August 25

References

1. (CR1) Curtis and Reiner: Methods of Representation Theory, I and II
2. (CR2) Curtis and Reiner: Representation Theory of Finite Groups and Associative Algebras
3. (DB) D. J. Benson, Representations and Cohomology I, pp. 1-19
4. (DF) Dummitt and Foote: Abstract Algebra

The modern approach to representation theory involves group-rings over certain rings, not necessarily fields. Let G be a finite group an R a commutative ring with 1.

Definition 1 *An R-algebra A is a ring such that there is a homomorphism $\psi : R \to Z(A)$ with $\psi(1) = 1$.*

Observe that if $R = K$ is a field, that is $K \subset Z(A)$ then A is a vector space over K and is also a ring. That is, A is an R-module as

$$ra = \psi(r)a, \ r \in R, a \in A$$

as well as a ring.

For arbitrary rings, the structure of A can be quite complicated.

Example 1 *The Group-ring RG is a free R-module with basis $\{g : g \in G\}$ (of finite rank since G is finite). That is,*

$$RG = \left\{ \sum_{x \in G} a_x x : a_x \in R \right\}$$

with multiplication inherited from the group operation.

If $R = K$ is a field, then KG is a group algebra.

Definition 2 *An R-subalgebra of A is an R-submodule plus a subring containing 1. A map $\psi : A \to B$ is an R-algebra homomorphism if it is a ring homomorphism and a R-module homomorphism ($\psi(ra) = r\psi(a)$).*

Definition 3 *A* representation of *A is a A-algebra homomorphism $\rho : A \to M_n(R)$, ($n \times n$ matrices over R) Similarly, a group homomorphsim $\rho : G \to GL(n, R)$, ($n \times n$ invertible matrices over R) is a* representation of *G over R.*

If $A = RG$, a representation ρ of G gives rise to a representation of A and conversely.

Definition 4 *Two representations ρ and ρ' of A (or G) are equivalent if there exists $T \in GL(n, R)$ such that $\rho(a) = T\rho'(a)T^{-1}$ for all $a \in A$, and similarly for G.*

Example 2 *Representations equivalent over $\mathbb{Q}$ but not over $\mathbb{Z}$ (check this) [CR, p.205]*

1. *$S_3 = \langle a, b : a^2 = b^2 = 1, a^{-1}ba = b^{-1}\rangle$ can be represented as*

$$\rho_1 : a \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} b \mapsto \begin{pmatrix} 0 & -1 \\ 0 & -1 \end{pmatrix}$$

$$\rho_2 : a \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} b \mapsto \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

2. *$D_8 = \langle a, b : a^2 = b^4 = (ab)^2 = 1\rangle$ can be represented as*

$$\rho_1 : a \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} b \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\rho_2 : a \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} b \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Definition 5 *Given $\rho : A \to M_n(R)$, we get an A-module M which is a free R-module of rank n as $a \cdot m = \rho(a)m$. We define* $\dim \rho = \text{rank } M = n$.

Conversely, given an A-module M (free over R, finite rank), if we pick an R-basis of M, we get a representation of ρ. Furthermore, ρ, ρ' are equivalent iff M, M' are isomorphic. (see DF, p. 812)

Definition 6 *An A-module M is* irreducible *or* simple *if the only submodules of M are M and $\{0\}$. M is* indecomposable *if we cannot write M as the direct sum of proper, non-zero submodules, i.e., $M = M_1 \oplus M_2$*

Now if $R = K$ is a field, M is irreducible (ρ is irreducible) means that we cannot find T with

$$T\rho(a)T^{-1} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

for all a. Similarly, ρ is indecomposable means we can't have

$$T\rho(a)T^{-1} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}.$$

Example 3 *$G = Z_2 \times Z_2 = \langle a, b : a^2 = b^2 = 1, ab = ba\rangle$. Consider representations over a field K of characteristic 2*

$$KG = K[x, y]/\left\langle (x-1)^2, (y-1)^2 \right\rangle$$

and note that in this case $(x-1)^2 = x^2 - 1$ and $(y-1)^2 = y^2 - 1$. If J is a $n \times n$ matrix in indecomposable rational canonical form

$$\rho : x \to \begin{pmatrix} I & I \\ 0 & I \end{pmatrix}$$

$$\rho : y \to \begin{pmatrix} I & J \\ 0 & I \end{pmatrix}$$

is a $2n$-dimensional indecomposible representation. So there are an infinite number of indecomposable representations over K. This is proved in Heller and Reiner, Illinois J. Math 5 (1961); we will a special case later.

Theorem 1 *If $p||G|$, K a field of characteristic p, then G has a finite number of indecomposable representations over K (up to equivalence) iff G has a cyclic Sylow-p subgroup. (D. G. Higman, Duke Math. J. 21 (1954))*

Then, given the hopelessness of enumerating such representations current research looks at $KG = \bigoplus_i M_i$, M_i indecomposable.

August 27

Aug 27

The R-algebra A is the basic object of study where R is commutative with 1, and the basic example we should have in mind is the group-ring $A = RG$, G a finite group. Normally, we want A to be free over R with finite rank. When we look at representations, this is the same as looking at A-modules or G-modules M. We study representations because matrices are more concrete than abstract groups; hence, we hope to obtain info about groups via representations.

Example 4 *$G = \langle a : a^p = 1\rangle$. By Higman's theorem, there is only a finite number of representations. Take K to be of characteristic p. Since $KG \cong K[x]/(x-1)^p$, the indecomposable representations of KG are given by*

$$\rho(a) = \begin{pmatrix} 1 & 1 & & \cdots & 0 & 0 \\ 0 & 1 & 1 & & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & & & 1 & 1 \\ 0 & 0 & & & & 1 \end{pmatrix} (r \times r)$$

where $1 \le r \le p$. We get precisely p indecomposable representations. A KG-module has the form

$$M = M_0 \supset M_1 \supset \cdots \supset M_r = \{0\}$$

where M_i are KG-submodules with $\dim M_i/M_{i+1} = 1$ so that M_i/M_{i+1} is a trivial KG-module, i.e. gives the representation $\rho(a) = 1$. This follows from the Jordan form.

Definition 7 *The* trivial *RG-module is R with $gr = r$ for all $r \in R, g \in G$.*

Proposition 1 *Let $|G| = p^n$ and $\mathrm{char}(K) = p$. Then the only irreducible KG-module is the trivial one.*

Proof. Let V be an irreducible KG-module. Let $H \le G$ be the kernel of the representation, that is,

$$H = \{x \in G : \rho(x) = I\}$$

If $H \neq 1$, consider G/H. We have $|G/H| < |G|$ and apply induction as follows. If W is a G/H module, W can be regarded as a KG-module by $g \cdot x = (gH) \cdot x$. This is well defined because the representation is trivial on H. W is irreducible as a G/H-module implies W is irreducible as a G-module also, and the result follows by induction.

Now suppose $H = 1$. Choose $x \in Z(G)$ with $x \neq 1$ (recall that the center of a p-group is always ≥ 1). Consider $(x-1)V$. We show this is a submodule of V. If $v \in V, g \in G$, $g(x-1)v = (x-1)gv$ because $x \in Z(G)$ so that $g(x-1)v \in (x-1)V$. Also, $(x-1)V$ is not 0 since $x \neq 1$. Therefore, since V is irreducible, we have that $V = (x-1)V$. But similarly we have $V = (x-1)^2V = (x-1)^3V = \cdots = (x^{p^n}-1)V = 0$, a contradiction. Note that 0 is not irreducible by definition. ■

Definition 8 *Let A be any ring with 1 and let M be an A-module. Then a series of submodules*

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

is called a composition series *if each M_i/M_{i+1} is irreducible.*

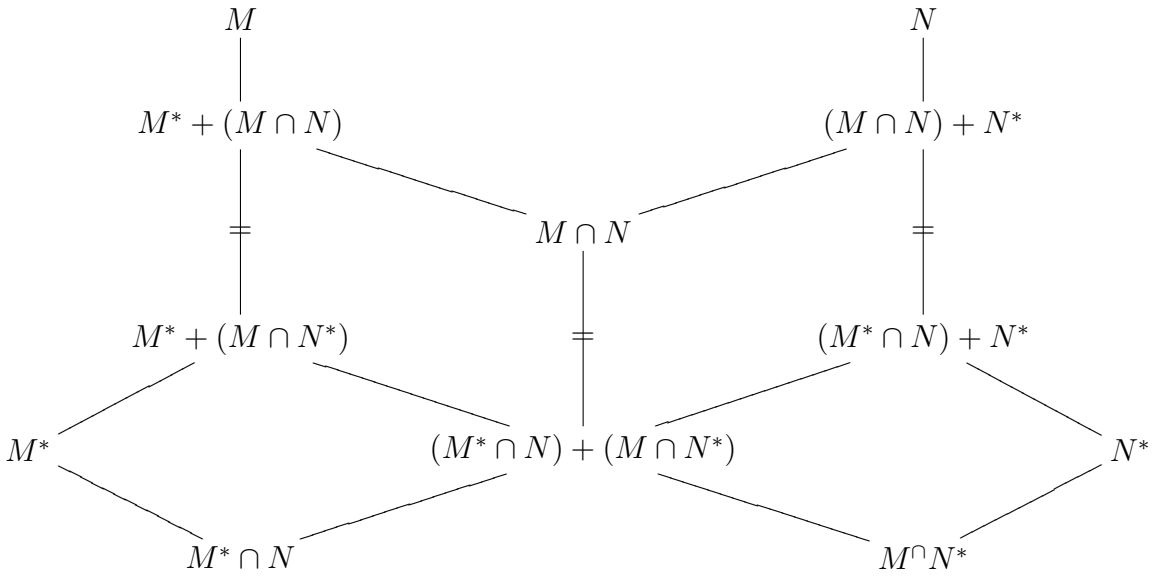
Not every module has a composition series. For example, $\mathbb{Z}$ does not; for example, the series

$$\mathbb{Z} \supset (p) \supset (p^2) \supset \cdots \supset (p^n) \supset \cdots$$

does not terminate.

Proposition 2 *(Butterfly Lemma) If $M^* \leq M$, $N^* \leq N$ are submodules of some module, then $M^* + (M \cap N^*) \leq M^* + (M \cap N)$, $N^* + (M^* \cap N) \leq N^* + (M \cap N)$, and*

$$\Big(M^* + (M \cap N)\Big) \Big/ \Big(M^* + (M \cap N^*)\Big) \cong \Big((M \cap N) + N^*\Big) \Big/ \Big((M^* \cap N) + N^*\Big)$$



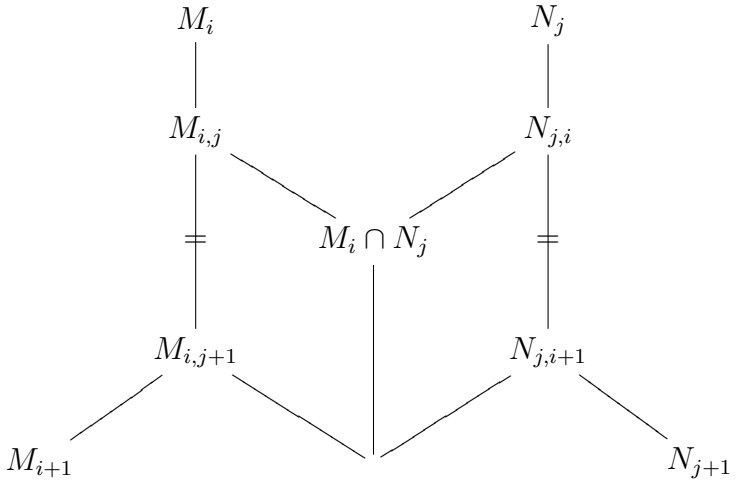
Proposition 3 *(Schreider's Theorem) If*

$$M = M_1 \geq M_2 \geq \cdots M_r = \{0\}$$

$$N = N_1 \geq N_2 \geq \cdots N_s = \{0\}$$

are two series for an A-module M, and if M has a composition series, we can refine the two series to two composition series such that the factors in the first series are isomorphic

in some order to the factors in the second series.



where $M_{i,j} = M_{i+1} + (M_i \cap N_j)$ *and* $N_{j,i} = N_j + (M_i \cap N_j)$.

Corollary 1 *(Jordan Hölder Theorem) Any two composition series of* M *have the same composition factors up to isomorphism.*

Proposition 4 *M has a composition series iff M satisfies the Ascending Chain Condition and the Descending Chain Condition.*

August 29

Proposition 5 *(1) If A is any ring, M has a composition series iff (2) M has ACC and DCC for submodules iff (3) every series of submodules of M can be refined to a composition series. [DF, p. 438, 637-638, 717]*

(1) $\Longleftrightarrow$ (3) follows from the Butterfly lemma.
For (1) $\Longleftrightarrow$ (2), see e.g.[CR2, §13].

Example 5 *$\mathbb{Z}$ as a $\mathbb{Z}$-module has ACC but not DCC and the $\mathbb{Z}$-module*

$$\mathbb{Z}_{p\infty} = \left\langle a_1, a_2 \ldots a_n \ldots : a_1^p = 1, a_2^p = a_1 \ldots a_{i+1}^p = a_i \ldots \right\rangle$$

is an abelian p-group such that

$$\langle a_1 \rangle < \langle a_2 \rangle < \cdots < \mathbb{Z}_{p\infty}.$$

This group has DCC but not ACC as a $\mathbb{Z}$-module.

We see from this example that to get a finite series, we need to be able to go both up and down from a submodule and end in a finite number of steps.

Now given an R-algebra A, our goal is to find and classify the irreducible A-modules. However, this is obviously too ambitious!

Definition 9 *A itself as a left A-module, sometimes written ${}_AA$, gives rise to the* regular representation.

In this situation, the submodules of ${}_AA$ are the left ideals.

Let M be a simple A-module (recall that this doesn't include the zero module) and let $m \in M$, $m \neq 0$. Then $Am = \{am : a \in A\}$ is a non-zero submodule, so $Am = M$. Also $\varphi : A \to M$ defined $a \mapsto am$ is a surjective A-module homomorphism, that is, $\varphi(am) = a\varphi(m)$ for $a \in A$, $m \in M$. The kernel of φ is a maximal left ideal L (since M is simple) such that $A/L \cong M$. From this we explore the idea that simple modules correspond to maximal left ideals. This will lead to the Jacobson radical.

Next, we will want to extend concepts from commutative rings to non-commutative rings. Recall from [DF p.650] that if R is a commutative ring with 1, we have the nilradical

$$N = \bigcap_{P \text{ prime}} P = \{x \in R : x^n = 0, \text{ some } n \geq 1\}$$

and the radical

$$\text{rad } R = \bigcap_{L \text{ maximal}} L.$$

Then $N \subset \text{rad } R$. Recall also that $x \in \text{rad } R$ iff $1 - rx$ is a unit for all $r \in R$.

Now let A be any ring with 1, possibly non-commutative.

Definition 10 *Define the* Jacobson radical $J(A)$*, sometimes written* rad A*,*

$$J(A) = \bigcap_{\substack{L \text{ a maximal} \\ \text{left ideal}}} L$$

Definition 11 *If M is an A-module,* ann $M = \{a \in A : aM = 0\}$*. If $m \in M$,* $\text{ann}(m) = \{a \in A : am = 0\}$*.*

Note that ann M is a two-sided ideal and $\text{ann}(m)$ is a left ideal.

Proposition 6 *$J(A)$ is the annihilator of all the simple A modules, i.e.,*

$$J(A) = \bigcap_{M \text{ simple}} \text{ann } M$$

Note that if M is an A-module, we have a ring homomorphism $A \to \text{End}_R(M)\,(= \text{Hom}_R(M, M))$ whose kernel is two-sided ideal. (This expresses the fact that we have a representation.) So the proposition shows that $J(A)$ is a two-sided ideal and not simply a left ideal.

Proof. Suppose M is simple and as before, $M = Am$ for some $m \neq 0$. We have a homomorphism $\varphi : A \to Am$ defined $a \mapsto am$. Then φ is a surjective A-module homomorphism so that $A/L \cong M$ where $L = \ker \varphi$ is a maximal left ideal. That is

$$L = \{a \in A : am = 0\} = \text{ann}(m).$$

Then

$$\bigcap_{M \text{ simple}} \text{ann } M = \bigcap_{M \text{ simple}} \bigcap_{0 \neq m \in M} \text{ann}(m) \supset \bigcap_{L \text{ maximal}} L = J(A).$$

Conversely, if $aM = 0$, then $am = 0$ so $a \in \text{ann}(m) = L$, where L is a maximal left ideal, for all $m \in M$. Also every maximal left ideal arises in this way. Then

$$\bigcap_{M \text{ simple}} \text{ann}(M) \subset \bigcap_{\substack{L \text{ a maximal} \\ \text{left ideal}}} L = J(A)$$

■

Example 6 *Let G be a cyclic group of order p and let $A = KG$ for K with* char $K = p$. *M is simple implies that M is the trivial module. Then $J(A)$ is the ideal of A spanned by $g - 1, g \in G$. Then* dim $J(A) = p - 1 =$ dim $A - 1$.

Exercise 1 *Look at the example in DF on page 828 of $G = S_3$ in which a simple module of dimension 2 is constructed.*

September 3

Note that we generally use the symbol R for a commutative ring with 1 and the symbol A for any ring with 1.

Additional reference: [H] T. Hungerford, Algebra. Look at the section on Jacobson radicals in chapter 9. Note also that when Jacobson introduced the radical, he was considering any ring, not necessarily with 1.

Recall that

$$J(A) = \bigcap_{\substack{M \text{ a maximal} \\ \text{left ideal}}} M = \bigcap_{M \text{ simple}} \text{ann}(M)$$

If we only want to consider simple modules, we may as well study $A/J(A)$. Since these descriptions involve maximal ideals, which we don't want to compute, and simple modules, which are what we want to determine in the first place, we develop an intrinsic description of $J(A)$. (CR, §5 or H, Ch. 9)

Theorem 2

$$\begin{aligned} J(A) &= \{x \in A : 1 - axb \text{ is a unit for all } a, b \in A\} \\ &= \{x \in A : 1 - ax \text{ has a left inverse for all } a \in A\}. \end{aligned}$$

Proof. We prove first that $J(A) = \{x \in A : 1 - ax$ has a left inverse for all $a \in A\}$. Let $x \notin J$. Then $x \notin L$, some maximal left ideal L. then $\langle L, x\rangle = A$ (the ideal generated by L and x). Therefore, $1 = y + ax$ for some $y \in L, a \in A$. Therefore $1 - ax = y \in L$. Then $1 - ax$ does not have a left inverse else $y \in L$ has a left inverse and then $1 \in L$.

Alternately, assume $1 - ax$ has a left inverse for all $a \in A$. If $xW \neq 0$ for some W simple, then $xw \neq 0$ for some $w \in W$. Then $W = Axw$. Then $w = axw$ for some a so that $(1 - ax)w = 0$. Then, since $1 - ax$ has a left inverse,$w = 0$, a contradiction. So $xW = 0$ for all simple W , and $x \in J$. For the converse, it suffices to show that $1-x$ has a left inverse for $x \in J$, i.e. $A(1-x) = A$. If not, $A(1-x) \subset L$ for some maximal left ideal L. Then $1 - x \in L$, but since $x \in L$ since $x \in J$, we have that $1 \in L$, a contradiction.

Next, to prove the first equality, note that from the above proof, $1 - axb$ is a unit implies $x \in J$. To show the converse, it suffices to show that if $x \in J$, then $1 - x$ is a unit.

Again, by the first part, take some t with $t(1 - x) = 1$. Then $t - tx = 1$ so that $1 - t = -tx \in J$. So $1 - (1 - t) = t$ has a left inverse u, that is $ut = 1$. Then $u = ut(1-x) = 1-x$ so that $tu = 1$. Thus, $t(1-x) = 1$, $(1-x)t = 1$, i.e. t is a two-sided inverse of $1 - x$. ■

Remark 1 *Write $t = 1-y$. Then $(1-y)(1-x) = 1$. Expanding, we have $1-y-x+xy = 1$ so that $xy-x-y = 0$ and note that we've eliminated the reference to 1. Now for any ring, not necessarily with 1, define x to be* left-quasi-regular *if there exists y with $x+y+xy = 0$. Then J can be defined in this case using this concept, see e.g. (H, p.426).*

Recall now that if A has a 1, every proper left ideal is contained in a maximal left ideal (DF, p.255, H, p. 128, CR2). Therefore we know that there exist maximal ideals in our case and hence there exist simple A-modules. It is therefore non-vacuous to say that J "kills" all simple modules. If however $a \notin A$ and there are no simple A-modules, we say that $J(A) = A$ is a *radical ring.*

Now our goal is to study $A/J(A)$. Recall the example where G is cyclic of order p^n and K is a field is a field of characteristic p. If $A = KG$, $\dim A = p^n$ and $\dim J(A) = p^n - 1$.

Example 7 *Let $A = M_n(K)$ for K a field. Our aim is to write this as a direct sum of simple modules, i.e. as a sum of minimal left ideals. Write*

$$E_{i,j} = \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & & & \\ 0 & & 1 & & \\ \vdots & & & & \\ 0 & & & & \end{pmatrix}$$

where the 1 is in position i, j. Then $E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}$ and

$$_AA = \bigoplus_{i=1}^{n} L_i$$

where

$$L_i = \left\{ \sum_j a_j E_{j,i} : a_j \in K \right\} = \begin{pmatrix} & * & \\ & * & \\ 0 & * & 0 \\ & * & \\ & * & \end{pmatrix}$$

L_i is an irreducible module as follows. Let $x \in L_i$ with $x \neq 0$. Let $x = \sum_j a_j E_{j,i}$, and suppose $a_k \neq 0$. Then $E_{j,k}x \in L_i$ and has $a_{k,i}$ in the jth row and 0 in the other rows. Thus we get all the $E_{j,i}$ in L_i, showing that any non-zero element in L_i generates all of L_i. Thus L_i is irreducible. (Remark: We used the fact that K is a field here.)

$L_i \cong L_j$ for each i, j: This follows from the matrix representation given by L_i as $x \to x$ for $x \in A$. Also, note that $J(A) = 0$ since we have maximal left ideals $L'_j = \bigoplus_{i \neq j}^{n} L_i$, whose intersection is 0.

September 5

Example 8 *Let $A = M_n(D)$ forD a division ring. The decomposition of A into the direct sum of simple modules can be done in the same way as for $M_n(K)$ with K a field, as in the previous example. Again $A = L_1 \oplus L_2 \oplus \cdots \oplus L_r$ for L_j, the left ideals and simple A-modules constructed before. Also as before, $J(A) = 0$ since $x \in J$ implies $xA = 0$ since it kills all the simple modules, but A has 1, so $x = 0$. Also note that if we set $e_i = E_{i,i}$, then $e_1^2 = e_1$ and $L_i = Ae_i$. This says that each L_i is generated by e_i an idempotent.*

Digression. Let $T : V \to V$ be a linear transformation. $T^2 = T$ means that T is a projection. With a suitable basis, T has matrix

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

and in fact $V = \ker T \oplus \operatorname{im} T$. Now if $e \in A$ with $e^2 = e$, then $A = Ae \oplus A(1-e)$ since if $x \in A$, $x = xe + x(1-e)$ so that if $x \in Ae$, then $xe = x$ and if $x \in A(1-e)$, then $xe = 0$.

Definition 12 *A is called* (left) artinian *if ${}_AA$ has the DCC on submodules.*

Then A is artinian if and only if every non-empty set of left ideals has a minimal element.

Proposition 7 *Assume A is artinian. Then every nilpotent left ideal is contained in J and J itself is nilpotent. (CR1)*

Proof. We have a chain

$$J \supset J^2 \supset \cdots \supset J^i \supset \cdots$$

which terminates as

$$J^m = J^{m+1} = \cdots = J^{2m} = \cdots$$

If $J^m \neq 0$, then $J^{2m} = J^m J^m \neq 0$. Choose a minimal left ideal I such that $J^m I \neq 0$. Then for some $a \in I$, we have $J^m a \neq 0$ and $J^m a \subset I$, but $J^m(J^m a) = J^m a \neq 0$ so that $J^m a = I$ since I is the minimal ideal for which $J^m I \neq 0$. Now since $a \in I$ we can write $a = xa$ for some $x \in J^m$. Then $(1-x)a = 0$ implies $a = 0$ since $1 - x$ has a left inverse. But this is a contradiction, so $J^m = 0$, that is J is nilpotent.

Now let N be a nil left ideal, that is, every element is nilpotent. Then $x \in N$ implies $x^k = 0$ for some $k \geq 1$ so that $1 - x$ is invertible. This means that $x \in J$ so that $N \subset J$. ■

Example 9 *If $A = KG$, then $J(A)$ is nilpotent. If G is some p-group, then J is the span of $\{x - 1 : x \in G\}$ and $(x-1)^{p^n} = 0$*

Proposition 8 *Assume A is artinian. If I is a non-nilpotent left ideal, then I contains an idempotent (CR2, 24.2)*

In particular if $J = 0$, then A would be non-nilpotent and we would be able to do the decomposition as in Example 8.

Proof. Let I_1 be a minimal left ideal among the non-nilpotent left ideals contained in I. Then $I_1^2 = I_1$ by minimality. Let L_1 be minimal in $\{L \subset I_1 : I_1 L \neq 0\}$. Then since $I_1 x \neq 0$ for some $x \in L_1$ and $I_1 x \subset L_1$, we have by minimality that $I_1 x = L_1$. Then $x = ax$ for some $a \in I_1$. But then $x = ax = a^2 x = \cdots$ so that $(a^2 - a)x = 0$. Let $N = \{u \in I_1 : ux = 0\} \subset I_1$ and $N \neq I_1$ for if $N = I_1$ then

$$0 = Nx = I_1 x = L_1 \neq 0,$$

a contradiction. Then $a^2 - a \in N$ and N is nilpotent since $N \subsetneq I_1$ and I_1 was chosen to minimal among non-nilpotent ideals. Let $n_1 = a^2 - a$. If $n_1 = 0$, we're done as a would be an idempotent. If not, let $a_1 = a + n_1 - 2an_1 \in I_1$ and repeat the above process producing $n_2 = a_1^2 - a_1$. We will get a sequence which will eventually give an idempotent. ■

September 8

Sketch of proof of the previous proposition (for details see the last lecture):

We have found $I_1 \leq I$, non nilpotent, and $N \subset I_1$ with N nilpotent. We have an a-sequence in I and an n-sequence in N. As before, take $n_1 = a^2 - a$. If this is zero, we're done. If not, recursively define $a_i = a_{i-1} + n_i(1 - 2a_{i-1})$ and $n_{i+1} = a_i^2 - a_i$. In fact $n_2 = 4n_1^3 - 3n_1^2$ so $n_1^2 | n_2$ in A. Inductively, n_{i+1} has $n_1^{2^i}$ as a factor. N is nilpotent implies that $n_1^{2^k} = 0$ for some k. Hence $n_{k+1} = 0$ and $a_k^2 = a_k$, that is, a_k is an idempotent.

The definition of a_i may have been motivated by calculus as follows (folklore). We're trying to solve $f(x) = x^2 - x$. Thus

$$\begin{aligned} a_1 &= a + n_1(1 - 2a) \\ &= a - (a^2 - a)(2a - 1) \\ &= a - f(a)f'(a) \end{aligned}$$

Recall that $M_n(D) = \bigoplus_{j=1}^n L_j$ is the direct sum of simple left ideals L_j with $L_i \cong L_j$. Also, note that simple left ideals are the same as irreducible left ideals and the same as minimal left ideals.

Definition 13 *Let A be any ring with 1. We say that A is* left-semi-simple *or* completely reducible *if ${}_AA$ is the direct sum of simple left ideals. Similarly, an A-module M is* left-semi-simple *or* completely reducible *if M is the direct sum of simple submodules.*

Proposition 9 *(H, Ch. 9, Th 3.6 or CR2, §15.3) The following are equivalent:*

1. *$M = \bigoplus_{i \in I} M_i$ with M_i simple*
2. *$M = \sum_{j \in J} M_j$ with M_j simple*
3. *For any M' a submodule of M, we have $M = M' \oplus M''$ for some submodule M'' of M.*

Observe that if $N \leq M$ and $L \leq M$ with L simple, then $N \cap L$ is either L or 0. Hence $N + L$ is either N or $N \oplus L$.

Proof. The proof uses Zorn's Lemma over and over. (1) $\Rightarrow$ (2) is obvious. For (2) $\Rightarrow$ (1), among all partial sums $\sum_{i \in I} M_i$, $I \subset J$, which are direct, choose a maximal L and then show that $L = M$ by observing that if some $j \notin I$, then $L \oplus M_j$ is direct by the observation above, a contradiction.

For (2) $\Rightarrow$ (3), given M', choose a maximal $M'' = \sum_{i \in I} M_i$ with $M'' \cap M' = 0$ by Zorn's lemma. Then show that $M = M' \oplus M''$. If not, pick $m \in M$ with $m \notin M' \oplus M''$. Then m is in a sum of a finite number of simple submodules, and at least one of them, say M_k, is not contained in $M' \oplus M''$. This would contradict maximality of M''.

For (3) $\Rightarrow$ (2), first show that if $N \leq M$ with $N \neq 0$, then N has a simple submodule. Pick some $0 \neq n \in N$ and choose some N_0 maximal such that $n \notin N_0$. By the assumption, we have $N = N_0 \oplus N_1$ for some N_1. Then N_1 is simple, for if not, $N_1 = N_2 \oplus N_3$, but then $n \notin N_0 + N_2$ or $n \notin N_0 + N_3$ which contradicts maximality. In particular, M contains simple modules. Among all $\sum_{i \in T} M_i$ with M_i simple, find a maximal L. If $L \neq M$, then $M = L \oplus L'$ and L' contains a simple submodule, which contradicts the maximality of L

■

Finally, we have the main theorem on Artinian rings.

Theorem 3 *If A is an Artinian ring with 1, then $J(A) = 0$ if and only iff ${}_AA$ is semi-simple.*

Proof. If $J = 0$, let L_1 be a minimal left ideal. Then L_1 is not nilpotent, so $L_1 = Ae$ for some e with $e^2 = e$ so that $A = Ae \oplus A(1-e) = L_1 \oplus L_1'$. If L_1' is non minimal, let $L_2 \leq L_1'$ be minimal and $A = L_1 \oplus L_2 \oplus L_2'$, etc. Then $L_1' \supset L_2' \supset \cdots$ terminates so that $A = \oplus_{j=0}^{n} L_j$.

Conversely, let ${}_AA$ be semi-simple and write $A = J \oplus J'$ by criterion (3). We then have that $1 = x + x'$ with $x \in J$ and $x' \in J'$. Then $x = x^2 + xx'$ which means that $x^2 - x \in J \cap J' = 0$. But $x - x^2 = x(1-x) = 0$ means that $x = 0$ since $1 - x$ is a unit. This means that $x' = 1$ so that $J' = A$ and $J = 0$. ■

A counterexample for this in non-artinian rings is $J(\mathbb{Z}) = 0$ since the maximal ideals are $\{(p) : p \text{ prime}\}$, but $\mathbb{Z}$ is not semi-simple (in our sense). For a structure theorem on arbitrary rings A with $J(A) = 0$ see H, Chapter 9, 3.2.

September 10

We proved last time that if A is artinian, then $J(A) = 0$ if and only if ${}_AA$ is semi-simple. From this, it follows that if $J(A) \neq 0$, then $A/J(A)$ is semi-simple since $J(A/J(A)) = 0$.

Proposition 10 *Let A be any ring with 1. Then submodules and quotient modules of completely reducible modules are completely reducible.*

Proof. (Schur's Lemma) First note that if L and M are simple A-modules and $\varphi : L \to M$ is a A-module homomorphism, then $\varphi(L)$ is either 0 or M and $\ker\varphi$ is either 0 or L, so φ is ether 0 or an isomorphism. In particular, $\mathrm{End}_A(M)$ is a division ring.

If M is completely reducible and $N \leq M$, then $M = \sum_{i\in I} M_i$ for M_i simple so that $M/N = \sum_{i\in I} M_i/N_i$. If $\varphi : M \to M/N$ is the canonical map, then $\varphi(M)$ is the sum of those M_i such that $\varphi(M_i) \neq 0$ and such that $\varphi(M_i)$ is simple.

Now if M is completely reducible and $N \leq M$, then $M = N \oplus N'$ for some N' and so $N \cong M/N'$. ■

Proposition 11 *Assume ${}_AA$ is semisimple. Then*

1. *${}_AA$ is the direct sum of a finite number of left A-ideals.*
2. *Every finitely generated A-module is completely reducible.*
3. *Every A-module is completely reducible.*

Proof. If ${}_AA$ is semisimple, then ${}_AA = \sum_{i\in I} L_i$ with L_i minimal left ideals. But since the ring has 1, we have $1 \in L_{i_1} + L_{i_2} + \cdots + L_{i_n}$ and similarly for $a \in A$ so that $A = L_{i_1} + L_{i_2} + \cdots + L_{i_n}$.

Suppose M is finitely generated by $\{m_1, m_2, \cdots m_r\}$. Then we have a surjective A-module homomorphism

$$\varphi : \underbrace{A \oplus A \oplus \cdots \oplus A}_{r} \to M \text{ given by } \varphi(a_1, a_2, \cdots a_r) = \sum_{i=1}^{r} a_i m_i.$$

Since $A \oplus A \oplus \cdots \oplus A$ is semisimple, M is semisimple.

Finally, suppose M is an A-module. Then

$$M = AM = \left(\sum_{i\in I} L_i\right) M = \sum_{i\in I}\sum_{m\in M} L_i m.$$

But by the above proposition, each $L_i m$ is either 0 or simple, so M is completely reducible ■

The following theorem provides the main example of an artinian, semisimple ring.

Theorem 4 *(Maschke's Theorem) If G is a finite group and K is a field of characteristic either 0 or p with $p \nmid |G|$, then KG is semisimple (DF, p. 815).*

Note that KG is artinian as it is a finite dimensional algebra and a vector space over K
Remark: If M is an A-module and $N \leq M$, then N is a direct summand of M if and only if there exists a A-module homomorphism $\pi : M \to N$ with $\pi|N = i$, the identity map. Confirm that if we have such a π, then $M = N \oplus \ker \pi$.
Proof. Let M be a KG-submodule and $N \leq M$. Since M, N are vector spaces over K, find subspace W of M such that $M = N \oplus W$ where $\oplus$ denotes direct sum as vector spaces. Then we have a K-homomorphism $\pi : M \to N$ with $\pi|_N = i$. Let $\pi' : M \to M$ be given by

$$\pi'(u) = \frac{1}{|G|}\sum_{g\in G} g\pi\left(g^{-1}u\right).$$

Show that π' is a KG-module homomorphism, $\pi'|_N = i$, and $\mathrm{Im}\,(\pi') = N$. For example, if $u \in N$,

$$\pi'(u) = \frac{1}{|G|}\sum_{g\in G} g\left(g^{-1}u\right) = u$$

as $g^{-1}u \in N$, and if $x \in G$, $u \in M$,

$$\pi'(xu) = \frac{1}{|G|}\sum_{g\in G} g\pi\left(g^{-1}xu\right) = \frac{1}{|G|}\sum_{g\in G} x\left(x^{-1}g\right)\pi\left(g^{-1}xu\right) = x\pi'(u)$$

so that π' is a G-module homomorphism, hence a KG-module homomorphism. ■

Exercise 1 *(DF p.828) Let $G = S_3$ and let $V = \langle e_1, e_2, e_3\rangle$ be the* natural module *defined $ge_i = e_{g(i)}$. Let $V_1 = \langle e_1 + e_2 + e_3\rangle \leq V$. Then $V = V_1 \oplus W$ as K-spaces where the characteristic of K is 0 and $W = \langle e_2, e_2\rangle$. However, W is not a KG-module. Go through Maschke's Theorem to start from W to find a KG-module W_1 with $V = V_1 \oplus W_1$*

Preview: If A is an artinan ring and semisimple, we know that $A = \sum L_i$. What is the structure of A as a ring?

September 12

We've shown that if A is artinian with 1 and semisimple, then ${}_AA$ is completely reducible. Consider the ring $A = M_n(D)$ where D is a division ring. We know that $A = \bigoplus_{j=1}^n L_j$ where $L_j = AE_{j,j}$ and $L_i \cong L_j$ for all i, j. Now we're interested in recovering D knowing the above decomposition.

Recall that $\mathrm{Hom}_A\,(M, N)$ is an abelian group when A is a ring, but if A is an R-algebra where R is a commutative ring, then $\mathrm{Hom}_A(M, N)$ becomes an R-module.

Consider

$$\mathrm{Hom}_A(L_i, L_j) = \mathrm{Hom}_A(AE_{i,i}, AE_{j,j}).$$

By Schur's lemma, every element of this vector space over D is either 0 or an isomorphism.

Lemma 1 *If A is any ring, M is an A-module, and $e \in A$ with $e^2 = e$, then $\mathrm{Hom}_A(Ae, M) \cong eM$.*

Proof. Let $\varphi : eM \to \mathrm{Hom}_A(Ae, M)$ be given by $em \mapsto \alpha : e \mapsto em$ for $m \in M$. Now let $\psi : \mathrm{Hom}_A(Ae, M) \to eM$ be given by $\alpha \mapsto \alpha(e)$. Note that if $\alpha(e) = m$, then $\alpha(e \cdot e) = em$ so $m = em \in eM$. Then, φ and ψ are inverses. ■

Corollary 2 $\mathrm{End}_A(Ae)^{\mathrm{op}} \cong eAe$ *where for rings B, B^{op} is the abelian group B with multiplication reversed.*

Proof. Check that the isomorphism given in the theorem reverses the multiplication in the two rings. ■

Then $\mathrm{Hom}_A(AE_{i,i}, AE_{j,j}) \cong E_{i,i}AE_{j,j}$. So if $x \in A$, $x = \sum_{k,l} a_{k,l}E_{k,l}$ so that $E_{i,i}xE_{j,j} = a_{i,j}E_{i,j}$ (check this). Hence $\mathrm{Hom}_A(AE_{i,i}, AE_{j,j}) \cong D$. In particular, $\mathrm{End}(AE_{i,i}) \cong D^{\mathrm{op}}$. Then we have that if $A = M_n(D)$ and L is a minimal left ideal, then $\mathrm{End}_A(L) \cong D^{\mathrm{op}}$.

Suppose now that V_1, V_2, W_1, W_2 are A-modules for A any ring. Consider

$$\mathrm{Hom}_A(V_1 \oplus V_2, W_2 \oplus W_2) \cong \mathrm{Hom}_A(V_1, W_1) \oplus \mathrm{Hom}_A(V_1, W_2) \oplus$$

$$\mathrm{Hom}_A(V_2, W_1) \oplus \mathrm{Hom}_A(V_2, W_2)$$

$$\theta \to \begin{pmatrix} \theta_{1,1} & \theta_{2,1} \\ \theta_{1,2} & \theta_{2,2} \end{pmatrix} \tag{1}$$

where $\theta_{i,j} = P_j \theta L_i$, the L_i being injections of V_i into $V_1 \oplus V_2$ and the P_j being projections of $W_1 \oplus W_2$ on W_j.

Formally, if $\theta \in \mathrm{Hom}_A(V_1 \oplus V_2, W_1 \oplus W_2)$, then θ corresponds to the matrix as in (1)

$$\theta : \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \to \begin{pmatrix} \theta_{1,1} & \theta_{2,1} \\ \theta_{1,2} & \theta_{2,2} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

for $v_1 \in V_1$ and $v_2 \in V_2$. This gives an additive group isomorphism $\mathrm{End}_A(V_1 \oplus V_2) \cong$Group of matrices as in (1). Finally, if $V_1 = V_2 = V$, then

$$\mathrm{End}_A(V \oplus V) \cong M_2(\mathrm{End}_A(V))$$

Check that if $\theta \to (\theta_{j,i})$ and $\Phi \to (\varphi_{j,i})$, then $\theta\Phi \to (\theta_{j,i})(\varphi_{j,i})$.

The same proof shows that $\mathrm{End}_A(nV) \cong M_n(\mathrm{End}_A(V))$.

If V is simple, then $\mathrm{End}_A(V) = D$ a division ring and then $\mathrm{End}_A(nV) \cong M_n(D)$.

Lemma 2 $\mathrm{End}_A({}_AA) \cong A^{\mathrm{op}}$

Proof. Let $\varphi \in \mathrm{End}_A({}_AA)$. Then $\varphi : A \to A$ and if $1 \to x$, so that $a \to ax$, φ is just right multiplication by x. Conversely, if $x \in A$, $\varphi : a \to ax$ is an A-module homomorphism ${}_AA \to_A A$. Now if $\varphi \longleftrightarrow x$, i.e., $\varphi(1) = x$, and $\psi \longleftrightarrow y$, i.e., $\psi(1) = y$, then $(\varphi\psi)(1) = \varphi(y) = yx$ ■

Finally, let A be artinian and semisimple. Then ${}_AA \cong \bigoplus_{j=1}^r n_j S_j$ for S_j simple A-modules with S_i not isomorphic to S_j if $i \neq j$. Then

$$\begin{aligned} \mathrm{End}_A({}_AA) &\cong \bigoplus_{j=1}^r \mathrm{End}_A(n_j S_j) \\ &\cong \bigoplus_{j=1}^r M_{n_j}(D_j') \end{aligned}$$

Note that $(M_n(D))^{\mathrm{op}} \cong M_n(D^{\mathrm{op}})$ (take transposes of matrices).

Finally, $A \cong \bigoplus_{j=1}^r M_n(D_j)$ and this is the Wedderburn decomposition with $D_j \cong \mathrm{End}_A(S_j)^{\mathrm{op}}$.

September 15

Last time we proved the Wedderburn Theory, that is, if A is artinian with 1 and semi-simple, then $A \cong \bigoplus_{j=1}^r M_{n_j}(D_j)$. Here, if ${}_AA \cong \bigoplus n_j S_j$ for S_j simple, then $D_j \cong \mathrm{End}_A(S_j)^{\mathrm{op}}$

Corollary 3 *If A is commutative, then A is the direct sum of fields.*

This follows since if $M_{n_j}(D_j)$ is a field, then n_j will have to be 1 and D_j has to be commutative.
Remark: If A is a finite dimensional D-algebra with D a division ring and

$$A = L_0 \supsetneq L_1 \supsetneq \cdots \supsetneq \cdots$$

is a chain of left ideals, the chain has to terminate as $\dim_D L_i > \dim_D L_{i+1}$. Compare this with $\mathbb{Z} \supset (p) \supset (p^2) \cdots$ where the rank does not decrease.

Definition 14 *A ring A is* simple *if it has no two-sided ideals except $\{0\}$ and A.*

We know that $M_n(D)$ is simple so that the Wedderburn theory says that if A is a semi-simple artinian ring with 1, then A is a direct sum of simple rings.

Proposition 12 *(CR1 §3.24) A simple artinian ring is semi-simple.*

Proof. Let L be a minimal left ideal of A. Take $B = \sum_{a \in A} La$. Then B is a two-sided ideal since if $x \in A$, then $(La)x$ is either 0 or of the same form. Then $B = A$ so that A is semi-simple. ■

Now we want to study the internal structure of a semi-simple artinian ring A. Write $A = A_1 \oplus A_2 \oplus \cdots \oplus A_r$ for A_j subrings of A with $A_j \cong M_{n_j}(D_j)$. In fact, A_j is the sum of all the minimal left ideals which are isomorphic to S_j. First, observe that A_j is a two-sided ideal of A as follows.

If $x, y \in A$, then

$$x = x_1 + x_2 + \cdots + x_r \tag{2}$$

and

$$y = y_1 + y_2 + \cdots + y_r \tag{3}$$

for $x_j, y_j \in A_j$. Then $xy = x_1y_1 + \cdots x_ry_r$ so $xy_j = x_jy_j \in A_j$ as A_j is a subring. Similarly, $y_jx = y_jx_j \in A_j$.

Now let

$$1 = e_1 + e_2 + \cdots e_r \tag{4}$$

for $e_j \in A_j$. From (2) and (4), we have

$$x = x1 = \sum x_je_j = \sum x_j$$

so that $x_je_j = x_j$. Similarly, $e_jx_j = x_j$ which says that e_j is the identity element for A_j. Also, $e_j^2 = e_j$ and $e_j \in Z(A)$ as $e_jx = xe_j$ for all $x \in A$. Note also that $e_ie_i = e_i$ and $e_ie_j = 0$ for $i \neq j$ as $e_ie_j \in A_i \cap A_j$. Thus we say the e_i are *orthogonal idempotents*. They are also *central*, that is, contained in the center of A. Furthermore, $A_j = Ae_j$.

Theorem 5 *Let A be a semi-simple, artinian ring. Then A is the direct sum $A = \bigoplus A_j$ of two-sided ideals which are simple rings. Each A_j itself is the direct sum of minimal left ideals, all isomorphic to a simple A-module S_j. Furthermore, every simple A-module is isomorphic to some S_j.*

Example 10 *Let $n = 3$ and $G = \langle a : a^3 = 1\rangle$. Take $A = \mathbb{Q}G$. Then $\dim_{\mathbb{Q}} A = 3$. We can take $e_1 = \frac{1}{3}(1 + a + a^2)$. Then e_1 is a central idempotent (as similarly defined elements are for all group-rings) Then $Ae_1 \cong M_1(\mathbb{Q})$. Next, we need to fill in the blank in $A \cong M_1(\mathbb{Q}) \oplus$ _____ with some algebra of dimension 2.*

September 17

In the last decomposition, $1 = e_1 + e_2 + \cdots e_r$ for $e_j \in A_j$. The e_j are central idempotents, i.e., $xe_j = e_jx$ for all $x \in A$ and x_j is the identity element of $A_j = Ae_j$.

Definition 15 *Idempotents e and f are* orthogonal *if $ef = fe = 0$. An idempotent e is* primitive *if e can't be written as the sum $e_1 + e_2$ of orthogonal idempotents.*

Then the e_j above are primitive central and orthogonal idempotents (i.e. can't be written as a sum of orthogonal *central* idempotents), for otherwise if $e_j = e_j' + e_j''$, then $Ae_j = Ae_j' \oplus Ae_j''$ contradicts the simplicity of $A_j = Ae_j$.

Remark: The A_j and the e_j are unique with respect to a decomposition of A into the direct sum of simple rings. This is because the A_j are defined as the sum of all the minimal left ideals isomorphic to one fixed simple module S_j. Note that a simple artinian ring has only one simple module up to isomorphism (this follows from the proof given earlier that a simple artinian ring is semisimple). However, ${}_AA = \bigoplus L_j$ is not unique. For example, in $M_n(D)$ there are many ways of writing 1 as a sum of orthogonal idempotents.

Example:Returning to $G = S_3 = \langle (12), (23)\rangle$ V the standard module $\langle v_1, v_2, v_3\rangle$, and $A = KG$ for K a field, we have two cases to consider.

Case 1. char $K \neq 3$. Then $V = V_1 \oplus V_2$ where $V_1 = \langle v_1 + v_2 + v_3 \rangle$ and $V_2 = \langle v_1 - v_2, v_2 - v_3 \rangle$ as before.
Case 2. char $K = 3$. If

$$(123) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

then the eigenvalues are all 1. We need to find a basis for V to exhibit a composition series. We begin with $v_1 + v_2 + v_3$ as the first basis element and extend to a full basis of V. Consider the basis $\{v_1 + v_2 + v_3, v_1 - v_2, v_1\}$ and check that with respect to this basis,

$$(12) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$(23) \mapsto \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$(123) \mapsto \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Then

$$V_1 = \langle v_1 + v_2 + v_3 \rangle \subset V_2 = \langle v_1 + v_2 + v_3, v_1 - v_2 \rangle \subset V$$

This chain is called a *flag* and is fixed by G. Also, it is a composition series with simple factors giving the trivial and the sign representations as follows. On V_1, G has the trivial representation. This corresponds to the 1,1 entry of the matrices. On V_2/V_1, G has the sign representation, i.e., $g \mapsto \text{sgn } g$, This corresponds to the 2,2 entry of the matrices. On V/V_2, G again has the trivial representation. In the previous example, we initially took a representation of G in char 0, and then regarded the matricies $\rho(g)$ as matricies over K with char $K = 3$. This method is known as the method of *going mod p*.

From now on, A will be a group ring. We will consider K a field of charactersitic 0 containing a suitable ring R which has a prime ideal $\mathfrak{p}$, such that $R/\mathfrak{p} = k$ is a field of charactersitc p. Now if we have a representaion ρ of G over K, we write the matrices $\rho(g)$ over R and then reduce the entries mod $\mathfrak{p}$ to get a modular representation $\overline{\rho}$ of G over k of charactersitc p. For example, going mod 3 on the two dimensional representation of S_3 gave rise to two one-dimensional representations over $\mathbb{F}_3$. In that case, $K = \mathbb{Q}$, $R = \mathbb{Z}$, and $k = \mathbb{F}_3$.

The course bifurcates from this point into two branches, one branch involving further development in characterstic 0, and the other further exploring *going mod p*. The latter path leads to current research in representation theory.

September 19

We continue with group algebras of characteristic 0. Let G be a finite group and A=CG.

Remark 2 *If K is an algebraically closed field and $D \supset K$ is a division algebra with $[D : K] < \infty$, then $D = K$*

Proof. Let $a \in D$. Then a is algebraic over K, so let $f(x)$ be the minimal polynomial of A over K. If $f(x) = h(x)k(x)$ with $\deg h, \deg k < \deg f$. Then

$$0 = f(a) = h(a)k(a)$$

so that one of $h(a)$ or $k(a)$ is 0 since D is a division algebra. This contradicts minimality of f. Hence, $f(x)$ is irreducible. This together with the fact that K is algebraically closed imply that $\deg f = 1$ so that $f(x) = x - a$. Thus, $a \in K$. ∎

We therefore have

$$\mathbb{C}G \cong \bigoplus_j M_{n_j}(\mathbb{C}).$$

Note that each factor of this sum corresponds to one simple algebra A_j in the decomposition $A = \bigoplus A_j$. We know that M_{n_j} is the sum of n_j irreducible left ideals, each of which has dimension n_j. (Recall that these irreducible left ideals are columns of the matrix algebras and hence have dimension n_j.) Therefore, each A_j corresponds to one irreducible A- module of dimension n_j repeated n_j times (in the sense that it occurs n_j times in a decomposition of A as left A-module) . So we get $\sum_j n_j^2 = |G|$ where the n_j are the dimensions of the irreducible representations of G. For example, with $G = S_3$, we have $6 = 1 + 1 + 2^2$.

Next, we want to describe r in terms of the group. We have

$$A = \mathbb{C}G = A_1 \oplus A_2 \oplus \cdots \oplus A_r.$$

Consider the center Z of A. We then have

$$Z = Z_1 \oplus Z_2 \oplus \cdots \oplus Z_r$$

with $Z_j \cong Z(A_j)$. However, since each A_j is a matrix algebra over $\mathbb{C}$, we have $r = \dim_{\mathbb{C}} Z$. We construct a basis of Z over $\mathbb{C}$. If $\mathcal{C}_1, \mathcal{C}_2 \cdots \mathcal{C}_s$ are the conjugacy classes of G, we claim that the set

$$\left\{ k_j = \sum_{g \in \mathcal{C}_|} g : j = 1, 2, \ldots, s \right\}$$

forms a basis of Z. The k_j are clearly independent. To see that they generate Z, let $x \in \sum_g a_g g \in Z$ and let $h \in G$. Then $hxh^{-1} = \sum_g a_g (hxh^{-1}) = \sum_g a_g g = \sum a_{hgh^{-1}} hgh^{-1}$ so that $a_g = a_{hgh^{-1}}$ for all $g, h \in G$. That is, if $x \in Z$, then conjugates must have the same coefficients (see DF, p.827). This says that x is a linear combination of the k_j.

Therefore $r = s$ and the number of irreducible representations of G is equal to the number of conjugacy classes of G. Note also that this holds only when the field is $\mathbb{C}$. This was not the case in the homework problem about $\mathbb{Z}_n$ over $\mathbb{Q}$, for example.

We now develop the theory of characters. Let $\rho : G \to GL(n, \mathbb{C})$ be a group homomorphism and $\rho : A = \mathbb{C}G \to M_n(\mathbb{C})$ be an algebra homomorphism. Define the function $\chi : G \to \mathbb{C}$ by $\chi(g) = \text{Tr}\ (g)$ for $g \in G$, and similarly $\chi(x) = \text{Tr}\ (x)$ for $x \in A$. Now since $\text{Tr}\ (X) = \text{Tr}\ (PXP^{-1})$ for matrices X and P, we have that equivalent representations have the same character. Also $\chi(hgh^{-1}) = \chi(g)$ for $g, h \in G$ so that χ is constant on conjugacy classes. We call such functions *class functions*.

Recall that $\text{Tr}\ (x + y) = \text{Tr}\ x + \text{Tr}\ y$ and $\text{Tr}\ (xy) = \text{Tr}\ (yx)$.

Remark 3 *What if the field has characteristic p? For example, S_3 has a representation of dimension 2 given by $V_2 = \langle v_1 - v_2, v_2 - v_3 \rangle$. Consider V_2 as a module over a field K of characteristic 2, then we get*

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

But then $\chi(1) = 0$, but we would want $\chi(1)$ to be the dimension of the representation. There is a way to get around this and define characters in characteristic p due to Brauer which we will see later.

September 22

Hint for homework: Produce e_1 and e_2, the trivial and sign idempotents. Take $e_3 = 1 - e_1 - e_2$, write $Ae_3 = M_2(\mathbb{Q})$, and figure out explicitly what the isomorphism is.

Next we study characters. Let $A = RG$ for R a commutative ring with 1. Let M and N be A-modules which are finitely generated and free as R-modules. Construct the following new A-modules from M and N.

1. $M^* = \mathrm{Hom}_R(M, R)$, the dual of M, that is, R linear maps of M into R. If M has an R- basis $\{v_1, v_2 \cdots v_n\}$, then M^* has the dual basis $\{f_1, f_2 \cdots f_n\}$ where $f_i(v_j) = \delta_{i,j}$. Then M^* can be made into a left A-module by

   $$(g \cdot f)(m) = f\left(g^{-1}m\right).$$

   Note also that we can make M^* into a *right* A-module by

   $$(f \cdot g)(m) = f(gm).$$

   (The latter right module is more natural, but we convert it into a left module by using the "antipode" $g \to g^{-1}$.) If χ is the character of the representation of G on M and ψ is the character of the representation of G on M^*, we see that $\chi(g) = \psi(g^{-1})$. Hence, if $R = \mathbb{C}$, then $\psi = \overline{\chi}$ since the eigenvalues of $\rho(g)$ where ρ is the representation are roots of unity and for roots of unity, inverses are complex conjugates.

2. $M \otimes_R N$ is an A-module by

   $$g(m \otimes n) = gm \otimes gn.$$

   Note that $M \otimes_R N$ is naturally a $(G \times G)$-module by

   $$(g, g')(m \otimes n) = gm \otimes g'n.$$

   Then we have the diagonal embedding $G \to G \times G$ given by $G \mapsto (g, g)$. Also, there is a nice isomorphism $M^* \otimes_R N \cong \mathrm{Hom}_R(M, N)$ given by

   $$f \otimes n \mapsto \Big[m \mapsto f(m) \cdot n \in R\Big].$$

   Using this we make $\mathrm{Hom}_R(M, N)$ into an A-module by $(g \cdot f)(m) = g \cdot f((g^{-1}m))$.

September 24

Continuing from last time, Hom, Dual, and the tensor product are three functors deriving from an A-module. If $A = RG$ and M is a finitely generated free R-module, we make $M^* = \mathrm{Hom}_R(M, R)$ and $M \otimes_R N$ into A-modules as in the last lecture. Note that

$$M^* \otimes_R N \cong \mathrm{Hom}_R(M, N). \tag{5}$$

$\mathrm{Hom}_R(M, N)$ is an A-module by

$$(gf)(m) = g \cdot f\left(g^{-1}m\right)$$

and this definition is compatible with (5), that is, the map given to induce (5) is G-equivariant i.e., $\varphi : M^* \otimes_R N \to \mathrm{Hom}_R(M, N)$ is such that $g\varphi = \varphi g$ for $g \in G$. Check this. Also $M \oplus N$ is an A-module by

$$g(m, n) = (gm, gn).$$

Finally, recall that if A and B are R-algebras, then so is $A \otimes_R B$ as in DF, p. 355. Then if M is an RG-module and N is a RH module, then $M \otimes_R N$ is an $RG \otimes RH$-module by

$$(g \otimes h)(m \otimes n) = gm \otimes hn$$

In fact, this comes from the following. Let M, N, M' and N' be R-modules . If $\varphi : M \to N$ and $\varphi' : M' \to N'$ are R-module homomorphisms then we get an R- homomorphism $\varphi \otimes \varphi' : M \otimes_R M' \to N \otimes_R N'$ by $m \otimes m' \mapsto \varphi(m) \otimes \varphi(m')$. Now if M and N are RG-modules and M' and N' are RH-modules, $\varphi : M \to N$ is an RG-homomorphism, and $\varphi' : M' \to N'$ is an RH-homomorphism, then $\varphi \otimes \varphi' : M \otimes M' \to N \otimes N'$ is an $RG \otimes RH$-homomorphism. We note that $RG \otimes RH \cong R(G \times H)$.
Now if we have $\rho : RG \to \mathrm{End}_R(M)$ and $\rho' : RG \to \mathrm{End}_R(N)$, then we get $\rho \otimes \rho' : RG \to \mathrm{End}_R(M \otimes_R N)$ using the diagonal embedding $G \to G \times G$ given by $g \to (g, g)$.

Digression: (CR2, p.69) Let $S = (\alpha_{i,j})$ for $1 \le i, j \le n$ and $T = (\beta_{i,j})$ for $1 \le i, j \le m$ be matrices of linear transformations ρ, ρ' of a vector space V and a vector space W respectively with respect to bases $(v_i : 1 \le i \le n\}$ and $\{w_j : 1 \le j \le m\}$ of V and W . Then $\{v_i \otimes w_j : 1 \le i \le n, 1 \le j \le m\}$ is a basis for $V \otimes W$, and the matrix $S \otimes T$ for $\rho \otimes \rho'$ with respect to a suitable ordering of the above basis looks like

$$\begin{pmatrix} & & \\ & \beta_{j,k}S & \\ & & \end{pmatrix}$$

Then $\mathrm{Tr}(S \otimes T) = \mathrm{Tr}\ S \times \mathrm{Tr}\ T$.

Let M be an A-module, corresponding to a representation ρ of $A = \mathbb{C}G$ with character χ. Then $\rho : A \to \mathrm{End}_{\mathbb{C}}(M)$ and $\chi(g) = \mathrm{Tr}(\rho(g)) = \mathrm{Tr}(g, M) = \chi_M$ and similarly for N. We then have the following correspondence:

Representation	Character
M^*	$\overline{\chi}$ i.e. $\chi_{M^*}(g) = \overline{\chi(g)} = \chi(g^{-1})$
$M \otimes N$	$\chi \cdot \psi$ i.e. $\chi_{M \otimes N}(g) = \chi(g)\psi(g)$
$M \oplus N$	$\chi + \psi$

Now if $n_i = \dim \chi_i$ for $1 \leq i \leq r$ with χ_i the irreducible characters, then we know $\sum_i n_i^2 = |G|$ and r is the number of conjugacy classes of G. Pick a representative $g_i \in \mathcal{C}_i$ where $\{\mathcal{C}_i : 1 \leq i \leq r\}$ are the conjugacy classes of G with $\mathcal{C}_1 = 1$

We record all the irreducible characters in a table, called *the character table* of G:

Character	$\mathcal{C}_1$	$\mathcal{C}_2$	$\cdots$	$\mathcal{C}_j$	$\cdots$	$\mathcal{C}_r$
χ_1	1	1		1		1
$\vdots$						
χ_i	$\chi_i(1)$	$\chi_i(g_2)$		$\chi_i(g_j)$		$\chi_i(g_r)$
$\vdots$						

For example, the character table for S_3 is given by

	1	(123)	(12)
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

Now look at KS_3 for K a field of characteristic 3. Only the columns for 1 and (12) are relevant since the eigenvalues of (123) are all 1. We get two modular irreducible characters, the trivial and the sign.

We have so far considered left A-modules, and right A-modules are similar.

For A and B algebras, we can also consider bimodules. Thus M is an (A, B)-bimodule if A acts on the left, B on the right, and $a(m \cdot b) = (a \cdot m)b$ for $a \in A$,$m \in M$, and $b \in B$. (DF p. 347). For example, if $A = RG$, then A is a bimodule whose submodules are 2-sided ideals. Consider $A = M_n(\mathrm{C})$. What is its structure as an A-bimodule, that is, what is the representation of $A \otimes A^{\mathrm{op}}$ on A?

September 26

Exercise 2 *Let $A = M_n(K)$ for K a field. Consider the linear transformation*

$$(x, y) \mapsto \left[\varphi_{x,y} : s \mapsto xsy\right]$$

for $x, y \in A$. Then this is a map $A \otimes A \to \mathrm{End}_K(A)$. Check that $\mathrm{Tr}\varphi_{x,y} = \mathrm{Tr}x\mathrm{Tr}y$ by considering the natural basis $\{E_{i,j} : 1 \leq i, j \leq n\}$ of A and computing each $xE_{i,j}y$.

Let $A = \mathbb{C}G$. We have the left regular map

$$a \mapsto \left[\rho_a : x \mapsto ax\right]$$

and the right regular map

$$a \mapsto \left[\psi_a : x \mapsto xa\right].$$

The right regular map is an anti-representation because $\psi_a\psi_b = \psi_a(xb) = xba$ whereas $\psi_{ab}(x) = xab$. We therefore consider A as an $A \otimes A$-module or an A-bimodule by

$$g \otimes h \mapsto \left[x \mapsto gxh^{-1}\right]. \tag{6}$$

Remark 4 *The trace of the regular representation R afforded by ρ_a is*

$$R(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1 \end{cases}$$

We compute the trace of (6) in two ways.

1. The trace of $g \otimes h$ is the number of $x \in G$ such that $x = gxh^{-1}$, that is, $x^{-1}gx = h$. In particular, if g is not conjugate to h, then the trace is 0. Fix $x \in G$ with $x^{-1}gx = h$. Then for any $y \in G$, we have

$$y^{-1}gy = h \Leftrightarrow xy^{-1} \in C_G(g) \Leftrightarrow yx^{-1} \in C_G(g) \Leftrightarrow y \in C_G(g) \cdot x$$

   so that

$$\operatorname{Tr}(g \otimes h) = \begin{cases} |C_G(g)| & g, h \text{ conjugate} \\ 0 & \text{otherwise} \end{cases}$$

2. We have $A = \bigoplus_{j=1}^{r} A_j$ for A_j simple two sided ideals. Then the trace of $g \otimes h$ is

$$\sum_{j=1}^{r} \chi_j(g) \chi_j\left(h^{-1}\right)$$

   where χ_j is the irreducible character corresponding to A_j by Exercise 2.

We therefore have

$$\sum_{j=1}^{r} \chi_j(g) \chi_j\left(h^{-1}\right) = \begin{cases} |C_G(g)| & g, h \text{ conjugate} \\ 0 & \text{otherwise} \end{cases}$$

This is known as the *second orthogonality relation*. It gives a relation between the columns of the character table.

Example 11 *The character table for S_3.*

1	(123)	(12)	
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	-1	0

We can rewrite the second orthogonality relation as

$$\sum_{j=1}^{r} \chi_j(g) \overline{\chi_j(g)} = |C_G(g)| \tag{7}$$

since

$$\overline{\chi_j(g)} = \overline{\sum_k \varepsilon_k} = \sum_k \overline{\varepsilon_k} = \sum_k \varepsilon_k^{-1} = \chi_j\left(g^{-1}\right)$$

where ε_k are the eigenvalues of $\rho_j(g)$.

Take $\{g_j \in \mathcal{C}_j : 1 \leq j \leq r\}$ to be representatives of the conjugacy classes of G and write (7) in matrix form as follows.

$$\begin{pmatrix} \chi_1(g_1) & \chi_2(g_1) & \cdots & \chi_r(g_1) \\ \chi_1(g_2) & \chi_2(g_2) & & \\ \vdots & & & \\ \chi_1(g_r) & & & \chi_r(g_r) \end{pmatrix} \begin{pmatrix} \overline{\chi_1(g_1)} & \overline{\chi_2(g_1)} & \cdots & \overline{\chi_r(g_1)} \\ \overline{\chi_1(g_2)} & \overline{\chi_2(g_2)} & & \\ \vdots & & & \\ \overline{\chi_1(g_r)} & & & \overline{\chi_r(g_r)} \end{pmatrix}$$

$$= \begin{pmatrix} |C_G(g_1)| & & & 0 \\ & |C_G(g_2)| & & \\ & & \ddots & \\ 0 & & & |C_G(g_r)| \end{pmatrix}$$

But since $AB = D$ for D diagonal implies that $BA = D$, we have

$$\begin{pmatrix} \frac{\overline{\chi_1(g_1)}}{m_1} & \frac{\overline{\chi_2(g_1)}}{m_2} & \cdots & \frac{\overline{\chi_r(g_1)}}{m_r} \\ \frac{\overline{\chi_1(g_2)}}{m_1} & \frac{\overline{\chi_2(g_2)}}{m_2} & & \\ \vdots & & & \\ \frac{\overline{\chi_1(g_r)}}{m_1} & & & \frac{\overline{\chi_r(g_r)}}{m_r} \end{pmatrix} \begin{pmatrix} \chi_1(g_1) & \chi_2(g_1) & \cdots & \chi_r(g_1) \\ \chi_1(g_2) & \chi_2(g_2) & & \\ \vdots & & & \\ \chi_1(g_r) & & & \chi_r(g_r) \end{pmatrix} = I_r$$

where $m_j = |C_G(g_j)|$. Then

$$\sum_{j=1}^{r} \frac{\overline{\chi_k(g_j)}\chi_l(g_j)}{m_j} = \begin{cases} 1 & k = l \\ 0 & \text{otherwise} \end{cases}$$

so that

$$\frac{1}{|G|} \sum_{j=1}^{r} |\mathcal{C}_j| \, \overline{\chi_k(g_i)}\chi_l(g_j) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_k(g)}\chi_l(g) = \delta_{k,l}$$

and this is known as the *first orthogonality relation.* This is a relation between the rows of the character table.

Now if $N \lhd G$ and ψ is a representation of G/N, we get a representation of G by $\widetilde{\psi} : g \mapsto \psi(gN)$. Then $\widetilde{\psi}$ is a pullback as in

$$G \longrightarrow G/N \longrightarrow GL(n, k)$$

and ψ is irreducible if and only if $\widetilde{\psi}$ is irreducible. We can see this more easily via the orthogonality relations.

September 29

Definition 16 *$\mathcal{C}(G)$ is the vector space over $\mathbb{C}$ of class functions on G.*

There is a natural inner product on $\mathcal{C}(G)$ given by

$$\langle \varphi_1, \varphi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi_1(g) \overline{\varphi_2(g)}$$

Then the set of irreducible characters $\{\chi_1, \chi_2 \cdots \chi_r\}$ form an orthonormal basis of $\mathcal{C}(G)$. Now if χ is any character, we can write $\chi = \sum_j n_j \chi_j$ for $n_j \geq 0, n_j \in \mathbb{Z}$ and $\langle \chi, \chi_j \rangle = n_j$. Note also that any character χ is irreducible iff $\langle \chi, \chi \rangle = 1$. In terms of modules, if χ corresponds with M and χ_j corresponds with S_j, then $M \cong \bigoplus_j n_j S_j$ where $n_j = \dim \mathrm{Hom}_A(S_j, M) = \dim \mathrm{Hom}_A(M, S_j)$ by Schur's lemma since $\mathrm{Hom}_A(S_i, S_j) = \delta_{i,j}$.

Proposition 13 *If χ, ψ are irreducible characters of G and H respectively, then $\chi \times \psi$ defined $(\chi \times \psi)(x, y) = \chi(x)\psi(y)$ is an irreducible character of $G \times H$ and all the irreducible characters of $G \times H$ are obtained in this way.*

Proof. Show that

$$\frac{1}{|G \times H|} \sum_{(x,y)} (\chi \times \psi)(x, y) \overline{(\chi \times \psi)(x, y)} = 1$$

and also note that the number of conjugacy classes of $G \times H$ is the number of conjugacy classes of G times the number of conjucacy classes of H. ■

If χ is a *virtual character*, that is, $\chi = \sum_j n_j \chi_j$ with $n_j \in \mathbb{Z}$, then $\pm\chi$ is an irreducible character iff $\langle \chi, \chi \rangle = \pm 1$. This will not be true, however, if $n_j \notin \mathbb{Z}$. For example, if $\chi = \frac{1}{2}\chi_1 + \frac{1}{2}\chi_2 + \frac{1}{2}\chi_3 + \frac{1}{2}\chi_4$, then $\langle \chi, \chi \rangle = 1$.

Let ρ be a representation of G with character χ and let $g \in G$. Then the eigenvalues of $\rho(g)$ are $\{\varepsilon_j : 1 \leq j \leq n\}$ where ε_j is an mth root of unity if g has order m. Note that $\chi(g) = \sum_j \varepsilon_j$ and that

$$|\chi(g)| = \left| \sum_j \varepsilon_j \right| \leq \sum_j |\varepsilon_j| = n$$

with equality iff each ϵ_j is real. Hence, $\chi(g) = n = \chi(1)$ iff $\rho(g) = I$. Note that if we consider the subgroup $\langle g \rangle \subset G$ and look at an irreducible representation ρ on $\langle g \rangle$, we have that $\rho(g)$ are scalar matrices. From the character table, we see that if $\chi(g) = n$, then $g \in \ker \rho$. Hence, we can identify normal subgroups of G from the character table.

October 1

Comments on homework 3.

If M is a completely reducible A-module and e is a central idempotent in A, then $M = eM \oplus (1 - e)M$. Note that since e is central, we have that eM and $(1 - e)M$ are submodules, and $e^2 = e$. Therefore e acts as a projection of M on eM. eM is the sum of all the simple submodules of M isomorphic to the simple A-module corresponding to e. For example, $A = \bigoplus Ae_j$ is a special case with $M =_A A$.

In the homework problem on finding f_3, take $H = \langle (12) \rangle$ and take e to be $\frac{1}{2}(1 + (12))$. This is an idempotent corresponding to the trivial representation of the subgroup H. Now take M to be Ae. Then $Ae = Aee_3 \oplus Ae(1 - e_3)$ and apply the above comments. In other words, we find the part of the module Ae which gives the representation of dimension 2, which is Aee_3 and is irreducible. Thus we can take f_3 to be ee_3.

We consider characters of Abelian groups. Let G be Abelian and let ρ be an irreducible representation of G over $\mathbb{C}$ as usual. By Schur's lemma, if $g \in G$, $\rho(g) = \lambda_g I$. But since block diagonal matrices can't be irreducible, we must have that $\dim \rho = 1$, that is, $\rho(g) = \lambda_g$ so that $\rho : G \to \mathbb{C}^\times$ is a homomorphism. (We can also show that each

irreducible representation of an Abelian group is of dimension 1 by Wedderburn theory; see e.g. [DF, p.827].)

For general G, if $g \in G$ and ρ is any representation of G, consider $\langle g \rangle$. Since ρ is completely reducible, we have $\rho(g)$ is diagonalizable since $\langle g \rangle$ is Abelian. Last time we saw that $\chi(g) = \chi(1)$ implies each ε_j is 1. Then $\rho(g) = I$ so that $g \in \ker \rho$. The converse is also true, that is, if $g \in \ker \rho$, then $\chi(g) = \chi(1)$.

We therefore have that normal subgroups can be detected from the character table. In fact, $N \lhd G$ iff

$$N = \bigcap_j \left\{ \ker \chi_j : \chi_j \text{ irreducible with } N \subset \ker \chi_j \right\} \tag{8}$$

Proof. First note that the intersection of the kernels of *all* the χ_j is precisely $\{1\}$ by the Wedderburn decomposition $A = \bigoplus_j Ae_j$. Then if $N \lhd G$, consider G/N and note that the irreducible representations of G/N are obtained from the irreducible representations of G which contain N in their kernel. Conversely, every irreducible representation of G/N gives rise to a representation of G containing N in its kernel. This proves (8). ■

Next, we want to construct the central idempotents of $A = \mathbb{C}G$. Consider $Z = Z(A)$. (Incidentally, note that $x \in Z$ if x is a linear combination of class sums; this can be used in homework 3.) Then Z has dimension r and a basis $\{C_j : 1 \leq j \leq r\}$ where $C_j = \sum_{g \in \mathcal{C}_j} g$. Let $h_j = |\mathcal{C}_j|$. Also, note that $Z = \bigoplus_{j=1}^r Ze_j$ with $Ze_j \cong \mathbb{C}$. So $\{e_j : 1 \leq j \leq r\}$ is another basis of Z. Let $C_i = \sum_j a_{i,j} e_j$ and $e_i = \sum_j b_{i,j} C_j$. We want $b_{i,j} \in \mathbb{C}$.

Observe that Ze_j is the center of Ae_j and χ_j is the character of the representation corresponding to Ae_j by our notational convention.

Note that $\chi_i(e_j) = 0$ when $i \neq j$ and $\chi_i(e_j) = n_i = \chi_i(1)$. Now C_i are represented (in the representation corresponding to χ_j), by scalar matrices, say

$$C_i \mapsto \begin{pmatrix} \omega_j(C_i) & & & \\ & \omega_j(C_i) & & \\ & & \ddots & \\ & & & \omega_j(C_i) \end{pmatrix}.$$

Taking traces, $h_i \chi_j(g_i) = n_j \omega_j(C_i)$. Here $g_i \in C_i$. So we let

$$\omega_j(C_i) = \frac{h_i \chi_j(g_i)}{n_j}.$$

The notation $\omega_j(C_i)$ reflects the fact that $C_i \mapsto \omega_j(C_i)$ is a homomorphism of Z into $\mathbb{C}$. The ω_i are the characters (1-dimensional representations) of Z into $\mathbb{C}$.

Then for $g \in \mathcal{C}_i$, $\chi_j(C_i) = h_i \chi_j(g_i) = a_{i,j} n_j$ so that

$$a_{i,j} = \frac{h_i \chi_j(g_i)}{n_j} = \omega_j(C_i).$$

Substituting, we have

$$C_i = \sum_j \frac{h_i \chi_j(g_i)\, e_j}{n_j},$$

$$\frac{1}{|G|}\sum_{i=1}^{r}\overline{\chi_k(g_i)}C_i=\frac{1}{|G|}\sum_j\sum_i\frac{h_i}{n_j}\chi_j(g_i)\overline{\chi_j(g_i)}e_j=\sum_j\frac{1}{n_j}e_j\delta_{j,k}=\frac{e_k}{n_k}$$

so that

$$e_k=\frac{n_k}{|G|}\sum_{i=1}^{r}\overline{\chi_k(g_i)}C_i.$$

See DF, p.836 for a different way of getting the e_k. This method is important because we will be using the ω_j later. This proof can be found in [CR2, p.236].

October 3

We explain the idea behind the calculation of the central idempotents. Let C_i be the class sum, $g_i\in\mathcal{C}_i$, $n_k=\chi_k(1)$, and h_i the number of elements of $\mathcal{C}_i$.

We have two bases of $Z(A)$ given by

$$C_i=\sum_j a_{i,j}e_j \tag{9}$$

$$e_i=\sum_j b_{i,j}C_j. \tag{10}$$

The $a_{i,j}$ are easier to find. We have $\chi_j(C_i)=\sum_j a_{i,j}\chi_j(e_j)=a_{i,j}n_j$ since $\chi_j(e_i)=\delta_{i,j}n_j$, but on the other hand, $\chi_j(C_i)=h_i\chi_j(g_i)$. So $h_i\chi_j(g_i)=a_{i,j}n_j$ or $a_{i,j}=h_i\chi_j(g_i)/h_j$. Invert the equation (9) to get (10) by multiplying (9) by $\overline{\chi_k(g_i)}$ and summing over i to get the idempotents e_j.

Let

$$\omega_j(C_i)=\frac{h_i\chi_j(g_i)}{n_j} \tag{11}$$

Then $\omega_j:Z\to\mathbb{C}$ given by (11) is a character of Z obtained by restricting χ_j to Z, that is, in the representation of A corresponding to Ae_j, $C_i\to\omega_j(C_i)\,I$

We digress to consider algebraic integers [see, e.g. DF p. 853]. If $K\supset\mathbb{Q}$ is an extension field, an element $a\in K$ is *algebraic over* $\mathbb{Q}$ if a is a root of a monic polynomial $p(x)\in\mathbb{Q}[x]$. If $p(x)\in\mathbb{Z}[x]$, then a is an *algebraic integer*.

We have [e.g. DF, p 853] that

1. sums and products of algebraic integers are algebraic integers,
2. if $a\in\mathbb{C}$, a is an algebraic integer over $\mathbb{Q}$ iff $\mathbb{Z}[a]$ is a finitely generated $\mathbb{Z}$=module,
3. if a is an algebraic integer and is in $\mathbb{Q}$, then $a\in\mathbb{Z}$.

Returning to characters, we have that $\chi_j(g_i)$ is an algebraic integer, since it is a sum of roots of unity. We want to show that $\omega_j(C_i)$ is an algebraic integer

Now

$$\omega_j(C_i)=\frac{h_i\chi_j(g_i)}{n_j}.$$

Consider the basis $\{C_i\}$ of $Z=Z(A)$ and write $C_kC_j=\sum_l c_{k,j,l}C_l$ for some $c_{k,j,l}$. In fact, $c_{j,k,l}$ is the number of pairs g,g' with $gg'=h$ a fixed element in $\mathcal{C}_l$ where $g\in\mathcal{C}_k$ and $g'\in\mathcal{C}_j$. In particular, $c_{j,k,l}$ is an integer. Since ω_i is a character of Z, $\omega_i(C_k)\,\omega_i(C_j)=\sum_l c_{k,j,l}\omega_i(C_l)$. Hence, $\mathbb{Z}[1,\omega_i(C_k):1\le i,k\le r]$ is finitely generated. Since $\mathbb{Z}$ is a PID, $\mathbb{Z}[\omega_j(C_i)]$ is finitely generated so that $\omega_j(C_i)$ is an algebraic integer.

Theorem 6 *If $\chi_i(1) = n_i$, then $n_i \big| |G|$ for each i.*

Proof.

$$\sum_{j=1}^{r} \omega_i(C_j)\overline{\chi_i(g_j)} = \sum_{j=1}^{r} \frac{h_j\chi_i(g_j)\overline{\chi_i(g_j)}}{n_i} = \frac{1}{n_i}\sum_{j=1}^{r} \chi_i(g_j)\overline{\chi_i(g_j)} = \frac{|G|}{n_i}.$$

Now we use the fact that $\frac{|G|}{n_i}$ is an algebraic integer and is rational, hence an integer. ■

Remark 5 *$n_i \big| |G|$ is not true in fields of characteristic p where $p \big| |G|$*

Our last topic in this section is that of *induced representations*. Many of our computations have involved lifting characters from normal subgroups. When we don't have normal subgroups, we want to be able to do something similar for arbitrary subgroups. If $H \leq G$ and ρ is a representation of G, then we get a *restriction* of ρ to H, written ρ_H, $\rho|_H$, or $\mathrm{Res}^G_H(\rho)$. Can we go the other way?

Now if ρ is a representation of H, we want to construct $\mathrm{Ind}^G_H(\rho)$ a representation of G and correspondingly for characters, that is, if ψ is a character of H, we want to construct a character $\mathrm{Ind}^G_H(\psi)$. and we would like

$$\left\langle \mathrm{Ind}^G_H(\psi), \zeta \right\rangle = \left\langle \mathrm{Res}^G_H(\zeta), \psi \right\rangle,$$

where ζ is an arbitrary character of G. That is, Ind and Res should be adjoint operators.

October 6

Today we develop the theory of induced representations, which is discussed in CR1 §10, p.227 (see also DF, p.858). As before R is a commutative ring with 1. Let $H \leq G$ and let $A = RG$ and $B = RH$.

In fact, let A be a ring with 1 and B a subring of A containing 1. Restriction gives a way to produce B-modules from A-module as follows. If M is an A-module, we get a B-module $M|_B$ or $\mathrm{Res}^A_B(M)$ obtained by restricting the scalars.

The reverse operation is called *induction*, which allows us to produce A-modules from B-modules. If L is a B-module, define an A-module, written $\mathrm{Ind}^A_B(L)$, by $\mathrm{Ind}^A_B(L) = A \otimes_B L$. It is then regarded as a A module by

$$a(x \otimes l) = ax \otimes l$$

for $a, x \in A$ and $l \in L$.

Now let $A = RG$. In this situation, this construction is known as Frobenius induction. If M is an A-module, then $\mathrm{Res}^G_H(M)$ is a B-module as before, and if L is a B-module, then $\mathrm{Ind}^G_H(L)$, also written L^G, is an A module by

$$g(x \otimes l) = gx \otimes l$$

for $g, x \in G$ and $l \in L$.

We have alternate descriptions of $\mathrm{Ind}^G_H(L)$ in the context of modules, matrix representations, and characters.

1. (Modules) Let $\{x_1, x_2 \cdots x_n\}$ be left coset representatives for H in G. Then $G = \bigcup_i x_i H$, a disjoint union. Then $\{x_i \otimes l : 1 \leq i \leq n, l \in L\}$ generate L^G since $g \in G$ implies $g = x_i h$ for some x_i and some h, so that

$$g \otimes l = x_i h \otimes l = x_i \otimes hl.$$

We could express this as

$$L^G = \bigoplus_{i=1}^{n} x_i \otimes L$$

and under this identification, $1 \otimes L \cong L$ so that L can be regarded as an RH-submodule of L^G.

2. (Matrices) Let L correspond to the matrix representation $\mathcal{L}$ of H, that is, $h \mapsto \mathcal{L}(h)$. Now since $g(x_i \otimes l) = gx_i \otimes l$ for $g, x_i \in G$ we have $gx_i = x_j h$ for some coset representative x_j and some $h \in H$, and x_j is unique given g and x_i. Then

$$gx_i \otimes l = x_j h \otimes l = x_j \otimes \underbrace{hl}_{\in L}.$$

Note that $h = x_j^{-1} g x_i$

Now if L^G corresponds to the matrix representation $\mathcal{L}^G$,

$$\mathcal{L}^G(g) = \left(\begin{array}{c|c|c|c} \ddots & & 0 & \\ \hline & \ddots & 0 & \\ \hline 0 & 0 & \mathcal{L}\left(x_j^{-1} g x_i\right) & \\ \hline & & & \end{array}\right)$$

This can be seen as follows. Given x_i, g, we have $x_j^{-1} g x_i \in H$ for precisely one j and we get $\mathcal{L}(x^{-1} g x_i)$ in the (j, i) block of $\mathcal{L}^G$.

Example 12 *When $G = S_3$ and $H = \langle (123) \rangle$, let $\mathcal{L}$ be the trivial representation of H. then $G = H \cup (12) H$ with representatives $x_1 = 1$ and $x_2 = (12)$. We want to compute $\mathcal{L}((13))$. Write $g = (13)$. Then*

$$gx_1 = (13)\,1 = (13) = (12)\,(132) = x_2 \cdot h$$

for $h = (132)$ and

$$gx_2 = (13)\,(12) = (123) = x_1 h'$$

for $h' = (123)$. Then $\mathcal{L}^G((12)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Similarly, $\mathcal{L}^G((1)) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\mathcal{L}^G((123)) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Example 13 *Let $H \leq G$. Then $\mathrm{Ind}_H^G(1)$ is the permutation representation of G on the cosets of H. Conversely, if π is a transitive permeation representation of G on a set S, let H be the stabilizer of a fixed element $x \in S$. Then π is equivalent to $\mathrm{Ind}_H^G(1)$.*

3. (Characters) Let $A = KG$ and $B = KH$. Let λ be the character of the representation $\mathcal{L}$ corresponding to L. We want to find λ^G, the character of $\mathcal{L}^G$. It is sufficient to look at blocks of the form $\mathcal{L}\left(x_i^{-1} g x_j\right)$. Thus,

$$\lambda^G(g) = \sum_{i=1}^{n} \lambda\left(x_i^{-1} g x_k\right)$$

with the convention that $\lambda\left(x_i^{-1} g x_i\right) = 0$ if $x_i^{-1} g x_i \notin H$. Alternately, set

$$\dot{\lambda}\left(x_i^{-1} g x_i\right) = \begin{cases} \lambda\left(x_i^{-1} g x_i\right) & x_i^{-1} g x_i \in H \\ 0 & \text{otherwise} \end{cases}$$

Then $\lambda^G(g) = \sum_{i=1}^{n} \dot{\lambda}\left(x_i^{-1} g x_i\right)$.

Alternately, take

$$\lambda^G(g) = \frac{1}{|H|} \sum_{x \in G} \dot{\lambda}\left(x^{-1} g x\right)$$

and this is choice free.

Note that $\lambda^G(1) = [G : H]$

Remark 6 *(a) Ind is additive, that is,* $\mathrm{Ind}_H^G(L_1 \oplus L_2) \cong \mathrm{Ind}_H^G(L_1) \oplus \mathrm{Ind}_H^G(L_2)$.

(b) Ind is transitive, that is, If $K \leq H \leq G$, *then*

$$\mathrm{Ind}_K^G(L) = \mathrm{Ind}_H^G \mathrm{Ind}_K^H(L).$$

Next time we consider Frobenius reciprocity, that is

$$\mathrm{Hom}_{RG}\left(L^G, M\right) \cong \mathrm{Hom}_{RH}\left(L, M|_H\right)$$

for L an RH-module, and M and RG-module.

October 8

Theorem 7 *(Adjoint Associativity, CR1 §2.19) If* A *and* B *are two rings,* L' *a left* A*-module,* M' *is a* (B, A)*-bimodule and* N' *is a left* B *module. Then*

$$\mathrm{Hom}_A\left(L', \mathrm{Hom}_B\left(M', N'\right)\right) \cong \mathrm{Hom}_B\left(M' \otimes_A L', N'\right)$$

as abelian groups.

Theorem 8 *(Frobenius Reciprocity CR1 p. 232) Let* $H \leq G$ *and let* L *be a* RH*-module and* M *an* RG*-module. Then*

$$\mathrm{Hom}_{RH}\left(L, M_H\right) \cong \mathrm{Hom}_{RG}\left(L^G, M\right)$$

Proof. Set $A = RH$, $B = RG$ $L' = L$, $M' = RG$, and $N' = M$ as in (7). Then

$$\mathrm{Hom}_{RG}\left(L, \mathrm{Hom}_{RG}\left(RG, M\right)\right) \cong \mathrm{Hom}_{RG}\left(RG \otimes_{RH} L, M\right)$$

Then the right hand side is as required. For the left hand side, we have $\mathrm{Hom}_{RG}\left(RG, M\right)$ is an RH-module by

$$\left(bf\right)\left(a\right) = f\left(ab\right)$$

for $b \in RH$, $a \in RG$, and $f \in \mathrm{Hom}_{RG}\left(RG, \right)$. Then $\tau : \mathrm{Hom}_{RG}\left(RG, M\right) \to M$ which maps f to $f(1)$ is an RH-isomorphism as follows.

$$\tau\left(bf\right) = \left(bf\right)\left(1\right) = f(b) = bf(1) = b\tau\left(f\right)$$

since f is an RG-module homomorphism. Then the left hand side is as required. ■

Corollary 4 *If $R = \mathbb{C}$ or some other field of charactersic 0, ψ is a character of H and ζ is a character of G, then*

$$\left\langle \mathrm{Ind}_H^G\left(\psi\right), \zeta \right\rangle_G = \left\langle \psi, \mathrm{Res}_H^G\left(\zeta\right) \right\rangle_H.$$

This says that Ind and Res are adjoint functors.

Returning to characters,

$$\lambda^G\left(g\right) = \frac{1}{|H|} \sum_{x \in G} \dot{\lambda}\left(x^{-1} g x\right)$$

where λ is a character of H and $g \in G$. Now we want to simplify this to a more manageable form.

First we digress to consider double cosets (DF p. 119, problem 10) If $H, K \leq G$, then $G = \bigcup_x HxK$ for disjoint double cosets HxK. We count

$$\begin{aligned} |HxK| &= \frac{|H|}{[K : K \cap x^{-1}Hx]} \\ &= \frac{|K|}{[H : H \cap xKx^{-1}]} \\ &= \frac{|K|\,|H|}{[H \cap xKx^{-1}]} \end{aligned}$$

We fix the following notation. Write $\mathcal{C}$ for the conjugacy class of g in G and

$$\mathcal{C} \cap H = \bigcup_{i=1}^{s} \mathcal{C}_i'$$

where $\mathcal{C}_i'$ are the conjugacy classes of H contained in $\mathcal{C}$. Let $h_i \in \mathcal{C}_i'$. Then

$$\lambda^G\left(g\right) = |C_G\left(g\right)| \sum_{i=1}^{s} \frac{1}{|C_H\left(h_i\right)|} \lambda\left(h_i\right)$$

where $\lambda^G\left(g\right) = 0$ if $\mathcal{C} \cap H = \emptyset$.

Proof. Let

$$X_i = \left\{ x \in G : x^{-1} g x \text{ conjugate to } h_i \text{ in} H \right\}$$

Then

$$\lambda^G(g) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \lambda\left(x^{-1}gx\right) = \frac{1}{|H|} \sum_{i=1}^{s} |X_i| \lambda(h_i). \tag{12}$$

For each i, fix $t_i \in X_i$ such that $t_i^{-1} g t_i = h_i$.

Then

$$\begin{aligned} x \in X_i &\Leftrightarrow x^{-1}gx = h^{-1}h_i h (h \in H) \\ &\Leftrightarrow hx^{-1}gxh^{-1} = h_i = t_i^{-1}gt_i \\ &\Leftrightarrow \left(t_i h x_i^{-1}\right) g \left(x h^{-1} t_i^{-1}\right) = g \\ &\Leftrightarrow x h^{-1} t_i^{-1} \in C_G(g) \\ &\Leftrightarrow x \in C_G(g)\, t_i H \end{aligned}$$

so

$$|X_i| = |C_g(g)\, t_i h| = \frac{|C_G(g)|\,|H|}{\left|H \cap t_i^{-1} C_G(g)\, t_i\right|}$$

Substituting this into (20) and noting that $\left|H \cap t_i^{-1} C_G(g)\, t_i\right| = |C_H(h_i)|$ we get the result. ■

Example 14 *Let $H = A_4$ and $G = S_4$. Then*

$$\begin{aligned} \mathrm{Ind}_H^G(\chi_2) &= \chi_3, \\ \mathrm{Ind}_H^G(\chi_3) &= \chi_3, \\ \mathrm{Ind}_H^G(\chi_4) &= \chi_4 + \chi_5, \\ \mathrm{Ind}_H^G(\chi_1) &= \chi_1 + \chi_2. \end{aligned}$$

Now let $K = S_3$ (acting on {1,2,3}), regarded as a subgroup of G. Then

$$\mathrm{Ind}_K^G(\chi_1) = \chi_1 + \chi_4.$$

Thus we obtain all the characters of G.

October 10

We discuss the example of $G = S_4$, $H = A_4$, further. By Frobenius reciprocity, $\chi_3|_H = \chi_2 + \chi_3$, $\chi_1|_H = \chi_2 + \chi_3$, and $\chi_4|_H = \chi_5|_H = \chi_4$.

As a demonstration of induction by the simplified formula, we compute $\chi_2^G((123))$. Note that the class of (123) splits in A_4 into two classes, those of (123) and (124). Then $\chi_2^G((123)) = 3\left(\frac{1}{3}\zeta + \frac{1}{3}\zeta^2\right) = -1$.

We discuss the characters of $GL(3,2)$. We first make some general comments about $G = GL_n(\mathbb{F}_q)$. We have $|G| = q^{\frac{n(n-1)}{2}}(q-1)(q^2-1)\cdots(q^n-1)$. G acts on a vector space V over $\mathbb{F}_q$ of dimension n. A *flag* in V is a sequence of subspaces

$$0 \subset V_1 \subset V_2 \subset \cdots \subset V_m = V.$$

Then G permutes the flags transitively. A flag is *complete* if $n = m$ and $\dim V_j = j$. For example,

$$0 \leq \langle v_1 \rangle \leq \langle v_1, v_2 \rangle \leq \cdots \leq \langle v_1, v_2 \cdots v_n \rangle = V$$

is a complete flag where $\{v_1, v_2 \cdots v_n\}$ is a basis of V. Then the stabilizer B (for *B*orel) of a complete flag is the set of upper triangular matrices. The stabilizer of an arbitrary flag is called a *parabolic subgroup.*

When $n = 3$, take $\{v_1, v_2, v_3\}$ to be a basis. Then B is the stabilizer of

$$0 \leq \langle v_1 \rangle \leq \langle v_1, v_2 \rangle \leq v.$$

and $|B| = q^3 (q-1)^3$. G acts transitively on the complete flags, equivalently on the cosets of B.

The permutation representation of G on the flags is $\mathrm{Ind}_B^G(1)$ is a representation of degree $\frac{|G|}{|B|} = (q+1)(q^2+q+1)$.

When $q = 2$ as in the homework, $|B| = 8$. Then $\mathrm{Ind}_B^G(1)(g)$ should be the number of flags fixed by $g \in G$. This can be used to compute the values of the induced character. (See the example below.) The trivial character will be a constituent of this by Frobenius reciprocity.

For P the stabilizer of $0 \leq \langle v_1 \rangle \leq V$, $\mathrm{Ind}_P^G(1)$ should be the sum of the trivial character and one other.

We determine that P is a semidirect product $(GL_2 \times GL_1) U$, $U \lhd P$ and use this to compute $\mathrm{Ind}_P^G(\epsilon)$.

As an example, if $g = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, then consider g as an element of $GL(3, \overline{\mathbb{F}}_q)$ where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$. The set of complete flags in a corresponding vector space over $\overline{\mathbb{F}}_q$, fixed by g is an algebraic variety which is the intersection of two projective lines. The number of such flags over $\mathbb{F}_q$ is $2q+1$. To compute this last number, work with the basis given above and write down the possible flags fixed by g.

Remark 7 *If $G = GL_n(\mathbb{F}_q) \subset \overline{G} = GL_n\left(\overline{\mathbb{F}}_q\right)$ then $B \subset \overline{B}$. The variety over $\overline{\mathbb{F}}_q$ of flags fixed by $g \in G$ is an important one.*

We now connect ordinary (characteristic 0) and modular (characteristic p for $p \big| |G|$) representations of G. The representations over $\mathbb{C}$ can be written (by taking matrices over $\mathbb{C}$, which are finite in number) in a finite extension of $\mathbb{Q}$, that is, an algebraic number field K.

Let $\mathcal{O} \subset K$ be the ring of algebraic integers in K, $\mathfrak{p}$ a prime ideal in $\mathcal{O}$ containing p. Then $\mathcal{O}/\mathfrak{p}$ is a field of characteristic p. The ring $\mathcal{O}$, however, is not a PID, but we can fix this by taking the localization of $\mathcal{O}$ at $\mathfrak{p}$, which is the set $\mathcal{O}_{\mathfrak{p}} = \left\{\frac{a}{b} : a, b \in \mathcal{O}, b \notin p\right\}$. Then $\mathcal{O}_{\mathfrak{p}}$ is a DVR.

For the properties of a DVR, see DF p.721 or CR1 p. 81. Start with a discrete valuation on K, i.e. a map $\nu : K^* \to \mathbb{Z}$ with, among other properties, $\nu(x+y) \geq \min(\nu(x), \nu(y))$. Then $R = \{x \in K^* : \nu(x) \geq 0\} \cup \{0\}$ is a DVR.

The valuation induces a metric on K and we can form the completion $\widehat{K}$ of K and $\widehat{R}$ of R with respect to this metric. [See DF p. 725, or CR1, p.83.]

Our goal is to consider KG, RG, and kG where K is a field of characteristic 0, R is a DVR in K, and $\mathfrak{p}$ is a prime ideal in R such that $k = R/\mathfrak{p}$ is a field of characteristic p.

October 13

Final Homework Hint. The funny number $\frac{-1+i\sqrt{7}}{2}$ that appears in the character table is a sum of three seventh roots of unity.

Final Remarks on $\mathbb{C}G$.

1. The number of linear characters of G is $[G : G']$, the index of the commutator subgroup of G (DF p.827).

2. To compute characters of abelian groups, we write the group as a direct product of cyclic groups. We know how to compute characters for cyclic groups and for direct products.

3. An application of the theory of representations over $\mathbb{C}G$ is the classical theorem of Burnside that a group of order $p^a q^b$ is solvable for p and q primes (see DF p. 852). This theorem later lead to the famous theorem of Feit and Thompson from 1963 that every group of odd order is solvable. This year is the 40th anniversary of that famous theorem.

4. Hossein is going to Feit's retirement conference, which also celebrates that anniversary.

Let p be a fixed prime. We call (K, R, k) a p-modular system when K is a field of characteristic 0, usually an algebraic number field, that is, a finite extension of $\mathbb{Q}$, in which we can write the complex irreducible representations of G and its subgroups. $R \subset K$ is a DVR, sometimes taken to be complete, $\mathfrak{p}$ is a prime ideal of R containing p, and $k = R/\mathfrak{p}$, a field of characteristic p.

We can take $\mathfrak{p} = R\pi$ to be a principal ideal. If K is complete and $a \in K$, then

$$a = \pi^{-k}\left(a_0 + a_1\pi + \cdots\right)$$

and $a \in R$ if and only if $a = a_0 + a_1\pi + \cdots$. The $a_i \in \mathcal{S}$, a set of representatives of R over $\mathfrak{p}$.

Consider KG, RG, and kG. We have $RG \subset KG$, $KG = K \otimes_R RG$ (known an extension of scalars) and $kG = k \otimes_R RG$ (known as reduction mod p). Also, KG and kG are finite-dimensional algebras over K and k respectively and hence are artinian. We don't know much about the structure of RG, but KG and kG/J are semisimple. Write

$$kG/J = \bigoplus_i (kG/J)f_i$$

for f_i primitive, orthogonal idempotents. Surprisingly, we can lift this decomposition to kG and provided that R is complete, we can lift the decomposition of kG to RG.

Let V be a KG-module with basis $\{v_1, v_2 \cdots v_n\}$. Let M be the RG-module defined by

$$M = \sum_{i=1}^{n} RGv_i = \sum_{g\in G}\sum_{i=1}^{n} Rgv_i.$$

Then M is a finitely generated, torsion-free R-module and R a PID. Hence, M is a free R-module. Pick a basis $\{u_1, u_2, \ldots, u_m\}$ of M (over R). Then

$$V = K \otimes_R M$$

so that $m = n$ and $\{u_1, u_2, \ldots, u_m\}$ is a also a basis of V over K. This all means that we can find a basis of V which generates, over R, an RG-module M, that is, starting with a representation ρ of G such that $\rho(g)$ has entries in K, we find an equivalent representation $\widehat{\rho}$ of G which has entries in R. Then reducing $\bmod \mathfrak{p}$, we have that $\overline{\widehat{\rho(g)}}$ are matrices over k. Note that M is not unique since we could have selected a different basis for V initially. We call M an RG-lattice in V.

Furthermore, we can take

$$\overline{M} = k \otimes_R M$$

giving us modules V over K, M over R, and $\overline{M}$ over k.

Preview of Idempotent Lifting Let A be an R-algebra for R a commutative ring with 1. If N is an ideal of A the *N-adic topology* on A consists of the system of neighborhoods of $a \in A$ given by $a + N^k$ for $k = 0, 1, 2 \cdots$.

Theorem 9 *Let N be an ideal of A such that A is complete in the N-adic topology. Let f be an idempotent of A/N. Then there is an idempotent $e \in A$ such that $\overline{e} = f$ where $\bar{\cdot}$ denotes reduction* $\bmod N$. *Furthermore, e is primitive if and only if $\overline{e}$ is primitive.*

October 15

Further Hint for Homework, if you want to use MAPLE

We have $P \leq G$ with $|P| = 24$. If we take a suitable ε, the induced character will be irreducible. Select coset representatives as follows. Let S be the 7-Sylow subgroup generated by $A = \left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$. Now for G/P (not a group, a set of cosets) take representatives $\{A^j : 0 \leq j \leq 6\}$. We need to determine if $x_j^{-1} g x_i \in H$ and then put in $\varepsilon\left(x_j^{-1} g x_i\right)$ in the formula for the induced character. As g runs over the representatives of conjugacy classes of G, find out whether $A^{-j} g A^i \in P$ using Maple.

Let A be a ring, N a two sided ideal in A such that A is complete in the N-adic topology. This is explained as follows. That is, if $a \in A$, the neighborhoods of A are $\left\{a + N^k : k = 0, 1, 2 \cdots\right\}$. A *Cauchy sequence* $\{a_n : n \geq 1\}$ is a sequence where given N^k, we have $a_m - a_n \in N^k$ for $m, n > n_0$ for some n_0. A is *complete* if every Cauchy sequence converges to some point in A, that is, there exists $l \in A$ such that given N^k, $a_n - l \in N^k$ for $n > n_0$.

For example, if A is Artinian and $N \subset J$, then A is complete since $N^k = 0$ for sufficiently large k.

Theorem 10 *Let A be a ring and let N be a two-sided ideal such that A is complete in the N-adic topology. Write $\overline{A} = A/N$.*

1. *If f is an idempotent of $\overline{A}$, then there exists an idempotent e of A with $\overline{e} = f$.*
2. *Furthermore, if $N \subset J(A)$, e is primitive if and only if f is primitive.*

For example, if A were Artinian, then A/J would be semisimple so that the idempotents of A/J we found previously would lift to idempotents of A.

Proof. In $\mathbb{Z}[x]$, write

$$1 = x + (1 - x) = (x + (1 - x))^{2n} = \sum_{j=0}^{2n} \binom{2n}{j} x^{2n-j} (1 - x)^j .$$

Let

$$f_n(x) = \sum_{j=0}^{n} \binom{2n}{j} x^{2n-j} (1-x)^j \in \mathbb{Z}[x].$$

We make the following preliminary computations.

1. $f_n \equiv 0 \left(\mathrm{mod} x^n\right)$, since every term in f_n is divisible by x^n.
2. $f_n \equiv 1 \left(\mathrm{mod} (x-1)^n\right)$ since

$$1 = f_n(x) + \sum_{j=n+1}^{2n} \binom{2n}{j} x^{2n-j} (1-x)^j.$$

3. $f_n(x)^2 \equiv f_n(x) \left(\mathrm{mod} x^n (1-x)^n\right)$ from above.
4. $f_n(x) \equiv f_{n-1}(x) \left(\mathrm{mod} x^{n-1} (x-1)^{n-1}\right)$ since

$$f_n - f_{n-1} = \binom{2n}{n} x^{n-1} (x-1)^{n-1}.$$

5. Finally, $f_1(x) \equiv x \left(\mathrm{mod} x - x^2\right)$ since

$$f_1 = x^2 + 2x(1-x) = 2x - x^2$$

so that $f_1 - x = x - x^2$.

Returning to $\overline{A}$, suppose $f^2 = f$ in $\overline{A}$. Pick $a \in A$ with $\overline{a} = f$. Then $a(a-1) = a^2 - a \in N$. Since a and $a-1$ commute, this means that for any j,

$$a^{j-1} (a-1)^{j-1} \in N^{j-1}$$

so that

$$f_j(a) \equiv f_{j-1}(a) \left(\mathrm{mod} N^{j-1}\right)$$

and

$$f_{j+k}(a) \equiv f_k(a) \left(\mathrm{mod} N^k\right)$$

for any k so that $\{f_n(a) : n \geq 1\}$ is a Cauchy sequence in A. This sequence has a limit $e \in A$. By part 3 above, we have that $e^2 = e$, since what part 3 means is that the sequence $f_n(a)^2 - f_n(a)$ has the limit 0. Also we have $e - a \in N$ and so $\overline{e} = f$ by the last two calculations.

October 17

Final, Final Homework Hint. $P \cong S_4$. You will use the character table of $GL(3,2)$ to verify the Alperin-Mckay and Isaacs-Navarro conjectures for this group.

Last time we had A complete in the N-adic topology and f an idempotent of $\overline{A} = A/N$. We picked $a \in A$ with $\overline{a} = f$. Then $a^2 - a \in N$. We defined a sequence $\{f_n(a) \in A : n \geq 1\}$ and showed that

$$\begin{aligned} f_1(a) - a &\in N \\ &\vdots \\ f_n(a) - f_{n-1}(a) &\in N^{n-1} \end{aligned}$$

and that $f_n(a)^2 - f_n(a) \in N^n$. We let $\lim_{n\to\infty} f_n(a) = e$ so that $e^2 = e$ and $\overline{e} = \overline{a} = f$.

We now consider the second part of the claim. Assuming $N \subset J(A)$, we want to show that f is primitive if and only if e is primitive.

Proof. If $e = e_1 + e_2$ for $e_1^2 = e_2$, $e_2^2 = e_2$, $e_1e_2 = e_2e_1 = 0$, then $\overline{e} = \overline{e_1} + \overline{e_2}$. If $\overline{e}$ is primitive, then one $\overline{e_1} = 0$ say, that is, $e_1 \in N \subset J$. But then $1 - e_1$ has a left inverse which is not possible as $(1 - e_1)\, e_1 = 0$.
Conversely, if $\overline{e} = e_1' + e_2'$ for $e_1'^2 = e_1$ etc, pick $a \in A$ with $\overline{a} = e_1'$. Let $b = eae$. Then

$$be = eb = b \text{ and } \overline{b} = \overline{e}e_1'\overline{e} = e_1' \tag{13}$$

Let $\lim_{n\to\infty} f_n(b) = e_1 \in A$. Then $\overline{e_1} = e_1' \left(= \overline{b}\right)$ and $ee_1 = e_1e = e_1$ by 13.
Let $e - e_1 = e_2$ so that $e = e_1 + e_2$ and $e_1e_2 = 0$ and $e_2^2 = e_2$. Then e is not primitive.
■

Apply the lifting of idempotents to the group algebras RG and kG where (K, R, k) is a p-modular system with $R/P \cong k$. We apply the theorem in the following cases. The notation below is insane and is not intended to match that of Theorem (3).

1. $\overline{A} = kG$ and $N = J\left(\overline{A}\right)$. The completeness follows from the fact that $\overline{A}$ is artinian, so that J is nilpotent.

   In this situation, $\overline{A}/J\left(\overline{A}\right)$ is semisimple so that

   $$\overline{A}/J\left(\overline{A}\right) \cong \bigoplus_i \overline{A}/J\left(\overline{A}\right)\widetilde{\overline{e_i}}$$

   where the $\widetilde{\overline{e_i}}$ are primitive, orthogonal idempotents.

   Then

   $$\overline{A} = \bigoplus_i \overline{A}\overline{e_i}$$

   where the $\overline{e_i}$ are primitive, orthogonal idempotents. The $\overline{A}\overline{e_i}$ are generally not irreducible and have composition factors. We have

   $$J\left(\overline{A}\right)\overline{e_i} \subset \overline{A}\overline{e_i}$$

   with $\overline{A}\overline{e_i}/J\left(\overline{A}\right)e_i$ completely reducible.

2. We go from kG to $RG = A$. Note that $A/PA \cong \overline{A}$.

   Recall Nakayama's Lemma (DF p. 717, CR1 5.7)

   Lemma 3 *If A is a ring, M is a finitely generated A-module, and $L \leq M$, then $L + J(A) = M$ implies $L = M$.*

   We use this to show the following lemma.

   Lemma 4 $PA \subset J(A)$

Proof. Since M is a simple A-module, $M = Am$ for some $0 \neq m \in M$. Then $(PA)\,M \leq M$ so that $(PA)\,M$ is M or 0. If $(PA)\,M = M$, then by Nakayama's lemma, $M = 0$ since $P = J(R)$ and M is finitely generated as R-module. Hence $(PA)\,M = 0$, PA kills every simple module, that is, $PA \subset J(A)$ ■

Finally, $A/PA = \overline{A}$ is artinian and

$$J(A/PA) = J(A)/PA$$

so that $J(A)^t \subset PA$ for some t. A is a finitely generated R-module and R is complete in the P-adic topology imply that A is complete in the PA-adic topology. This implies that A is also complete in the J-adic topology.

We have, by lifting from A/PA to A,

$$\begin{array}{c} A \\ | \\ J(A) \\ | \\ PA \end{array}$$

$\overline{A} = A/PA = \bigoplus \overline{A}\overline{e_i}$ leads to $A = \bigoplus Ae_i$ for $A = RG$ where the e_i are a set of primitive orthogonal idempotents. Thus we have lifted idempotents from characteristic p to characteristic 0. We can also lift from $A/J(A)$ to A, and this will be done next time.

October 20

Further discussion on Homework 5. Let $G = GL_3(\mathbb{F}_2)$. Then B, the subgroup of upper triangular matrices, has order 8 and is the stabilizer of a "standard flag"

$$\langle v_1 \rangle \leq \langle v_1, v_2 \rangle \leq V$$

where $\{v_1, v_2, v_3\}$ is a basis of the vector space V over $\mathbb{F}_2$ on which G acts. G acts transitively on the set of flags, and thus the induced representation $\mathrm{Ind}_B^G(1)$ is just the permutation representation of G on the set of flags. Given an element $g \in G$, we can compute the number of flags fixed by g, and this gives the value of this induced character at g. For example if g is unipotent (eigenvalues 1) with Jordan blocks of sizes 2 and 1, we compute the number of flags fixed by g to be 5 ($1 + 2q$ if we replace $\mathbb{F}_2$ by $\mathbb{F}_q$).

From last time, we have the rings $A = RG$ which is neither semisimple nor artinian and $\overline{A} = A/PA = kG$, which is not semisimple but artinian. We have

$$\overline{A} = \bigoplus_i \overline{A}\overline{e_i}$$

where the $\overline{e_i}$ are lifted from idempotents $\widetilde{\overline{e_i}}$ in $\overline{A}/J\overline{A}$ and

$$A = \bigoplus Ae_i$$

where the e_i are lifted from the idempotents $\overline{e_i}$.

In fact we can also look at A/JA which is semisimple so that

$$A/JA = \bigoplus_i (A/JA)\,\widetilde{e_i}.$$

We want to consider the structure of Ae_i and $\overline{A}\overline{e_i}$ when $\overline{e_i}$ and e_i are primitive.

Proposition 14 *For A any ring with e a primitive idempotent, Ae is an indecomposable left A-module.*

Proof. Let $Ae = L_1 \oplus L_2$ for left ideals L_1 and L_2 and let $e = e_1 + e_2$ for $e_1 \in L_1$, $e_2 \in L_2$. For any $x \in Ae$, $xe = x$ for $x = ye$, $xe = ye^2 = ye = x$ so $e_1e = e_1$ so $e_1 = e_1(e_1 + e_2) = e_1^2 + e_1e_2$ where $e_1^2 \in L_1$ and $e_1e_2 \in L_2$. Hence $e_1 = e_1^2$ and $e_1e_2 = 0$. Similarly, $e_2^2 = e_2$ and $e_2e_1 = 0$. Therefore e_1, e_2 are orthogonal idempotents. Thus e is not primitive. Hence Ae is indecomposable.

Conversely, if Ae is indecomposable, suppose $e = e_1 + e_2$ with $e_1^2 = e_1$, $e_2^2 = e_2$ and $e_1e_2 = e_2e_1 = 0$. Then $x \in Ae$ implies $x = xe = xe_1 + xe_2 \in Ae_1 + Ae_2$. Also, $Ae_1 \cap Ae_2 = 0$ since $xe_1 = ye_2$ implies $xe_1^2 = ye_2e_1 = 0$ so that $xe_1 = 0$ ■

Hence *irreducible* in the semisimple case is replaced by *indecomposable* in the general case. In the semisimple case, if M is an irreducible A-module, then $\mathrm{End}_A(M)$ is a division ring. In the general case, we will see that M is indecomposable implies that $\mathrm{End}_A(M)$ is a local ring.

Recall that a *local ring* is a ring which has a unique maximal left ideal and that a ring A is local if and only if $J(A)$ is maximal. Also, M is indecomposable if and only if $\mathrm{End}_A(M)$ has no idempotents except 0 and 1 since and idempotent in End_A is a projection on a direct summand.

October 22

Let A be any ring and e an idempotent in A. We showed last time that e is primitive if and only if Ae is indecomposable. We also know that if Ae is irreducible, then $\mathrm{End}_A(Ae) \cong eAe$ is a division ring by Schur's lemma. We want to prove the corresponding claim that Ae is indecomposable implies $\mathrm{End}_A(Ae)$ is a local ring. If B is a ring, recall that the following are equivalent.

1. B is a local ring
2. B has a unique maximal left ideal
3. $J(B)$ is maximal
4. the non-units form a left ideal
5. $B/J(B)$ is a division ring.

The proof of this claim is similar to the proof of the commutative case given in DF, p.684. For the general case see CR§5.21.

Example 15 *Let $A = kG$ for k a field of characteristic p and G a p-group. Then $J(A)$ is spanned by $\{1 - x : x \in G\}$ since $(1-x)^{p^n} = 0$ where $p^n = |G|$. Also, $\dim_k A/J(A) = 1$ so $J(A)$ is maximal and A is a local ring.*

Now let A be any ring. We begin with the following important lemma.

Lemma 5 *(Fitting's Lemma) Let M a an A-module with ACC and DCC. Then M has a composition series. Let $f \in \mathrm{End}_A(M)$. Then $M = \mathrm{Im}(f^n) \oplus \ker(f^n)$ for sufficiently large n. (DB, Lemma 1.4.4; DF p. 646 in some form)*

Proof. Since M has ACC and DCC, we can find n with $\mathrm{Im}(f^n) = \mathrm{Im}\left(f^{n+k}\right)$ and $\ker(f^n) = \ker\left(f^{n+k}\right)$ for $k > 0$. Let $x \in M$. Then $f^n(x) = f^{2n}(x)$ and

$$x = \underbrace{f^n(x)}_{\in \mathrm{Im}(f^n)} + \underbrace{(x - f^n(x))}_{\in \ker f^n(x)}.$$

If $x \in \mathrm{Im}(f^n) \cap \ker(f^n)$, then $x = f^n(y)$ so that $0 = f^n(x) = f^{2n}(y) = f^n(y) = x$. ■

Proposition 15 *Let M be an indecomposable A-module with ACC and DCC. Then $\mathrm{End}_A(M)$ is a local ring.*

Proof. Let $E = \mathrm{End}_A(M)$ and let I be a maximal ideal in E. Let $a \notin I$. We show that a is a unit in E. We have $E = Ea + I$ as I is maximal so we have $1 = \lambda a + \mu$ for $0 \neq \lambda \in E$ and $\mu \in I$. Then $1 - \mu = \lambda a$ and μ is not a unit since $\mu \in I$. Hence $\mathrm{Im}(\mu) \neq M$. By Fitting's Lemma, $M = \mathrm{Im}(\mu^n) \oplus \ker(\mu^n)$. Now since M is indecomposable, we have $\mathrm{Im}(\mu^n) = 0$ and $\ker(\mu^n) = M$ so that $\mu^n = 0$. Then $1-\mu$ has the inverse $1+\mu+\cdots+\mu^{n-1}$ so that λa is invertible and a is a unit. ■

Remark 8 Fitting's Lemma is sometimes stated as the following. If M is indecomposable and $\mu \in \mathrm{End}_A(M)$, then μ is an isomorphism or is nilpotent. Note the analogy with Schur's Lemma.

Theorem 11 *(Krull-Schmidt Theorem, CR1 p.128) Let A be any ring and M a finitely generated A-module which is a direct sum $M = \bigoplus_{i=1}^r M_i$ for M_i indecomposable and $\mathrm{End}_A(M_i)$ local. Then if also $M = \bigoplus_{j=1}^s N_j$ with N_j indecomposable, then $r = s$ and $M_i \cong N_j$ after some reordering.*

Proof. We prove this by induction on r. When $r = 1$ the statement is clear. Assume $r \geq 2$. We then have

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_r$$
$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_s.$$

Let $\mu_i : M \to M_i$ and $\nu : M \to N_i$ be projections. Then $\sum_{j=1}^s \nu_j = 1$. On M_1, we have

$$\sum_{j=1}^{s} \mu_1 \nu_j = 1_M.$$

Now since $\mathrm{End}_A(M_1)$ is a local ring so that a sum of non-units is a non-unit, we have that some $\mu_1\nu_j$ is a unit, say $\mu_1\nu_1$ after some reordering.

Let $\varphi = \mu_1\nu_1 : M_1 \to M_1$. Then

$$\begin{aligned} \nu_1 &: M_1 \to N_1 \\ \varphi^{-1}\mu_1 &: N_1 \to M_1 \end{aligned} \tag{14}$$

are inverses of one another, that is,

$$\left(\varphi^{-1}\mu_1\right)\nu_1 = 1_{M_1},$$

that is, N_1 is a direct summand of M_1. Since M_1 is indecomposable, we have $N_1 = \nu_1(M_1)$.

Consider $M' = N_1 \oplus M_2 \oplus \cdots \oplus M_r \leq M$. If $n_1 + m_2 + \cdots + m_r = 0$, then $\mu_1(n_1) = 0$ so that $n_1 = 0$ since μ_1 is injective by (14). Then $m_2 = \cdots = m_r = 0$, that is, the sum is direct.

Next we show that $M' = M$ and that we have an automorphism $\rho : M \to M$ which takes $M_1 \to N_1$ and hence induces an isomorphism $M/M_1 \to M/N_1$. We then apply induction. ■

October 24

The philosophy of modular representations is to obtain global information from local information. Having fixed a prime p, obtaining *local* or *p-local* information means gathering information from subgroups of G such as number of characters or character values, which is related to p-subgroups such as normalizers of p-subgroups.

We complete the proof of the Krull-Schmidt Theorem:

Proof. Given

$$\begin{aligned} M &= M_1 \oplus M_2 \oplus \cdots \oplus M_r \\ M &= N_1 \oplus N_2 \oplus \cdots \oplus N_r \end{aligned}$$

we defined projections

$$\begin{aligned} \mu_i &: M \to M_i \\ \nu_i &: M \to N_i \\ \mu_1 &: M \to M_i \\ \varphi^{-1}\mu_1 &: N_1 \to M_1 \end{aligned}$$

with the last two being isomorphisms, and we defined

$$M' = N_1 \oplus M_2 \oplus \cdots \oplus M_r \leq M$$

Now $\sum_i \mu_i = 1_M$. If $x \in N_1$,

$$\begin{aligned} x &= \mu_1(x) + \mu_2(x) + \cdots + \mu_r(x) \\ \mu_1(x) &= \underbrace{x}_{\in N_1} - \underbrace{\mu_2(x) - \cdots - \mu_r(x)}_{\in M_2 \oplus \cdots \oplus M_r} \end{aligned}$$

so that $\mu_1(x) \in M'$, that is, $\mu_1(N_1) \subset M'$, that is, $M_1 \subset M'$ so $M = M'$

Then $\nu_1\mu_1 + \mu_2 \cdots \mu_r$ is an action on M which takes $M_1 \to N_1$ and $M_i \to M_i$ for $i > 1$ and this induces an isomorphism

$$M_2 \oplus \cdots \oplus M_r \cong M/M_1 \to M/N_1 \cong N_2 \oplus \cdots \oplus N_s.$$

Applying induction, we are done. ■

Hence we have uniqueness of decomposition into indecomposable submodules of a module M if M has ACC and DCC.

This can be applied to the A-modules $A = KG$ and $A = kG$, which are finite dimensional algebras. It remains to show that Krull-Schmidt Theorem for RG. For this, we need to show that if $A = RG$ and M is a finitely generated A-module, then $\mathrm{End}_A(M)$ is a local ring.

The following discussion is in CR1 p. 105 and p. 112.

Lemma 6 *If $f : B \to B'$ is a surjective map of rings, then $f(J(B)) \subset J(B')$ and we get a surjective map $\overline{f} : B/JB \to B'/JB'$.*

This can be verified by considering maximal left ideals.

Proposition 16 *If R is a commutative, local ring, $P \subset R$ A a finitely generated R-algebra which is finitely generated as an R-module, then A/JA is artinian semisimple.*

Proof. We proved in Lemma 4 that $PA \subset JA$. Therefore, $A/JA \cong \frac{A/PA}{JA/PA}$ by the isomorphism theorems. We then have a map

$$f : A/PA \to A/JA$$

which induces a surjective homomorphism as in the Lemma 6

$$\frac{A/PA}{J(A/PA)} \to A/JA$$

since $J(A/JA) = 0$. We also have an onto homomorphism $A \to A/PA$ inducing

$$A/JA \to \frac{A/PA}{A(A/PA)}.$$

Therefore, A/PA is a finite dimensional algebra over $R/P = k$, so by comparing dimensions, we have $JA = J(J/PA)$. ■

We now want to apply this to our situation KG, RG, kG, V a KG-module, M an RG-module, and $V = K \otimes_R M$. Let $A = RG$ and $E = \mathrm{End}_A(M) \subset \mathrm{End}_R(M)$. Then since $\mathrm{End}_R(M)$ is finitely generated, we have $\mathrm{End}_A(M)$ is finitely generated as an R-module. Now let M be an indecomposable R-complete A-module. It remains to show the following.

Proposition 17 *E is a local ring.*

Proof. Consider $E/J(E)$. If this is *not* a division ring, suppose it has a proper non-zero left ideal L. E/JE is artinian semisimple, so there exists an idempotent $1 \neq \varepsilon \in L$. Since R is complete, we can lift ε to an idempotent $e \neq 1$ of E. But since M is indecomposable, this is not possible. ■

Hence, the Krull-Schmidt Theorem holds for A-modules when A is KG, RG, and kG. We make the following comparison

General case, kG, and RG	The semisimple case and KG
Indecomposable module M	Irreducible module M
$\mathrm{End}_A(M)$ is local	$\mathrm{End}_A(M)$ is a division ring
Krull-Schmidt Theorem	Jordan-Hölder Theorem
$A = \bigoplus Ae_i$ for indecompasble left ideals	$A = \bigoplus Af_i$ for minimal left ideals

Finally, review Proposition 30 on p. 369 of DF. on projective modules.

October 31

Homework Comments. There is a typographic error in the character table for S_5 given in DF. The character of degree 6 has the value 1 at the class of elements of order 5.
Also, recall that $\chi(x^{-1}) = \overline{\chi(x)}$. From this it follows that if x and x^{-1} are conjugate in a finite group G, then $\chi(x) = \chi(x^{-1}) = \overline{\chi(x)}$ so that $\chi(x)$ is real.
Also note that

$$N_{A_5}(\langle(12345)\rangle) = \langle(12345), (25)(34)\rangle \cong D_{10}.$$

Remark 9 *The connection between A_5 and the simple group of order 168 is that $A_5 \cong PSL(2,5)$ and the simple group of order 168 is isomorphic to $PSL(2,7)$, that is, both are $PSL(2,q)$ for some q.*

Let $A = RG$ and $\overline{A} = kG$ where (K, R, k) is a p-modular system with $R/\mathfrak{p} \cong k$. We have the decomposition

$$\begin{aligned} A &= Ae_1 \oplus Ae_2 \oplus \cdots \oplus Ae_r \\ \overline{A} &= \overline{A}\overline{e}_1 \oplus \overline{A}\overline{e}_2 \oplus \cdots \oplus \overline{A}\overline{e}_s. \end{aligned}$$

The Ae_i are indecomposable left ideals of A and the $\overline{A}\overline{e}_i$ are are indecomposable left ideals of $\overline{A}$. Hence, they are projective A-modules and $\overline{A}$-modules respectively, being direct summands of free modules. They are called *principal indecomposable modules* or *PIM*s for A and $\overline{A}$ respectively.

One of the main problems of modular representation theory is the following. Given G and p, describe the PIMs. This is a difficult problem. To do this, we typically take K to be some finite extension of $\mathbb{Q}$ in which we can write all the (complex) irreducible characters of G, $\mathcal{O}$ the ring of integers in K, $R = \mathcal{O}_{\mathfrak{p}}$, the localization at a prime ideal $\mathfrak{p}$ which contains p, and $k = \mathcal{O}_p/\mathfrak{p}$, a field of characteristic p.

We want to consider now the central idempotents of A and $\overline{A}$. Consider A, $Z(A)$ and $Z\left(\overline{A}\right)$. We can apply the theory of idempotent lifting to $Z(A)$ and $Z\left(\overline{A}\right)$, since in the natural homomorphism $A \to \overline{A}$, we have $Z(A) \to Z\left(\overline{A}\right)$. This follows from the observation that we have a basis for $Z(A)$ given by class sums.

Suppose in $\overline{A}$ we have

$$1 = \overline{E}_1 + \overline{E}_2 + \cdots + \overline{E}_k \tag{15}$$

for $\overline{E}_i$ central primitive idempotents, and in $Z(A)$ we have

$$1 = E_1 + E_2 + \cdots + E_k$$

for E_i central primitive idempotents. Then

$$A = AE_1 \oplus AE_2 \oplus \cdots \oplus AE_k$$

$$\overline{A} = \overline{AE}_1 \oplus \overline{AE}_2 \oplus \cdots \oplus \overline{AE}_k$$

where the AE_i are indecomposable two-sided ideals of A and similarly for $\overline{A}$.

Remark 10 *Just as for the $\overline{e}_i$, we could look at $\overline{A}/J\left(\overline{A}\right)$, which is semisimple and lift its central idempotents. Then we get (15).*

The AE_i are called *blocks* or *p-blocks* of A. Similarly, $\overline{AE}_i$ are *p-blocks* of $\overline{A}$. Each AE_i is a sum of indecomposable left ideals of A. Hence, we have a (possibly easier) problem of finding the p-blocks of A. This is done for S_n and the solution is attractive.

We revisit the example $G = S_3$. We computed the central idempotents in $\mathbb{Q}G$ to be

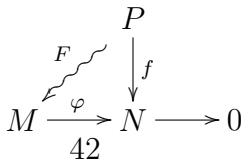
$$\begin{aligned} f_1 &= \frac{1}{6}\Big((1) + (12) + \cdots + (123) \Big) \\ f_2 &= \frac{1}{6}\Big((1) - (12) + \cdots + (123) \Big) \\ f_3 &= \frac{2}{3}(1) - \frac{1}{3}\Big((123) + (132) \Big) \end{aligned}$$

Let $p = 2$. Let $E_1 = f_1 + f_2, E_2 = f_3$. Then E_1 and E_2 are central primitive idempotents in A and $\overline{E_1}$ and $\overline{E_2}$ are central primitive idempotents in $\overline{A}$. Thus $\overline{AE}_1$ and $\overline{AE}_2$ are the 2-blocks of $\overline{A}$.

November 3

We consider Proposition 30 from DF, which corresponds with CR1 p.29. Let R be a ring and P an R-module. The following are equivalent.

1. P is projective
2. P is a direct summand of a free R-module
3. Given an exact sequence $M \xrightarrow{\varphi} N \to 0$ and an R-module homomorphism $f : P \to N$, we have an R-module homomorphism $F : P \to M$ such that the diagram below commutes.



4. Any short exact sequence of the following form splits. That is, given

$$0 \longrightarrow L \longrightarrow M \xrightarrow{\psi} P \longrightarrow 0$$

we have an R-module homomorphism $\mu : P \to M$ such that $\psi \circ \mu = i$.

$$0 \longrightarrow L \longrightarrow M \underset{\mu}{\overset{\psi}{\rightleftarrows}} P \longrightarrow 0$$

5. Given a short exact sequence

$$0 \longrightarrow L \longrightarrow M \longrightarrow P \longrightarrow 0$$

we have that

$$0 \longrightarrow \mathrm{Hom}\,(P, L) \longrightarrow \mathrm{Hom}\,(P, M) \longrightarrow \mathrm{Hom}\,(P, N) \longrightarrow 0$$

is exact.

Returning to (K, R, k) with $A = RG$ and $\overline{A} = kG$, we recall that the PIM's of A are Ae_i for e_i primitive, and the PIM's of $\overline{A}$ are $\overline{A}\overline{e_i}$ for $\overline{e_i}$ primitive. A large open problem is to describe the PIM's of $\overline{A}$.

For this section, let A be a finite dimensional algebra over k and assume A-modules have composition series. Fitting's lemma therefore holds in this case.

Proposition 18 *If two indecomposable, projective A-modules P_1 and P_2 have isomorphic quotients, then $P_1 \cong P_2$. [CR]*

Proof. Lifting the map $P_1 \xrightarrow{\pi_1} V_1 \xrightarrow{\alpha} V_2$, we get $P_1 \xrightarrow{\xi} P_2$ with $\pi_2\xi = \alpha\pi_1$ by part 3 above as in the following diagram.

$$\begin{array}{ccccc} & & P_1 & & \\ & \overset{\xi}{\swarrow} & \downarrow{\scriptstyle \alpha\pi_1} & & \\ P_2 & \xrightarrow{\pi_2} & V_2 & \longrightarrow & 0 \end{array}$$

Similarly, we get $\mu : P_2 \to P_1$ with $\pi_1\mu = \alpha^{-1}\pi_2$ as in the diagram below.

$$\begin{array}{ccc} P_1 & \underset{\mu}{\overset{\xi}{\rightleftarrows}} & P_2 \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ V_1 & \underset{\alpha^{-1}}{\overset{\alpha}{\rightleftarrows}} & V_2 \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array}$$

Then

$$\pi_1\mu\xi = \alpha^{-1}\pi_2\xi = \alpha^{-1}\alpha\pi_1 = \pi_1$$

and similarly $\pi_2\xi\mu = \pi_2$.

Now $\mu\xi \in \mathrm{End}_A\,(P_1)$ which is local since P_1 is indecomposable. Let $\beta = \mu\xi$. Then β is either nilpotent or an automorphsim by Fitting's Lemma. We have

$$\pi_1\beta = \pi_1 \implies \pi_1\beta^2 = \pi_1\beta = \pi_1 \implies \ldots \implies \pi_1\beta^k = \pi_1$$

for $k \geq 1$. This means that $\beta^k \neq 0$ for all $k \geq 1$ since otherwise, we would have $\pi_1 = 0$. Thus, β is an automorphsim. Similarly, $\xi\mu$ is an automorphism of P_2 so that $P_1 \cong P_2$. ∎

Proposition 19 *If Q is an indecomposable, projective A-module, then any quotient is also indecomposable*

$$\begin{array}{ccc} Q & \xrightarrow{\eta} & Q \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ U & \xrightarrow{\varepsilon} & U \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array}$$

If U is not indecomposable, there exists $\varepsilon \in \mathrm{End}_A(U)$ with $\varepsilon^2 = \varepsilon$ and $\varepsilon \neq 0, 1$. Since Q is projective, there exists $\eta \in \mathrm{End}_A(Q)$ with $\pi\eta = \varepsilon\pi$. Then

$$\pi\eta^2 = \varepsilon\pi\eta = \varepsilon^2\pi = \varepsilon\pi = \pi\eta$$

and similarly $\pi\eta^k = \pi\eta$ for $k \geq 1$. If $\eta^k = 0$, then $\pi\eta = 0$. But then $\eta = 0$ since π is surjective. Hence, η is an automorphsim of Q so that

$$(\pi\eta)(Q) = \pi(Q) = U$$
$$\varepsilon\pi(Q) = \varepsilon(U) \subsetneq U,$$

a contradiction. Therefore, U is indecomposable.

Definition 17 *If M is any A-module, define*

$$\mathrm{Rad}\ M = \bigcap_{M\ maximal} M.$$

Corollary 5 *If Q is indecomposable and projective, then Q has a unique maximal submodule* Rad Q.

Proof. If M_1 and M_2 are maximal submodules of Q, then

$$Q/M_1 \cap M_2 \cong Q/M_1 \oplus Q/M_2,$$

a contradiction since $Q/M_1 \cap M_2$ is indecomposable. ■

Returning to $\overline{A} = kG$ which is artinian and semisimple, we have

$$\overline{A} = \bigoplus_i \overline{A}\overline{e_i}$$

is the sum of indecomposable projective modules, and

$$\widetilde{\overline{A}} = \overline{A}/J\left(\overline{A}\right) = \bigoplus_i \widetilde{\overline{A}}\widetilde{\overline{e_i}}$$

is the sum of irreducible modules. In fact,

$$\widetilde{\overline{A}}\widetilde{\overline{e_i}} \cong \overline{A}\overline{e_i}/J\overline{e_i}.$$

Then $J\overline{e_i}$ is the unique maximal submodule of $\overline{A}\overline{e_i}$ and

$$\overline{A}\overline{e_i}/J\overline{e_i}$$

is a simple $\overline{A}$-module. Also,

$$\overline{A}\overline{e_i} \cong \overline{A}\overline{e_j}$$

if and only if

$$\overline{A}\overline{e_i}/J\overline{e_i} \cong \overline{A}\overline{e_j}/J\overline{e_j}.$$

Remark 11 *Dualizing, we have a similar theory for injective modules. In fact, the* $\overline{A}\overline{e_i}$ *are also injective, and have a unique minimal submodule.*

November 5

Here are some comments on the homework. To construct the normalizer of the Sylow 7-subgroup in $GL(3,2)$, recall the construction for groups of order pq with $q|p-1$. Let S_1 be a Sylow p-subgroup and S_2 a Sylow q-subgroup. Then we have $G = S_1S_2$ with $S_1 \lhd G$ and

$$G = \left\langle a, b : a^p = b^q = 1, b^{-1}ab = a^r \text{ for } r \text{ with } r^q \equiv 1 \pmod{p} \right\rangle.$$

with $S_1 = \langle a \rangle$ and $S_2 = \langle b \rangle$.

For groups of order 21, we have $a^7 = b^3 = 1$ and $b^{-1}ab = a^2$ and the conjugacy classes and their sizes are as follows.

element	1	a	a^3	b	ab
size	1	3	3	7	7

Also note that a Sylow 2-subgroup of $GL(3,2)$ is the group of all upper triangular matrices with diagonal entries 1, and that S_3 is naturally embedded in $GL(3,2)$ as the group of permutation matrices. Note that the normalizer of a Sylow 3-subgroup is isomorphic to S_3.

Returning to $\overline{A} = kG$, we have

$$\overline{A} = \bigoplus_i \overline{A}\overline{e_i}$$

and each $\overline{A}\overline{e_i}$ has a unique maximal submodule $J(\overline{e_i})$ with

$$\overline{A}\overline{e_i}/J(\overline{e_i}) \cong \overline{A}\overline{e_j}/J(\overline{e_j}) \text{ iff } \overline{A}\overline{e_i} \cong \overline{A}\overline{e_j}.$$

This says that there is a bijection

$$\{\text{PIMs (up to isomorphism)}\} \longleftrightarrow \{\text{Irreducible modules (up to isomorphism)}\}$$

A similar result holds for $A = RG$ as in (CR1 §6.6, p. 123). If P_1 and P_2 are finitely generated A-modules and we have $N \subset J(A)$, $V_1 = P_1/NP_1$ and $V_2 = P_2/NP_2$, then $V_1 \cong V_2$ if and only if $P_1 \cong P_2$. The proof consists of diagram arguments and an application of Nakayama's Lemma.

I'll do this later

There exists a map $\xi : P_1 \to P_2$ with $\pi_2\xi = \alpha\pi_1$. Let $T = P_2/\zeta(P_1)$. We need to show that $NT = T$, that is, that $P_2 \equiv NP_2 \pmod{\zeta(P_1)}$. To do this, let $x \in P_2$. Then $\alpha^{-1}\pi_2 \in V_1$ so there exists $y \in P_1$ with

$$\pi_1(y) = \alpha^{-1}\pi_2(x) \text{ so that } \alpha\pi_1(y) = \pi_2(x) \tag{16}$$

Then $\pi_2(x - \xi(y)) = \pi_2(x) - \pi_2\xi(y) = 0$ from (16) Then $T = NT$ and T is finitely generated, so by Nakayama's lemma, we have $T = 0$. Then $P_2 = \xi(P_1)$ implies ξ is surjective. Consider

$$0 \to \ker\xi \to P_1 \to P_2 \to 0$$

which splits since P_2 is projective, so $\ker \xi$ is finitely generated. Now if $x \in \ker \xi$, then $\pi_2 \xi(x) = 0$ so that $\pi_1(x) = 0$ and $x \in NP_1$ so that $\ker \xi = N \ker \xi$ and $\ker \xi = 0$ again. Hence $P_1 \cong P_2$.

Thus we have, also for A, a bijection

$$\{\text{PIMs (up to isomorphism)}\} \longleftrightarrow \{\text{Irreducible modules (up to isomorphism)}\}.$$

In addition we have $Ae_i \cong Ae_j$ as A-modules if and only if $\overline{A}\overline{e_i} \cong \overline{A}\overline{e_j}$ as $\overline{A}$-modules. This follows by taking $N = J(A)$ or $N = PA$.

Write $\widehat{A} = KG$, a semisimple algebra. Then we study $\widehat{A}$ for the ordinary irreducible representation of G, $A = RG$ (not semisimple) for the principal indecomposable representations of G over R, and $\overline{A} = kG$ (also not semisimple) for the principal indecomposable and modular irreducible representations of G over k.

As in the case of $\widehat{A}$ we want to study *characters* of modular representations, i.e. representations of $\overline{A} = kG$. The usual definition of "trace" leads to difficulties. For example, if we have a representation of dimension divisible by p, then the trace of the identity matrix would be 0. The concept of *Brauer characters* (discussed in CR1 §17) handles this difficulty.

Definition 18 *Let (K, R, k) be a p-modular system and G a group with $|G| = p^a m$ and $(p, m) = 1$. Then $g \in G$ is* p-regular *if the order of g is prime to p and hence divides m.*

Choose K and k large enough to contain the mth roots of unity and choose a bijection

$$\left\{\text{Group of } m^{\text{th}} \text{ roots of unity in } K^\times\right\} \longleftrightarrow \left\{m^{\text{th}} \text{ roots of 1 in } k^\times\right\}$$

Write $\omega \longleftrightarrow \overline{\omega}$. Given a p-regular g, suppose that in a representation ρ of G over k, the eigenvalues of $\rho(g)$ are $\left\{\overline{\omega}^{i_1}, \overline{\omega}^{i_2}, \ldots \overline{\omega}^{i_n}\right\}$. Define a *Brauer character* λ of ρ to be given by

$$\lambda(g) = \omega^{i_1} + \omega^{i_2} + \cdots + \omega^{i_n} \in K.$$

Thus λ is a function from G to K.

November 7

Example 16 *(See CR2, p.648.) For $G = S_4$ and $p = 2$, consider*

$$G_{p'} = \{1 \text{ and the elements of order } 3\} \leq G$$

We have

	1	(123)	
χ_1	1	1	$\longleftarrow$ *remains irreducible*
χ_2	1	1	
χ_3	2	-1	$\longleftarrow$ *irreducible as follows*
χ_4	3	0	$\longleftarrow \chi_3 + \chi_1$
χ_5	3	0	

If the two-dimensional representation was reducible mod 2, then all matrices would be of the form $\begin{pmatrix} 1 & \clubsuit \\ 0 & 1 \end{pmatrix}$ hence would have trace 0. This would contradict the values in the character table. So it must be irreducible. So the irreducible Brauer characters are χ_1 and χ_3. Note that the degrees of the characters need not divide the order of the group. A difficult problem is to find the Brauer characters, or at least their degrees.

Next we consider blocks. Let $\widehat{A} = KG$, $A = RG$, and $\overline{A} = kG$. Let $\{V_j : 1 \leq j \leq s\}$ be irreducible $\widehat{A}$-modules up to isomorphism. Let $M_i \leq V_i$ so that $K \otimes_R M_i \cong V_i$ for $1 \leq i \leq s$. Write $\overline{M_i}$ for the reduction of M_i mod P for P a prime ideal of R. Then $\overline{M_i} \cong k \otimes_R M_i$ and

$$Z\left(\widehat{A}\right) = \bigoplus_{i=1}^{s} \widehat{A}F_i$$

for F_i central primitive idempotents which can be computed from the character by the formula

$$F_i = \frac{\chi_1(1)}{|G|} \sum_{g \in G} \chi_i(g)\, g^{-1}.$$

In $Z(A)$, write $1 = E_1 + E_2 + \cdots + E_t$ where each E_i is a sum of some of the F_j. The E_i are central primitive idempotents in $Z(A)$ but not primitive in $Z\left(\widehat{A}\right)$. Then

$$A = AE_1 \oplus AE_2 \oplus \cdots \oplus AE_t$$

is the sum of indecomposable two-sided ideals. The AE_i are called the *blocks* or *p-blocks* of G.

Also,

$$\overline{A} = \overline{AE_1} \oplus \overline{AE_2} \oplus \cdots \oplus \overline{AE_t}$$

and the $\overline{AE_i}$ are also called *p-blocks* of G. Also

$$\widehat{A} = \widehat{A}E_1 \oplus \widehat{A}E_2 \oplus \cdots \oplus \widehat{A}E_t$$

. Each $\widehat{A}E_i$ is the sum of matrix algebras, hence corresponds to a *set* of ordinary characters. Thus, $\{\chi_1, \chi_2, \ldots, \chi_s\}$ are divided into disjoint subsets, also called *p-blocks* of G.

Example 17 *For $G = S_3$ and $p = 2$, the 2-blocks are $\{\chi_1, \chi_2\}$ and $\{\chi_3\}$.*

Recall that

$$\omega_i(C_j) = \frac{\chi_i(g_j)}{\chi_i(1)} h_j$$

for $1 \leq i \leq s$ where the χ_i are the characters of $Z\left(\widehat{A}\right)$, the C_j are the class sums of $\mathcal{C}_j$, $h_j = |\mathcal{C}_j|$, and $g_j \in \mathcal{C}_j$ is a representative of its conjugacy class. Take K to be sufficiently large.

Now since $\omega_i(C_j)$ is an algebraic integer, we can assume $\omega_i(C_j) \in R$ and hence we can reduce mod P. Let

$$\overline{\omega_i} : Z\left(\overline{A}\right) \to k \text{ be given by } C_j \mapsto \overline{\omega_i(C_j)}.$$

Then the $\overline{\omega_i}$ are all the characters of $Z\left(\overline{A}\right)$ as follows.

$$\ker\left(\overline{\omega_i}\right) = \bigoplus_{l \neq i} Z\left(\overline{A}\right) \overline{E_l} \oplus J\left(Z\left(\overline{A}\right)\right) \overline{E_i}.$$

$$Z\left(\overline{A}\right) = Z\left(\overline{A}\right) \overline{E_1} \oplus Z\left(\overline{A}\right) \overline{E_2} \oplus \cdots \oplus Z\left(\overline{A}\right) \overline{E_t}$$

.

(To be continued next time.)

November 10

Recall that $\widehat{A} = KG$, $A = RG$ and $\overline{A} = kG$ with K and k sufficiently large so that the irreducible representations of G over $\mathbb{C}$ can be realized over K.

To study p-blocks, consider

$$Z(A) = Z(A) E_1 \oplus \dots Z(A) E_t$$

and in fact

$$A = AE_1 \oplus \dots AE_t$$

where each AE_i is a p-block. The E_i are primitive in RG, but not in KG. Write

$$E_i = F_{i,1} + F_{i,2} + \cdots + F_{i,\alpha_i}$$

where $F_{i,1} = F_i$, and the $F_{i,j}$ are primitive central idempotents in KG. Then

$$\overline{A} = \overline{AE}_1 \oplus \cdots \oplus \overline{AE}_t.$$

The $\overline{AE}_t$ are also p-blocks. Then

$$Z\left(\overline{A}\right) = Z\left(\overline{A}\right) \overline{E}_1 \oplus \cdots \oplus Z\left(\overline{A}\right) \overline{E}_t. \tag{17}$$

Each F_i and hence χ_i corresponds to a character ω_i of $Z\left(\widehat{A}\right)$ and

$$\omega_i(C_j) = \frac{\chi_i(g_j) h_j}{\chi_i(1)} \in R \tag{18}$$

where C_j are the class sums of $\mathcal{C}_j$, $g_j \in \mathcal{C}_j$, and $h_j = |\mathcal{C}_j|$. Then $\omega_i(F_i) = 1$ and $\omega_i(F_j) = 0$ for $i \neq j$. Hence $\omega_i(E_i) = 1$ and $\omega_{i,j}(E_i) = 1$ for $1 \leq j \leq \alpha_j$ where $\omega_{i,j}$ is the character corresponding to $F_{i,j}$ and $\omega_i = \omega_{i,1}$.

Define $\overline{\omega} : Z\left(\overline{A}\right) \to k$ by $\overline{\omega}(C_j) = \overline{\omega_i(C_j)}$. Then we get t linear characters of $Z\left(\overline{A}\right)$. We can compute $\ker \overline{\omega}_i$ as follows. We have from (17) that

$$\overline{\omega}_{i,l}\left(\overline{E_j}\right) = 0$$

if $i \neq j$. Also, we have $\ker \overline{\omega}_i$ is a maximal ideal of $Z\left(\overline{A}\right)$. Hence,

$$\ker \overline{\omega}_i = \bigoplus_{l \neq i} Z\left(\overline{A}\right) \overline{E}_l \oplus \underbrace{J\left(Z\left(\overline{A}\right)\right) \overline{E}_i}_{\substack{\text{unique maximal} \\ \text{ideal of } Z\left(\overline{A}\right)\overline{E}_i}}.$$

Since (17) is the unique decomposition of $Z\left(\overline{A}\right)$ into indecomposable ideals, any maximal ideal is of this form. Therefore, $\overline{\omega_i}$ are the only irreducible characters of $Z\left(\overline{A}\right)$. Hence χ_i and χ_j are in the same p-block if and only if $\overline{\omega_i} = \overline{\omega_j}$ if and only if $\omega_i \equiv \omega_j \pmod{P}$ as functions. Thus, blocks are identified by characters of the center of KG mod $\mathfrak{p}$. (Note that here we are going back to the old notation of characters $\chi_i, i = 1, 2, \dots s$ of G.)

Definition 19 *$B_p(G)$ is the block containing the trivial character, called the principal block.*

Example 18 *(CR2, p. 649) Work out the $\omega_i(C_j)$ from the character table. For S_4, we have the following table.*

(1)	(12)	(123)	(1234)	(12)(34)
1	1	1	1	1
1	−1	1	−1	1
2	0	−1	0	2
3	1	0	−1	−1
3	−1	0	1	−1

We compute the character table for $Z(\overline{A})$ using formula 18. For example, $\omega_4(C_2) = \frac{1}{3}6 = 2$ and we have the following table.

1	6	8	6	3
1	−6	8	−6	3
1	0	−4	0	3
1	2	0	−2	−1
1	−2	0	2	−1

Mod 2, this table becomes

1	0	0	0	1
1	0	0	0	1
1	0	0	0	1
1	0	0	0	1
1	0	0	0	1

so we have only one block. Mod 3, we have

1	0	2	0	0
1	0	2	0	0
1	0	2	0	0
1	2	0	1	2
1	1	0	2	2

so that the first three form one block and the last two each form one block.

Look next at the restrictions of the ordinary characters to the 3-regular classes. We have four Brauer characters, two arising from the first three characters of S_4 and one each for the last two characters. (Recall that by a Brauer character we mean the character of a p-modular irreducible representation, regarded as a complex function by Brauer's procedure.) Note that the first two characters of S_4 (trivial and sign) give two Brauer characters, whereas the third character of S_4 is the sum of the first two.

Example 19 For $G = A_5$, $B_5(G) = \{1, \chi_4, \chi_3, \chi_3'\}$. Note that the degree of the character is the subscript here. Note also that χ_3 and χ_3' are not rational. Write $\zeta = e^{2\pi i/5}$. Then $\chi_3((12345)) = \zeta + \zeta^4$, $\chi_3'((12345)) = \zeta^2 + \zeta^3$. To show that these two characters are in the same 5-block, check that

$$(1-\zeta)\left(1-\zeta^2\right)\left(1-\zeta^3\right)\left(1-\zeta^4\right) = 5$$

which follows from $\sum_{j=0}^{4}\zeta^j = 0$. For $p = 5$, take $P = (1-\zeta)$, $K = \mathbb{Q}(\zeta)$ and R the ring of integers $\mathbb{Z}\left[\frac{1+\zeta}{2}\right]$ (see e.g. DF, p.230). Then $\zeta \equiv \zeta^2 \pmod{P}$, $\zeta^3 \equiv \zeta^4 \pmod{P}$. From this we can show that $\omega_3 \equiv \omega_{3'} \pmod{P}$. (This example will be continued next time.)

November 12

Continuing with $\omega_i(C_j)$ for A_5, we have

ω_1	1	20	15	12	12
ω_4	1	5	0	-3	-3
ω_5	1	-4	3	0	0
ω_3	1	0	-5	$2\left(1+\sqrt{5}\right)$	$2\left(1-\sqrt{5}\right)$
ω_3'	1	0	-5	$2\left(1-\sqrt{5}\right)$	$2\left(1+\sqrt{5}\right)$

For this example, we took $R = \mathbb{Z}[\zeta]$, $P = (1-\zeta)$. Note that in this case, for our purpose of calculating the blocks, we didn't need to take the localization of R at P or the completion.

Note: We have $\zeta + \zeta^4 + 1 = \frac{1+\sqrt{5}}{2}$ and $\zeta^2 + \zeta^3 + 1 = \frac{1-\sqrt{5}}{2}$. This is used in computing the blocks, using the calculations of last time.

The Isaacs-Navarro conjecture looks at the degrees of characters of G and $N_G(P)$. We refine this in the following ways.

1. Take $B_p(G)$
2. There should be a bijection of characters, not just equality of number of characters. That is, χ is attached to $\pm\gamma$ in some way. The handout calls this map I_p, an *isotypy*.
3. We want to know the significance of the sign in the map in 2. There is a sign involved in the Isaacs-Navarro conjecture, where you look at congruence classes k or $-k$ mod p. There is a sign involved in isotypies. Is there a connection?

Note that in the table above ω_5 is in a block by itself. This isn't an accident as explained in the following proposition.

Proposition 20 *Let $A = RG$ and $\widehat{A} = KG$. Let F be a primitive central idempotent of $\widehat{A}$ such that F corresponds to χ, an irreducible ordinary character of G and $p^a|\chi(1)$ where $|G| = p^a m$ for $(m,p) = 1$. Then $F \in A$ and AF is a block of A, that is, χ is the only irreducible character in its block.*

Proof. Take

$$F = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi\left(g^{-1}\right)g = \frac{p^a l}{p^a m}\sum_{g\in G}\chi\left(g^{-1}\right)g \in RG$$

Then $AF \subset \widehat{A}F$ so that $AF \cong M_n(R)$ and $\overline{AF} \cong M_n(k)$. ■

Corollary 6 *χ is irreducible mod p.*

Returning now to A_5 with $p = 5$, we can use this information to compute the Brauer characters. Restricting the ordinary characters to $G_{5'}$, we have the following.

	1	(123)	(12)(34)
φ_1	1	1	1
	4	1	0
φ_3	5	-1	1
φ_2	3	0	-1
	3	0	-1

The first and third are irreducible. We discard the last character, and it remains to consider which is the other Brauer character, since there can be only three. It turns out that the fourth character is irreducible as we will discover next time. Then the Brauer characters are the ones labeled φ_1, φ_2 and φ_3 in the table above. Normally it won't be so easy to compute the Brauer characters. Then we have

$$\begin{aligned} \chi_1|_{G_{5'}} &= \varphi_1 \\ \chi_3|_{G_{5'}}, \chi_{3'}|_{G_{5'}} &= \varphi_2 \\ \chi_4|_{G_{5'}} &= \varphi_1 + \varphi_2 \\ \chi_5|_{G_{5'}} &= \varphi_3 \end{aligned}$$

Writing this information in matrix form, we have

	φ_1	φ_2	φ_3
χ_1	1	0	0
χ_2	0	1	0
χ_3	0	1	0
χ_4	1	1	0
χ_5	0	0	1

This matrix is called the decomposition matrix, to be discussed below.

Next,we want to consider the Cartan invariants and the decomposition numbers. Let K be sufficiently large and $A = RG$. Write

$$A = Ae_1 \oplus Ae_2 \oplus \cdots = \bigoplus_{i=1}^{s} Ae_1 \oplus \bigoplus_{i=s+1} Ae_2.$$

where the Ae_i in the first expression are the representatives of the isomorphism classes of the Ae_j. Write $Q_i = Ae_i$. Therefore, the Q_i are the projective indecomposable A-modules. Also, write $P_i = \overline{A}\overline{e_i}$ for the projective, indecomposable $\overline{A}$ modules. Write $\widehat{Q_i} = \widehat{A}e_i$ and $S_i = P_i/J\left(\overline{A}\right)P_i$ for $1 \leq i \leq s$. The S_i are simple $\overline{A}$-modules. Write V_i for the irreducible $\widehat{A}$ modules for $1 \leq i \leq r$. Let M_i be an A-module with $M_i \leq V_i$ such that $V_i = K \otimes_R M_i$. Then $d_{i,j}$, the i,j entry in the decomposition table above, are the multiplicity of S_j as a composition factor of $\overline{M_i}$. Our shorthand for this will be $d_{i,j} = \left(\overline{M} : S_j\right)$.

November 14

Homework Addition: Add Part 6 to Homework 8: Do for $p = 7$ what you were asked to do in Part 5 for $p = 3$.

Remark 12 The Brauer characters are known for $SL\,(2,p)$ for p prime (see CR1, 17.17) This is used for A_5, $p = 5$, as mentioned last time, and for the 168-group, which is isomorphic to $PSL(2,7)$, for $p = 7$.

Remark 13 *If* $\zeta = e^{2\pi i/5}$, *then* $\zeta + \zeta^{-1} = 2\cos\left(\frac{2\pi}{5}\right) \in \mathbb{R}$ *and*

$$1 + \zeta + \zeta^{-1} = \frac{1+\sqrt{5}}{2}$$

and

$$1 + \zeta^2 + \zeta^{-2} = \frac{1 - \sqrt{5}}{2}$$

Use this information to confirm the character table of A_5.

We fix the following notation, introduced last time. A reference for this section is DB, p.19.

$\widehat{A} = KG$	$A = RG$	$\overline{A} = kG$
$\{V_i \text{ simple} : i = 1, 2, \ldots, s\}$	$M_i \leq V_i$	$\{S_i \text{ simple}; i = 1, \ldots, r\}$
$V_i \longleftrightarrow \chi_i$	RG-lattice in V_i	
$V_i = K \otimes_R M_i$	Q_i projective, indecomposable lift of P_i	$S_i \longleftrightarrow P_i$ projective, indecomp
$\widehat{Q}_i = K \otimes_R Q_i$	$d_{i,j} = \left(\overline{M}_i : S_j\right)$	$c_{i,j} = (P_j : S_i)$

For any KG-module L, write $(L : V_i)$ for the multiplicity of V_i as a composition factor of L. Similarly, for any kG-module L, write $(L : S_i)$ for the multiplicity of S_i as a composition factor of L.

Definition 20 $d_{i,j} = \left(\overline{M}_i : S_j\right)$ *are the* decomposition numbers *and* $c_{i,j} = (P_j : S_i)$ *are the* Cartan invariants.

Another major problem in modular representation theory is to determine the decomposition numbers and Cartan invariants, given G and p.

$D = (d_{i,j})$ is a $s \times r$ matrix. It connects the characteristic 0 and the characteristic p representations, and $C = (c_{i,j})$ is an $r \times r$ matrix which connects projective and simple modules in characteristic p. The matrix D can be expressed as a transition matrix between ordinary and Brauer characters as

$$\chi_i = \sum_{j=1}^{r} d_{i,j} \varphi_j$$

restricted to $G_{p'}$, the set of p regular elements.

We are now curious as to the connection between C and D. Note K, R, and k are chosen sufficiently large as before.

Proposition 21

$$\operatorname{Hom}_{\overline{A}}(P_i, S_j) = \begin{cases} k \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}$$

Proof. We showed that S_i is the unique top composition factor of P_i. Since any homomorphism of $P_i \to S_i$ can be regarded as the canonical homomorphism composed with an element of $\operatorname{Hom}_{\overline{A}}(S_i, S_i)$, we get the proposition. ■

Remark 14 Also we have that $c_{i,j} = \dim_k \operatorname{Hom}_{\overline{A}}(P_i, P_j)$ This follows from a more general proposition below.

Proposition 22

$$\dim_k \operatorname{Hom}_{\overline{A}}(P_i, M) = (M : S_i)$$

for any $\overline{A}$*-module* M.

Proof. Suppose S_j is a top composition factor of M. Then we have an exact sequence

$$0 \to M' \to M \to S_j \to 0$$

now since P_i is projective, we have

$$0 \to \mathrm{Hom}_{\overline{A}}(P_i, M') \to \mathrm{Hom}_{\overline{A}}(P_i, M) \to \mathrm{Hom}_{\overline{A}}(P_i, S_j) \to 0$$

is exact. If $i \neq j$, we have $\mathrm{Hom}_{\overline{A}}(P_i, S_j) = 0$ which implies that $\mathrm{Hom}_{\overline{A}}(P_i, M') \cong \mathrm{Hom}_{\overline{A}}(P_i, M)$. Apply induction on the composition length of M. Then

$$\dim_k \mathrm{Hom}_{\overline{A}}(P_i, M) = \dim_k \mathrm{Hom}_{\overline{A}}(P_i, M') = (M' : S_j) = (M : S_j)$$

Next if $j = i$,

$$\dim_k \mathrm{Hom}_{\overline{A}}(P_i, M) = \dim_k \mathrm{Hom}_{\overline{A}}(P_i, M') + 1$$

and $(M : S_i) = (M', S_i) + 1$ and we have the result. ■

We can now compute the $c_{i,j}$. We have

$$d_{i,j} = \left(\overline{M}_i, S_j\right) = \dim_k \mathrm{Hom}_{\overline{A}}\left(P_j, \overline{M}_i\right) = \mathrm{rank}_R \mathrm{Hom}_A(Q_j, M_i)$$

since Q_j is projective. That is, a homomorphism of P_j into $\overline{M}_i$ can be lifted to a homomorphism of Q_j into M_i. Note also that $\mathrm{rank}_R \mathrm{Hom}_A(Q_j, M_i) = (\widehat{Q_j} : V_i)$.

$$\begin{array}{ccccc} Q_j & \longrightarrow & P_j & \longrightarrow & 0 \\ & \searrow & & \searrow & \\ & & M_i & \longrightarrow & \overline{M}_i \longrightarrow 0 \end{array}$$

Now consider

$$d_{k,i} d_{k,j} = \left(\overline{M}_k : S_i\right)(Q_j : M_k)$$

where $(Q_j : M_k)$ is interpreted as $\mathrm{rank}_R \mathrm{Hom}_A(Q_j, M_k)\ ) = \left(\overline{M}_k : S_i\right)\left(\widehat{Q_j} : V_i\right)\Big)$. Then $\sum_k d_{k,i} d_{k,j} = \sum_k \left(\widehat{Q}_j : V_k\right)\left(\overline{M}_k, S_i\right)$. This counts the number of composition factors isomorphic to S_i where $\widehat{Q}_j$ is taken mod P which is $(P_j : S_i) = c_{i,j}$.

Hence we have the following.

Theorem 12 $\mathbf{C} =^{\mathbf{t}} \mathbf{DD}$.

November 17

Recall that we have the following situation.

$\widehat{A}KG$	$A = RG$	$\overline{A} = kG$
V_i irreducible	$M_i \leq V_i$	S_i ireducible
(χ_i)		(φ_i)
$\widehat{Q}_i$	Q_i projective, indecomosable	P_i projective, indecomposable

Theorem 13 $C = D^T D$.

Proof. Write $d_{ij} = \left(\overline{M}_i : S_j\right)$. (Then note $\chi_i|_{G'_p} = \sum_j d_{i,j}\varphi_j$.) The last proposition showed that

$$d_{i,j} = \dim_k \mathrm{Hom}_{\overline{A}}\left(P_j, \overline{M_i}\right) = \mathrm{rank}_R \mathrm{Hom}_A\left(Q_j, M_i\right) = \dim \mathrm{Hom}_{\widehat{A}}\left(\widehat{Q}_j, V_i\right) = \left(\widehat{Q}_j : V_i\right)$$

Then $\sum_k d_{k,i}d_{k,j} = \sum_k \left(\widehat{Q}_j : V_k\right)\left(\overline{M}_k, S_i\right)$. This counts the number of composition factors isomorphic to S_i where $\widehat{Q}_j$ is taken mod P, which is $(P_j : S_i) = c_{i,j}$ ■

Returning to A_5 with $p = 5$, we computed

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

The third is the same as the second mod 5, the fourth is a linear combination of the first two, and the last character is in a block by itself. Then

$$C = {}^t DD = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The block $\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$ shows that P_1 corresponds with the trivial module S_1 and the only possible composition series is

$$\begin{array}{c} S_1 \\ \downarrow \\ S_2 \\ \downarrow \\ S_1 \end{array}$$

P_2 has one of the following composition series.

$$\begin{array}{cc} S_2 & S_2 \\ \downarrow & \downarrow \\ S_1 & S_2 \\ \downarrow & \downarrow \\ S_2 & S_1 \\ \downarrow & \downarrow \\ S_2 & S_2 \end{array}$$

We have not yet shown that the irreducible ordinary character mod 3 is irreducible mod 5. This would be the same as showing that there is a 5-modular irreducible representation of degree 3. Recall for the following discussion that $A_5 \cong PSL\,(2,5)$.

We can show (see CR1, 17.17, hand-out) that $G = SL(2,p)$ has p irreducible modular representations over a field k of characteristic p. Take $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G$. Then G can be regarded as acting on a vector space of dimension 2, and then on $k[x,y]$ by

$$g \cdot x = \alpha x + \beta y \qquad g \cdot y = \gamma x + \delta y.$$

Take M_d to be the subspace of $k[x,y]$ spanned by $x^d, x^d - 1y, \ldots, y^d$. We can show that M_d is irreducible. For example, when $d = 2$, we have $M_2 = \langle x^2, xy, y^2 \rangle$. Then

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : \begin{cases} x \to x \\ y \to x + y \end{cases}$$
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} : \begin{cases} x \to x + y \\ y \to y \end{cases}$$

Now let $V = \langle v_1, v_2, v_3 \rangle$ be a vector space of dimension k over k. In kG, take

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then

$$A : \begin{cases} v_1 \to 0 \\ v_2 \to v_1 \\ v_3 \to 2v_2 + v_1 \end{cases} \qquad B : \begin{cases} v_1 \to 2v_2 + v_3 \\ v_2 \to v_3 \\ v_3 \to 0 \end{cases}$$

and

$$A \to \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \qquad B \to \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

on V. We then have

$$A^2 : \begin{cases} v_1 \to 0 \\ v_2 \to 0 \\ v_3 \to 2v_1 \end{cases} \quad \text{and } B^2 : \begin{cases} v_1 \to 2v_3 \\ v_2 \to 0 \\ v_3 \to 0 \end{cases}.$$

It is easy to check that if $0 \neq U \leq V$, and $\alpha v_1 + \beta v_2 + \gamma v_3 \in U$ with at least one of α, β, γ not 0, by applying A, A^2, B, and B^2 to this element we get all of V. Thus V is irreducible.

Returning to $GL(3,2) = G$, we look at the characters from the point of view of the general theory for $GL(n,q)$. We had characters of degrees 1, 3, 3, 6, 7, and 8. We obtained them by taking $B = \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \right\}$ of size 8 and $P = \left\{ \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{pmatrix} \right\}$ of size 24. We found $\mathrm{Ind}_P^G(1) = \chi_1 + \chi_2$ by counting lines fixed by P. χ_2 is the character of degree 6. We found $\mathrm{Ind}_B^G(1) = 2\chi_1 + \chi_2 + \chi_4$ by counting flags fixed by B. χ_3 is the character of degree 8. Finally, $\mathrm{Ind}_P^G(\varepsilon) = \chi_3$ is the character of degree 7. The remaining characters χ_5 and χ_6 were obtained from S_7 the Sylow 7-subgroup.

November 19

Complete the series of homeworks on $GL(3,2)$ by writing an intoduction to $GL(3,2)$ which begins "Let $G = GL(3,2)$. We compute…". This should be a one-page document.

Recall that in computing the characters of $GL(3,2)$, the characters of degree 1, 6, 7, and 8 came from $\mathrm{Ind}_B^G(1)$, $\mathrm{Ind}_P^G(1)$, and $\mathrm{Ind}_P^G(\epsilon)$. The two characters of degree 3 remain and are explained in terms of *Harish-Chandra Theory* or *Theory of Cusp Forms*.

First let G be any finite group and let $H \leq G$. Write $A = KG$ for K sufficiently large. We want to decompose $\mathrm{Ind}_H^G(1)$ into a sum of irreducible representations of G. Recall that A is artinian and semisimple so that we have such a decomposition.

Recall from September 12 that

$$\mathrm{Hom}_A(V_1 \oplus V_2, W_1 \oplus W_2)$$

is isomorphic the group of matrices $\begin{pmatrix} \theta_{1,1} & \theta_{2,1} \\ \theta_{1,2} & \theta_{2,2} \end{pmatrix}$ where $\theta_{i,j} \in \mathrm{Hom}(V_i, W_j)$. The $\theta_{i,j}$ involve injections and projections. This is relevant because decomposing $V = \mathrm{Ind}_H^G(1)$ involves projections in $\mathrm{End}_A(V)$.

More generally, if

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$$
$$W = W_1 \oplus W_2 \oplus \cdots \oplus W_n,$$

then $\mathrm{Hom}_A(V,W)$ will be isomorphic to a group of matrices $(\theta_{i,j})$ with $\theta_{i,j} \in \mathrm{Hom}_A(V_i, W_j)$ and if $V = W$, the matrices are $(\theta_{i,j})$ with $\theta_{i,j} \in \mathrm{Hom}_A(V_i, V_j)$.

Returning to $A = KG$ with A semisimple, suppose

$$V \cong \bigoplus_{i=1}^{s} n_i S_i$$

for S_i simple modules. Then in this case, we have $\mathrm{Hom}_A(S_i, S_j) = \delta_{i,j}K$. (Since K is sufficiently large, a matrix commuting with all the matrices representing elements of G in the representation corresponding to S_i is a scalar matrix. This is one way of saying that $End_A(V) \cong K$. Hence

$$E := \mathrm{End}_A(V) \cong \bigoplus_i M_{n_i}(K)$$

This connects the representations of A and E given a fixed V. Let L_i be the simple $M_{n_i}(K)$- module. There is only one up to isomorphism. Hence, we have a bijection

$$\{\text{Irreducible } A\text{-modules in } V\} \longleftrightarrow \{\text{Irreducible } E\text{-modules}\}$$

given by $S_i \longleftrightarrow L_i$ Also $n_i = (V : S_i) = \dim_K L_i$

Example 20 Returning to $G = GL(3,2)$, we computed $V = \mathrm{Ind}_B^G(1)$ has character $\chi_1 + 2\chi_2 + \chi_4$ so E has irreducible representations of degree 1, 2, and 1. We observe that S_3 also has irreducible representations of degree 1, 2, and 1 and in fact, $E \cong KS_3$ by the theory we will develop later.

Let $H \leq G$, $A = KG$, and $V = \mathrm{Ind}_H^G(1)$. We want to consider $E = \mathrm{End}_A(V)$. In $B = KH$, the trivial representation is realized by Be where

$$e = \frac{1}{|H|} \sum_{h \in H} h. \tag{19}$$

Proposition 23 *Let e be any idempotent in B. Then Ae is the module corresponding to the representation of A induced from the representation of B given by Be.*

Proof. The module for the induced representation is

$$A \otimes_B Be \cong Ae.$$

■

Now take e as in (19) and consider Ae. Recall that

$$\mathrm{Hom}_A(Ae, M) \cong M \cong eM$$

and

$$\mathrm{End}_A(Ae) \cong (eAe)^{\mathrm{op}}.$$

Hence, we want to study $\mathcal{H} := eAe$, the "opposite" of the endomorphism algebra of Ae which is called the *Iwalori-Hecke Algebra*. (A reference for this is CR1, 11D.)

Now eAe is a subalgebra of A where $e = \frac{1}{|H|} \sum_{h \in H} h$. Then a basis for $\mathcal{H}$ is given by

$$\{exe : x \text{ runs over a set of representatives for } H\backslash G/H\}$$

because $\mathcal{H}$ is spanned by $\{exe : x \in G\}$ and $exe = eye \iff x = hyh'$ for $h, h' \in H$.

Definition 21 $\mathrm{ind}x = \frac{|H|}{|H \cap^x H|}$

Note that

$$|HxH| = \frac{|H|\,|H|}{|H \cap^x H|}.$$

Let $\{x_j : j = 1, 2, \dots\}$ be a set of representatives of $H\backslash G/H$.

Definition 22 $a_j = (\mathrm{ind}x_j)\, ex_je$.

Then $\mathcal{H}$ has basis $\{a_j\}$ with multiplication given by $a_ia_j = \sum_k \mu_{i,j,k} a_k$. Next time we will consider how to describe the $\mu_{i,j,k}$.

November 21

Recall that $H \leq G$ and $\mathcal{H} = eAe$. A in this case is KG, thought this works sometimes in more general cases. Recall that $\mathbb{E} \ltimes_A (Ae) \cong (eAe)^{\mathrm{op}}$ and that $e = \frac{1}{|H|} \sum_{h \in H} h$. Then $\mathcal{H}$ is spanned by $\{exe : x \text{ a representative of } H\backslash G/H\}$. We also write

$$\mathrm{ind}\ x = \frac{|H|}{|H \cap^x H|}.$$

Theorem 14 *A basis for $\mathcal{H}$ is given by*

$$a_j = \frac{1}{|H|} \sum_{x \in D_j} x$$

where $D_j = Hx_jH$ for $1 \leq j$ are the double cosets of H in G. Then $a_i a_j = \sum_k \mu_{i,j,k} a_k$ where

$$\mu_{i,j,k} = |H|^{-1} \left| D_i \cap x_k D_j^{-1} \right|.$$

Proof. We know that $\mathcal{H}$ is spanned by the ex_je for $1 \leq j$ and these are also independent as ex_je and ex_ke for $j \neq k$ contain distinct elements of G. For simplicity, write $x = x_j$. Then

$$exe = \frac{1}{|H|^2} \sum_{h_1, h_2 \in H} h1xh_2 \frac{1}{|H|^2} \sum_{h_1 x h_2 \in D} |H \cap^x H| \, h_1 x h_2$$

where the sum is taken over distinct elements in D and this works because the number of elements in D is

$$\frac{|H|^2}{|H \cap^x H|}$$

In particular, $exe \neq 0$ since K in this case has characteristic 0. This may not work so will for other fields. Let

$$a_j = (\text{ind } x_j)\, exe == \frac{|H|}{|H \cap^x H|} exe = \frac{|H|}{|H \cap^x H|} \frac{1}{|H|^2} |H \cap^x H| \sum_{y \in D} y = \frac{1}{|H|} \sum_{y \in D} y.$$

Then

$$a_i a_j = \frac{1}{|H|^2} \left(\sum_{y \in D} y \right) \left(\sum_{z \in D} z \right)$$

and count the number of times x_k appears in this product, that is, the number of pairs $y \in D_i, z \in D_j$ with $yz = x_k$. That is, $z = y^{-1}xk$ and $y = x_k z^{-1} \in D_k \cap x_k D_j^{-1}$ where $D^{-1} = \{d^{-1} : d \in D\}$. Hence, the number of such pairs is $\left| D_i \cap x_k D_j^{-1} \right|$ and the coefficient of x_k in $a_i a_j$ is

$$\frac{1}{|H|^2} \left| D_i \cap x_k D_j^{-1} \right|.$$

Hence,

$$\frac{1}{|H|} \mu_{i,j,k} = \frac{1}{|H|^2} \left| D_i \cap x_k D_j^{-1} \right|$$

so that $\mu_{i,j,k} = \frac{1}{|H|} \left| D_i \cap x_k D_j^{-1} \right|$ as required. ■ Consider $G = GL(n, q)$ with $H = B$, the subgroup of upper triangular matrices. We need the double coset decomposition $B \backslash G / B$. This can be accomplished by the famous *Bruhat decomposition*.

Theorem 15 *G is the disjoint union*

$$G = \bigcap_w BwB$$

for $w \in S_n$.

Proof. Let $X_{i,j}(\alpha)$ be the elementary matrix

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

where the α is in position i, j. We want to show that if $g \in G$, $g = b_1 w b_2$ for b_1, b_2 upper triangular and w a unique permutation matrix. By multiplying g on the left by matrices of the form $X_{i,j}(\alpha)$, we get every entry in the first column except the k_1 position to be zero for some k_1. After all, we can never have *all* the elements zero or g wouldn't be invertible. Repeat for the other columns giving a matrix for which the ith column is zero for every row except k_ith row. Since g is invertible, $(k_1, k_2, \ldots, d_n)$ is a permutation of $(1, 2, \ldots, n)$. We now have $b_1^{-1} g$ for some $b_1 \in B$ since all the $X_{i,j}(\alpha)$ are upper triangular. Now left-multiplying by some $w^{-1} \in S_n$ makes $w^{-1} b_1^{-1} g =: b_2$ upper triangular. Then $g = b_1 w b_2$. ■

This gives us the double coset decomposition since $b_1 w b_2 \in BwB$. Next, we want to see that this decomposition is unique.

Proof. (Uniqueness) If we had

$$b_1 w b_2 = b_1' w' b_2',$$

then we would have

$$w b_2 b_1'^{-1} = b_1^{-1} b_1' w'$$

so that

$$wb - 2b_2'^{-1} = b_1^{-1} b_1' \in B$$

If $w b_1 w'^{-1}$ is upper triangular, then $w = w'$. For example, if we had

$$\underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}}_{w_1} \begin{pmatrix} b_1 & * & * \\ 0 & b_2 & * \\ 0 & 0 & b_3 \end{pmatrix} = \begin{pmatrix} 0 & b_2 & * \\ 0 & 0 & b_3 \\ b_1 & * & * \end{pmatrix}$$

but the only $w \in S_3$ which takes this matrix to an upper triangular matrix is w_1^{-1}. ■

November 24

If $w_1 = (132)$, then

$$w_1 \cdot b = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} b_1 & \clubsuit & \clubsuit \\ 0 & b_2 & \clubsuit \\ 0 & 0 & b_3 \end{pmatrix} = \begin{pmatrix} 0 & b_2 & \clubsuit \\ 0 & 0 & b_3 \\ b_1 & \clubsuit & \clubsuit \end{pmatrix}$$

Now if $w_1 b w_2 \in B$, then $w_2 = w_1^-$. Note that this does not mean that $w_1 b w_1^{-1}$ is in B. It could be in B for some b. This shows that if $G = GL(n, q)$ and B is the set of upper triangular matricies, then

$$G = \bigcup_{w \in W} BwB$$

is a disjoint union with $W = S_n$. Then consider $\mathcal{H} = (eAe)^{\mathrm{op}}$, $A = KG$, and $e = \frac{1}{|B|} \sum_{g \in B} g$.

Proposition 24 *$\mathcal{H}$ has basis $\{a_w : w \in W\}$ where $a_w = \sum 1|B|sum_{g\in BwB}g$ with multiplication constants as described earlier.*

Lemma 7 *(CR, Exercise 11.19) Let G be any finite group and $H \leq G$ and define $\mathcal{H}$ as before. Also, define $ind(x) = \frac{|H|}{|H\cap {}^x H|}$ as before for $x \in H$. Then the linear map*

$$ind : \mathcal{H} \to K \text{ given by}$$
$$a_j \to ind\ (x_j)$$

is a character of $\mathcal{H}$. Recall that

$$a_j = \frac{1}{|H||}\sum_{x\in D_j} g \text{ and } D_j = Hx_jH$$

Proof. Consider the trivial character ψ of KG restricted to $\mathcal{H}$. We have

$$\begin{aligned}\psi(a_j) &= \frac{1}{|H|}|D_j| \\ &= \frac{1}{|H|}|Hx_jH| \\ &= \frac{1}{|H|}\frac{|H|^2}{|H\cap^{x_j} H|} \\ &= \text{ind}(x_j)\end{aligned}$$

■

Remark 15 *Recall that the dimensions of the irreducible representations of $\mathcal{H}$ give the multiplicities of the multiplicities of the irreducible constituants of* $\text{Ind}_H^G(1)$.

Application. Let $n = 2$, $G = GL(2,q)$, $H = B$, and $W = S_2 = \{1,2\}$. Then $\mathcal{H}$ has basis $\{a_1, a_w\}$. Recall that $a_i a_j = \sum_k \mu_{i,j,k}a_k$ and $\mu_{i,j,k} = \frac{1}{|H|}\left|D_i \cap x_k D_j^{-1}\right|$. Then $a_1 \cdot a_1 = a_1$ and $a_1 \cdot a_w = a_2 \cdot a_1 = a_w$ which is easy to check. It is more difficult to compute $a_w \cdot a_w$. Let $a_w \cdot a_w = \mu a_1 + \lambda a_w$ for somr μ and λ. Then

$$\mu = \frac{1}{|B|}\left((BwB)\cap(BwB)^{-1}\right) = \frac{1}{|B|}|BwB|$$

since $w = w^{-1}$ But since $G = B \cup BwB$, we have $|G| = |B| + |BxB|$ giving $|BwB| = q(q-1)(q^2-q) = q^2(q-1)^2$ so that

$$\mu = \frac{q^2(q-1)^2}{q(q-1)^2} = q.$$

Then $a_2^2 = qa_1 + \lambda a_w$. Apply the charaacter from the lemma to this formula giving

$$(\text{ind } a_w)^2 = q(\text{ind } a_1) + \lambda(\text{ind } a_w) \tag{20}$$

so that $\text{ind}(a_1) = 1$ and $\text{ind}(a_w) = q$ since $B \cap^w B = T$, the subgroup of diagonal matricies giving $\text{ind}(a_w) = \frac{q(q-1)^2}{(q-1)^2} = q$. From (20), we have

$$\begin{aligned}q^2 &= q + \lambda q \\ \lambda q &= q(q-1) \\ \lambda &= q-1\end{aligned}$$

Thus, for $n = 2$ we have $\mathcal{H} = \langle a_1, a_w \rangle$ with multipliciation given by $a_1^2 = a_1$, $a_1 a_w = a_w a_1 = a_2$ and $a_w^2 = q a_1 + (q-1) a_w$. Note that if $q = 1$, then $\mathcal{H}$ is isomorphic to the group algebra of S_2.

Remark 16 *In general, for $G = GL(n, q)$, $\mathcal{H}$ is isomorphic to the group algebra of S_n, which explains why for $GL(3, 2)$, the constituants of of $\mathrm{Ind}_B^G(1)$ occur with mulitpilicities 1, 2, and 1, the degrees of the characters of S_3.*

The *Harish-Chandra theory* or *Theory of Cusp Forms* similarly develops $\mathcal{H}$ for characters other than the trivial character. Let $G = GL(n, q)$ and B the set of upper- triangular matricies.

Definition 23 *A* Borel subgroup *of G is any conjugate of B*

Then the Borel subgroups are solvable subgroups and $B = TU$ for T the diagonal matricies and U the unipotent matricies. Then $|U| = q^{\frac{n(n-1)}{2}}$ is a p-group as $q = p^m$, so U is solvable. Also, T is abelian and $U \lhd B$ so that $B/U \cong T$.

Definition 24 *A* parabolic subgroup *of G is one which contains a Borel subgroup.*

November 26

Let $G = GL(n, q)$ and T the subgroup of diagonal matrices. Then $B = TU$ for U the subgroup of unipotent matrices in B. (Note that the set of unipotent matrices in G is not a subgroup.) A *Borel* subgroup is any conjugate of B and a *parabolic* subgroup is a subgroup containing a Borel subgroup. A parabolic subgroup is conjugate to a subgroup of the form

$$\left\{ \begin{pmatrix} \clubsuit & & & \\ & \clubsuit & & \\ & & \ddots & \\ 0 & & & \clubsuit \end{pmatrix} \right\}$$

For $n = 3$, for example, there are, up to conjugacy, four parabolic subgroups B, P_1, P_2, and G

Insert picture here

and P_1 is *not* conjugate to P_2.

We have a *Levi decomposition* of P given by $P = LV$, a semidirect product, with V the *unipotent radical* of P, that is, the maximal normal unipotent subgroup of P. Then L is a direct product $GL(n_1, q) \times GL(n_2, q) \times \cdots \times GL(n_r, q)$. If P is as in the example above, we have

$$L = \left\{ \begin{pmatrix} \clubsuit & & & 0 \\ & \clubsuit & & \\ & & \ddots & \\ 0 & & & \clubsuit \end{pmatrix} \right\}$$

and

$$V = \left\{ \begin{pmatrix} I & & & 0 \\ & I & & \\ & & \ddots & \\ 0 & & & I \end{pmatrix} \right\}$$

In fact, V is a p-group.

Remark 17 *The characters of U are not known.*

To conclude this section, we want to state the main result of the Harish-Chandra theory. We consider representations of G over a field K of characteristic 0.

If ψ is a character of L, we get a character $\widetilde{\psi}$ of P since $L \cong P/V$. Recall that this is accomplished as follows. If $g \in P$, then $g = lv$ for some $l \in L$, $v \in V$ and we take $\widetilde{\psi}(g) = \psi(l)$. Then we consider $\mathrm{Ind}_P^G\left(\widetilde{\psi}\right)$. Note that $\mathrm{Ind}_B^G(1)$ is a special case.

Definition 25 *An irreducible character χ of G is said to be* cuspidal *or* in the discrete series *if*

$$\left\langle \mathrm{Ind}_P^G\left(\widetilde{\psi}\right), \chi \right\rangle = 0$$

for any $P < G$ with $P \neq G$ and any ψ.

Now cuspidal characters are defined for L where $P = LV$ and

$$L = GL(n_1, q) \times GL(n_2, q) \times \cdots \times GL(n_r, q).$$

Then a cuspidal character ψ of L is $(\psi_1, \psi_2, \ldots, \psi_r)$ for ψ_i cuspidal in the ith block of L

Definition 26 *Let P_1 and P_2 be parabolic subgroups. Then P_1 and P_2 are* associated *if $P_1 = L_1V_1$ and $P_2 = L_2V_2$ for L_1 conjugate to L_2 in G.*

Theorem 16 *(CR1, Vol II, §70B, 70.15A and B but stated there in more generality) Let χ be an irreducible character of G. Then there is a unique pair (P, ψ) such that ψ is cuspidal for L where $P = LV$, and such that $\left\langle \mathrm{Ind}_P^G\left(\widetilde{\psi}\right), \chi \right\rangle \neq 0$. That is, if (P_1, ψ_1) and (P_2, ψ_2) are two such pairs, then ${}^xL_1 = L_2$ and ${}^x\psi_1 = \psi_2$ for some $x \in G$.*

Recall that the last statement means $xL_1x^{-1} = L_2$ and $\psi_2(xl_1x^{-1}) = \psi_1(l_1)$ for $l_1 \in L_1$.

Hence, the characters of G are divided into disjoint sets called *Harish-Chandra families*, each family corresponding to a "cuspidal pair" (L, ψ).

Example 21 *Let $G = GL(3, 2)$. One family is $\{\chi_1, \chi_2, \chi_4\}$ of degrees 1, 6, and 8, from the pair $(T, 1)$ where T is the diagonal subgroup. The second family is $\{\chi_3\}$ from the pair (L, ε) where $L \cong GL(2, 2) \times GL(1, 2) \cong S_3$ and ε is the sign character on the $GL(2, 2)$ block and is cuspidal for L. The remaining characters χ_5 and χ_6 of degree 3 are cuspidal for G.*

The remaining characters in the homework discussed above were constructed an an ad-hoc manner. Indeed, there are two remaining problems.

1. Decompose $\mathrm{Ind}_P^G\left(\widetilde{\psi}\right)$.
2. Construct cuspidals for G (and hence for L).

The following is from the file Hints518 on `ftp://dirichlet.math.uic.edu`

Hints for Homework

Brauer characters for $p = 3$:

You can first use the following theorem. If p^a is the exact power of p dividing the order of the group, and if χ is an irreducible character of the group whose degree is divisible by p^a then χ is irreducible mod P, and is in a block by itself. (This was proved on November 12)

Note that two characters in different blocks will not have any Brauer characters in common. This follows from the decomposition of A or $\overline{A}$ as a sum of indecomposable two-sided ideals.

Using this one gets four Brauer characters for $p = 3$. You have to find only one more. Look at the character of degree 7. Can this decompose mod P? Or is it irreducible? That is what you have to answer.

Brauer characters for $p = 7$:

Here you have to use the fact that $G \cong PSL(2,7)$. We described (and you have a hand-out) describing the representations of $SL(2,7)$ over a field of characteristic 7. The Brauer characters you get from these have degrees 1 through 7, of which the ones of degrees 1,3,5,7 will be Brauer characters for $PSL(2,7)$. You can take elements of orders 1, 2, 3, 4 (which are the ones you want) in $SL(2,7)$, and in fact since you only want the traces of these elements in the representations, you can take them to be diagonal in some extension field. For example, an element of order 4 in $SL(2,7)$ can be taken to be a diagonal matrix D with $i, -i$ on the diagonal (here i is a fourth root of unity in an extension of F_7). Suppose you consider the representation of degree 3, which is in a space spanned by X^2, XY, Y^2 (see the hand-out; this was also discussed in class, on November 17). How does D act on this space? It will have eigenvalues $i^2, i(-i), (-i)^2$, with trace $-1 + 1 + (-1) = -1$, which is exactly what you expect. (Why? Look at the reduction mod P of the character(s) of degree 3 of G to the 7-regular elements; you get the values $3, -1, 0, 1$. Note that D modulo the center of $SL(2,7)$ is of order 2, and so you should expect -1 for the value of the character of degree 3 there, and this is what you got above.) For the element of order 4 in G you must start with a diagonal matrix with eighth roots of unity along the diagonal in $SL(2,7)$, and so on. So the solution is just computational, once you know the theory for $SL(2,p)$.

December 1

Here is a summary of the techniques we used so far to produce characters.

1. Frobenius induction. Given a character ψ of $H \leq G$ (here G is any finite group), we can find a character $\mathrm{Ind}_H^G \psi$ of G. This also works for some groups other than finite groups.

2. Harish-Chandra induction. This works for groups G of Lie type such as $GL(n,q)$. If $G = GL(n,q)$ we take a parabolic subgroup $P \leq G$ and write $P = LV$ where L is a product of smaller GL's. We take a character ψ of L and *inflate* (or *pull-back*) ψ producing a character $\widetilde{\psi}$ of P We then get the induced character $\mathrm{Ind}_H^G\left(\widetilde{\psi}\right)$ of G. This also works for some groups other than finite groups.

3. Cuspidal characters of G do not arise as constituents of $\mathrm{Ind}_H^G\left(\widetilde{\psi}\right)$ for any ψ

From this procedure, the characters of G fall into *Harish-Chandra families*, one for each P up to *associativity* (which means the L's are conjugate; see the definition given earlier) and a cuspidal character of L, or equivalently for each "cuspidal pair" (L, ψ) up to G-conjugacy.

For $GL(2,q)$, the conjugacy classes are described in terms of their "types". Suppose that in $\overline{\mathbb{F}_q}$ we have selected a primitive $(q^2-1)^{\text{st}}$ root of unity ε, that is $\varepsilon^{q^2-1}=1$ and ε is a generator of $\mathbb{F}_{q^2}^{\times}$. Let $\rho = \epsilon^{q+1}$. Then ρ generates $\mathbb{F}_q^{\times}$. Then we can pick representatives for the conjugacy classes as follows.

The identity: $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

Classes arising from the decomposition $B=TU$: $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ from U and $\begin{pmatrix}\rho^a & 0\\ 0 & \rho^b\end{pmatrix}$ from T with $a \neq b$.

Classes containing elements of the form $\begin{pmatrix}\varepsilon^a & 0\\ 0 & \varepsilon^{aq}\end{pmatrix}$ for $a \not\equiv 0 \pmod{q+1}$, over $\mathbb{F}_{q^2}$. Over $\mathbb{F}_q$ such elements would be given in rational form.

Other classes are omitted such as $\begin{pmatrix}x & 0\\ 0 & x\end{pmatrix}$ and $\begin{pmatrix}x & 1\\ 0 & x\end{pmatrix}$.

We pick a complex primitive $(q^2-1)^{\text{st}}$ root of unity $\widetilde{\varepsilon}$ and let $\widetilde{\rho} = \widetilde{\varepsilon}^{q+1}$. We have a correspondence $\rho^a \longleftrightarrow \widetilde{\rho}^a$ and $\varepsilon^a \longleftrightarrow \widetilde{\varepsilon}^a$.

Most importantly, we do the Harish-Chandra induction from $B=TU$ writing

$$T = \left\{ \begin{pmatrix}\rho^a & 0\\ 0 & \rho^b\end{pmatrix} \right\}$$

as a direct product of two cyclic groups of order $q-1$. We get characters of G in Harish-Chandra families corresponding to pairs (T,ψ), as we see below.

We also have some cuspidal characters of G which don't arise as constituents $\operatorname{Ind}_B^G\left(\widetilde{\psi}\right)$. For example,

$$\left\{ \begin{pmatrix}\varepsilon^a & 0\\ 0 & \varepsilon^{aq}\end{pmatrix} \right) \leq GL\left(2,q^2\right)$$

is a subgroup of order q^2-1, which is conjugate in $GL(2,q^2)$ to a subgroup of $GL(2,q)$ in rational form. We expect some characters "supported" by this subgroup.

We have the following table.

	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}\rho^a & 0\\ 0 & \rho^b\end{pmatrix}$	$\begin{pmatrix}\varepsilon^a & 0\\ 0 & \varepsilon^{aq}\end{pmatrix}$	
1	1	1	1	1	and other linerar characters
$\operatorname{Ind}_B^G\left(\widetilde{\psi}\right), m \neq n$	$q+1$	1	$\widetilde{\rho}^{am}\widetilde{\rho}^{bn} + \widetilde{\rho}^{an}\widetilde{\rho}^{bm}$	0	
S	q	0	1	-1	S is the Steinberg character of d

Here 1 and S arise as constituents of $\operatorname{Ind}_B^G(1)$.

To construct cuspidal characters, we use an important concept called the *Brauer Lift*, described in CR1, p. 436. For any G a finite group with (K,R,k) as before, we lift characters from kG to KG. Note that this is the reverse of what we did before. Given $x \in G$, we can write

$$x = su = us$$

where u has order a power of p and s has order prime to p. Then we have the following deep theorem.

Theorem 17 *Let λ be the Brauer character of a kG module L. Then define a function*

$$\widehat{\lambda} : G \to K \text{ by } \widehat{\lambda}(x) = \lambda(s).$$

then $\widehat{\lambda}$ is a virtual character of G, that is, a $\mathbb{Z}$-linear combination of irreducible characters.

Then we take λ to be the Brauer character of the "natural representation" representing each element of G by itself as a matrix over k. From this we have the virtual character

$$2 \mid 2 \mid \widetilde{\rho}^a + \widetilde{\rho}^b \mid \widetilde{\varepsilon}^a + \widetilde{\varepsilon}^{aq}$$

If we subtract from this the character of degree $q+1$ constructed above with $m = n = 1$, we have the character

$$q-1 \mid -1 \mid 0 \mid -(\widetilde{\varepsilon}^a + \widetilde{\varepsilon}^{aq})$$

which is cuspidal. By using other Brauer characters we can construct all the missing cuspidal characters.

For the character tables of $GL(2,q)$ and $GL(3,q)$ see a paper of Steinberg [Canadian Journal of Math, 1951]. The Brauer lift is not used there, but was used in an important paper of J.A.Green (Trans. Amer. Math. Soc. 88 (1955)).

December 3

Consider $G = GL(3,q)$ and $T \leq G$ the diagonal matricies. Then $|T| = (q-1)^3$. For Harish-Chandra induction, we use $B = TU$ and $P = LV$ where $L = \left\{ \begin{pmatrix} \clubsuit & \clubsuit & 0 \\ \clubsuit & \clubsuit & 0 \\ 0 & 0 & \clubsuit \end{pmatrix} \right\}$ and $P = \left\{ \begin{pmatrix} \clubsuit & \clubsuit & \clubsuit \\ \clubsuit & \clubsuit & \clubsuit \\ 0 & 0 & \clubsuit \end{pmatrix} \right\}$. This was accomplished in Homework 5, for $q = 2$. Note that $|B| = q^3(q-1)^3$ Let $T := \left\{ \begin{pmatrix} \rho^a & 0 & 0 \\ 0 & \rho^b & 0 \\ 0 & 0 & \rho^c \end{pmatrix} \right\}$ where ρ is a generator of $\mathbb{F}_q^\times$ and let

$$\psi = \psi_{l,m,n} : \left\{ \begin{pmatrix} \rho^a & 0 & 0 \\ 0 & \rho^b & 0 \\ 0 & 0 & \rho^c \end{pmatrix} \right\} \mapsto \widetilde{\rho}^{la} \widetilde{\rho}^{mb} \widetilde{\rho}^{nc}$$

Here $\widetilde{\rho}$ is as in the case of $GL(2,q)$.

We must construct $\mathrm{Ind}_B^G\left(\widetilde{\psi}\right)$. When l, m, n are distinct mod $q-1$, we get an irreducible character of degree $(q+1)(q^2+q+1)$. When $l \equiv m \not\equiv n$, we get characters of degree q^2+q+1 and $q(q^2+q+1)$. When $l \equiv m \equiv n$, we get characters of degree 1, q^2+q with multiplicity 2, and q^3.

For example, when $q = 2$ as in our group, we have $|B| = 8$ and $[G : B] = 21$. We get charactes of degree 1, 6, and 8.

Now construct $\mathrm{Ind}_P^G(\widetilde{\varphi})$ for φ a cuspidal character of L of degree $q-1$. We have $|P| = q^3(q-1)(q^2-1)(q-1)$ and $[G:P] = q^2+q+1$ and we get an irreducible character of degree $(q-1)(q^2+q+1) = q^3-1$. For example, when $q=2$ as in our group, this produces a character of degree 7.

Finally, G has cuspidal characters of degree $(q-1)(q^2-1)$. For example, when $q=2$ as in our group, these are characters of degree 3.

Remark 18 *To construct cuspidal characters for groups other than $GL(n,q)$, we need Deligne-Lusztig theory, which we will discuss next time.*

Here is a summary of what we've done this semester, but viewing the material covered in a different order:

Let G be a finite group and F a field. We want to study the representation of G over F, which is the same as studying the representations of the group algebra FG, that is, the FG-modules, which are finite-dimensional vector spaces over F. Hence, it is natrual to consider A-modules with A an Artinian ring where we have the minimum condition on left ideals of A. Then

1. every non-nilpotent ideal contains an idempotent,
2. J is nilpotent
3. A/J is semi-simple or completely reducible.

We then develop the Wedderburn theory for semisimple Artinian rings. Now let $A = FG$ and M an A-module. It is natural to ask whether $M = M_1 \oplus M_2$, and if so, whether we can decompose further. Since A is finite dimensional, we must get $M = \bigoplus_i M_i$ for M_i indecomposable. Using the Krull-Schmidt theorem, we have that this decomposition is unique.

Next, we decompose ${}_AA = \bigoplus_i L_i$ for L_i indecomposable left ideals. This produces e_i orthogonal primitive idempotents by taking $1 = \sum_i e_i$ so that $A = \bigoplus_i Ae_i$. We notice that Ae_i are projective A-modules. This implies that Ae_i has a unique maximal submodule Je_i and hence a unique, irreducible quotient Ae_i/Je_i. Furthermore, $Ae_i \cong Ae_j$ if and only if $Ae_i/Je_i \cong Ae_j/Je_j$.

At this point, it is natural to consider the characteristic of F. If char $F = 0$, then A is semisimple by Maschke's theorem. We develop a character theory over $\mathbb{C}$ or over a sufficiently large field K of characersic 0. We introduce the p-modular system (K,R,k) as a way to pass between characersic 0 and characersic p. The idea is that representations should give us information about the group G, hence the representations over fields of characersic p should give us information about, and reflect, the p- structure of G. The homework has been intended to illustrate the "global information" from "local information" philosophy.

Further hints for the homework

This is a hint for the Brauer characters for $p=3$ for $GL(3,2)$. The main question is whether the character of degree 7, restricted to the $3'$-elements, is irreducible as a Brauer character. Consider the value of the character at the 7- elements, which is 0. See whether this is possible if the Brauer character decomposes, since the eigenvalues of these elements are 7-th roots of unity.

Further hints for the homework (added December 10)

With the hints I gave you earlier for the Brauer characters of the group of order 168 for p=3, you can get to the stage where the character of degree 7 is either irreducible (the correct answer) or the sum of the trivial character and a Brauer character of degree 6. I was too hasty in thinking that it is obvious to rule out the possibility that the character of degree 7 is reducible. Here is one way of doing this.

Recall that we constructed the character of degree 7 as an induced character $Ind_P^G(\epsilon)$ where P is a parabolic subgroup (isomorphic to S_4) and ϵ is the sign character of P. We can take an RG-module for this induced module and go mod P (here p=3) as usual, and get a kG-module L. Then L is still an induced module from P (the point is that the sign character of P is irreducible mod 3). If L contains the trivial module as a composition factor then $Hom_{kG}(L, S)$ is non-zero, where S is a module for kG for the trivial representation, or $Hom_{kG}(S, L)$ is non-zero. But both these are zero by Frobenius reciprocity (see the October 8 lecture, where it is proved that $Hom_{RH}(L, M_H) = Hom_{RG}(L^G, M)$. In this formula put L to be a module for ϵ and M to be S). One other point is that from this formula you get $Hom_{kG}(L, S) = 0$. To show that $Hom_{kG}(S, L) = 0$ you use dual modules; L is dual to itself.

December 5

More on the nasty handout. We have $|SL(2,p)| = p(p-1)(p+1)$. Also, a Sylow p-subgroup is $U = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$. The elements of order p are unipotent. If $x \in SL(2,p)$ then $x = su = us$ for s a p'-element and u a unipotent element. However, if $u \in U$, the only s such that $su = us$ is $s = 1$. So every element is either a p'-element or of order p. Suppose s is a p'-element. If the order of s divides $p-1$ then s is conjugate to an element of T, the subgroup of diagonal matrices. On the other hand if the order of s divides $p+1$ then s can be put in rational form. In each case, two p'-elements are conjugate if and only if their characteristic polynomials are the same.

Brief Introduction to Deligne-Lusztig Theory [Carter, Finite Groups of Lie Type]

The philosophy is the following. Let $G = GL(n,q)$. We have $\mathrm{Ind}_B^G\left(\widetilde{\psi}\right)$ irreducible in many cases. For example, when $n = 3$, we can take $\psi = \psi_{l,m,n}$ for l, m, n distinct mod $q-1$. Here $B = TU$, ψ is a character of T, and its lift to B is the character $\widetilde{\psi}$ of B. But if S is a cyclic Sylow subgroup of order $q^n - 1$, then

$$S = \langle A \rangle, \text{ for } A = \begin{pmatrix} 0 & 0 & & \clubsuit \\ 1 & 0 & & \clubsuit \\ 0 & 1 & & \clubsuit \\ \vdots & & & \\ 0 & 0 & 1 & \clubsuit \end{pmatrix}$$

in rational form. Here S is *not* a subgroup of a bigger subgroup of G. Then $\mathrm{Ind}_S^G(\theta)$ for θ a character of S will be hard to decompose.
For example, in $GL(3,2)$, $(S| = 7$.

Now look at $G \leq \widetilde{G} = GL\left(n, \overline{\mathbb{F}_q}\right)$. In $\widetilde{G}$, we have $\widetilde{B} = \widetilde{T}\widetilde{U}$ and $T \leq \widetilde{T}$ and $B \leq \widetilde{B}$. (Here $\widetilde{B}, \widetilde{T}, \widetilde{U}$ are defined analogously to B, T, U in G.)
Then $g^{-1}Sg \leq \widetilde{T}$ for some $g \in \widetilde{G}$ so that $S \leq g\widetilde{T}g^{-1} = \widetilde{T}_1 \leq g\widetilde{B}g^{-1} = \widetilde{B}_1$. Set $g\widetilde{U}g^{-1} = \widetilde{U}_1$.

Definition 27 *Define the* Frobenius map *to be the homomorphism*

$$F : \widetilde{G} \to \widetilde{G} \text{ given by } (a_{i,j}) \to \left(a_{i,j}^q\right)$$

Then

$$G = \widetilde{G}^F = \left\{F\text{-fixed points of } \widetilde{G}\right\}$$

and similarly, $B = \widetilde{B}^F$ and $T = \widetilde{T}^F$, but $\widetilde{B}_1$ need not be F-stable.

We now return to $\mathrm{Ind}_B^G\left(\widetilde{\psi}\right)$. Since $B = TU$, we have $\mathrm{Ind}_U^G(1) = \mathrm{Ind}_B^G\left(\mathrm{Ind}_U^B(1)\right) = \mathrm{Ind}_B^G\left(\sum_\psi \widetilde{\psi}\right) = \sum_\psi \mathrm{Ind}_B^G\left(\widetilde{\psi}\right)$. A module for $\mathrm{Ind}_U^G(1)$ is

$$KG \otimes_B \left(\bigoplus V_\psi\right)$$

where V_ψ is a module for B for the 1-dimensional representation $\widetilde{\psi}$. This is a bi-module with G acting on the left and T acting on the right.
We have $G \leq \widetilde{G}$ and $S \leq \widetilde{B}_1 = \widetilde{T}_1\widetilde{U}_1$. Define an algebraic variety

$$X = \left\{g \in \widetilde{G} : g^{-1}F(g) \in \widetilde{U}_1\right\}$$

(This is analogous to the coset space G/U where $F(gU) = F(g)U$ for $g \in G$ and also $F(gU) = gU$. Hence, $g^{-1}F(g) \in U$.)

We have G acting on the left and S on the right of X. If $h \in G$, $g \in X$, we have to check that $hg \in X$. We have

$$(hg)^{-1} F(hg) = g^{-1} \underbrace{h^{-1}F(h)}_{1} F(g) \in X$$

Next, we have to check that if $t \in S$ and $g \in X$, then $gt \in X$ which follows from: $\widetilde{U}_1$ is normal in $\widetilde{B}_1$. We have

$$(gt)^{-1} F(gt) = \underbrace{t^{-1}g^{-1}F(g)\,t}_{\in \widetilde{U}_1} \in \widetilde{U}_1$$

since t normalizes $\widetilde{U}_1$.

We need an action of G on some vector space over a field of characteristic 0 associated with X. This is constructed using a deep theory of Grothendieck and others of l-adic cohomology. Take l prime with l not dividing q. Take $\overline{Q_l}$ the algebraic closure of the field of l-adic numbers. We then have, corresponding to X, a vector space $H_c^i\left(X, \overline{Q_l}\right)$ (for each $i \geq 0$) over $\overline{Q_l}$ (i.e. l-adic cohomology groups with compact support). Then G acts on the left and S acts on the right of the cohomology groups, by functoriality.

The final step is to take θ a character of S which produces $R_S^G(\theta)$, a virtual character of G, called a Deligne-Lusztig character, given by

$$R_S^G(\theta) = \sum_{i \geq 0} (-1)^i H_c^i\left(X, \overline{Q_l}\right)_\theta$$

where $H_c^i\left(X, \overline{Q_l}\right)_\theta$ is the part of $H_c^i\left(X, \overline{Q_l}\right)$ on which S acts by the character θ. If $g \in G$, we get the character value

$$R_S^G(\theta)(g) = \sum_{i \geq 0} (-1)^i \operatorname{Trace}(g, H_c^i\left(X, \overline{Q_l}\right)_\theta)$$

.

Finally, the construction given above generalizes to finite groups of Lie type (such as symplectic groups, orthogonal groups over finite fields). For details see the book by Carter referred to above, p.205.

Thus we have arrived at the end of the course, which showed you some of the beautiful aspects of the Representation Theory of Finite Groups. If you wish to go further, Bon Voyage and Bon Courage!