$ is a non-split extension between θ and θ^{-1}, and to tensor it with θ^{i+1} to get a nonsplit extension between θ^{i+2} and θ^i).

Thus, B has two blocks - one consisting of the θ^i with i even, and another consisting of the θ^i with i odd. And $SL_2(\mathbb{F}_p)$ has exactly two blocks of nontrivial defect, each consisting of the V_i, $1 \leqslant i \leqslant p-1$, with a given parity.

So what is the Brauer correspondence from the two blocks of B to the two blocks of $SL_2(\mathbb{F}_p)$ with nontrivial defect? For this, by the Theorem 2.7.4, we need to merely find out the blocks of the direct summands of each $V_i|_B$.

It is easily verified that, for $1 \leqslant i \leqslant p-1$, the Jordan-Holder factors of $V_i|_B$ are $\theta^{i-1}, \theta^{i-3}, \dots, \theta^{-(i-1)}$. Clearly, all of these belong to the unique block of B containing θ^{i-1}.

Thus, for any $1 \leqslant i \leqslant p-1$, the unique block of $SL_2(\mathbb{F}_p)$ containing V_i arises by Brauer correspondence from the unique block of B containing θ^{i-1}.

Some material from the Tutorial on Friday, December 13

3.1 Blocks for S_4. You may recall that, during the tutorial on Friday, December 13, Professor Ghate suggested working out the blocks for S_4 when the characteristic of k is 3, and accordingly the tutor, Anand Chitrao, described them. So let us discuss it here. Assume that $p = 3$ and that $k = \bar{k}$.

3.1.1 The number of irreducible representations up to isomorphism. First, how many simple $k[S_4]$-modules are there up to isomorphism? We know that this is precisely the number of 3-regular conjugacy classes in S_4 (Theorem 1.7.2). Conjugacy classes in S_4 are determined by their cycle type, and hence representatives for conjugacy classes in S_4 can be taken to be $\{1, (1,2), (1,2)(3,4), (1,2,3), (1,2,3,4)\}$. Of these, all but $(1,2,3)$ are 3-regular, so there are four 3-regular conjugacy classes in S_4, and hence four irreducible representations of S_4 up to isomorphism.

3.1.2 The list of irreducible representations of S_4 up to isomorphism. Here are four irreducible representations of S_4:

(i) ρ_1, the trivial character of S_4, namely the map $S_4 \to k^\times = GL_1(k)$ taking the constant value 1.

(ii) ρ_2, the sign character of S_4, namely the unique nontrivial homomorphism $S_4 \to GL_1(k)$ which factors as:

$$\text{sgn} : S_4 \to S_4/A_4 \cong \{\pm 1\} \hookrightarrow k^\times = GL_1(k). \tag{4}$$

(iii) Each element of S_4 acts by permutation on the standard basis $\{e_1, e_2, e_3, e_4\}$ of k^4, and hence extends k-linearly to a vector space automorphism of k^4, resulting in a representation $S_4 \to GL_k(k^4) = GL_4(k)$. This representation is not irreducible, because it has an S_4-invariant subspace given by

$$V_{\text{std}} := \{a_1e_1 + a_2e_2 + a_3e_3 + a_4e_4 \mid a_1 + a_2 + a_3 + a_4 = 0\}. \tag{5}$$

This way, we get a representation $\rho_3 : S_4 \to GL_k(V_{\text{std}})$, which is three dimensional since V_{std} is three dimensional. This representation is called the standard representation of S_4. I leave it to you to check that this representation of S_4 is irreducible.

(iv) A fourth representation of S_4 is given by $\rho_4 : S_4 \to GL_k(V_{\text{std}})$, where V_{std} is the three dimensional vector space considered in (iii) above, given by $\rho_4(g) = \rho_3(g)\text{sgn}(g)$, where ρ_3 is as in (iii) and $\text{sgn}(g)$ is as in (4). It is immediate from the irreducibility of ρ_3 that ρ_4 is irreducible too.

However, to justify that we indeed have four pairwise nonisomorphic irreducible representations of S_4 at this point, we need to show that the representations ρ_3 and ρ_4 are not isomorphic, i.e., that there exists no $T \in GL_k(V_{\text{std}})$ such that $\rho_3(g) = T\rho_4(g)T^{-1}$ for all $g \in S_4$. This follows if we show that $\det \rho_3(g) \neq \det \rho_4(g)$ for some $g \in S_4$. However, note that for all $g \in S_4$:

$$\det \rho_4(g) = \det(\rho_3(g)\text{sgn}(g)) = (\det \rho_3(g))(\text{sgn}(g))^{\dim V_{\text{std}}} = (\det \rho_3(g)) \cdot \text{sgn}(g),$$

since $\dim V_{\text{std}}$ is odd and $\text{sgn}(g) \in \{\pm 1\}$. Thus, any $g \in S_4$ such that $\text{sgn}(g) = -1$ (i.e., any $g \in S_4 \backslash A_4$) will satisfy that $\det \rho_3(g) \neq \det \rho_4(g)$, as needed.

Thus, we have finished constructing the four simple $k[S_4]$-modules ρ_1, ρ_2, ρ_3 and ρ_4, where the first two are of dimension 1 each over k and the latter two are of dimension 3 each over k.

3.1.3 Some facts we will use. Here are two facts that will help us deal with problems such as determining projectivity of modules:

(i) *Checking projectivity after restricting to a Sylow subgroup.* A G-representation V is projective if the restriction $V|_H$ of V to a p-Sylow subgroup H is projective. This follows from Example 2.5.2(i), which tells us that a surjection $W \twoheadrightarrow V$ of $k[G]$-modules has a $k[G]$-linear section if and only if it has a $k[H]$-linear section, where $H \subset G$ is a p-Sylow subgroup. For S_4, we can use the 3-Sylow subgroup $A_3 \subset S_4$ that acts by three cycles on $\{1, 2, 3\}$ and fixes 4.

(ii) *Checking non-projectivity using a quotient.* Suppose the action of G on a representation V factors through a surjective group homomorphism $G \twoheadrightarrow G'$ - i.e., V is a representation of G', viewed as a representation of G via the surjective group homomorphism $G \twoheadrightarrow G'$. If V is non-projective as a $k[G']$-module, i.e., there is a surjection $W \to V$ of $k[G']$-modules without a $k[G']$-linear section, it is immediate that this is also a surjection of $k[G]$-modules without a $k[G]$-linear section, so that V is also non-projective as a $k[G]$-module. For our group $G = S_4$, we will use as the quotient $G \to G'$ a surjection $S_4 \to S_3$ that will be defined in Subsubsection 3.1.5 below.

3.1.4 ρ_3 and ρ_4 are projective. Let us show that the $k[S_4]$-modules ρ_3 and ρ_4 are projective, using (i) of Subsubsection 3.1.3.

As mentioned there, we consider the 3-Sylow subgroup of S_4 which is the copy of $A_3 \subset S_4$ (recall that we are considering $p = 3$) that fixes $4 \in \{1, 2, 3, 4\}$ and cyclically permutes $\{1, 2, 3\}$.

To show that ρ_3 is projective, by (i) of Subsubsection 3.1.3, it suffices to show that the restriction of ρ_3 to this subgroup A_3 is a projective $k[A_3]$-module. In fact, this subspace is even a free $k[A_3]$-module: I will leave it to you to check this; use that the space of ρ_3 is V_{std} (from (5)), which is isomorphic to k^3 by the isomorphism $(a_1, a_2, a_3, a_4) \mapsto (a_1, a_2, a_3)$ (because if $a_1e_1 + a_2e_2 + a_3e_3 + a_4e_4 \in V_{\text{std}}$, then $a_4 = -(a_1 + a_2 + a_3)$ is determined by a_1, a_2 and a_3).

Since $\rho_4|_{A_3} \cong \rho_3|_{A_3}$ (as sgn is trivial on A_3), it follows that ρ_4 is projective as a $k[A_3]$-module. By Subsubsection 3.1.3, it follows that ρ_4 is $k[S_4]$-projective as well.

3.1.5 A surjection $S_4 \to S_3$. However, it turns out that ρ_1 and ρ_2 are not $k[S_4]$-projective, and we will need to find projective covers for them.

The proof of non-projectivity and the construction of projective covers for ρ_1 and ρ_2 will use (ii) of Subsubsection 3.1.3, for which we need to construct a surjection $\tau : S_4 \to S_3$ (which is commonly seen in the characteristic zero representation theory of S_4 as well).

Such a surjection τ can be obtained as follows (I am explaining this at greater length than necessary to drive home the following point whose utility is perhaps not emphasized well in elementary courses on group theory). To get a homomorphism $S_4 \to S_n$ for some n, one simply needs to get S_4 act on an n-element set. There are several 'natural' sets with an action of S_4, such as the (set of) elements of $\{1, 2, 3, 4\}$, pairs of elements of $\{1, 2, 3, 4\}$, unordered pairs of distinct elements of $\{1, 2, 3, 4\}$, triples of elements of $\{1, 2, 3, 4\}$, elements or pairs of elements or triples of elements of S_4 (by left or right multiplication), conjugacy classes of S_4, Sylow subgroups of S_4, subgroups of S_4 of a fixed cardinality etc.

So we should look for a set of three elements 'naturally related to S_4 or to $\{1, 2, 3, 4\}$', and this can be found in the set of partitions of $\{1, 2, 3, 4\}$ into two disjoint sets of order two each:

$$\{1, 2, 3, 4\} = \{1, 2\} \cup \{3, 4\} = \{1, 3\} \cup \{2, 4\} = \{1, 4\} \cup \{2, 3\}.$$

Clearly S_4 acts by permutation on these, giving a homomorphism $\tau : S_4 \to S_3$. We claim that τ is surjective: for this, it suffices to check that any transposition in S_3 lies in the image of this homomorphism, something that is readily verified. Hence, as described earlier, the composite of any irreducible representation of S_3 with τ is an irreducible representation of S_4.

It will help to know the kernel of this surjection, which has order $(\#S_4)/(\#S_3) = 4$. I leave it to you to check that this kernel is the normal subgroup $N \subset S_3$ with elements $\{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$. Since N consists of elements of order dividing two, we have that $N \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3.1.6 Projective covers for ρ_1 and ρ_2. To study ρ_1 and ρ_2, we claim that they factor through the surjection $\tau : S_4 \to S_3$. This is immediate: N consists of even permutations, so both the trivial representation and the sign character are trivial on N. Now it is easy to see that ρ_1 and ρ_2 are obtained by viewing the trivial representation and the sign character of S_3, respectively, as S_4-representations via the surjection $\tau : S_4 \to S_3$.

In other words, if V_1 and V_2 denote the one-dimensional vector spaces hosting the trivial representation and sign character (respectively) of S_3, then we may view ρ_1 and ρ_2 as the representations of S_4 on V_1 and V_2, respectively, with S_4 acting through $\tau : S_4 \twoheadrightarrow S_3$ on V_1 and V_2.

To prove that neither V_1 nor V_2 is projective as a $k[S_4]$-module, by Subsubsection 3.1.3(ii), it suffices to show that V_1 and V_2 are not projective as $k[S_3]$-modules; but this follows from the fact that both the projective indecomposable modules of S_3 up to isomorphism have dimension 3 as a k-vector space (see Example 1.10.3).

This motivates a construction of projective covers for ρ_1 and ρ_2 as follows. Let P_1 be a projective cover of the trivial representation of S_3, and P_2 one of the sign character of S_3. Viewing P_1 and P_2 as S_4-representations via τ, the surjections $P_1 \to V_1$ and $P_2 \to V_2$ are also surjections of $k[S_4]$-modules. It is immediate that $P_1 \to V_1$ and $P_2 \to V_2$ are essential, because they are essential as maps of S_3-modules.

This doesn't yet prove that P_i is a projective cover of V_i for $i = 1, 2$, because it is not obvious that any projective S_3 module remains projective when viewed as an S_4-module via τ (e.g., if we considered a surjection to the trivial group instead of to S_3, an analogous assertion would not be true). Rather, we can use (i) of Subsubsection 3.1.3, which reduces us to checking that $P_1|_{A_3}$ and $P_2|_{A_3}$ are projective, where $A_3 \subset S_4$ is a 3-Sylow subgroup, which we choose as in Subsection 3.1.3(i). Now, via $\tau : S_4 \to S_3$, $A_3 \subset S_4$ maps isomorphically onto the unique 3-Sylow subgroup $\tau(A_3) \subset S_3$, so it is enough to show that $P_1|_{\tau(A_3)}$ and $P_2|_{\tau(A_3)}$ are projective.

But this is easy, as follows. The S_3-representations P_1 and P_2 are direct summands of $k[S_3]$, so $P_1|_{\tau(A_3)}$ and $P_2|_{\tau(A_3)}$ are direct summands of the $k[A_3]$-module $k[S_3]|_{\tau(A_3)}$, and you can check that $k[S_3]|_{\tau(A_3)} \cong k[\tau(A_3)] \oplus k[\tau(A_3)]$ (e.g., if $H \subset G$ is any subgroup, by writing G as the union of the cosets Hg, it is easy to see that $k[G]$ is isomorphic to $k[H]^{\#(H\backslash G)}$ as a left-$k[H]$-module, and is hence free).

3.1.7 Blocks for S_4, $p = 3$. Let P_3 and P_4 be the spaces on which ρ_3 and ρ_4 act (these can be identified with V_{std}). Therefore, P_3 and P_4 are projective indecomposable modules over $k[S_4]$, and for $i = 1, 2, 3, 4$, P_i is a projective cover of ρ_i.

Now P_3 and P_4 are both simple and projective, while the composition factors of P_1 and P_2 are ρ_1, ρ_2, ρ_1 and ρ_2, ρ_1, ρ_2 respectively (because this reduces to the description of indecomposable projective modules for S_3 when $p = 3$, see Example 1.10.3).

Therefore, by Proposition 2.2.6, it follows that P_1 and P_2 belong to the same block, while each of P_3 and P_4 constitutes the only simple module in the block containing it. In other words, there are three blocks for S_4 when $p = 3$ - one containing P_1 and P_2, one containing P_3, and one containing P_4.

The defect groups of these blocks are easy to compute. Any finitely generated module belonging to a block containing P_3 will have only P_3 among its Jordan-Holder factors, and since P_3 is projective, it follows from the Jordan-Holder theorem that these modules will all be direct sums of finitely many copies of P_3, and hence projective. Therefore, they all have the trivial group as their vertex. Thus, by Proposition 2.6.5, the defect group of this block is the trivial group. Exactly the same applies to P_4 to show that the defect group of the block containing P_4 is the trivial group.

On the other hand, since ρ_1 and ρ_2 are not projective, we see from Proposition 2.6.5 that neither P_1 nor P_2 can have the trivial group as its defect group. Since the defect group is always a 3-group, and since 3 is the largest power of 3 dividing $24 = \#S_4$, it follows that a defect group of the block containing P_1 (and therefore also P_2) is given by any copy of A_3 inside S_4.