[s:lr]

11. Local Representation Theory

We are now going to study *Local Representation Theory* following Alperin's book. Here are the conventions fixed for the rest of the course:

- k an algebraically closed field of prime characteristic p
- A a finite dimensional associative k-algebra with identity
- Modules are all left modules and finite dimensional over k
- G a finite group, kG the group ring with coefficients in k
- When we talk of p-groups, p-subgroups, etc., p refers to the characteristic of k.

Observe that A is Artinian and that modules have finite length.

Results about A and A-modules established in Alperin's book are very special cases of those we have studied from Bourbaki's Algebra Chapter 8. Here for example are three equivalent descriptions of the radical of A:

- the smallest submodule of A such that the quotient is semisimple;
- the intersection of the maximal submodules of A;
- the largest nilpotent ideal of A.

The second description is our definition: the radical $\mathfrak{Rad}\, M$ of a module M is defined as the intersection of its maximal proper submodules, and the radical of a ring as its radical as a (left) module over itself. The first description follows from an item in the list of observations in §10.2: $\mathfrak{Rad}\, M$ is the smallest submodule such that $M/\mathfrak{Rad}\, M$ is semisimple. As to the third, the radical of an Artinian ring is nilpotent (Theorem 10.3); on the other hand, the radical of a ring contains every nil ideal (left, right, or two-sided)—see the corollaries of Theorem 10.1.

Here are some important observations:

- $A/\mathfrak{Rad}\, A$ is semisimple. Indeed, by the Artinianness of A, $\mathfrak{Rad}\, A$ is an intersection of finitely many maximal left ideals, say $\mathfrak{l}_1, \ldots, \mathfrak{l}_k$; so $A/\mathfrak{Rad}\, A$ imbeds into the semisimple module $A/\mathfrak{l}_1 \oplus \cdots \oplus A/\mathfrak{l}_k$.
- $\mathfrak{Rad}\, M = (\mathfrak{Rad}\, A)M$. Indeed, $\mathfrak{Rad}\, M \supseteq (\mathfrak{Rad}\, A)M$ in general (for $\mathfrak{Rad}\, A$ kills any semisimple module, hence $M/\mathfrak{Rad}\, M$); on the other hand, $M/(\mathfrak{Rad}\, A)M$ is a module for $A/\mathfrak{Rad}\, A$ and therefore semisimple.
- The *socle*, denoted $\operatorname{soc} M$, of a module M is the largest semisimple submodule: it is the sum of all simple submodules of M. It equals $(0 :_M \mathfrak{Rad}\, A) := \{m \in M \mid (\mathfrak{Rad}\, A)m = 0\}$. (Indeed, $\mathfrak{Rad}\, A$ kills any semisimple module, in particular the socle. On the other hand, $(0 :_M \mathfrak{Rad}\, A)$ is a module for $A/\mathfrak{Rad}\, A$, and so semisimple.)

[ss:radsocseries]

11.1. **The radical and socle series.** The *radcial series* of a module M is this decreasing sequence of submodules: $\mathfrak{Rad}^0\, M \supseteq \mathfrak{Rad}^1\, M \supseteq \mathfrak{Rad}^2\, M \ldots$, where $\mathfrak{Rad}^0\, M := M$ and $\mathfrak{Rad}^n\, M$ for $n > 0$ is defined by induction: $\mathfrak{Rad}^n\, M := \mathfrak{Rad}\,(\mathfrak{Rad}^{n-1}\, M)$. It is a strictly decreasing sequence and so is eventually 0. The least r such that $\mathfrak{Rad}^r\, M = 0$ is called the *radical length* of M.

The *socle series* of a module M is this increasing sequence of submodules: $\operatorname{soc}^0 M \subseteq \operatorname{soc}^1 M \subseteq \operatorname{soc}^2 M \ldots$, where $\operatorname{soc}^0 M := 0$ and, $\operatorname{soc}^j M$ for $j > 0$ is defined by induction: it is the submodule of M such that $\operatorname{soc}^j M/\operatorname{soc}^{j-1} M = \operatorname{soc}(M/\operatorname{soc}^{j-1} M)$. It is a strictly increasing sequence and so is eventually M. The least s such that $\operatorname{soc}^s M = M$ is called the *socle length* of M.

- The radical length equals the socle length and is called the *Loewy length*. (Indeed, setting $J := \mathfrak{Rad}\, A$, we have, as observed above, $\mathfrak{Rad}\, M = JM$ and $\operatorname{soc} M = (0 :_M J)$. Thus $\mathfrak{Rad}^k\, M = J^k M$ and $\operatorname{soc}^k M = (0 :_M J^k)$. Since the least k such that $J^k M = 0$ is also the least k such that $(0 : J^k) = M$, the assertion follows.)
- Denoting by ℓ the Loewy length of M, we have $\mathfrak{Rad}^i\, M \subseteq \operatorname{soc}^{\ell - i} M$ for $0 \leq i \leq \ell$. (Indeed, following the notation and drift of the argument in the previous item, we have $J^i M \subseteq (0 :_M J^{\ell - i} M)$.)

11.2. **Group algebras.**

[t:kgss]

Theorem 11.1. *The group algebra kG is semisimple if and only if p does not divide the order of the group G.*

Proof. The semisimplicity of G in case p does not divide $|G|$ is proved by averaging (as we have already seen in class). We now show that kG is not semisimple in case p divides $|G|$. (For a different proof, see Exercise 11.6.3.) If it were semisimple, it would follow from Wedderburn structure theory that every simple module occurs in the left regular representation of kG as many times as the dimension of that module as a vector space over k. It suffices therefore to show that the trivial module occurs at least twice.

Let $\Delta(G)$ denote the kernel of the natural map from kG to k defined by $g \mapsto 1$ for every g in G. The quotient $kG/\Delta(G)$ is evidently the trivial module. Let σ denote the element $\sum_{g \in G} g$ of kG. Its span is a copy of the trivial module, and (this is where we use the hypothesis) $\Delta(G) \supseteq k\sigma$. Thus we have $kG \supseteq \Delta(G) \supseteq k\sigma \supseteq 0$, which shows that the trivial module occurs at least twice in the left regular representation. □

[t:brauer1]

Theorem 11.2. (Brauer) *The number of simple kG-modules equals the number of p-regular conjugacy classes (i.e., those in which the order of any element is coprime to p).*

We explore some corollaries before giving the proof of the theorem in §11.5.

[c1:t:brauer1]

Corollary 11.3. *The only simple kG-module for G a p-group is the trivial module.*

Proof. This is clear from the theorem. We give an independent proof based on the class equation. Let V be a simple kG-module. Let $0 \neq v$ be an element of V and consider the $\mathbb{Z}/p\mathbb{Z}$-span W of the orbit Gv of v. Then W is a finite G-set of cardinality a positive power of p. Since 0 is a G-fixed point in W, there is, by Eq. (1.7), at least one other G-fixed element in W. The k-span of this element is, on the one hand, a non-zero G-invariant subspace of V and so equals V, and, on the other, trivial as a kG-module.

Yet another proof can be given using Theorem 11.5. Proceed by induction on $|G|$. If $|G| > p$, then there exists a non-trivial proper normal subgroup N of G. The restriction of a simple G-module S to N is semisimple by the theorem. By induction, simple kN-modules are trivial, so $S|_N$ is trivial. Thus S is a $k(G/N)$-module. But since $|G/N| < |G|$, another application of the induction hypothesis shows that S is trivial. The case $G = \mathbb{Z}/p\mathbb{Z}$ needs to be handled separately, but that is easily done: by commutativity, simple modules are 1-dimensional (Corollary 8.3), and the only root in k of $x^p - 1$ is 1. □

[c2:t:brauer1]

Corollary 11.4. *Let G be cyclic of order n. Write $n = p^e r$ with $(p, r) = 1$. Then the number of isomorphism classes of simple kG-modules is r. The simple modules are all 1-dimensional.*

Proof. G being abelian, the conjugacy classes are all singletons. The order of $x \in G$ is coprime to p if and only if $x^r = 1$. The collection $\{x \in G \,|\, x^r = 1\}$ has cardinality r: in fact, it is the subgroup of G of order r. The first assertion now follows from the theorem. We now produce r distinct 1-dimensional modules, and this will prove the second assertion. The equation $X^r - 1$ is separable over k, so it has r distinct roots over k. Given a root, we can define an algebra homomorphism $kG \to k$ by sending a fixed generator of G to the given root. Varying the roots, we get r non-isomorphic 1-dimensional kG-modules.

As for the earlier corollary, we give an independent proof of this too. We know from Corollary 8.3 that the simple modules of kG are all 1-dimensional. Let $kG \to k$ be the homomorphism defining a 1-dimensional module. Let x be the image in k under this of a generator of G. Then $x^n = 1$. But $x^n = 1$ if and only if $x^r = 1$. Now argue as in the previous paragraph to get r distinct simple modules corresponding bijectively to the r distinct roots in k of the equation $X^r = 1$. □

[ss:sl2p]

11.3. **Simple moodules for the group $\mathbf{SL}(2, p)$.** Let $G = \mathrm{SL}(2, q)$, the group of 2×2 matrices with entries in the field of $q = p^e$ elements and determinant 1. Then the number of simple kG-modules is q. This follows from Theorem 11.2 and the fact that the number of p-regular conjugacy classes in G is q (Exercise 11.6.2).

Let V be the 'defining representation' of G, i.e., E is the vector space of 2×1 matrices with entries in k on which G acts by left multiplication. Consider the action of G on the space V_d of polynomial k-valued functions of degree d on V. Evidently $\dim_k V_d = d + 1$. For $0 \leq d < p$, the kG-modules V_d are simple (Exercise **??**).

Thus for $G = \mathrm{SL}(2, p)$, the V_d, $0 \leq d < p$, are a complete set of simple kG-modules.

[ss:clifford1]

11.4. **A first contact with Clifford theory.** 'Clifford theory' relates representation theory to normal subgroups. The following basic theorem was used to give an alternative proof of Corollary 11.3.

[t:clifford1]

Theorem 11.5. *The restriction to a normal sugbroup N of a semisimple G-module is semisimple.*

Proof. It is enough to show that the restriction of a simple module S is semisimple. Let W be a kN simple submodule of S. For $g \in G$, consider the subspace gW of S. The key observation is:

gW is an N-submodule of S. Moreover it is simple.

Since $ngw = g(g^{-1}ng)w \in gW$, it follows that gW is N-invariant, and that, as an N-module, gW is the pull-back of W via the automorphism $n \mapsto g^{-1}ng$ of N (§1.4.3). This proves the observation.

Now consider $\sum_{g \in G} gW$. It is evidently G-invariant, and so equals S (it is non-zero since $W \neq 0$). The equation $S = \sum_{g \in G} gW$ expresses S as a sum of simple N-modules, so S is semisimple as an N-module. □

[ss:pf:t:brauer1]

11.5. **Proof of Brauer's Theorem 11.2.** Enter the subspaces that are the main characters in the proof: $T := [kG, kG]$ and $S := \mathfrak{Rad}\,(kG) + T$. We make a series of observations, Eq. (11.3) being the most crucial of them. The theorem itself follows immediately from Eqs. (11.2) and (11.4).

(11.1) the number of conjugacy classes in G = the codimension of T in kG.

If x and y are conjugate in G, say $x = gxg^{-1}$, then

$$x - y = x - gxg^{-1} = g^{-1}(gx) - (gx)g^{-1} \in T$$

so $\geq$ holds. Now suppose $x_1, \ldots, x_k$ belong to different conjugacy classes in G and let $\sum_{i=1}^{k} \alpha_i x_i \equiv 0 \pmod{T}$. Consider the characteristic function φ_1 the class of x_1. It extends naturally to a linear functional on kG. We observe that it vanishes on T. Indeed, T is linearly spanned by $gh - hg$ with g, h in G, but gh and hg are conjugate: $gh = h^{-1}(hg)h$. Applying φ_1 to the linear dependence relation, we see that $\alpha_1 = 0$. Similarly the other coefficients too vanish, and Eq. (11.1) is proved. The proof in fact shows that classes in kG/T of representatives in G of the conjugacy classes form a k-basis.

(11.2) the number of distinct simple kG-modules = the codimension of S in kG.

The number of simple kG-modules is the same as the number of simple modules for $A := kG/\mathfrak{Rad}\,(kG)$. Since A is semisimple, the latter number equals the number r, where $A = A_1 \times \cdots \times A_r$ is the Wedderburn decomposition of A into a product of simple algebras. The question now is: how can we probe A and extract r without troubling ourselves with the full decomposition into simple algebras? Given below are two ways of doing this.

Each simple algebra A_i being a matrix algebra over k, we have:

- The centre of $M_n(k)$ being the space of scalar matrices, it is 1-dimensional over k. The centre of A being the product of the centres of the A_i, we conclude that the centre of A has dimension r over k.
- $[M_n(k), M_n(k)]$ being the space of traceless $n \times n$ matrices, the codimension of $[A_i, A_i]$ in A_i is 1. Since $[A, A] = [A_1, A_1] \times \cdots \times [A_r, A_r]$, we conclude that the codimension of $[A, A]$ in A is r.

We use the second characterization of r to finish the proof. Indeed

$$[A, A] = [\frac{kG}{\mathfrak{Rad}\,(kG)}, \frac{kG}{\mathfrak{Rad}\,(kG)}] = \frac{[kG, kG] + \mathfrak{Rad}\,(kG)}{\mathfrak{Rad}\,(kG)} \text{ so that } \frac{A}{[A, A]} \simeq \frac{kG}{S},$$

and Eq. (11.2) is proved.

The next observation is the key to the proof of the theorem:

$$S = \{x \mid x^{p^e} \in T \text{ for some } e \geq 0\} \tag{11.3}$$

Suppose x belongs to the right hand side. To show $x \in S$, it suffices to do so modulo $\mathfrak{Rad}\,(kG)$, since $S \supseteq \mathfrak{Rad}\,(kG)$. Now, $S/\mathfrak{Rad}\,(kG)$ is just the commutator $[kG/\mathfrak{Rad}\,(kG), kG/\mathfrak{Rad}\,(kG)]$. Thinking of $kG/\mathfrak{Rad}\,(kG)$ as a product of matrix algebras, we need to show that x has trace 0 as a linear operator on any simple kG-module. But this is clear since x^{p^e} has trace 0 and $\mathrm{Tr}\,(x^{p^e}) = (\mathrm{Tr}\,x)^{p^e}$.

To prove the other containment, it suffices to prove that the right hand side is a subspace, for $S := T + \mathfrak{Rad}\,(kG)$ and both T, $\mathfrak{Rad}\,(kG)$ belong to the right hand side: the case of T is evident, and $\mathfrak{Rad}\,(kG)$ is nilpotent. It is clear that the right hand side is closed under scalar multiples. What requires proof is its closure under addition. For this, we use the following properties of T:

(1) $(x+y)^p \equiv x^p + y^p \pmod{T}$ for x, y in kG.
(2) $x^p \in T$ for $x \in T$.

Let us proceed with the proof of Eq. (11.3) assuming the above properties.We claim:

(3) $(x+y)^{p^e} \equiv x^{p^e} + y^{p^e} \pmod{T}$ for x, y in kG.

To prove (3), proceed by induction on e, the case $e = 1$ being (1). By induction $(x+y)^{p^{e-1}} = x^{p^{e-1}} + y^{p^{e-1}} + t$ for some $t \in T$, so that $(x+y)^{p^e} = ((x+y)^{p^{e-1}})^p = (x^{p^{e-1}} + y^{P^{e-1}} + t)^p \equiv x^{p^e} + y^{p^e} + t^p \pmod{T}$, the last equality being justified by (1). By (2), $t^p \in T$, so we are done with the proof of (3).

Now, if x^{p^e} and y^{p^f} are in T, then assuming (without loss of generality) that $e \geq f$, we have $y^{p^e} \in T$ (by (2)) and $(x+y)^{p^e} \in T$ by (3). This finishes the proof of Eq. (11.3) except that we still need to prove (1) and (2).

To prove (1), we expand $(x+y)^p$ and partition the terms other than x^p and y^p into sets of cardinality p, the elements of each set being in the same equivalence class with respect to cyclic permutation of the factors. For (2), it is enough, by (1), to show that $(xy - yx)^p \in T$ for x, y in kG. But, again by (1), $(xy - yx)^p \equiv (xy)^p - (yx)^p \pmod{T}$, and $(xy)^p - (yx)^p = ((xy)^{p-1}x)y) - y((xy)^{p-1}x) \in T$. The proof of Eq. (11.3) is now complete.

Our final observation is:

(11.4) the codimension of S in kG = the number of p-regular conjugacy classes

We will show in fact that the images in kG/S of representatives in G of the p-regular conjugacy classes form a k-basis for kG/S. Images in kG/T of representative of all classes form a basis for kG/T (by the proof of Eq. (11.1). Since $T \subseteq S$, it suffices to prove the following:

(a) If $g = us$ be the 'Jordan decomposition' (see Exercise 11.6.7) of g in G, then $g \equiv s \pmod{S}$.
(b) images in kG/S of representatives of p-regular classes are linearly independent.

To prove (a), observe that $(g-s)^{p^e} = ((u-1)s)^{p^e} = (u^{p^e} - 1)s^{p^e} = 0$ (when e is large enough that $u^{p^e} = 1$). For (b), if x_i belong to different p-regular conjugacy classes in G and $\sum \alpha_i x_i \equiv 0 \pmod{S}$, then $(\sum \alpha_i x_i)^{p^e} \equiv 0 \pmod{T}$, and, by (3) above, $\sum \alpha_i^{p^e} x_i^{p^e} \equiv 0 \pmod{T}$, but $x_i^{p^e}$ belong to distinct conjugacy classes (Exercise 11.6.8), so by Eq. (11.1), $\alpha_i^{p^e} = 0$, so $\alpha_i = 0$.

The proof of Theorem 11.2 is complete.

11.6. **Exercises.**

11.6.1. Determine the radical and socle series of the $T_n(k)$-module $T_n(k)$, where $T_n(k)$ denotes the ring of lower triangular $n \times n$ matrices with entries in k.

[sss:sl2p]

11.6.2. The number of p-regular conjugacy classes in $\mathrm{SL}(2, q)$ is q.

[sss:sigmanilp]

11.6.3. Let p divide $|G|$. Then $k\sigma$ is a nilpotent two sided ideal of kG, where $\sigma = \sum_{g \in G} g$.

11.6.4. If G is a p-group, then $\mathfrak{Rad}\,(kG) = \Delta(G)$ (where $\Delta(G)$ is defined to be the kernel of the map $kG \to k$ defining the trivial module).

11.6.5. If N is a normal subgroup of G, then $\mathfrak{Rad}\,(kN) = kN \cap \mathfrak{Rad}\,(kG)$.

11.6.6. If N is a normal subgroup of G and T a simple kN-module, then there exists a simple kG-module S such that T is a direct summand of $S|_N$.

11.6.7. For g in G, there is a unique expression[11] $g = su$, with s, u in G, such that [sss:jd]

- the order of s is coprime to p, that of u is a power of p;
- s and u commute.

Evidently, s has order r and u order p^e, where $p^e r$, $(p, r) = 1$, is the order of g.

11.6.8. Let elements x, y of a group be non-conjugate. Let their orders be coprime to p (where p is a prime). Then x^{p^e} and y^{p^e} are non-conjugate (for all $e \geq 0$). [sss:pconj]

[11]This is the Jordan decomposition when the finite group G is considered as a linear algebraic group over k.