

Noncommutative Algebra for Part III of Serre's *Linear Representations of Finite Groups*

Minor Thesis in Mathematics by David Savitt

February 3, 1997

The third part of J.-P. Serre's book *Linear Representations of Finite Groups* discusses of modular representations, i.e., representations of finite groups over a field of nonzero characteristic. The aim of this work is to complement Serre's work by introducing the reader to some noncommutative algebra used in the study of modular representations, and in particular to the theory of semisimple and projective modules over noncommutative rings.

Throughout, G will denote a finite group, all rings will be rings with identity (denoted by 1). Also, every module should be taken to be finitely generated; where that condition is stated explicitly, it is for clarity.

1 Representations are modules

1.1 The Group Ring

Given a group G and a ring R , we can construct an object $R[G]$ called the group ring. The elements of $R[G]$ are the formal sums

$$\sum_{g \in G} r_g \cdot g$$

with $r_g \in R$, so that to each element of G we have associated an element of R . Two such sums add in the natural way:

$$\sum_{g \in G} r_g^1 \cdot g + \sum_{g \in G} r_g^2 \cdot g = \sum_{g \in G} (r_g^1 + r_g^2) \cdot g.$$

Multiplication is defined by setting $(r \cdot g)(s \cdot h) = (rs) \cdot (gh)$ for $r, s \in R$, $g, h \in G$, and extending the operation to the whole group ring by linearity. It is not difficult to check that these operations make $R[G]$ into a ring.

We may evidently identify the group G inside the group ring as the multiplicative subset consisting of elements of the form $1 \cdot g$ (i.e., the set of elements where g has coefficient 1 and all other elements of G have coefficient 0), and we can identify R as the subring of $R[G]$ composed of elements of the form

$r \cdot e$, where e is the identity element of G . The group ring can be made into an R -module by putting

$$r \cdot \left(\sum_{g \in G} r_g \cdot g \right) = \sum_{g \in G} (rr_g) \cdot g.$$

As an R -module, $R[G]$ is isomorphic to the free R -module $R^{\#G}$, where $\#G$ denotes the order of the group G .

Henceforth, for abbreviation we will write rg instead of $r \cdot g$ in such sums, and instead of $1g$ we may write simply g .

1.2 Representations

A linear representation ρ of a group G over a field L is a homomorphism from G to the group of automorphisms of an L -vector space V , that is,

$$\rho : G \rightarrow \text{GL}(V).$$

In essence, ρ does concretely represent G (or, at least, a quotient of G , since ρ is not necessarily injective) as a group of $n \times n$ matrices with entries in L , where n is the dimension of V . We say that such a representation is of degree (or dimension) n .

Since ρ associates to each $g \in G$ a linear transformation of V , we can define a left action of G on V via

$$g \cdot v = \rho(g)(v)$$

for all $v \in V$. This action extends by linearity to give an action of the group ring $L[G]$ on V with

$$\left(\sum_{g \in G} l_g g \right) \cdot v = \sum_{g \in G} l_g \rho(g)(v).$$

Under this action, V becomes an $L[G]$ -module. On the other hand, every $L[G]$ -module can be obtained in this fashion from a representation: if M is such a module, then the underlying set of M can be regarded as an L -vector space under the action of L (identified as a subring of $L[G]$ as described in section 1.1). It can then be checked that the action of any element x of $L[G]$ on that vector space is a linear transformation $\rho(x)$. Since for any $g \in G$, $\rho(g)$ must be invertible with inverse $\rho(g^{-1})$, it follows that ρ , when restricted to G (again, identified as a subset of $L[G]$), is indeed a representation. One notes immediately that the $L[G]$ -module that this ρ produces is precisely equal to the original module M .

To study representations, we therefore turn to the study of modules over group rings. The thrust of our investigation is to examine how modules can be seen as composed of smaller modules—basic building blocks—and then to examine the smaller modules themselves. We will need to look at two types of building

blocks: simple modules and indecomposable modules. A nonzero module is termed simple if it contains no submodules, and is indecomposable if it cannot be written as a direct sum of nontrivial submodules. The representations associated with simple modules are called irreducible.

Notice that while a simple module must be indecomposable, the converse does not necessarily hold. For example, the \mathbb{Z} -module $\mathbb{Z}/p^2\mathbb{Z}$ is indecomposable, yet contains the submodule $p\mathbb{Z}/p^2\mathbb{Z}$. While understanding their structure will prove more immediately tractable for simple modules than for indecomposable ones, the direct sum is by far the most basic way of building a larger module out of smaller ones. Thus the indecomposable modules will nevertheless prove to be of interest.

We can make one observation now about simple modules. If M is a simple R -module and if $m \in M$ is nonzero, then the set Rm is certainly a nonzero submodule of M . By the simplicity of M , $Rm = M$. Thus M is generated by any single nonzero element. Further, we can map $R \rightarrow M$ surjectively via $1 \mapsto m$, so that M is a quotient R/I . The simplicity of M implies I is in fact a maximal left ideal.

2 A short course in noncommutative ring theory

2.1 Chain conditions

Let S be a set which is partially ordered by the relation \leq . S is said to satisfy the ascending chain condition (a.c.c.) provided that any chain $x_0 \leq x_1 \leq x_2 \leq \dots$ eventually becomes stationary—that is, provided there exists n such that $x_k = x_n$ for all $k \geq n$. Equivalently, S has the a.c.c. if and only if every nonempty subset of S has a maximal element. (An element $x \in T \subset S$ is maximal provided that $x \leq y$ for $y \in T$ implies $x = y$.) The descending chain condition (d.c.c.) is defined analogously.

A ring R for which the a.c.c. (respectively, d.c.c.) is satisfied on the set of left ideals ordered under inclusion is called Noetherian (respectively, Artinian). Similarly, an R -module M whose submodules satisfy the a.c.c. (resp., d.c.c.) is also termed Noetherian (resp., Artinian). Evidently, a ring is Noetherian (resp., Artinian) if and only if it is Noetherian (resp., Artinian) when regarded as a left module over itself, since left ideals are then precisely equal to submodules.

It is clear from the definitions that a submodule of a Noetherian (resp., Artinian) R -module is again Noetherian (resp., Artinian). This is not necessarily the case for rings, however, since if $S \subset R$ is a subring, the R -ideals contained in S can be very different from the S -ideals in S . For example, the integral domain $\mathbb{C}[x_1, x_2, \dots]$ is not Noetherian (check!), but is nevertheless a subring of its field of fractions—and every field is Noetherian (and Artinian), since a field has no nontrivial ideals.

Proposition 1 *If $0 \rightarrow M \xrightarrow{\alpha} M' \xrightarrow{\beta} M'' \rightarrow 0$ is a short exact sequence of R -modules, then M' is Noetherian if and only if both M and M'' are. (The same holds with Noetherian replaced by Artinian.)*

Proof Suppose first that M' is Noetherian. If we have an ascending chain $M_0 \subset M_1 \subset \dots$ of submodules in M , then $\alpha(M_0) \subset \alpha(M_1) \subset \dots$ is an ascending chain in M' , which by assumption must become stationary. By the injectivity of α , it follows that the original chain becomes stationary, so M is Noetherian. The proof that M'' is Noetherian is similar.

On the other hand, suppose M and M'' are Noetherian, and let $M'_0 \subset M'_1 \subset \dots$ be an ascending chain in M' . Then

$$\beta(M'_0) \subset \beta(M'_1) \subset \dots$$

and

$$\alpha^{-1}(M'_0) \subset \alpha^{-1}(M'_1) \subset \dots$$

are ascending chains in M'' and M respectively, and so eventually become stationary. To complete the proof, it therefore suffices to show that if P and Q are submodules of M' with $P \subset Q$, $\beta(P) = \beta(Q)$, and $\alpha^{-1}(P) = \alpha^{-1}(Q)$, then $P = Q$. To that end, note that

$$\beta(P) = (P + \alpha(M))/\alpha(M)$$

and

$$\beta(Q) = (Q + \alpha(M))/\alpha(M),$$

so that under the given conditions, $P + \alpha(M) = Q + \alpha(M)$. If $q \in Q$, we can therefore write $q = p + \alpha(m)$ with $p \in P$ and $m \in M$. Since $p \in P \subset Q$, we find that $\alpha(m) = q - p \in Q$. But then $m \in \alpha^{-1}(Q) = \alpha^{-1}(P)$, so $\alpha(m) \in P$ as well, and as a result $q \in P$. Thus $Q \subset P$, and the result is proved.

The proof in the Artinian case is identical. ♠

Notice that if R is a Noetherian ring, then by repeated application of the lemma so is any free R -module R^k , k an integer. Given an R -module M with generators x_1, \dots, x_k , we obtain a map of R^k onto M by sending the element of $R \oplus \dots \oplus R$ with a 1 in the i th position and zeros elsewhere to x_i . Thus M is a quotient of R^k . However, the quotient of a Noetherian module is quite evidently also Noetherian, and since the converse is trivial we have proved

Proposition 2 *A ring R is Noetherian if and only if every finitely generated left R -module is Noetherian.*

Once again the result also holds with Noetherian replaced by Artinian. As an example, we can prove

Proposition 3 *If a ring R satisfies a.c.c., then so does the group ring $R[G]$. Similarly, if R satisfies d.c.c., so does $R[G]$.*

Proof Suppose R is Noetherian. As we noted in section 1.1, we can regard $R[G]$ as a left R -module, and as R -modules we have $R[G] \cong R^{\#G}$. Thus $R[G]$ is Noetherian as a left R -module. But every left ideal of the ring $R[G]$ is in fact also an R -submodule, so every collection of left ideals is also a collection of R -submodules, and has a maximal element. The proof in the Artinian case is identical. ♠

The reader who is unfamiliar with these concepts should verify another characterization of the ascending chain condition: an R -module M is Noetherian if and only if every submodule of M is finitely generated, and consequently a ring R is Noetherian if and only if every ideal of R is finitely generated. Since every finitely generated module over a Noetherian ring R is Noetherian, it follows that every submodule of a finitely generated module over a Noetherian ring is again finitely generated.

2.2 Composition series; the Jordan-Hölder theorem

A composition series for an R -module M is a finite chain $M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$ of distinct modules such that each successive quotient M_{i-1}/M_i , $1 \leq i \leq n$, is a simple module.

Given a module M with a composition series, we define the length $l(M)$ of M to be the length of the shortest composition series for M . (For example, a simple module has length 1.) Let $M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$ be such a minimal composition series, and let N be any submodule of M . We then have a chain

$$N = N \cap M_0 \supset N \cap M_1 \supset \cdots \supset N \cap M_n = 0. \quad (*)$$

Furthermore, for $0 \leq i \leq n-1$ we can define a map $\phi_i : (N \cap M_i)/(N \cap M_{i+1}) \rightarrow M_i/M_{i+1}$ by sending

$$x + N \cap M_{i+1} \mapsto x + M_{i+1}.$$

It is easily seen that ϕ_i is well-defined and, since $M_{i+1} \cap (N \cap M_i) = N \cap M_{i+1}$, ϕ_i is injective. Since M_i/M_{i+1} is simple, the image of ϕ_i must either be 0 or M_i/M_{i+1} , and thus $(N \cap M_i)/(N \cap M_{i+1})$ is either 0 or simple. Therefore, once repetitions where $N \cap M_i = N \cap M_{i+1}$ are removed, (*) yields a composition series for N .

Suppose that N is a proper submodule of M . Since $M_n = N \cap M_n = 0$ and $M = M_0 \neq N \cap M_0 = N$, there exists a positive integer k such that $N \cap M_k = M_k$ but $N \cap M_{k-1} \subsetneq M_{k-1}$. Then

$$(N \cap M_{k-1})/(N \cap M_k) = (N \cap M_{k-1})/M_k \subsetneq M_{k-1}/M_k$$

and by the simplicity of M_{k-1}/M_k we see that $N \cap M_{k-1} = N \cap M_k$. Therefore, there does in fact exist a repetition in (*), so the composition series for N is shorter than that for M , and $l(N) < l(M)$. Thus, proper submodules have strictly smaller lengths. We can now prove:

Proposition 4 *For an R -module M to have a composition series it is necessary and sufficient that M satisfy both a.c.c. and d.c.c.*

Proof If M has a composition series, we know that every submodule of M does, and that the length of any submodule lies between 0 and $l(M)$. Given any collection of submodules of M , by the well-ordering of the integers there exist members M_{max} and M_{min} of the collection with maximal and minimal lengths

respectively. Since proper submodules have strictly smaller lengths, it follows that M_{max} and M_{min} are in fact maximal and minimal under inclusion, and M therefore satisfies both chain conditions.

Conversely, if M satisfies both chain conditions, then by the a.c.c. there exists a maximal proper submodule M_1 of M . Since M_1 is maximal, M/M_1 is simple. We may repeat this process to obtain a chain of submodules $M \supset M_1 \supset M_2 \supset \dots$ where, unless $M_k = 0$, the inclusion $M_k \supset M_{k+1}$ is proper and the quotient M_k/M_{k+1} is simple. By the d.c.c., $M_k = 0$ for some k , and we obtain a composition series. ♠

Notice that if $l(M) = n$, any strictly decreasing chain of submodules of M has length at most n , since the lengths of the modules in the chain must also be strictly decreasing. It follows at once that every composition series for M must have length precisely n . Two composition series are said to be equivalent if any given simple module appears (up to isomorphism) as a successive quotient exactly the same number of times in both composition series. It is to that extent that composition series are unique:

Theorem 5 (Jordan-Hölder) *If the R -module M possesses a composition series, then any two composition series for M are equivalent.*

Proof We proceed by induction on $l(M)$. Suppose we have two composition series for M ,

$$M = M_0 \supset M_1 \supset \dots \supset M_k = 0 \quad (1)$$

and

$$M = N_0 \supset N_1 \supset \dots \supset N_k = 0. \quad (2)$$

If $M_1 = N_1$, we are done, by the induction hypothesis. If $M_1 \neq N_1$, by maximality we have $M = M_1 + N_1$, and so

$$M_1/(M_1 \cap N_1) \cong (M_1 + N_1)/N_1 = M/N_1 \quad (*)$$

and

$$N_1/(M_1 \cap N_1) \cong (M_1 + N_1)/M_1 = M/M_1. \quad (*')$$

Taking any composition series

$$M_1 \cap N_1 \supset L_2 \supset \dots \supset L_k = 0$$

for $M_1 \cap N_1$, we therefore obtain two more composition series for M :

$$M \supset M_1 \supset M_1 \cap N_1 \supset L_2 \supset \dots \supset L_k = 0 \quad (3)$$

and

$$M \supset N_1 \supset M_1 \cap N_1 \supset L_2 \supset \dots \supset L_k = 0 \quad (4).$$

By the induction assumption, (1) and (3) are equivalent and (2) and (4) are equivalent. However, by (*) and (*'), (3) and (4) are equivalent. Consequently, (1) and (2) are also equivalent. ♠

2.3 Indecomposable modules and the Krull-Schmidt theorem

We have seen, then, that if a module satisfies both chain conditions, it is built via successive quotients from a (unique) list of simple modules. We turn now to an analogous structure theorem, with simple modules replaced by the more complicated indecomposable modules, and with quotients replaced by the easier mechanism of direct sums.

Proposition 6 *If an R -module M is Artinian, it can be written as a direct sum of finitely many indecomposable submodules.*

Proof Let S be the collection of all nonzero submodules of M that cannot be written as a direct sum of finitely many indecomposable submodules. If S is nonempty, by the d.c.c. there exists a minimal module $N \in S$. If N were indecomposable, it would trivially be a direct sum of finitely many indecomposable submodules, and so there must exist nontrivial submodules N_1 and N_2 such that $N = N_1 \oplus N_2$. By the minimality of N in S , we see that each N_i must in fact be a sum of finitely many indecomposable submodules, and so N is such a sum as well. This contradiction leads to the conclusion that S must be empty, and that therefore M can be written as the sum of finitely many indecomposable submodules. ♠

Once again, we wish to obtain a uniqueness result. We first need:

Lemma 7 *Let M be an indecomposable R -module satisfying both chain conditions. Then any endomorphism ϕ of M is either nilpotent ($\phi^k = 0$ for some k) or an automorphism.*

Proof From ϕ we obtain two chains of submodules

$$M \supset \text{im}(\phi) \supset \text{im}(\phi^2) \supset \dots$$

and

$$0 \subset \ker(\phi) \subset \ker(\phi^2) \subset \dots$$

Since M satisfies both chain conditions, there consequently exists k such that $\text{im}(\phi^n) = \text{im}(\phi^k)$ and $\ker(\phi^n) = \ker(\phi^k)$ for all $n \geq k$. Suppose $m \in \text{im}(\phi^k) \cap \ker(\phi^k)$. Writing $m = \phi^k(n)$, we see

$$\phi^{2k}(n) = \phi^k(m) = 0$$

, and so $n \in \ker(\phi^{2k})$. But $\ker(\phi^{2k}) = \ker(\phi^k)$, so $n \in \ker(\phi^k)$ and $m = \phi^k(n) = 0$. Therefore

$$\text{im}(\phi^k) \cap \ker(\phi^k) = 0,$$

and the sum $\text{im}(\phi^k) + \ker(\phi^k)$ is direct. If $x \in M$, the fact that $\text{im}(\phi^{2k}) = \text{im}(\phi^k)$ implies that there exists $y \in \text{im}(\phi^k)$ such that $\phi^k(y) = \phi^k(x)$. Then $x = y + (x - y)$ with $\phi^k(x - y) = 0$, which proves that $x \in \text{im}(\phi^k) + \ker(\phi^k)$ and

$$M = \text{im}(\phi^k) \oplus \ker(\phi^k).$$

Since M is indecomposable, we find that either $\text{im}(\phi^k) = 0$, in which case ϕ is nilpotent, or else $\text{im}(\phi^k) = M$ and $\text{ker}(\phi^k) = 0$. In the latter case $\text{im}(\phi) = M$ and $\text{ker}(\phi) = 0$ as well, and ϕ is an isomorphism. ♠

Lemma 8 *Let M be an indecomposable R -module satisfying both chain conditions. If ϕ_1, \dots, ϕ_n are endomorphisms of M such that the sum $\phi_1 + \dots + \phi_n$ is an automorphism of M , then at least one of the ϕ_i must be an automorphism.*

Proof If the lemma is established in the case $n = 2$, then for $n > 2$, $\phi_1 + \dots + \phi_n = \phi_1 + (\phi_2 + \dots + \phi_n)$. Either ϕ_1 or $\phi_2 + \dots + \phi_n$ is then an automorphism, and the result follows by induction. In the case $n = 2$, put $\phi = \phi_1 + \phi_2$. Since ϕ by assumption is an automorphism, $1_M = (\phi_1 \circ \phi^{-1}) + (\phi_2 \circ \phi^{-1})$, so without loss of generality we can suppose $\phi = 1_M$. Then $\phi_2 = 1_M - \phi_1$, so ϕ_1 and ϕ_2 commute. Commutativity ensures that the binomial theorem holds for ϕ_1 and ϕ_2 , so if both maps are nilpotent, say with $\phi_1^{k_1} = 0$ and $\phi_2^{k_2} = 0$, then

$$0 = \sum_{k=-k_1}^{k_2} \binom{k_1+k_2}{k_1+k} \phi_1^{k_1+k} \phi_2^{k_2-k} = (\phi_1 + \phi_2)^{k_1+k_2} = 1_M^{k_1+k_2} = 1_M.$$

This would be a contradiction, so one of ϕ_1 and ϕ_2 is not nilpotent and, by the preceding lemma, must be an automorphism. ♠

Theorem 9 (Krull-Schmidt) *Let M is an R -module satisfying both chain conditions. Suppose M has two decompositions as direct sums of indecomposable submodules:*

$$M = U_1 + U_2 + \dots + U_r$$

and

$$M = V_1 + V_2 + \dots + V_s.$$

Then $r = s$ and, for a suitable rearrangement of the indices, $U_i \cong V_i$.

Proof Our proof is by induction on r , and the result is clear in the case $r = 1$. Suppose $r > 1$.

From the direct sum decompositions, we obtain canonical projections $\pi_i : M \rightarrow U_i$ and $\rho_i : M \rightarrow V_i$ such that $1_M = \pi_1 + \dots + \pi_r = \rho_1 + \dots + \rho_s$, $\pi_i^2 = \pi_i$, $\rho_i^2 = \rho_i$, and $\pi_i \pi_j = \rho_i \rho_j = 0$ for $i \neq j$.

Then

$$\pi_1 = \pi_1 \rho_1 + \dots + \pi_1 \rho_s$$

and, restricting to U_1 , we have

$$1_{U_1} = \pi_1|_{V_1} \rho_1|_{U_1} + \dots + \pi_1|_{V_s} \rho_s|_{U_1}.$$

Since U_1 inherits both chain conditions from M , by the above lemma one of the $\pi_1|_{V_i} \rho_i|_{U_1}$ (suppose after reordering that $i = 1$) is an automorphism of U_1 . For brevity of notation, set $\pi = \pi_1|_{V_1}$ and $\rho = \rho_1|_{U_1}$. The current situation, then, is that the composition of the two maps in the following diagram is an automorphism of U_1 :

$$U_1 @> \rho >> V_1 @> \pi >> U_1.$$

Thus ρ is injective and π is surjective. Consider the associate diagram

$$V_1 @> \pi >> U_1 @> \rho >> V_1.$$

The composition $\rho\pi$ cannot be nilpotent: if $(\rho\pi)^k = \rho(\pi\rho)^{k-1}\pi = 0$, then by the surjectivity of π and injectivity of ρ we get $(\pi\rho)^{k-1} = 0$. But $\pi\rho$ is an automorphism, so indeed this cannot be the case. By lemma 7, then, $\rho\pi$ is an automorphism of V_1 , and therefore ρ is surjective, π is injective, both are isomorphisms, and $U_1 \cong V_1$.

We wish next to show that the sum $V_1 + U_2 + \cdots + U_r$ is direct and equal to M . Once that is established, we can conclude

$$M/V_1 \cong U_2 + \cdots + U_r \cong V_2 + \cdots + V_s$$

and the theorem follows by induction.

Since π_1 is an isomorphism from V_1 to U_1 , for any $u \in U_1$ we can select $v \in V_1$ such that $\pi_1 v = u$. The direct sum decomposition of M with respect to the U_i allows us to write $v = u_1 + \cdots + u_r$ with $u_i \in U_i$. Then $u = \pi_1 v = u_1$. So $u = v - u_2 - \cdots - u_r$, which proves that

$$U_1 \subset V_1 + U_2 + \cdots + U_r,$$

and therefore that $V_1 + U_2 + \cdots + U_r = M$. Similarly, if

$$v \in V_1 \cap (U_2 + \cdots + U_r)$$

and $v = u_1 + \cdots + u_r$, then $u_1 = 0$ and $\pi_1 v = 0$. Since π_1 restricted to V_1 is an isomorphism onto U_1 , we conclude $v = 0$, the above intersection is 0, and the sum

$$M = V_1 + U_2 + \cdots + U_r$$

is direct. ♠

2.4 Semisimple modules

We have seen that an Artinian R -module M can be written as a finite direct sum of indecomposable submodules. Of particular importance will be the class of modules where these direct summands are in fact all simple modules; these are called semisimple modules. In fact, a module is labelled semisimple whenever it can be written as a direct sum of simple submodules, whether or not that sum is finite. There are several important characterizations of semisimple modules:

Proposition 10 *Let M be an R -module. The following conditions are equivalent:*

1. M is semisimple

2. Every R -submodule of M is a direct summand. That is, if $N \subset M$ is a submodule, there exists another submodule N' such that $M = N \oplus N'$.
3. M is spanned by the simple R -modules contained in M .

Lemma 11 *If M is a module satisfying condition (2) of the above proposition, then any submodule of M also satisfies that condition.*

Proof of 11 Suppose $N \subset M$ is a submodule, and let $N_0 \subset N$ be a submodule of N . Then N_0 has a complement N' in M , so that $M = N_0 \oplus N'$. It is easily verified that $N = N_0 \oplus (N' \cap N)$. ♠

Proof of 10 To show that (1) \implies (2), suppose

$$M = \bigoplus_{\alpha \in I} M_\alpha$$

with all M_α simple, and suppose $N \subset M$ is an R -submodule. Let S be the collection of all subsets $J \subset I$ such that the sum

$$N + \bigoplus_{\alpha \in J} M_\alpha$$

is direct. S is nonempty, as the empty set is contained in S . Consider a chain

$$J_1 \subset J_2 \subset \cdots$$

of elements of S . Set

$$J_\infty = \bigcup_{n=1}^{\infty} J_n.$$

Any element $m \in \bigoplus_{\alpha \in J_\infty} M_\alpha$ is a finite sum

$$m = m_{\alpha_1} + \cdots + m_{\alpha_k}$$

with $m_{\alpha_i} \in M_{\alpha_i}$ and each $\alpha_i \in J_\infty$. Since the number of α_i is finite, there must exist q such that $\alpha_i \in J_q$ for all i . Then

$$m \in \bigoplus_{\alpha \in J_q} M_\alpha$$

and since we assumed $N \cap \bigoplus_{\alpha \in J_q} M_\alpha = 0$, we conclude that

$$N \cap \bigoplus_{\alpha \in J_\infty} M_\alpha = 0,$$

and $J_\infty \in S$. We have shown, then, that any chain in S (ordered under inclusion) has an upper bound. Applying Zorn's lemma, we conclude that S has a maximal element. Let J be such a maximal element.

Put

$$N' = \bigoplus_{\alpha \in J} M_\alpha.$$

Choose $\beta \in I$. Since

$$M_\beta \cap (N \oplus N') \subset M_\beta$$

and M_β is simple, the intersection is either 0 or M_β . If the intersection were 0, the sum

$$(N \oplus N') + M_\beta = N + (N' \oplus M_\beta)$$

would be direct, contradicting the maximality of J . So instead $M_\beta \subset N \oplus N'$ for all $\beta \in I$, and it follows that $M = N \oplus N'$. We have thus constructed a complement for N .

(It is not necessarily true that the sum

$$N + \bigoplus_{\substack{\alpha \in I \\ M_\alpha \cap N = 0}} M_\alpha$$

is direct. For example, the submodule $\{(x, x) \mid x \in \mathbb{Q}\}$ of $\mathbb{Q} \oplus \mathbb{Q}$ has intersection zero with both direct summands.)

Next, we show (2) \implies (3). Suppose M satisfies (2). Let N be any nonzero submodule of M , and take $x \in N$. Suppose the homomorphism $R \rightarrow Rx$ via $1 \mapsto x$ has kernel I . Then $Rx \cong R/I$. I is an ideal of R , and is therefore contained in a maximal left ideal \mathfrak{m} . Then \mathfrak{m}/I is a submodule of R/I , and by lemma 11 has a complement S such that

$$R/I = S \oplus \mathfrak{m}/I.$$

But then

$$S \cong (R/I)/(\mathfrak{m}/I) \cong R/\mathfrak{m},$$

so by the maximality of \mathfrak{m} we find that S is simple. The upshot of all this, then, is that any nonzero submodule of M contains a simple submodule.

Let N be the sum of all the simple submodules of M . By our assumption that M satisfies (2), N has a complement N' in M . If N' is nonzero, by the preceding argument it contains a simple submodule. This contradicts our assumption that N contains every simple submodule of M , so $N' = 0$ and $N = M$.

Last, we need to prove that (3) \implies (1). If $\{M_\alpha \mid \alpha \in I\}$ is the set of simple submodules of M , following a procedure like that in the proof that (1) \implies (2) we get a subset $J \subset I$ which is maximal with the property that the sum of the M_α ranging over $\alpha \in J$ is in fact direct. As before, the intersection of any simple submodule M_β with that direct sum is either 0 or the M_β . Once again, the former possibility contradicts the maximality of J , so

$$M_\beta \subset \bigoplus_{\alpha \in J} M_\alpha.$$

Recalling our assumption that the simple submodules of M span M , we get that

$$M = \bigoplus_{\alpha \in J} M_\alpha,$$

and we are done. ♠

Corollary 1 *A submodule of a semisimple module is again semisimple. The direct sum of any set of semisimple modules is again semisimple.*

The first statement follows immediately from proposition 10 and lemma 11. The second statement is obvious, by proposition 10.

Corollary 2 *A quotient of a semisimple module is again semisimple.*

Proof If M is semisimple, suppose $Q = M/N$. Then there exists $Q' \subset M$ such that $M = Q' \oplus N$, and $Q' \cong M/N = Q$. But Q' is semisimple, so Q is. ♠

We also define the term semisimple for rings: a ring R is semisimple when the left R -module obtained from R acting on itself via multiplication is a semisimple module.

This leads to the beautiful:

Proposition 12 *A ring R is a semisimple ring if and only if every (not necessarily finitely generated) R -module is a semisimple module.*

Proof We know that any finitely generated R -module is of the form R^k/S for some submodule S of R^k . By the preceding corollaries, R^k and its quotients are all semisimple, so the proposition is true for finitely generated modules. If M is any R -module, then

$$M = \sum_{m \in M} Rm,$$

since each $m \in Rm$. Using the preceding case, each Rm is generated by the single element m , so is a sum of simple submodules. Thus M is also a sum of simple submodules, and by proposition 10 is semisimple. The converse is clear. ♠

Whether or not a semisimple module is Artinian is exactly the determining factor in whether or not the decomposition of M as a direct sum of simple submodules is finite sum:

Proposition 13 *If M is a semisimple R -module, then M can be written as a direct sum of finitely many simple submodules if and only if the module is Artinian.*

Proof If M is Artinian, then proposition 6 shows that M can be written as a finite direct sum of indecomposable submodules. Since each of the indecomposable submodules is again semisimple, and an indecomposable semisimple module

certainly must be simple, M is indeed a finite direct sum of simple submodules. Conversely, by an appeal to definitions, any simple module is Artinian: it has only two submodules, and so clearly will satisfy the descending chain condition. A finite direct sum of Artinian modules is again Artinian, by proposition 1. ♠

Notice that a finite direct sum of simple modules is also Noetherian—this observation proves that any Artinian semisimple module is also Noetherian. It is not true in general that any Artinian module is Noetherian—for example, the \mathbb{Z} -module \mathbb{Q}/\mathbb{Z} is Artinian but fails to be finitely generated.

We now begin to examine the structure of semisimple rings.

Proposition 14 (Schur’s Lemma) *If $\phi : M \rightarrow N$ is a homomorphism of simple R -modules, then either $\phi = 0$ or ϕ is an isomorphism. The endomorphism ring $\text{End}_R(M)$ is a division ring.*

Proof If ϕ is nonzero, then the image of ϕ is nonzero and the kernel of ϕ is not M . But since M and N are simple, the image of ϕ must be N and the kernel must be 0 , so ϕ is an isomorphism. In particular, when $\phi \in \text{End}_R(M)$ is nonzero, ϕ has an inverse. It is readily checked that the inverse is also an endomorphism of N , so the endomorphism ring is indeed a division ring. ♠

Proposition 15 *If $D = \text{End}_R(M)$, then $\text{End}_R(M^n)$ is equal to the ring of $n \times n$ matrices $M_n(D)$.*

Proof (sketch) Note that we have injections $i_k : M \rightarrow M^n$ and projections $\pi_k : M^n \rightarrow M$ from M to the k th component of M^n and vice-versa. If ϕ is an endomorphism of M^n we obtain n^2 endomorphism of n , $\pi_j \circ \phi \circ i_k$. Thus, we get an $n \times n$ matrix of endomorphisms of M with $\pi_j \circ \phi \circ i_k$ as the j, k -entry, and we leave it to the reader to verify that this is indeed an isomorphism of $\text{End}_R(M^n)$ to $M_n(D)$. ♠

Let M be an Artinian semisimple R -module, so that M can be written as

$$M = M_1^{n_1} \oplus \cdots \oplus M_k^{n_k}$$

with the M_i being distinct semisimple R -module. Schur’s lemma shows us that

$$\text{End}_R(M) = \text{End}_R(M_1^{n_1}) \oplus \cdots \oplus \text{End}_R(M_k^{n_k}) = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$$

where D_k is the division ring $\text{End}_R(M_k)$.

In particular, put $R = M$. If ϕ is an R -endomorphism of R , then ϕ is determined by the image of 1, for if $\phi(1) = r$ then $\phi(x) = x\phi(1) = xr$. If $\phi_1(1) = r_1$ and $\phi_2(1) = r_2$, then

$$\phi_1(\phi_2(1)) = \phi_1(r_2) = r_2 r_1,$$

so that $\text{End}_R(R) \cong R^{op}$. (R^{op} is the opposite of R , with the same underlying set as R but the product of a and b in R^{op} equal to the product of b and a in R .) Thus

$$R^{op} = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$$

is a sum of matrix rings over division rings.

We leave it to the reader to check that $(R^{op})^{op} \cong R$, and that $M_n(D)^{op} \cong M_n(D^{op})$ via the transpose map, so that we find

$$R = M_{n_1}(D_1^{op}) \oplus \cdots \oplus M_{n_k}(D_k^{op}).$$

Thus every Artinian semisimple ring is in fact isomorphic to a direct sum of matrix rings over division rings.

If R is an L -algebra—that is, if R contains a field L which commutes with every element of R —then for an R -module M , each element of L gives a distinct endomorphism of M by scalar multiplication, and each of these scalar multiplications is in the center of $\text{End}_R(M)$. In particular each D_k and D_k^{op} contains a copy of L in its center. If M is finite dimensional as an L -vector space, then so is $\text{End}_R(M)$. Thus, if R is finite dimensional as an L -vector space, the division rings D_k and D_k^{op} are finite extensions of L .

Finally, observe that $(D_i^{op})^{n_i}$ is acted on by R (via $M_{n_i}(D_i^{op})$ embedded into R) and under that action is a simple module. This affords a direct sum decomposition of R as a sum of simple submodules, in particular a sum of n_i copies of each $(D_i^{op})^{n_i}$. However, any simple R -module is a quotient, and thus by semisimplicity a direct summand, of R , and an application of the Krull-Schmidt theorem shows that any simple R -module is isomorphic to one of the $((D_i)^{op})^{n_i}$ with the associated action of R .

2.5 The Jacobson radical

Let us define the (Jacobson) radical of a ring R to be the intersection of all the maximal left ideals of R ; we will denote the radical as $\text{rad } R$. Since every proper ideal is contained in a maximal ideal, the intersection is not vacuous.

The radical has several important characterizations. We begin with:

Proposition 16 *An element $x \in R$ is in $\text{rad } R$ if and only if $xM = 0$ for every simple R -module M .*

Proof To prove the if direction, suppose $xM = 0$ for every simple R -module M . Let \mathfrak{m} be a maximal ideal in R . Then R/\mathfrak{m} is indeed a simple R -module, so $x(R/\mathfrak{m}) = 0$, i.e. $xr \in \mathfrak{m}$ for any $r \in R$. In particular,

$$x = x \cdot 1 \in \mathfrak{m}.$$

Thus x is contained in every maximal left ideal, and so is contained in the radical.

Conversely, let M be a simple R -module. The R -module $(\text{rad } R)M$ is a submodule of M , and hence equals either 0 or M . Suppose the latter. Then there exists $m \in M$ such that $(\text{rad } R)m \neq 0$. Yet again $(\text{rad } R)m$ is a submodule of M , so that $(\text{rad } R)m = M$. In particular, we can choose $r \in \text{rad } R$ such that $rm = -m$, or $(r + 1)m = 0$. Thus

$$(1 + r) \in \text{Ann}(m),$$

where $\text{Ann}(m)$ denotes the annihilator of m , the left ideal of elements $x \in R$ such that $xm = 0$. But $\text{Ann}(m) \neq R$, since it does not contain 1, so $\text{Ann}(m)$ is contained in a maximal ideal \mathfrak{m} . However,

$$r \in \text{rad } R \subset \mathfrak{m},$$

so $(1 + r) - r = 1 \in \mathfrak{m}$. This is a contradiction, and we conclude that

$$(\text{rad } R)M = 0.$$

In particular, $xM = 0$ for any $x \in \text{rad } R$. ♠

Corollary *The radical of a ring is in fact a two-sided ideal.*

This follows from the fact that for any $a, b \in R$, $xM = 0$ implies $(axb)M = 0$.

Observe that the above proposition also implies that $\text{rad } R$ annihilates every semisimple R -module.

Proposition 17 *The element $x \in R$ is contained in $\text{rad } R$ if and only if for every $a, b \in R$, $1 - axb$ is a (two-sided) unit in R .*

Proof To show the only if portion, if $x \in \text{rad } R$ it suffices to show that $1 - x$ is a unit: since the radical is a two-sided ideal, every axb is also in $\text{rad } R$, and so $1 - axb$ is a unit by the same argument. Consider the ideal $R(1 - x)$ in R . If this ideal were proper, it is contained in a maximal ideal. That maximal ideal contains $1 - x$, but it also contains x , since x , as an element of the radical is in every maximal ideal. Thus we would have a maximal ideal containing 1, a contradiction. So $R(1 - x) = R$, and in particular there exists $u \in R$ such that

$$u(1 - x) = 1.$$

This shows that $1 - x$ has a left inverse for any $x \in \text{rad } R$. In particular $-ux \in \text{rad } R$, and $u = 1 + ux$, so u must have a left inverse. Thus u is a two-sided unit. But it is elementary that the left inverse and right inverse of a two-sided unit must always coincide, and so $1 - x$ is in fact also a unit.

To show the converse, let M be a simple R -module and let x be such that every $1 - axb$ is a unit. Let $m \in M$, and suppose $xm \neq 0$. Then $Rxm = m$, so there exists $y \in R$ such that $yxm = m$, or $(1 - yx)m = 0$. Since $(1 - yx)$ is a unit, it follows that $m = 0$, contradicting our earlier assumption. This shows that $xM = 0$ for any simple R -module M , and so by proposition 16, $x \in \text{rad } R$. ♠

Notice that the second equivalence in this proposition is left-right symmetric. This shows that the radical is independent of the handedness we have chosen—i.e., if we had formulated our theory in terms of right R -modules and right ideals, the radical would turn out to be exactly the same ideal.

Before proving our next characterization of the radical, we should note that it is not true, in general, that if M is a module then every proper submodule of

M is contained in a maximal submodule. (\mathbb{Q}/\mathbb{Z} is a counterexample.) On the other hand, it is true if M is finitely generated. Recall that the Zorn's lemma argument which shows that every proper ideal is contained in a maximal ideal succeeds because we have an ascending chain of ideals $I_1 \subset I_2 \subset \dots$ none of which contains the identity, so their union does not contain the identity, and is thus still a proper ideal. In the case of a module generated by x_1, \dots, x_n , we get an ascending chain of submodules $M_1 \subset M_2 \subset \dots$ none of which contains all the x_i . Thus the union does not contain all the x_i , and so the union is again a proper submodule, and the Zorn's lemma argument pulls through. We can now prove:

Theorem 18 (Nakayama's Lemma) *If $I \subset R$ is a left ideal, then the following are equivalent:*

1. $I \subset \text{rad } R$
2. For any finitely generated R -module M , $IM = M$ implies $M = 0$.
3. If N is a submodule of the R -module M such that M/N is finitely generated, $N + IM = M$ implies $N = M$.

Proof To see that (1) implies (2), let N be a maximal submodule of M . (N exists by the argument preceding the lemma.) Then M/N is simple, so

$$I(M/N) = (N + IM)/N = 0.$$

But $IM = M$, so in fact $M/N=0$. Thus $M = 0$.

For (2) \implies (3), note again that $I(M/N) = (N + IM)/N = M/N$, so by (2), $M/N = 0$ and $M = N$.

To show that (3) gives (1), let \mathfrak{m} be any maximal ideal of R . Then R/\mathfrak{m} is finitely generated, and by (3) we know $\mathfrak{m} + I = R$ implies $R = \mathfrak{m}$. Since this is not the case, we must instead have $\mathfrak{m} + I = \mathfrak{m}$ (by maximality of \mathfrak{m} , since $\mathfrak{m} + I$ is an ideal containing it). Thus $I \subset \mathfrak{m}$. So I is contained in every maximal left ideal of R , and is thus contained in the radical. ♠

The radical has some additional important properties in the case where R is Artinian.

Proposition 19 *If R is Artinian, then:*

1. $\text{rad } R$ is the largest nilpotent ideal of R .
2. The quotient $R/\text{rad } R$ is semisimple. In fact, $\text{rad } R$ is the smallest ideal of R whose quotient is semisimple.

Proof (1) We obtain a descending chain of ideals

$$R \supset \text{rad } R \supset (\text{rad } R)^2 \supset \dots$$

which, since R is Artinian, must become stationary. Suppose $(\text{rad } R)^n = (\text{rad } R)^k \neq 0$ for all $n \geq k$. Set $\mathfrak{a} = (\text{rad } R)^k$, and let S be the set of all ideals I of R such that $\mathfrak{a}I \neq 0$. Since $\mathfrak{a} \in S$, S is nonempty, and since R is Artinian S contains a minimal element \mathfrak{b} . Since $\mathfrak{a}\mathfrak{b} \neq 0$, there exists $b \in \mathfrak{b}$ such that $\mathfrak{a}b \neq 0$. Clearly $\mathfrak{a}b \in S$ and $\mathfrak{a}b \subset \mathfrak{b}$, so by minimality,

$$\mathfrak{b} = \mathfrak{a}b.$$

In particular, we get $a \in \mathfrak{a} \subset \text{rad } R$ such that $-b = \mathfrak{a}b$, i.e.

$$(1 + a)b = 0.$$

This contradicts proposition 17, which tells us that $1 + a$ is a unit. We must, therefore, have $(\text{rad } R)^k = 0$.

If I is a nilpotent left ideal of R and $x \in I$, then $ba x \in I$ for any $a, b \in R$, so $ba x$ is nilpotent, say $(ba x)^n = 0$. Then $(a x b)^{n+1} = a x (ba x)^n b = 0$, so $a x b$ is also nilpotent. But then $1 - a x b$ is a unit, with two-sided inverse $1 + a x b + \cdots + (a x b)^n$, so by proposition 17 we get $x \in \text{rad } R$, and thus $I \subset \text{rad } R$. So $\text{rad } R$ is indeed the largest nilpotent ideal.

(2) Let S be the set of ideals of R which are equal to a finite intersection of maximal left ideals. Since R is Artinian, S has a minimal element, which we shall denote

$$J = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n,$$

with each \mathfrak{m}_i maximal. Then $J \supset \text{rad } R$. If \mathfrak{m} is any other maximal left ideal of R , then $J \cap \mathfrak{m}$ is also a finite intersection of maximal ideals, so by minimality of J we get

$$J \cap \mathfrak{m} = J,$$

or $J \subset \mathfrak{m}$. J is therefore contained in every maximal ideal, and it follows that $J \subset \text{rad } R$. Thus $J = \text{rad } R$.

Consider the natural map ϕ from $R \rightarrow R/\mathfrak{m}_1 \oplus \cdots \oplus R/\mathfrak{m}_n$. The kernel of the map is clearly $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$, and thus ϕ is an injection from $R/\text{rad } R$ to $R/\mathfrak{m}_1 \oplus \cdots \oplus R/\mathfrak{m}_n$. But each R/\mathfrak{m}_i is a simple module by the maximality of \mathfrak{m}_i , so their sum is semisimple. Since every submodule of a semisimple module is semisimple, we conclude that $R/\text{rad } R$ is indeed semisimple.

On the other hand, if R/I is semisimple, then $(\text{rad } R)(R/I) = 0$. Since R has an identity, we immediately get $\text{rad } R \subset I$. ♠

Corollary 1 *If R is Artinian and semisimple, then $\text{rad } R = 0$ and R has no nilpotent ideals.*

Corollary 2 *If R is Artinian and M is an R -module such that $(\text{rad } R)M = 0$, then M is semisimple.*

Proof of 2 If $(\text{rad } R)M = 0$, we find that M can in fact be regarded as an $R/(\text{rad } R)$ -module: letting $R/\text{rad } R$ act on M by putting $(r + \text{rad } R)m = rm$ for $r \in R$, $m \in M$, the action is well-defined because $(\text{rad } R)m = 0$. Since R is

Artinian, $R/\text{rad } R$ is semisimple, so proposition 12 shows that M is a semisimple $R/(\text{rad } R)$ -module, and is therefore the sum of its simple $R/(\text{rad } R)$ -submodules. But each of these simple submodules can be regarded as an R -submodule of M , and it is not difficult to verify that they indeed remain simple when regarded as R -modules. Thus the R -module M is also a sum of simple submodules, so M is semisimple. ♠

This leads us to a fairly surprising theorem:

Theorem 20 (Hopkins) *An Artinian ring is also Noetherian.*

Proof Letting R be an Artinian ring, the idea of the proof is to construct a composition series for R . Then we know, by proposition 4, that R must also be Noetherian. Since the radical of R is nilpotent, we find that for some integer k ,

$$R \supset \text{rad } R \supset (\text{rad } R)^2 \supset \cdots \supset (\text{rad } R)^k = 0.$$

It suffices to show that each quotient $(\text{rad } R)^i/(\text{rad } R)^{i+1}$ has a composition series, since then the preimage of such a composition series in the natural map from $(\text{rad } R)^i \rightarrow (\text{rad } R)^i/(\text{rad } R)^{i+1}$ provides the modules which fit between $(\text{rad } R)^i$ and $(\text{rad } R)^{i+1}$ in the composition series for R .

Noting that

$$(\text{rad } R)(\text{rad } R)^i/(\text{rad } R)^{i+1} = 0,$$

we see that $(\text{rad } R)^i/(\text{rad } R)^{i+1}$ is a semisimple R -module. It is also Artinian: $\text{rad } R$ is a submodule of R , and a submodule of an Artinian module is Artinian, so $\text{rad } R$ is Artinian. By proposition 1, $(\text{rad } R)^i$ is also Artinian, and then so are its quotients. We observed at the end of the last section that any Artinian semisimple module is also Noetherian. This proves that $(\text{rad } R)^i/(\text{rad } R)^{i+1}$ possesses both a.c.c. and d.c.c, and by proposition 4 it has a composition series, completing the proof. ♠

Hopkins' theorem has some immediate corollaries:

Corollary 1 *If R is an Artinian ring and M is a finitely generated R -module or $R[G]$ -module, then:*

1. *Every submodule of M is finitely generated.*
2. *M possesses a composition series, any two of which are equivalent in the Jordan-Hölder sense. By (1), the same holds for any submodule of M .*
3. *M can be written as a finite direct sum of indecomposable submodules, and any two such sums are equivalent in the Krull-Schmidt sense. By (1), the same holds for any submodule of M .*

Corollary 2 *If R is an Artinian ring, up to isomorphism there exist only finitely many simple R -modules.*

Proof of 2 We know that any simple R -module is M isomorphic to R/\mathfrak{m} for a maximal left ideal \mathfrak{m} . Since \mathfrak{m} is a submodule of R , by the preceding corollary \mathfrak{m} possesses a composition series. Combined with the inclusion $R \supset \mathfrak{m}$, that composition series gives a composition series for R , and the first quotient in that composition series is $R/\mathfrak{m} \cong M$. So, every simple R -module appears as a quotient in a composition series for R . However, the Jordan-Hölder theorem tells us that the finite list of isomorphism classes of simple modules which appear in a composition series is independent of the composition series, and so there can be only finitely many different such isomorphism classes. ♠

The converse of Hopkins' theorem is false, as \mathbb{Z} is a Noetherian ring which is not Artinian.

We turn now to some implications for modules.

Proposition 21 *If R is Artinian and M is an R -module, then the following are equal:*

1. $(\text{rad } R)M$
2. The smallest submodule N of M such that M/N is semisimple
3. The intersection of all the maximal submodules of M .

If M is not finitely generated, we have seen that M may not have any maximal submodules, in which case we define the intersection of all the maximal submodules of M to be R .

Proof Since $(\text{rad } R)M/(\text{rad } R)M = 0$, we know $M/(\text{rad } R)M$ is semisimple. On the other hand, if M/N is semisimple then $(\text{rad } R)M/N = 0$, so $(\text{rad } R)M \subset N$. This proves that (1) = (2).

Let Q be the intersection of the maximal submodules of M . If N is any maximal submodule of M , then M/N is simple, and so

$$(\text{rad } R)(M/N) = (N + (\text{rad } R)M)/N = 0.$$

Thus $(\text{rad } R)M + N = N$, so $(\text{rad } R)M \subset N$. So $(\text{rad } R)M$ is contained in every maximal submodule, and as a result it is contained in Q . We are halfway to proving that (2) = (3).

To show the reverse inclusion, use the fact that $M/(\text{rad } R)M$ is semisimple to write it as a direct sum of simple submodules. Any submodule of $M/(\text{rad } R)M$ is of the form $L/(\text{rad } R)M$, and so we get the sum as

$$M/(\text{rad } R)M = \bigoplus_{\alpha \in I} L_{\alpha}/(\text{rad } R)M \quad (*)$$

The kernel of the resulting projection of M onto $L_{\beta}/(\text{rad } R)M$ is the set of $x \in M$ such that

$$x + (\text{rad } R)M \in \bigoplus_{\alpha \in I - \{\beta\}} L_{\alpha}/(\text{rad } R)M = \left(\sum_{\alpha \in I - \{\beta\}} L_{\alpha} \right) / (\text{rad } R)M$$

i.e. the kernel is equal to the sum of all the L_α excluding L_β . Since $L_\beta/(\text{rad } R)M$ is simple, it follows that

$$M_\beta = \sum_{\alpha \in I - \{\beta\}} L_\alpha$$

is a maximal submodule.

What is the intersection of all the M_β ? Well, M_β is the kernel of the projection of M onto the component with index β on the right-hand side of (*), and the intersection of those kernels is exactly the kernel of the projection of M onto the entire right-hand side in (*), which the equality in (*) shows plainly to be $(\text{rad } R)M$. Thus

$$(\text{rad } R)M = \bigcap_{\beta \in I} M_\beta.$$

We have therefore written $(\text{rad } R)M$ as an intersection of maximal submodules, and so it contains Q . ♠

The set in (1) is called the radical of M . Thus, we see how the radical of R is a measure of how far from semisimple a given module is.

Finally, we conclude this section with:

Proposition 22 *If R is Artinian and M is an R -module, then the following are equal:*

1. *The set of $m \in M$ with $(\text{rad } R)m = 0$*
2. *The largest semisimple submodule of M*
3. *The sum of all the simple submodules of M*

Proof The sum of all the simple submodules of M is a semisimple submodule of M . Further, there is no larger semisimple submodule of M , since any semisimple module is a sum of simple submodules. Thus (2) exists and equals (3). Since (2) is semisimple, it is annihilated by $\text{rad } R$ and is thus contained in (1). But the set annihilated by $\text{rad } R$ is a module, since $\text{rad } R$ is a two-sided ideal, and since it is annihilated by $\text{rad } R$ it is semisimple. Thus (1) = (2). ♠

3 First results of representation theory

We now take a brief look at some first results from representation theory. We begin with a proposition which explains why in general it is more difficult to study representations over a field of nonzero characteristic.

Proposition 23 *If L is a field of characteristic p (possibly 0), then $L[G]$ is a semisimple ring if and only if $p \nmid \#G$ (the order of the group G).*

Proof We would like to see whether or not each submodule M of $L[G]$ has a complement in $L[G]$. We can consider $L[G]$ as a (finite dimensional) L -vector space, and then M is an L -vector subspace of $L[G]$, and we can certainly find a complement M' of M as an L -vector space. The trouble, however, is that M' is *not* necessarily closed under the action of G upon it, and so is not necessarily actually an $L[G]$ -submodule of $L[G]$. Nevertheless, we can use the decomposition $L[G] = M \oplus M'$ as L -vector spaces to obtain an L -linear projection ρ of $L[G]$ onto M . The trick is to try to average ρ over the elements of G ; this will succeed only when we are permitted to divide by the number of elements in G , i.e. when $\text{char} L = p \nmid \#G$. Let us for now make that assumption. We put

$$\rho'(x) = \frac{1}{\#G} \sum_{g \in G} g^{-1} \rho(gx).$$

One checks easily not only that ρ' is again a projection from $L[G]$ onto M , but that this time

$$\rho'(gx) = g\rho'(x)$$

as well, so that the kernel of ρ' is an $L[G]$ -module M'' . Then $L[G] = M \oplus M''$ as $L[G]$ -modules, and $L[G]$ is semisimple.

On the other hand, suppose $p \mid \#G$. Let

$$v = \sum_{g \in G} g \in L[G],$$

and define the $L[G]$ -submodule $V = Lv \subset L[G]$. Suppose $L[G] = V \oplus W$ as $L[G]$ -modules. We can then write the identity of G uniquely as

$$e = cv + (e - cv)$$

with $c \in L$ and $e - cv \in W$. Since W is G -stable and $gv = v$ for all $g \in G$, we see that $g - cv \in W$ for all $g \in G$, and therefore by taking differences $g - e \in W$ for all $g \in G$. Summing over G , this shows that $v - (\#G)e \in W$. But since $p \mid \#G$, $(\#G)e = 0$ in W , and so $v \in W$. This contradicts the disjointness of V and W , so V has no $L[G]$ -module complement in $L[G]$, and $L[G]$ cannot be semisimple. ♠

In general, then, when L has characteristic zero, any $L[G]$ -module is semisimple, and so is a direct sum of simple $L[G]$ -modules. The analysis of all representations of G to L then reduces to the study of the simple modules, i.e. of the irreducible representations. Furthermore, the semisimplicity allows us quick access to some information about the representations.

3.1 The number of irreducible representations

Proposition 24 *Let k be the number of distinct irreducible representations of G over \mathbb{C} . If the irreducible representations have degrees n_1, \dots, n_k then*

$$\sum_{j=1}^k n_j^2$$

and, further, k is exactly equal to the number of conjugacy classes of elements of G .

Proof Our observations at the end of section 2.4 show that we can write

$$\mathbb{C}[G] = M_{m_1}(D_1) \oplus \cdots \oplus M_{m_k}(D_k)$$

for division rings D_i of finite degree over \mathbb{C} , and where the simple $\mathbb{C}[G]$ -modules are isomorphic to $(D_i)^{m_i}$. However, since \mathbb{C} is algebraically closed, and finite degree extension of \mathbb{C} is equal to \mathbb{C} , and therefore each simple $\mathbb{C}[G]$ -module is \mathbb{C}^{m_k} as a \mathbb{C} -vector space. Thus we get $m_k = n_k$ (after a suitable permutation), and so

$$\mathbb{C}[G] = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C}).$$

It remains to show that k equals the number of conjugacy classes in G . We do this by investigating the center $Z(\mathbb{C}[G])$ of the ring $\mathbb{C}[G]$. Suppose

$$x = \sum_{g \in G} a_g g$$

is in $Z(\mathbb{C}[G])$. Then $hx = xh$ and $h x h^{-1} = x$ for any $g \in G$, so

$$x = \sum_{g \in G} a_g h g h^{-1}$$

as well. Matching coefficients, we see that $a_g = a_{g'}$ if g and g' are conjugate. Noting that the element c_i of $\mathbb{C}[G]$ which has coefficient 1 for all elements of the i th conjugacy class of G and coefficient 0 for everything else is indeed in the center of $\mathbb{C}[G]$, we conclude that $Z(\mathbb{C}[G])$ is spanned by the c_i . On the other hand,

$$Z(\mathbb{C}[G]) = Z(M_{n_1}(\mathbb{C})) \oplus \cdots \oplus Z(M_{n_k}(\mathbb{C}))$$

and the center of a matrix ring over \mathbb{C} is precisely the set of scalar matrices and therefore is isomorphic to \mathbb{C} . So we also get $Z(\mathbb{C}[G]) \cong \mathbb{C}^k$. Thus we have counted the dimension of the center of $\mathbb{C}[G]$ in two ways, and shown that k equals the number of conjugacy classes in G . ♠

Example (The symmetric group S_4) The symmetric group S_4 has five conjugacy classes, each corresponding to a different cycle type. The classes have as representatives the identity, $(1\ 2)$, $(1\ 2\ 3)$, $(1\ 2\ 3\ 4)$, and $(1\ 2)(3\ 4)$. Notice that we obtain two 1-dimensional representations of S_5 : the trivial representation taking $\sigma \mapsto 1$ for all σ , and the sign representation, taking $\sigma \mapsto \text{sgn}(\sigma)$. (Any 1-dimensional representation over a field L is simply a map from a group to the multiplicative group of L and plainly must be irreducible.) The preceding proposition tells us that the sum of the squares of the dimensions of the three remaining irreducible representations must sum to 22. It is easily checked that the only possibility is $22 = 2^2 + 3^2 + 3^2$, so that S_4 has two irreducible representations of degree 1, one of degree 2, and two of degree 3.

Example (Abelian groups) If G is abelian, then the ring $\mathbb{C}[G]$ is commutative. Since $M_n(\mathbb{C})$ is commutative only when $n = 1$, it follows that every irreducible representation of G is of degree 1. Further, the number of distinct irreducible representations is exactly equal to $\#G$.

If $\#G$ happens to be cyclic of order n with generator g , then g must be mapped to an n th root of unity. Since the image of g determines the entire representation, the n irreducible representations must be given by $g \mapsto \zeta_n^k$ where ζ_n is a primitive n th root of unity and k runs over the integers $0, \dots, n - 1$.

Finally, the fundamental theorem of finite abelian groups tells us that any abelian group G can be written as a product of cyclic groups. The irreducible representations of G are then simply the products of irreducible representations of factors of G .

There is a result analogous to proposition 24 in the case of a representation to an algebraically closed field of nonzero characteristic. Our proof directly and shamelessly follows that given in Alperin [1].

Proposition 25 *If L is an algebraically closed field of nonzero characteristic p , then the number of irreducible representations of G over L is equal to the number of conjugacy classes whose order is relatively prime to p . (The order of a conjugacy class is defined to be the order of an element in the conjugacy class.)*

Proof Since $L[G]$ is not semisimple, it is not necessarily the case that we can write $L[G]$ as a direct sum of matrix rings. However, $L[G]/\text{rad } L[G]$ is semisimple, so it is a direct sum of matrix rings over division rings, and the fact that L is algebraically closed implies that the division rings all equal L . Any simple $L[G]$ -module is a quotient of $L[G]$ and is annihilated by the radical of $L[G]$, so can be considered to be a simple $L[G]/\text{rad } L[G]$ -module. Now since $L[G]/\text{rad } L[G]$ is semisimple, it is a direct sum of simple $L[G]/\text{rad } L[G]$ -modules, and as in the proof of proposition 24 the number of simple $L[G]/\text{rad } L[G]$ -modules is equal to the number of matrix rings appearing in the direct sum decomposition of $L[G]/\text{rad } L[G]$.

We define now a sort of commutator subspace of an L -algebra R : let $[R]$ be the L -vector subspace of R generated by all elements of the form $rs - sr$ for $r, s \in R$. (Note that $[R]$ does not purport to be an ideal, or even a subring, of R . It is only a vector subspace.) For a matrix ring $M_n(L)$, note that $\text{Tr}(AB - BA) = 0$ for any matrices A, B . Further, if E_{ij} has a 1 in the (i, j) -place and zeros elsewhere, then

$$E_{ij}E_{ji} - E_{ji}E_{ij} = E_{ii} - E_{jj}$$

and

$$E_{ij}E_{jj} - E_{jj}E_{ij} = E_{ij}$$

for $i \neq j$. But the $E_{ii} - E_{jj}$ and E_{ij} with $i \neq j$ span the space of matrices with trace 0. Thus $[M_n(L)]$ is the space of traceless matrices, and $M_n(L)/[M_n(L)]$ has dimension 1. Since we have written $L[G]/\text{rad } L[G]$ as a direct sum of such

matrix rings, one for each irreducible representation of G over L , it follows that the dimension of $(L[G]/\text{rad } L[G])/[L[G]/\text{rad } L[G]]$ is exactly the number of irreducible representations. (This uses the easy-to-check fact that $[R \oplus S] = [R] \oplus [S]$.) Next, we want to count that dimension in a different way.

Put

$$T = [L[G]]$$

and

$$S = T + \text{rad } L[G].$$

It is easy to verify that

$$S/\text{rad } L[G] = [L[G]/\text{rad } L[G]], \quad (*)$$

so that the dimension of $(L[G]/\text{rad } L[G])/[L[G]/\text{rad } L[G]]$ equals the dimension of $L[G]/S$.

Let S_0 be the set of elements x of $L[G]$ such that $x^{p^i} \in T$ for some natural number i . We wish to show that $S_0 = S$.

First, note that for $x, y \in L[G]$, $(x + y)^p$ is equal to $x^p + y^p$ plus $2^p - 2$ additional terms: the products of the distinct mixed strings of x and y of length p . The set of these strings can be partitioned into equivalence classes of size p , where each equivalence class consists of a string and its cyclic rearrangements. Consider one such string $a_1 a_2 \cdots a_p$ and a cyclic rearrangement $a_k a_{k+1} \cdots a_{k-1}$. We have

$$a_k a_{k+1} \cdots a_{k-1} = a_1 a_2 \cdots a_p + (a_k \cdots a_p)(a_1 \cdots a_{k-1}) - (a_1 \cdots a_{k-1})(a_k \cdots a_p)$$

and so

$$a_k a_{k+1} \cdots a_{k-1} = a_1 a_2 \cdots a_p + \text{an element of } T.$$

As a result, the sum of all the elements of an equivalence class is equal to

$$p(a_1 a_2 \cdots a_p) + \text{an element of } T = \text{an element of } T$$

since we are working in characteristic p . Thus the difference $(x + y)^p - x^p - y^p \in T$ for any $x, y \in L[G]$.

For any $x, y \in L[G]$ we already know

$$(xy - yx)^p - (xy)^p - (-yx)^p \in T,$$

and since

$$(xy)^p + (-yx)^p = x((yx)^{p-1}y) - ((yx)^{p-1}y)x,$$

we see that $(xy - yx)^p \in T$. Using the result of the preceding paragraph, it follows that $T^p \subset T$, i.e. $t^p \in T$ for any $t \in T$. An induction argument allows us to conclude that for any $x, y \in L[G]$,

$$(x + y)^{p^i} - x^{p^i} - y^{p^i} \in T.$$

In particular, if $x, y \in S_0$, then there is some i such that both $x^{p^i}, y^{p^i} \in T$. It follows that $(x+y)^{p^i} \in T$, so $x+y \in S_0$, and S_0 is closed under addition. Since $L[G]$ is Artinian, every element of $\text{rad } L[G]$ is nilpotent, and thus $\text{rad } L[G] \subset S_0$. Trivially, $T \subset S_0$, and so

$$S = T + \text{rad } L[G] \subset S_0.$$

To prove the reverse inclusion, suppose $x^{p^i} \in T$. We wish to show that $x \in T + \text{rad } L[G] = S$, i.e. (using (*), above) that

$$x + \text{rad } L[G] \in (T + \text{rad } L[G]) / \text{rad } L[G] = S / \text{rad } L[G] = [L[G] / \text{rad } L[G]].$$

But we know that $L[G] / \text{rad } L[G]$ is a direct sum of matrix rings, and therefore $x + \text{rad } L[G] \in [L[G] / \text{rad } L[G]]$ if and only if each component of $x + \text{rad } L[G]$ as a direct sum of matrices has trace 0. Since we're working in characteristic p , and since trace is equal to the sum of the eigenvalues,

$$\text{Tr}(M)^{p^i} = (\lambda_1 + \cdots + \lambda_k)^{p^i} = \lambda_1^{p^i} + \cdots + \lambda_k^{p^i} = \text{Tr}(M^{p^i})$$

for any square matrix M over L . But our assumption that $x^{p^i} \in T$ puts

$$x^{p^i} + \text{rad } L[G] = (x + \text{rad } L[G])^{p^i} \in [L[G] / \text{rad } L[G]].$$

Since the p^i th powers of the components of $x + \text{rad } L[G]$ have trace 0, it follows that the components themselves have trace 0, and the reverse inclusion follows. We have obtained the fact that $S = S_0$.

Let x_1, \dots, x_s be representatives of the conjugacy classes of G of order relatively prime to p , and let x_{s+1}, \dots, x_r be representatives of the remaining conjugacy classes. To prove the result, we will show that $x_1 + S, \dots, x_s + S$ form a basis for the vector space $L[G]/S$.

First of all, we will prove that $x_1 + T, \dots, x_r + T$ form a basis for $L[G]/T$. For any $g \in G$, there is an x_i and some h such that $g = hx_ih^{-1}$, and so

$$g - x_i = (hx_i)h^{-1} - h^{-1}(hx_i) \in T.$$

Thus $g + T = x_i + T$ and, since the g span $L[G]$, the $x_i + T$ span $L[G]/T$. To obtain linear independence, define the functional ϕ_i on $L[G]$ to have value 1 on each conjugate of x_i and 0 on the other elements of G , and extend by linearity to the remainder of G . We find that for $g, h \in G$,

$$\phi_i(gh - hg) = \phi_i(g(hg)g^{-1} - hg) = 0$$

and therefore $\phi_i = 0$ on T . Suppose it happens that

$$\sum_{i=1}^r \alpha_i(x_i + T) = \left(\sum_{i=1}^r \alpha_i x_i \right) + T = 0.$$

Then $\sum_{i=1}^r \alpha_i x_i \in T$, so that for each i ,

$$0 = \phi_i\left(\sum_{i=1}^r \alpha_i x_i\right) = \alpha_i,$$

which proves that the $x_i + T$ are linearly independent.

Finally, let $g \in G$ be of order $p^i m$ with m and p relatively prime. Pick integers a, b such that $ap^i + bm = 1$. Setting $u = g^{bm}$ and $x = g^{ap^i}$, we get $g = ux = xu$ with u of order p^i and x of order dividing m (and thus of order relatively prime to p). It follows that

$$g^{p^i} = x^{p^i} \quad \text{and so} \quad (g - x)^{p^i} = 0$$

since g, x commute. Thus $(g - x)^{p^i} \in T$, so $g - x \in S$, and so $g \in x + S$. Since x has order relatively prime to p , $x - x_j \in T \subset S$ for some $j \leq s$, and therefore $g \in x_j + S$. Thus $x_1 + S, \dots, x_s + S$ span $L[G]/S$.

To obtain linear independence over L , suppose

$$\alpha_1 x_1 + \dots + \alpha_s x_s \in S.$$

We then know that for some i ,

$$(\alpha_1 x_1 + \dots + \alpha_s x_s)^{p^i} \in T.$$

But we already know that $(x + y)^{p^i} - x^{p^i} - y^{p^i} \in T$ for any $x, y \in L[G]$, and repeated application of this tells us that

$$\alpha_1^{p^i} x_1^{p^i} + \dots + \alpha_s^{p^i} x_s^{p^i} \in T.$$

If we knew that each of the $x_j^{p^i}$ lie in a different conjugacy class, we could conclude by the linear independence of $x_1 + T, \dots, x_r + T$ that the $\alpha_j^{p^i}$, and thus the α_j , are all 0, and the linear independence of $x_1 + S, \dots, x_s + S$ would be established.

To that end, let c be the largest integer relatively prime to p which divides $\#G$, and pick d such that $c|(dp^i - 1)$. Since each x_i has order prime to p , the order of x_i divides c , and therefore $(x_i^{p^i})^d = x_i$. Consequently, if we had $hx_i^{p^i}h^{-1} = x_j^{p^i}$, we would also get $hx_i h^{-1} = x_j$, which is not the case. As a result, our proof, at long last, is done. ♠

Whew!

Example (abelian groups) Let G be a cyclic group of order $p^r m$ where m and p are relatively prime. Then there are exactly m elements (and thus conjugacy classes of elements, since G is abelian) with order prime to p : the elements in the subgroup of order m . Thus there are m irreducible representations of G to an algebraically closed field of characteristic p . A generator g of G must map

to a root of $x^{p^r m} - 1 = (x^m - 1)^{p^r} = 0$, i.e. to an m th root of unity, and sending g in turn to each of the m m th roots of unity yields all the representations. Once again the representations of a general finite abelian group are the products of the representations of its cyclic factors.

Example (p -groups) Let G be a group of order p^r . Then there is exactly one element—the identity—with order prime to p , and so there is exactly one irreducible representation—the trivial representation. This can also be proved relatively straightforwardly by induction on r , using the fact that a p -group has nontrivial center. However, this example also yields a perfect demonstration of why representation theory mod p is not so trivial: even though the trivial representation is the only irreducible representation, there nevertheless exist fairly nontrivial reducible representations. An example suggests itself immediately: the *regular* representation, the $K[G]$ -module $K[G]$.

The theorem, and these examples, demonstrate a not entirely shallow philosophy of representations mod p : working mod p , by taking away the p th roots of unity, in some sense kills off any interesting portion of a representation which falls on the " p -part" of a group, whatever that may happen to mean.

3.2 A trace of character theory

Let V be a $K[G]$ -module. Any element $g \in G$ acts as a K -linear transformation on V , and therefore we may define a function $\chi : G \rightarrow K$ where $\chi(g)$ equals the trace of the linear transformation that g performs on V . χ is called the character of the representation V . Note that if $g, h \in G$, and G, H are the associated linear transformations, then

$$\chi(hgh^{-1}) = \text{Tr}(HGH^{-1}) = \text{Tr}(GH^{-1}H) = \chi(g),$$

and so χ is constant along any conjugacy class. (In general, a function which is constant along a conjugacy class is known as a class function.)

Lemma 26 *Let V be a representation of G over $L \subset \mathbb{C}$ with character χ . Let V^G be the subspace of V which is fixed by the action of G . Then*

$$\dim V^G = \frac{1}{\#G} \sum_{g \in G} \chi(g).$$

Proof If we let p be the map which takes

$$x \mapsto \frac{1}{\#G} \sum_{g \in G} gx,$$

then p is a linear transformation from $V \rightarrow V^G$ which is the identity on V^G . Since V is semisimple, write $V = V^G \oplus W$, so that p is 0 on W . Then

$$\frac{1}{\#G} \sum_{g \in G} \chi(g) = \text{Tr } p = \text{Tr } p|_{V^G} + \text{Tr } p|_W = \text{Tr}(1_{V^G}) + 0 = \dim V^G$$

as desired. ♠

Let us briefly investigate the characters of representations over \mathbb{C} .

We have several natural ways in which to build new representations from ones we already have. For example, if V is a $\mathbb{C}[G]$ -module, we can turn the dual space $V^* = \text{Hom}(V, \mathbb{C})$ into a $\mathbb{C}[G]$ -module by asking that for $f \in V^*$,

$$f(v) = \langle f, v \rangle = \langle gf, gv \rangle,$$

i.e. by setting

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

and extending the action to $\mathbb{C}[G]$ by linearity. Let us attempt to find χ^* , the character of V^* , in terms of the character χ of V . Consider V under the action of the cyclic group $\langle g \rangle \in G$. Since all the representations of $\langle g \rangle$ are 1-dimensional, V under $\langle g \rangle$ can be written as a direct sum of 1-dimensional submodules. Therefore, we find a basis e_1, \dots, e_n of V so that the matrix of the action of $\langle g \rangle$ with respect to that basis is diagonal, say with $g(e_i) = \lambda_i e_i$. Each of the λ_i is a root of unity.

Let e_1^*, \dots, e_n^* be the dual basis of V^* , whereby $e_i^*(e_j) = \delta_{ij}$ (the Kronecker delta). Then

$$(ge_i^*)(e_j) = e_i^*(g^{-1}e_j) = e_i^*(\lambda_j^{-1}e_j) = \lambda_j^{-1}\delta_{ij}$$

and therefore

$$ge_i^* = \lambda_i^{-1}e_i^*.$$

As a result, we have

$$\chi(g) = \sum_i \lambda_i$$

and

$$\chi^*(g) = \sum_i \lambda_i^{-1} = \sum_i \overline{\lambda_i} = \overline{\chi(g)}.$$

(As a corollary to the argument, notice that $\chi(g^{-1}) = \overline{\chi(g)}$.)

Similarly, if V and W are representations of G , we can let $\mathbb{C}[G]$ act on: $V \oplus W$ via $g(v, w) = (gv, gw)$ and extended linearly, whence $\chi_{V \oplus W} = \chi_V + \chi_W$, and on $V \otimes W$ via $g(v \otimes w) = (gv \otimes gw)$. One can check that the latter action is well-defined, and that the resulting character is $\chi_{V \otimes W} = \chi_V \chi_W$.

Let $T \in \text{Hom}_{\mathbb{C}}(V, W)$ for representations V, W of G . We define

$$(gT)(v) = g(T(g^{-1}v)),$$

so that the action of g pulls back on V and pushes forward on W . To see that this indeed is an action, observe that

$$(h(gT))(v) = h((gT)(h^{-1}v)) = hg(T(g^{-1}h^{-1}v)) = ((hg)T)(v).$$

We wish to show that as $\mathbb{C}[G]$ -modules,

$$\text{Hom}_{\mathbb{C}}(V, W) \cong V^* \otimes W.$$

We get a \mathbb{C} -linear map

$$\phi : V^* \otimes W \rightarrow \text{Hom}_{\mathbb{C}}(V, W)$$

by setting

$$\phi(f \otimes w)(v) = f(v)w$$

and extending linearly, and it is not difficult to see that this map is surjective. Since the domain and the range evidently have the same dimension, the map is an isomorphism of vector spaces. To see that this is indeed a $\mathbb{C}[G]$ -module homomorphism, witness that

$$\phi(g(f \otimes w))(v) = \phi(gf \otimes gw)(v) = gf(v)(gw) = f(g^{-1}v)gw = g(\phi(f \otimes w))(v),$$

which proves the isomorphism.

In particular, we have $\chi = \overline{\chi_V} \chi_W$, where χ is the character of the representation we have just defined on $\text{Hom}_{\mathbb{C}}(V, W)$. Therefore, we get:

Proposition 27 *Let V, W be representations of G which characters χ_V, χ_W . Then*

$$\dim \text{Hom}_{\mathbb{C}[G]}(V, W) = \frac{1}{\#G} \sum_{g \in G} \overline{\chi_V(g)} \chi_W(g).$$

Proof Observe that for $T \in \text{Hom}_{\mathbb{C}}(V, W)$,

$$(gT)(v) = T(gv) \iff g(T(g^{-1}v)) = Tv,$$

i.e.

$$T \in \text{Hom}_{\mathbb{C}[G]}(V, W) \iff T \in \text{Hom}_{\mathbb{C}}^G(V, W),$$

and the result follows by lemma 26. ♠

Corollary 1 *We can define an inner product*

$$\langle \chi, \psi \rangle = \frac{1}{\#G} \sum_{g \in G} \overline{\chi(g)} \psi(g)$$

on the set of characters of representations of G . Then if χ and ψ are characters of distinct irreducible representations, we have

$$\langle \chi, \chi \rangle = 1 \quad \text{and} \quad \langle \chi, \psi \rangle = 0.$$

Proof Let χ and ψ be the characters of the representations V and W respectively. Recalling that Schur's lemma tells us that $\text{Hom}_{\mathbb{C}[G]}(V, W) = 0$ and $\text{Hom}_{\mathbb{C}[G]}(V, V) \cong \mathbb{C}$, the result follows. ♠

Corollary 2 *The characters of the irreducible representations over \mathbb{C} of a group G are linearly independent, and are a basis of the space of class functions on G .*

Proof The dimension of the space of class functions on G is the number of conjugacy classes of G , which is equal to the number of irreducible representations of G . If the characters of these representations are linearly independent, they therefore form a basis of the space of class functions. If χ_1, \dots, χ_k are the irreducible characters, then $\langle \alpha_1\chi_1 + \dots + \alpha_k\chi_k, \chi_i \rangle = \alpha_i$, and therefore the characters must be linearly independent. ♠

Corollary 3 *Two representations over \mathbb{C} are isomorphic if and only if their characters are equal.*

Proof If two representations have the same character, then they must be written in the same way as a sum of the irreducible characters, and so the representations are written in the same way as a direct sum of irreducible representations. ♠

We define the space of (virtual) characters of G over \mathbb{C} , $r_{\mathbb{C}}(G)$, to be the span over \mathbb{Z} of the χ_i . This is effectively the space of characters of representations of G , since every representation is a direct sum of the irreducible representations. However, we are allowing in $r_{\mathbb{C}}(G)$ things like $-\chi_i$, which is why we add the tag word virtual. Note that the space of class functions on G is very different from the set of virtual characters of G .

Finally, if $\chi = \alpha_1\chi_1 + \dots + \alpha_k\chi_k$, then $\langle \chi, \chi \rangle = \alpha_1^2 + \dots + \alpha_k^2$. In particular if χ is a character and $\langle \chi, \chi \rangle = 1$, then χ must be irreducible. Similarly, if $\langle \chi, \chi \rangle = 2$, then χ must be the sum of two distinct irreducible characters.

Example (The symmetric group S_4) We have seen already that S_4 has 5 irreducible representations: two of degree 1 (the identity and sign representations), one of degree 2, and two of degree 3. The characters of the identity and sign representations are evidently:

σ	e	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_{Id}	1	1	1	1	1
χ_{sgn}	1	-1	1	-1	1

We can easily exhibit a representation of degree 4 of S_4 : let $V = \mathbb{C}e_1 + \dots + \mathbb{C}e_4$, and let S_4 act on V by sending $\sigma e_i = e_{\sigma(i)}$.

The character χ of V can be found by noting that the matrix for σ over the basis e_1, \dots, e_4 has a 1 in the $i, \sigma(i)$ -places and zeros elsewhere. Therefore, $\chi(\sigma)$ is exactly the number of elements left fixed by σ , and we get:

σ	e	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ	4	2	1	0	0

Observe that $\langle \chi, \chi \rangle = (4^2 \cdot 1 + 2^2 \cdot 6 + 1^2 \cdot 8 + 0^2 \cdot 6 + 0^2 \cdot 3)/24 = 2$, so χ is the sum of two irreducible representations. But $\langle \chi, \chi_{Id} \rangle = (4 \cdot 1 + 2 \cdot 6 + 1 \cdot 8)/24 = 1$, and thus χ contains a copy of the identity character. We conclude that $\chi - \chi_{Id} = \chi_3$ is one of the irreducible characters of a degree 3 representation V . (The degree of a representation is equal to the character of that representation evaluated at

1, since the matrix is the identity matrix of the appropriate dimension.) One quickly verifies that $\chi_3\chi_{sgn}$ is another irreducible character for S_4 . It remains to find the character χ_2 of the representation of degree 2. But the orthogonality relations are enough to completely determine the last character once we know all the others, and we therefore have been able to find the entire *character table* for S_4 :

σ	e	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_{Id}	1	1	1	1	1
χ_{sgn}	1	-1	1	-1	1
χ_2	2	0	-1	0	2
χ_3	3	1	0	-1	-1
χ'_3	3	-1	0	1	-1

The computation of χ_2 can be aided somewhat by noting that $\chi_2((12))$ and $\chi_2((1234))$ must be zero, or else tensoring with the sign representation would get a new irreducible representation.

3.3 The non-algebraically closed case

The results we have just obtained are valid in the case of an algebraically closed field. It is natural to ask what analogous results hold in case our representations are over a smaller field. In particular, if L is a subfield of \mathbb{C} and V is an irreducible representation of V over L , we can obtain a representation over \mathbb{C} by extension of scalars via the tensor product to the $\mathbb{C}[G]$ -module $V_C = V \otimes_L \mathbb{C}$. We would like to know whether there are conditions we can place on L so which ensure that V_C is also irreducible.

Effectively, the question is whether or not L is in some sense large enough that the simple $\mathbb{C}[G]$ modules can be "realized" over L . The two nontrivial representations of the cyclic group $Z_3 = \{e, g, g^2\}$, for example, have elements act on \mathbb{C} as nontrivial cube roots of unity and therefore do not exist as representations over \mathbb{R} . Instead, as a direct sum of submodules

$$\mathbb{R}[Z_3] = \mathbb{R}(e + g + g^2) + \mathbb{R}_2,$$

where \mathbb{R}_2 is the submodule of $\mathbb{R}[Z_3]$ consisting of $\alpha_0e + \alpha_1g + \alpha_2g^2$. \mathbb{R}_2 is therefore isomorphic to \mathbb{R}^2 with G -action given by $g(a, b) = (-a - b, a)$, which one easily verifies is simple as the cube roots of unity are not in \mathbb{R} . However, $\mathbb{R}_2 \otimes \mathbb{C}$ does break up into the two remaining irreducible \mathbb{C} -representations of Z_3 .

Let V and W be two irreducible representations over $L \subset \mathbb{C}$, let their characters be χ_V and χ_W , and let V_C and W_C be $V \otimes \mathbb{C}$ and $W \otimes \mathbb{C}$ respectively. The characters of V_C and W_C are equal to χ_V and χ_W again: if v_1, \dots, v_k is a basis for V over L then $v_1 \otimes 1, \dots, v_k \otimes 1$ is a basis for V_C , and the matrix of any $g \in G$ is the same with respect to both bases.

It follows from lemma 26 that

$$\dim_L \text{Hom}^G(V, W) = \dim_{\mathbb{C}} \text{Hom}^G(V_C, W_C) = \langle \chi_V, \chi_W \rangle.$$

By Schur's Lemma, if V and W are not isomorphic, then $\dim_L \text{Hom}^G(V, W) = 0$, and we obtain several immediate conclusions. First, the characters of irreducible representations over L are indeed orthogonal. Second, it is again true over L that two representations are isomorphic if and only if their characters are equal. Last, if we look at V_C and W_C as a sum of irreducible \mathbb{C} -representations, the representations appearing in the decomposition of V_C must all be different from those appearing in W_C —otherwise, the inner product of their characters would not be 0. If the simple $L[G]$ -module V appears k times as a direct summand of $L[G]$ in a Krull-Schmidt decomposition, and if V_C contains the simple $\mathbb{C}[G]$ -module M of dimension n exactly m , then M appears precisely km times as a direct summand in $\mathbb{C}[G]$. Therefore $n = km$, and in particular both k and m divide n .

It is certainly not necessarily the case that $\langle \chi_V, \chi_V \rangle = 1$. One can verify, for example, that for the representation \mathbb{R}_2 described in the example above, the inner product of its character with itself is 2: $\mathbb{R}_2 \otimes \mathbb{C}$ decomposes as a sum of two distinct irreducible representations.

Proposition 28 *If χ is the character of a representation of G over \mathbb{C} , then χ is the character of a representation of G over L if and only if it is a virtual character of G over L .*

Proof Suppose that χ is a virtual character of G over L , i.e. that if V_1, \dots, V_k and χ_1, \dots, χ_k are the irreducible representations and characters, respectively, over L , then there are integers n_i such that

$$\chi = \sum_{i=1}^k n_i \chi_i.$$

Applying the inner product, by orthogonality of characters in L we get

$$\langle \chi, \chi_i \rangle = n_i.$$

But since χ and χ_i are characters of actual representations over \mathbb{C} , their inner product must in fact be a nonnegative integer. Then the representation

$$n_1 V_1 \oplus \dots \oplus n_k V_k$$

has the desired character. Notice that that representation must be the unique representation whose tensor product with \mathbb{C} has character χ . ♠

If H is a subgroup of G and V is a representation of H over L , there is a process which returns a representation $\text{Ind}_H^G V$ called an induced representation. I do not wish to discuss induced representations in this paper, but I would like to cite a pair of results.

1. The characters of the induced representations $\text{Ind}_H^G V$ over L and $\text{Ind}_H^G V_C$ over \mathbb{C} are equal.

2. (Brauer) Every character of G over \mathbb{C} can be written as a \mathbb{Z} -linear combination of characters of representations induced from representations of degree 1.

Let m be the least common multiple of the orders of the elements of G , and let L be a field of characteristic 0 containing all of the m th roots of unity (we call such a field sufficiently large). Since L contains the necessary roots of unity, any 1-dimensional representation of a subgroup H over \mathbb{C} does give rise to a 1-dimensional representation of H over L with the same character. Thus every character of G induced from a character of degree 1 over \mathbb{C} is indeed a character over L as well, and by the result of Brauer it follows that every character of G over \mathbb{C} is indeed a \mathbb{Z} -linear combination of characters of G over L , i.e. is a virtual character over L . By proposition 28, it follows that every character of G over \mathbb{C} is indeed a character of a representation of G over L . In consequence, one can verify that L *does* have the property that if V is an irreducible representation of G over L , then $V \otimes_L \mathbb{C}$ is an irreducible representation of G over \mathbb{C} .

4 Discrete Valuation Rings

Henceforth, we will let K be a field of characteristic 0 carrying a discrete valuation, that is, with an associated surjective homomorphism

$$v : K^* \rightarrow \mathbb{Z}$$

from the multiplicative group of K to the additive group of integers such that $v(x+y) \geq \min(v(x), v(y))$ for all $x, y \in K$. (We extend v to the whole of K by putting $v(0) = +\infty$.) A prototypical example to bear in mind is has $K = \mathbb{Q}$, p a prime, with $v_p(x) = \alpha$ when $x = p^{\alpha} \frac{r}{s}$ with $\gcd(rs, p) = 1$.

Observe that the set $A = \{x \in K \mid v(x) \geq 0\}$ is a subring of K called the valuation ring, and that we must have $v(1) = 0$, forcing $1 \in A$.

Proposition 29 *The nonzero ideals of A are all of the form*

$$I_n = \{x \in K \mid v(x) \geq n\}$$

for positive integers n .

Proof Let I be any nonzero ideal of A , let $n = \inf\{v(x) \mid x \in I\}$, and in particular suppose $y \in I$ has $v(y) = n$. Suppose $v(z) \geq n$. Then $v(zy^{-1}) = v(z) - v(y) \geq 0$, so $zy^{-1} \in A$, and since I is an ideal we have $zy^{-1}y = z \in I$. Therefore, $I = I_n$. ♠

Corollary *A is a principal ideal domain.*

Proof Since A is a subring of K and A contains 1, A is a domain. Let x_n be any element of I_n such that $v(x_n) = n$. (Such an element exists, since we assumed v was surjective.) Then the principal ideal generated by x_n is contained in I_n . But the argument in the preceding proof shows that the ideal generated by x_n contains I_n , so that in fact I_n is generated by x_n . ♠

We therefore know that A is a local ring, that is, it is a commutative ring with a single maximal ideal $\mathfrak{m} = I_1$. Every ideal $I_n = \mathfrak{m}^n$ is a power of that maximal ideal. We obtain a field $k = A/\mathfrak{m}$ called the residue field of A . Also, it is evident that A is Noetherian.

Example Returning to $K = \mathbb{Q}$ with v_p as described above, we get

$$A = \{r/s \mid (r, s) = 1 \text{ and } p \nmid s\},$$

$$\mathfrak{m} = \{r/s \mid (r, s) = 1 \text{ and } p \mid r\}.$$

Then $k = A/\mathfrak{m} \cong \mathbb{F}_p$ via the map

$$\frac{r}{s} \mapsto rs^{-1} \pmod{p}.$$

We can place the topology of a metric space on K by defining $d(x, y) = e^{-v(x-y)}$ for $x \neq y$ and $d(x, y) = 0$ for $x = y$. To check symmetry, notice that $v(-1) = -v(1) = 0$, so $v(x-y) = v(-1) + v(y-x) = v(y-x)$. To verify the triangle inequality, notice that $v(x-z) \geq \inf(v(x-y), v(y-z))$ so that

$$e^{-v(x-z)} \leq \sup(e^{-v(x-y)}, e^{-v(y-z)}),$$

and the inequality follows.

We may also define a new ring A' , the inverse limit of the A/\mathfrak{m}^n , the set of sequences

$$(x_1 + \mathfrak{m}, x_2 + \mathfrak{m}^2, \dots)$$

with $x_i + \mathfrak{m}^i \in A/\mathfrak{m}^i$ and

$$\phi_{ij}(x_j + \mathfrak{m}^j) = x_i + \mathfrak{m}^i$$

for all $i \leq j$, where ϕ_{ij} is the natural map $A/\mathfrak{m}^j \rightarrow A/\mathfrak{m}^i$. (In other words, we require $x_j - x_i \in \mathfrak{m}^i$.)

We obtain an map φ from A into A' by setting $\varphi(a) = (a + \mathfrak{m}, a + \mathfrak{m}^2, \dots)$. The kernel of φ is equal to the intersection of all of the \mathfrak{m}^i . However, that intersection is 0, since $x \in \mathfrak{m}^i$ if and only if $v(x) \geq i$, and therefore if $x \neq 0$ there exists i such that $x \notin \mathfrak{m}^i$. Consequently, φ is an injection.

Example We can form the inverse limit \mathbb{Z}_p of the groups $\mathbb{Z}/p^n\mathbb{Z}$. In this case the map φ is not an isomorphism, because the element

$$(1 + p\mathbb{Z}, 1 + p + p^2\mathbb{Z}, 1 + p + p^2 + p^3\mathbb{Z}, \dots) \in \mathbb{Z}_p$$

is not in the image of φ .

Proposition 30 *The metric space (K, d) is complete if and only if φ is an isomorphism.*

Proof Suppose (K, d) is complete, and let $(x_1 + \mathfrak{m}, x_2 + \mathfrak{m}^2, \dots)$ be an element of A' . Since $x_i - x_n \in \mathfrak{m}^i$ for $n \geq i$, we see that the sequence $\{x_i\}$ in K is Cauchy, and therefore has a limit x . Then $v(x - x_i) \rightarrow \infty$ as $i \rightarrow \infty$ and $v(x) \geq \inf(v(x - x_i), v(x_i))$. Therefore $v(x) \geq 0$, and $x \in A$. Moreover,

$$d(x_i, x) \leq \sup(d(x_i, x_n), d(x_n, x)) \leq e^{-i}$$

for n sufficiently large, and so $x - x_i \in \mathfrak{m}^i$. As a result, $\varphi(x) = (x_1 + \mathfrak{m}, x_2 + \mathfrak{m}^2, \dots)$.

Conversely, suppose $\{x_n\}$ is a Cauchy sequence in K . Noting that

$$v(x_j) \geq \inf(v(x_j - x_i), v(x_i)),$$

the set of values of v on $\{x_n\}$ must be bounded below, and therefore there exists nonzero $k \in K$ such that $\{kx_n\}$ is a sequence in A , still Cauchy. If the sequence $\{kx_n\}$ converges to x in K , the sequence $\{x_n\}$ will converge to $k^{-1}x$, and so we only need show that $\{kx_n\}$ converges. So that we don't have to write ks everywhere, we will suppose without loss of generality that $\{x_n\}$ is actually itself a sequence in A . It suffices to prove that a subsequence of $\{x_n\}$ converges. Inductively choose $y_k = x_{n_k}$ with n_k sufficiently large that $n_k > n_{k-1}$ and $d(x_{n_k}, x_j) \leq e^{-k}$ for $j \geq n_k$. Then

$$d(y_i, y_j) \leq e^{-i} \text{ for } j \geq i,$$

so $v(y_i - y_j) \geq i$ and therefore $y_i - y_j \in \mathfrak{m}^i$. Consequently

$$(y_1 + \mathfrak{m}, y_2 + \mathfrak{m}^2, \dots) \in A',$$

and since we have assumed φ to be surjective, suppose $\varphi(y) = (y_1 + \mathfrak{m}, y_2 + \mathfrak{m}^2, \dots)$. Then $y_i - y \in \mathfrak{m}^i$, so $\{y_i\} \rightarrow y$ and the proof is done. ♠

Throughout the remainder of this paper, the letters K , A , and k will denote the objects described in this section: K a complete field with a discrete valuation, A its valuation ring, and k the residue field of A . We shall assume that k has nonzero characteristic p . We will frequently take K to be sufficiently large. Unfortunately, in this paper we do not have space to prove the existence of such a structure. We refer the reader to Burrow [3] or almost any algebraic number theory text for such a proof.

5 Projective modules

Let R be a ring, and let F be a left R -module. F is said to be free on the set $\{x_\alpha\}$ if for every R -module M and every function $f : \{x_\alpha\} \rightarrow M$, there is a *unique* homomorphism $\phi_f : F \rightarrow M$ such that $\phi_f(x_\alpha) = f(x_\alpha)$. The reader should verify that a free R -module on a finite set of cardinality k is isomorphic to R^k .

An R -module P is said to be projective if P is a direct summand of a free module, i.e. if there exists an R -module Q such that $P \oplus Q$ is a free R -module.

Every free module is projective, but not vice-versa: one projective module which is not free, for example, is \mathbb{Z} regarded as a $\mathbb{Z} \oplus \mathbb{Z}$ -module

Observe, as an example, that if L is a field, then every vector space over L is projective: every vector space has a basis, and becomes a free L -module on that basis.

Proposition 31 *The following are equivalent:*

1. P is projective
2. If $P \xrightarrow{g'} E'$ is an R -module homomorphism and $E \xrightarrow{f} E'$ is a surjective R -module homomorphism, then there exists an R -module homomorphism $P \xrightarrow{g} E$ such that $g' = f \circ g$. That is, the following diagram can be completed such that it is commutative:

$$\begin{array}{ccc} & & P \\ & \nearrow \exists g & \downarrow g' \\ E & \xrightarrow{f} & E' \end{array}$$

3. If $B \xrightarrow{f} C$ is a surjection, then so is $\text{Hom}_R(P, B) \xrightarrow{f^*} \text{Hom}_R(P, C)$.
4. Any short exact sequence $0 \rightarrow B \xrightarrow{i} C \xrightarrow{\alpha} P \rightarrow 0$ splits, i.e. there is a map β from P into C such that $\alpha \circ \beta$ is the identity on P . (The reader should verify that it follows that $C = i(B) \oplus \beta(P)$).

Proof To show (1) \implies (2), suppose $F = P \oplus Q$ is free, and let $F \xrightarrow{p} E'$ be the projection along that sum. Then $g' \circ p$ is a map from F to E' . Letting $\{x_\alpha\}$ be a set on which F is free, by the surjectivity of f we can pick $y_\alpha \in E$ such that $f(y_\alpha) = g' \circ p(x_\alpha)$. Since F is free, we obtain a map h from F to E such that $h(x_\alpha) = y_\alpha$ for all α . Then $(h \circ p)(x_\alpha) = (g' \circ p)(x_\alpha)$, and therefore by the uniqueness property in the definition of free modules, $h \circ p = g' \circ p$, i.e. the following diagram commutes:

$$\begin{array}{ccc} & & F \\ & \nearrow h & \downarrow g' \circ p \\ E & \xrightarrow{f} & E' \end{array}$$

But $g' \circ p$ restricted to P is g' , so letting $g = h|_P$, we get the desired map.

(2) \implies (3) We begin with a surjection $f : B \twoheadrightarrow C$. We wish to show that the induced map $f^* : \text{Hom}_R(P, B) \rightarrow \text{Hom}_R(P, C)$ with $f^*(\phi) = f \circ \phi$ is surjective. Suppose we have $g' \in \text{Hom}_R(P, C)$. By the property (2), there is a map g which completes the diagram

$$\begin{array}{ccc}
 & & P \\
 & \nearrow \exists g & \downarrow g' \\
 B & \xrightarrow{f} & C
 \end{array}$$

and then $f^*(g) = g'$.

(3) \implies (4) We have a surjection $C @> \alpha >> P$, and since by (3) the map $\alpha^* : \text{Hom}_R(P, C) \rightarrow \text{Hom}_R(P, P)$ is surjective, there is a map $\beta \in \text{Hom}_R(P, C)$ such that $\alpha \circ \beta = 1_P$. This map β is the desired splitting map.

(4) \implies (1) Writing P as a quotient of a free module F (we know we can do this for any module), we get a surjection from F to P with kernel Q . Property (4) shows that $F = P \oplus Q$. \spadesuit

Corollary *A projective R -module P is finitely generated if and only if it can be written as a direct summand of a finitely generated free R -module.*

Proof P can be generated by k elements if and only if it can be written as a quotient of R^k , which by (4) above is the case if and only if P is a direct summand of R^k . \spadesuit

We can classify the left ideals of R which are direct summands in R as follows:

Proposition 32 *If $\mathfrak{a} \subset R$ is a left ideal, then \mathfrak{a} is a direct summand in R if and only if there exists $e \in R$ such that $e^2 = e$ and $Re = \mathfrak{a}$.*

Proof If \mathfrak{b} is an ideal such that $R = \mathfrak{a} \oplus \mathfrak{b}$ as R -modules, we can write $1 = e + f$ uniquely with $e \in \mathfrak{a}$ and $f \in \mathfrak{b}$. Then $e = e^2 + ef$ with $e^2 \in \mathfrak{a}$ and $ef \in \mathfrak{b}$. But $e = e + 0$ as well, so by uniqueness of the decomposition we get $e^2 = e$ (and $ef = 0$). Clearly $Re \subset \mathfrak{a}$, and if $a \in \mathfrak{a}$ we have $a = a + 0 = ae + af$, and so $Re = \mathfrak{a}$.

Conversely, if $\mathfrak{a} = Re$ with $e^2 = e$, the inclusion map $i : \mathfrak{a} \hookrightarrow R$ can be inverted on the left by $g : R \rightarrow \mathfrak{a}$ with $g : a \mapsto ae$. Thus the short exact sequence $0 \rightarrow \ker g \rightarrow R @> g >> \mathfrak{a} \rightarrow 0$ splits. \spadesuit

We have already noted that every projective module over a field is free. There is another important class of rings for which this is the case:

Lemma 33 *If Λ is a commutative local ring with maximal ideal \mathfrak{m} , then every finitely generated projective Λ -module is free. (Recall that a local ring is a ring with a single maximal ideal.)*

The strong result is in fact true that if Λ is a noncommutative local ring then every Λ -module, whether finitely generated or not, is projective, and the proof is due to Kaplansky. However, we prove the result only in the commutative and finitely generated case.

Proof Let P be a finitely generated projective Λ -module with minimal spanning set y_1, \dots, y_k . and let F be the free Λ -module on the set x_1, \dots, x_k together with the canonical homomorphism $\pi : F \rightarrow P$ with $\pi(x_i) = y_i$. Let x_1, \dots, x_k , and let $k = r_1x_1 + \dots + r_kx_k \in \ker \pi$. It follows by applying π that

$$0 = r_1y_1 + \dots + r_ky_k.$$

If one of the r_i is a unit, we have contradicted the minimality of k . However, in a local ring, any element r outside the maximal ideal must be a unit, as the principal ideal generated by r cannot lie in a maximal ideal and therefore is not a proper ideal. Therefore, all the $r_i \in \mathfrak{m}$, and so $\ker \pi \subset \mathfrak{m}F$.

Since $0 \rightarrow \ker \pi \rightarrow F \xrightarrow{\pi} P \rightarrow 0$ and P is projective, we have $F = \ker \pi \oplus P'$ for some isomorphic copy P' of P inside F . Since $\ker \pi \subset \mathfrak{m}F$, we have $F \subset \mathfrak{m}F + P'$, and therefore $P' + \mathfrak{m}F = F$. Because F/P' is finitely generated and $\mathfrak{m} = \text{rad } \Lambda$ (it's the only maximal ideal), we can use Nakayama's lemma (theorem 18) to conclude that $F = P'$ and $P \cong P'$ is indeed free. ♠

5.1 Manipulating projective modules

One of the most useful principles about projective modules is that in general, the projective property is fairly malleable. If we look at a projective module under a different light, or perform an operation on a projective module, we can provide reasonable conditions under which the module remains projective. We give a couple of easy examples first:

Proposition 34 *If P is a finitely generated projective $R[G]$ -module, then P is projective as an R -module.*

Proof We may write P as a direct summand of a free $R[G]$ -module $R[G]^k$. But $R[G]^k$ is certainly free as an R -module, so as an R -module P is again a direct summand of a free module. ♠

Lemma 35 *If R is a ring, P is an R -module, and S is an ideal of P such that $SP = 0$, then P is a projective S -module then it is projective when regarded as an R/S -module.*

Proof Suppose P is R -projective. Let $B \twoheadrightarrow P$ be an R/S -module surjection. Then we can regard it as an R -module surjection, so that we get $B = P \oplus Q$ as R -modules. Since $SB = SP = 0$, it follows that $SQ = 0$, and Q can be regarded as an R -module. So, P is a direct summand of B as an R/S -module as well, and P is projective. ♠

The converse of this lemma is false. For example, $\mathbb{Z}/2\mathbb{Z}$ is projective as an $\mathbb{Z}/2\mathbb{Z}$ -module, but not as a \mathbb{Z} -module, since the following diagram cannot be completed:

$$\begin{array}{ccc}
& & \mathbb{Z}/2\mathbb{Z} \\
& \nearrow \#g & \downarrow Id \\
\mathbb{Z} & \xrightarrow{\text{mod } 2} & \mathbb{Z}/2\mathbb{Z}
\end{array}$$

We now turn to some more sophisticated operations on projective modules. For example, extension of fields preserves the tensor product:

Proposition 36 *If $E \subset L$ is an extension of fields and P is a finitely generated projective $E[G]$ -module, then $P \otimes_E L$ is a projective $L[G]$ -module.*

Proof Since P is a direct summand of a finitely generated free $E[G]$ -module, we can write $E[G]^k = P \oplus Q$ for some k , and we get

$$(P \otimes_E L) \oplus (Q \otimes_E L) = E[G]^k \otimes_E L = (E[G] \otimes_E L)^k.$$

Therefore, it suffices to show that $E[G] \otimes_E L$ is a free $L[G]$ -module. But it is an easy exercise in the mechanics of the tensor product to prove that $E[G] \otimes_E L \cong L[G]$, so the result follows. ♠

Proposition 37 *If L is a field, P is a finitely generated projective $L[G]$ -module, and E is any finitely generated $L[G]$ -module, then $P \otimes_L E$ is a projective $L[G]$ -module (where $g(p \otimes e) = gp \otimes ge$.)*

Proof Using the same trick as in the preceding proof, it suffices to show that $L[G] \otimes_L E$ is a free $L[G]$ -module. If $v \in E$, then the $g \otimes gv$ are linearly independent over L (as their first factors are), so the $L[G]$ -submodule of $L[G] \otimes_L E$ generated by $1 \otimes v$ has dimension $\#G$ as an L -vector space. But any $L[G]$ -module generated by a single element is isomorphic to a quotient of $L[G]$, and so by the dimension count we find that $L[G](1 \otimes v)$ is isomorphic to $L[G]$.

Let v_1, \dots, v_k be a basis for E as an L -vector space, and let F_i be the $L[G]$ -submodule generated by $1 \otimes v_i$. Since the dimension of $L[G] \otimes_L E$ as an L -vector space is $\#G \cdot k$, if we can show that the sum of the F_i is equal to $L[G] \otimes_L E$ then by dimension-counting the sum would be direct. This would prove $L[G] \otimes_L E \cong L[G]^k$.

It suffices to show that given any $v \in E$ and $g \in G$ we have $g \otimes v$ in the sum of the F_i . Writing

$$g^{-1}v = \alpha_1 v_1 + \dots + \alpha_k v_k,$$

we get

$$1 \otimes g^{-1}v = \alpha_1(1 \otimes v_1) + \dots + \alpha_k(1 \otimes v_k)$$

and so

$$g \otimes v = \alpha_1(g \otimes gv_1) + \dots + \alpha_k(g \otimes gv_k),$$

and the result follows. ♠

In general, we cannot take the tensor product over R of two of the left $R[G]$ -modules we have been considering—tensor products don't work that way, one must tensor a left R -module with a right R -module. In the case where we are tensoring over a commutative ring, this problem does not arise, since left modules and right modules are one and the same. I do not know whether or not the above argument can be modified to remove the dimension counting and yield a result for commutative rings instead of fields. We do obtain analogous result in a very special case:

Proposition 38 *If R is a commutative ring, E is a projective $R[G]$ -module, and F is a projective R -module (i.e. we let G act trivially on F), then $E \otimes_R F$ is a projective $R[G]$ -module.*

Proof We leave it to the reader to verify that because F is acted on trivially by G , for any $R[G]$ -module B we achieve the following identity:

$$\mathrm{Hom}_{R[G]}(E \otimes_R F, B) = \mathrm{Hom}_R(F, \mathrm{Hom}_{R[G]}(E, B)).$$

Let $C \twoheadrightarrow B$ be an $R[G]$ -module surjection. Since E is a projective $R[G]$ -module, we get a surjection

$$\mathrm{Hom}_{R[G]}(E, C) \twoheadrightarrow \mathrm{Hom}_{R[G]}(E, B).$$

Employing the fact that F is projective R -module, we then get a surjection

$$\mathrm{Hom}_R(F, \mathrm{Hom}_{R[G]}(E, C)) \twoheadrightarrow \mathrm{Hom}_R(F, \mathrm{Hom}_{R[G]}(E, B)).$$

By our identity we obtain a surjection

$$\mathrm{Hom}_{R[G]}(E \otimes_R F, C) \twoheadrightarrow \mathrm{Hom}_{R[G]}(E \otimes_R F, B)$$

and by criterion (3) of proposition 31, $E \otimes_R F$ is projective. ♠

5.2 Projective Envelopes

A map surjective map $\phi : N \twoheadrightarrow M$ of R -modules is called essential if no proper submodule of N is mapped by ϕ onto M . An essential map $\phi : P \twoheadrightarrow M$ from a projective module P onto M is called a projective envelope for M .

It is easy to see that a projective envelope must be unique: if $\phi_1 : P_1 \twoheadrightarrow M$ and $\phi_2 : P_2 \twoheadrightarrow M$ are projective envelopes, by the projective property of P_1 we get a map $g : P_1 \rightarrow P_2$ such that $\phi_1 = \phi_2 \circ g$:

$$\begin{array}{ccc} & P_1 & \\ & \swarrow g & \downarrow \phi_1 \\ P_2 & \xrightarrow{\phi_2} & M \end{array}$$

By the essential property of ϕ_2 , we must have g surjective. Since P_2 is projective, it is thus a direct summand in P_1 , say $P_1 \cong P_2 \oplus Q$, with g being

the projection onto the first summand. Since the submodule of P_1 isomorphic to P_2 maps by $\phi_1 = \phi_2 \circ g$ onto M , the projective property of ϕ_1 tells us that $Q = 0$ and $P_1 \cong P_2$.

The existence question is somewhat more difficult. Following Serre [12]:

Proposition 39 *If R is Artinian and M is a finitely generated R -module, then M has a projective envelope.*

Proof Let F be a finitely generated free module such that M is a quotient of F , say $M = F/S$. For any submodule $N \subset S$, we therefore obtain a projection $f_N : F/N \rightarrow F/S = M$. Since M is Artinian and since $f_S = 1_M$ is essential, we may choose N to be minimal with the property that f_N is essential. We will show that F/N is projective, so that it is a projective envelope for M .

Set $P = F/N$, and let Q be a submodule of F minimal with the property that the projection ϕ of Q onto P along N is surjective. Let $p : F \rightarrow P$ be the projection along N , and let $q : F \rightarrow Q$ be the lifting of p to Q using the projective property of F . That is, the following triangle is commutative:

$$\begin{array}{ccc} & F & \\ q \swarrow & & \searrow p \\ Q & \xrightarrow{\phi} & P \end{array}$$

The map q must be surjective by the minimality of Q , so letting N' be the kernel of q we have $Q \cong F/N'$. Also, since $p = \phi \circ q$, we see

$$N' = \ker q \subset \ker p = N,$$

and the map $f'_N : F/N' \rightarrow M$ factors as:

$$F/N' \cong Q @> \phi >> F/N @> f_N >> M.$$

The minimality of Q shows that the first map is essential, and the second map was constructed to be essential. Therefore, their composition is essential and, since we have already seen that $N' \subset N$, the minimality of N shows that $N' = N$. Thus, ϕ is an isomorphism, so to show that $P \cong Q$ is projective we shall show that Q is a direct summand of F . Notice that from the definition of ϕ , $\phi(Q) = (Q + N)/N = P = F/N$, and so $Q + N = F$. To show that the sum is direct, suppose $x \in Q \cap N$, and from the surjectivity of q suppose $x = q(y)$ for $y \in F$. Since $x \in N$, $\phi(x) = 0$, i.e. we have the following triangle:

$$\begin{array}{ccc} & y & \\ q \swarrow & & \searrow p \\ x & \xrightarrow{\phi} & 0 \end{array}$$

Thus $p(y) = 0$, so $y \in \ker p = N$. But $N = \ker q$, so $x = q(y) = 0$ and the sum is direct. ♠

We give two basic tools for obtaining projective envelopes:

Proposition 40 *If $P_1 @ > \phi_1 \gg M_1$ and $P_2 @ > \phi_2 \gg M_2$ are projective envelopes, then $P_1 \oplus P_2 @ > \phi_1 \oplus \phi_2 \gg M_1 \oplus M_2$ is a projective envelope.*

Proof Write $\phi = \phi_1 \oplus \phi_2$. It suffices to show that $P_1 \oplus P_2 @ > \phi \gg M_1 \oplus M_2$ is an essential homomorphism. Suppose $S \subset P_1 \oplus P_2$ is mapped onto $M_1 \oplus M_2$ by ϕ . If $x \in P_1 \oplus P_2$, there is $y \in S$ such that $\phi(y) = \phi(x)$, and therefore $P_1 \oplus P_2 = S + \ker \phi = S + Q_1 + Q_2$ where Q_i is the natural injection of $\ker \phi_i$ into $P_1 \oplus P_2$. Consequently,

$$P_1 = Q_1 + (S + Q_2) \cap P_1.$$

The preceding equation shows that $(S + Q_2) \cap P_1$ is mapped surjectively onto M_1 by ϕ_1 , and therefore since ϕ_1 is essential we have

$$P_1 \subset S + Q_2.$$

But $Q_1 \subset P_1$, so $Q_1 \subset S + Q_2$, and therefore

$$P_1 \oplus P_2 = S + Q_1 + Q_2 = S + Q_2.$$

We essentially repeat the above argument: $P_2 \subset S + Q_2$, and therefore

$$P_2 = Q_2 + S \cap P_2.$$

Since ϕ_2 is essential, $P_2 \subset S$. Similarly $P_1 \subset S$, and $S = P_1 \oplus P_2$. ♠

Proposition 41 *Let P be a finitely generated projective R -module, and suppose $J \subset \text{rad } R$. Then P is a projective envelope for $P/J P$.*

Proof Let π be the natural projection from P to $P/J P$. Let S be a submodule of P such that $\pi(S) = P/J P$. Since $\pi(S) = (S + J P)/J P = P/J P$, we obtain

$$S + J P = P.$$

Since P is finitely generated, so is P/S , and by Nakayama's Lemma we conclude that $S = P$. Thus, π is essential. ♠

This has an immediate application to the structure of finitely generated projective modules over Artinian rings. Let R be an Artinian ring, and let P be a finitely generated projective R -module. Recall that by Hopkins' theorem, R is also Noetherian, so by the Krull-Schmidt theorem, P can be written as a direct sum of finitely many indecomposable R -modules. A direct summand of a projective module is projective, so P is in fact a direct sum of indecomposable projective modules. Let P' be one of the indecomposable projective modules. Then $P' / (\text{rad } R) P'$ is semisimple, so is a direct sum $E_1 \oplus \cdots \oplus E_k$ of simple modules. But each E_i has a projective envelope P_i , and proposition 40 tells us that $P' = P_1 \oplus \cdots \oplus P_k$. Since P' was assumed to be indecomposable, we must have $k = 1$ and $P' / (\text{rad } R) P'$ simple. The reverse argument shows that if E is simple, its projective envelope must be indecomposable. Therefore, we have proved:

Proposition 42 *If R is Artinian, then each finitely generated projective R -module can be written uniquely as a direct sum of indecomposable projective R -modules. Furthermore, the indecomposable projective R -modules are exactly the projective envelopes of the simple R -modules.*

Thus, if L is a field of characteristic p and $p \nmid \#G$, while it is not true that every $L[G]$ -module is a sum of simple $L[G]$ -modules, we do get a structure theorem close to this for the projective $L[G]$ -modules.

5.3 A Lifting Theorem

In this section, we wish to describe a theorem which lifts a projective $k[G]$ -module up to a projective $A[G]$ -module. (Recall that A, k are as in section 4.) $A[G]$ -modules are somewhat trickier to analyze, as in general A and $A[G]$ are not Artinian. For the complete argument, we refer the reader to Serre [12], section 14.4.

Lemma 43 *If E is a finitely generated $A[G]$ -module, then we have a $k[G]$ -module isomorphism*

$$E/\mathfrak{m}E \cong E \otimes_A k.$$

Proof Let $\varphi : E \rightarrow E \otimes_A k$ via $e \mapsto e \otimes 1$. For any $\alpha \in A$,

$$\varphi(\alpha e) = (\alpha e) \otimes 1 = e \otimes (\alpha + \mathfrak{m}),$$

so $\mathfrak{m}E \subset \ker \varphi$ and thus φ induces a map from $E/\mathfrak{m}E \rightarrow E \otimes_A k$. But we can easily construct an inverse for this map: if we send

$$e \otimes (\alpha + \mathfrak{m}) \mapsto \alpha e + \mathfrak{m}$$

then the map is well-defined, and the necessary relations are in the kernel of the map, so we indeed get a map from the tensor product to $E/\mathfrak{m}E$. This is evidently the inverse of our first map. ♠

Note that these lemmas apply equally well any local ring and its residue field replacing A and k .

We rely on the following lemma, which we quote without proof from section 14.4 of Serre:

Lemma 44 *Let P be a finitely generated $A[G]$ -module which is free as an A -module. For P to be $A[G]$ -projective, it is necessary and sufficient that the $k[G]$ -module $\bar{P} = P \otimes_A k$ be projective. Furthermore, two projective $A[G]$ -modules P and P' are isomorphic if and only if the reductions \bar{P} and \bar{P}' are.*

Given all the work we have done, the proof of the lemma should be relatively straightforward (but slightly laborious). There is one somewhat tricky step: Serre has an A -endomorphism u' of P such that $u' \equiv 1_P \pmod{\mathfrak{m}P}$, and concludes that u' is an automorphism of P . Since P is A -free, we can write

u' as a matrix with entries in A . The matrix is invertible if and only if its determinant is a unit. However, the fact that $u' \equiv 1_P \pmod{\mathfrak{m}P}$ tells us that the i, j -entry of the matrix of u' is contained in $\delta_{ij} + \mathfrak{m}$ (the Kronecker delta), so that the determinant of the matrix of u' is contained in $1 + \mathfrak{m}$. But since A is local, every element outside the maximal ideal is a unit, and Serre's assertion follows.

Lemma 45 *Let E be a finitely generated $A[G]$ -module. Then E is a projective $A[G]$ -module if and only if it is free as an A -module and the reduction $\bar{E} = E/\mathfrak{m}E = E \otimes_A k$ is a projective $k[G]$ -module.*

Proof If E is projective as an $A[G]$ -module, then it is certainly projective as an A -module by proposition 34. But A is local, so every projective A -module is free. The rest follows by the preceding lemma. ♠

We can now demonstrate an important lifting theorem:

Theorem 46 *Let F be a finitely generated projective $k[G]$ -module. Then there exists a unique projective $A[G]$ -module whose reduction mod \mathfrak{m} is equal to F .*

Proof Uniqueness follows from the last statement in lemma 44. Existence is a little bit more difficult. Let F be a projective $k[G]$ -module, and let A_n denote A/\mathfrak{m}^n . Since the only ideals of A_n are the $\mathfrak{m}^i/\mathfrak{m}^n$ for $0 \leq i \leq n$. A_n and $A_n[G]$ are therefore Artinian, so regarding F as an $A_n[G]$ -module it has a projective envelope P_n with surjection $\phi_n : P_n \rightarrow F$. Since $\mathfrak{m}F=0$, we have $\phi_n(\mathfrak{m}P_n) = 0$, and therefore ϕ_n factors as

$$P_n \twoheadrightarrow \pi_n \twoheadrightarrow P_n/\mathfrak{m}P_n \twoheadrightarrow \varphi_n \twoheadrightarrow F$$

Since φ_n is a surjective $k[G]$ -module homomorphism and F is $k[G]$ -projective, we can identify F as a direct summand in $P_n/\mathfrak{m}P_n$ so that φ_n becomes the projection along the direct sum. But the map $\phi_n : P_n \rightarrow F$ was essential, so the complement of F in $P_n/\mathfrak{m}P_n$ must be 0, and we have

$$F \cong P_n/\mathfrak{m}P_n.$$

Now, P_n is also an $A_{n+1}[G]$ -module, so that we obtain a commutative triangle:

$$\begin{array}{ccc} & P_{n+1} & \\ p_{n+1} \swarrow & & \downarrow \phi_{n+1} \\ P_n & \xrightarrow{\phi_n} & F \end{array}$$

Therefore, we obtain homomorphisms $p_{n+1} : P_{n+1} \rightarrow P_n$. Exactly as we did in section 4, we can take the limit of the P_n to be the A -module P of all sequences (x_1, x_2, \dots) with $x_i \in P_i$ satisfying the condition that $p_{i+1}(x_{i+1}) = x_i$. We leave it to the reader to prove two results: that the limit P has $F \cong P/\mathfrak{m}P$ as well, and that P is free as an A -module. (The latter result will use the fact

that each P_n is projective and therefore free as an A_n -module, as well as the fact that A' , the limit of the A_n which we constructed in section 4, is equal to A by our assumption that K is complete.) Then, the preceding lemma shows that P is projective, and therefore is the desired lift. ♠

We obtain an immediate corollary:

Proposition 47 *Every finitely generated projective $A[G]$ -module can be written uniquely as a direct sum of indecomposable projective $A[G]$ -modules. A projective indecomposable $A[G]$ -module is characterized by its reduction mod \mathfrak{m} to a projective indecomposable $k[G]$ -module.*

Proof If the reduction mod \mathfrak{m} of a projective $A[G]$ -module decomposes as a direct sum, the lifting theorem shows that the summands lift to a direct sum decomposition of the original $A[G]$ -module. This, together with the assertion of uniqueness in the theorem, proves the second statement of the proposition. Note that a projective indecomposable $k[G]$ -module must also lift up to an indecomposable $A[G]$ -module: a decomposition upstairs yields a decomposition downstairs, too. So, there is a bijection between the finitely generated projective indecomposable $A[G]$ - and $k[G]$ -modules.

The first statement is nontrivial, because $A[G]$ does not necessarily satisfy any of the chain conditions needed to use the Krull-Schmidt theorem. However, if we reduce a projective $A[G]$ -module mod \mathfrak{m} , we obtain a projective $k[G]$ -module. This we do know can be written uniquely as a sum of indecomposable $k[G]$ -modules, and by the results in the preceding paragraph that decomposition lifts to a unique decomposition of the $A[G]$ -module. ♠

6 Grothendieck groups

To a category of modules, we can associate a group, called the Grothendieck group. The Grothendieck group essentially allows us to forget how simple modules in a composition series fit together and focus in on the simple modules themselves—thus they prove to be a useful construct in the study of modular representations.

Let R be a ring, and let \mathcal{F} be a category of left R -modules. The Grothendieck group $K(\mathcal{F})$ is defined to be the group with a single generator for each isomorphism class of R -modules (we will let $[E]$ denote the generator corresponding to the module E) and with a relation $[E] = [E'] + [E'']$ for each short exact sequence

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0.$$

Let $\varphi : \mathcal{F} \rightarrow K(\mathcal{F})$ be the map which takes a module E to its class $[E]$.

Proposition 48 *Let G be an abelian group together with a map $\psi : \mathcal{F} \rightarrow G$ such that $\psi(E) = \psi(E') + \psi(E'')$ for short exact sequences as above. Suppose further that G has the following universal property: if H is an abelian group and $\lambda : \mathcal{F} \rightarrow H$ is a function such that $\lambda(E) = \lambda(E') + \lambda(E'')$ for each short*

exact sequence as above, then there exists a unique homomorphism $\lambda_0 : G \rightarrow H$ such that $\lambda_0(\psi(E)) = \lambda(E)$. Then $G = K(\mathcal{F})$ and $\psi = \varphi$.

Proof It is easy to see that $K(\mathcal{F})$ has this property: just define $\lambda_0([E]) = \lambda(E)$ for each generator $[E]$, extend by linearity, and notice that the sum property of λ means that the relations are in the kernel of λ_0 .

On the other hand, let G equipped with $\psi : \mathcal{F} \rightarrow G$, be any group with the above universal property. Put $H = K(\mathcal{F})$. Then, from the definitions of the Grothendieck group, φ has the additive property that $\varphi(E) = \varphi(E') + \varphi(E'')$ for short exact sequences. Consequently, there exists a unique homomorphism $\varphi_0 : G \rightarrow K(\mathcal{F})$ such that

$$\varphi_0(\psi(E)) = \varphi(E).$$

Furthermore, since $K(\mathcal{F})$ has the universal property, we have $\psi_0 : K(\mathcal{F}) \rightarrow G$ with

$$\psi_0(\varphi(E)) = \psi(E).$$

Therefore, we have

$$\psi_0(\varphi_0(\psi(E))) = \psi(E)$$

and

$$\varphi_0(\psi_0(\varphi(E))) = \varphi(E)$$

and so by the uniqueness portion of the universal property we find that φ_0 and ψ_0 are inverses of each other, and G and $K(\mathcal{F})$ are isomorphic. ♠

6.1 $R_L(G)$

Let L be a field. We define the group $R_L(G)$ to be the Grothendieck group of the category of all finitely generated $L[G]$ -modules.

Proposition 49 *The set of all elements $[E] \in R_L(G)$, where E is a simple $L[G]$ -module, is a \mathbb{Z} -basis for the group $R_L(G)$.*

Proof Let S_L be the set of all the isomorphism classes of simple $L[G]$ -modules, and let R be the free \mathbb{Z} -module on the set S_L . We get a map $\alpha : R \rightarrow R_L(G)$ via $[[E]] \mapsto [E]$ (where $[[E]]$ is the generator of R corresponding to $[E]$) extended linearly. We wish to construct an inverse for α . If F is a finitely generated $L[G]$ -module and if $E \in S_L$, let $l_E(F)$ be the number of times that E is in the composition series for F . By the Jordan-Hölder theorem, this is well-defined. Now, suppose $0 \rightarrow M \rightarrow N \rightarrow P \rightarrow 0$ is a short exact sequence. We saw (in the proof of Hopkins' theorem) how we can obtain a composition series for N by taking a composition series for M , and taking as the rest of the composition series the preimage in the projection along M of any composition series for P . Thus $l_E(N) = l_E(M) + l_E(P)$, and so by the universal property we obtain a map c_E from $R_L(G)$ to \mathbb{Z} such that $c_E([F]) = l_E(F)$ for a finitely generated $L[G]$ -module F . Suppose that for any $x \in R_L(G)$ we put

$$\beta(x) = \sum_{E \in S_L} c_E(x)[[E]].$$

It is easy to check that α and β are inverses of each other. (To show that $\alpha \circ \beta$ is the identity on F , use induction on the length of the composition series of F .) ♠

Observe that in the case where L has characteristic 0, by semisimplicity, we have that for any two $L[G]$ -modules E and E' , $[E] = [E']$ if and only if $E \cong E'$. This is not the case when L has characteristic p dividing $\#G$, since there are nonisomorphic $L[G]$ -modules with the same simple modules in their composition series.

Proposition 50 *The tensor product affords a ring structure on $R_L(G)$. That is, if we put $[E] \cdot [F] = [E \otimes_L F]$ and extend linearly, the multiplication is well-defined and gives a ring structure.*

Proof The rest of the proposition is clear once we know that the multiplication is indeed well-defined. To show well-definedness, we need to prove that if $0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0$ is a short exact sequence, then so is

$$0 \rightarrow E' \otimes_L F \rightarrow E \otimes_L F \rightarrow E'' \otimes_L F \rightarrow 0.$$

While this is not true in general, it certainly is true for finite-dimensional vector spaces like those we are dealing with here. ♠

6.2 $P_k(G)$ and $P_A(G)$

We define $P_k(G)$ and $P_A(G)$ to be the Grothendieck groups of the categories of finitely generated projective $k[G]$ - and $A[G]$ -modules respectively.

Proposition 51 *$P_k(G)$ is an $R_k(G)$ -module under the tensor product, defined as above.*

Proof The proof is exactly the same as the proof of proposition 50 above, with one added twist: if E is a projective $k[G]$ -module and F is any $k[G]$ -module, we need $E \otimes_k F$ to be projective. But this is precisely the content of proposition 37. ♠

The machinery of Grothendieck groups allows us to reinterpret proposition 42 in the following fashion:

Proposition 52 *For each simple $k[G]$ -module E , let P_E be its projective envelope. Then the $[P_E]$ form a basis of $P_k(G)$. Furthermore, if P and P' are projective $k[G]$ -modules, they are isomorphic if and only if $[P] = [P']$ in $P_k(G)$.*

Proof If P is a projective $k[G]$ -module, let c_E be the number of times that P_E appears as a direct summand of P , as per proposition 42. Since any short exact sequence of projective modules splits, c_E has the addition property necessary to define a function on $P_k(G)$. Therefore, if $[P] = [P']$, then P and P' contain each P_E the same number of times as a direct summand. So, P and P' are equal. The rest of the proposition follows from this. ♠

We turn now to the structure of $P_A(G)$:

Proposition 53 *Reduction mod \mathfrak{m} defines an isomorphism from $P_A(G)$ onto $P_k(G)$. Two projective $A[G]$ -modules P and P' are isomorphic if and only if $[P] = [P']$ in $P_A(G)$.*

Proof This follows immediately from proposition 47. ♠

6.3 The cde-triangle

The structure for $P_k(G)$, $P_A(G)$, $R_k(G)$, and $R_K(G)$ that we have determined, combined with the manipulation of modules that we have developed, allows us to define a commutative triangle of Grothendieck groups:

$$\begin{array}{ccc} & P_k(G) & \\ & \swarrow e & \downarrow c \\ R_K(G) & \xrightarrow{d} & R_k(G) \end{array}$$

In essence, the map c is defined by taking a projective $k[G]$ -module P with $[P] \in P_k(G)$, and sending $[P]$ to the class of P in $R_k(G)$. The map d will be defined by taking a $K[G]$ module M , finding an $A[G]$ -module (i.e. an A -lattice) inside M , and reducing the $A[G]$ -module modulo \mathfrak{m} . Finally, the map e is defined by taking a projective $k[G]$ -module P , lifting it using theorem 46 to an $A[G]$ -module, and tensoring the $A[G]$ -module with K to get a $K[G]$ -module.

Let us describe the maps c, d , and e more carefully. If $[P_E]$ is the class in $P_k(G)$ of the projective indecomposable $k[G]$ -module P_E , then we know that P_E is the unique module whose class in $P_k(G)$ is $[P_E]$. Consequently, any map we define on $P_k(G)$ via extending by linearity a mapping of each $[P_E]$ to an object obtained from P_E will be well-defined. In particular, to define the map c we send $[P_E]$ in $P_k(G)$ to the class of P_E in $R_k(G)$. Second, to obtain the map e , we create a $K[G]$ -module as follows: using theorem 46, lift P_E to a projective indecomposable $A[G]$ -module A_E . Then we define e by mapping

$$[P_E] \mapsto e \gg A_E \otimes_A K.$$

The description of the map d is somewhat more difficult. Let E be a simple $K[G]$ -module. Once again we may well-define a map on $R_K(G)$ by specifying in terms of E an element of $R_k(G)$. Since E is simple, we know it is equal to $K[G]e$ for some $e \in E$. Then $E_1 = A[G]e$ is a lattice, i.e. a subset of E which is an $A[G]$ -module and generates E as a $K[G]$ -module. (Note also that $E = E_1 \otimes_A K$.) We can reduce $\overline{E}_1 = E_1/\mathfrak{m}E_1$ to obtain a $k[G]$ -module, and we put

$$d([E]) = [\overline{E}_1] \in R_k(G).$$

While strictly speaking this is well-defined, it is not a useful map unless we can show that the image $d([E])$ is independent of our choice of lattice—for example,

it is difficult to prove commutativity of the cde -triangle without the result that d is independent of the lattice chosen. Our proof directly follows that in Serre [12]:

Theorem 54 *If E is a $K[G]$ -module and E_1 and E_2 are two lattice is E , then $[\overline{E_1}] = [\overline{E_2}]$ in $R_k(G)$. (It is not necessarily true, however, that $\overline{E_1} \cong \overline{E_2}$.)*

Proof Suppose first of all that

$$\mathfrak{m}E_1 \subset E_2 \subset E_1.$$

Let T be the module E_1/E_2 ; since $\mathfrak{m}E_1 \subset E_2$, T is in fact a $k[G]$ -module. Since \mathfrak{m} is a principal ideal, let π be a generator for it. Since we have a projection $E_1/\mathfrak{m}E_1 \twoheadrightarrow \varphi \twoheadrightarrow E_1/E_2$, we then get an exact sequence of $k[G]$ -modules

$$0 \rightarrow T \twoheadrightarrow \times \pi \twoheadrightarrow \overline{E_2} \twoheadrightarrow i^* \twoheadrightarrow \overline{E_1} \twoheadrightarrow \varphi \twoheadrightarrow T \rightarrow 0.$$

Consequently, in $R_k(G)$,

$$[T] - [\overline{E_2}] + [\overline{E_1}] - [T] = 0$$

and $[\overline{E_1}] = [\overline{E_2}]$.

In general, let E_2 be generated over A by x_1, \dots, x_k . Since E_1 generates E over K , there exist $k_i \in K$ and $y_i \in E_1$ such that $x_i = k_i y_i$. Recalling that K is endowed with a valuation v , let us pick j such that $v(k_j)$ is minimal. Then $k_i/k_j \in A$ for all i , and therefore

$$x_i = a_i(k_j y_i)$$

with $a_i \in A$, i.e. $E_2 \subset k_j E_1$. Since multiplying E_1 by a scalar does not affect $\overline{E_1}$, we may assume that $E_2 \subset E_1$. Furthermore, if $x_i = a_i y_i$ as above and n is the maximum of the $v(a_i)$, we obtain

$$\mathfrak{m}^n E_1 \subset E_2 \subset E_1.$$

We proceed by induction on n . Put $E_3 = \mathfrak{m}^{n-1} E_1 + E_2$. Then

$$\mathfrak{m}^{n-1} E_1 \subset E_3 \subset E_1 \quad \text{and} \quad \mathfrak{m} E_3 \subset E_2 \subset E_3$$

and by the first case and the induction hypothesis we get $[\overline{E_1}] = [\overline{E_2}] = [\overline{E_3}]$. ♠

To see that the cde -triangle is commutative, begin with $[P_E] \in P_k(G)$. To evaluate e , we lift P_E to an $A[G]$ -module A_E , and take the tensor product with K to get $e([P_E])$. To find $d(e([P_E]))$, we immediately take a lattice in $e([P_E])$, and by the independence of our choice of lattice A_E will do. We then reduce the lattice mod \mathfrak{m} . But we know $A_E/\mathfrak{m}A_E \cong P_E$, since lifting and reduction mod \mathfrak{m} is a bijective correspondence. Thus

$$d(e([P_E])) = [A_E/\mathfrak{m}A_E] = [P_E] = c([P_e]) \in R_k(G),$$

and the triangle is commutative.

We shall now list a few of the main results on the cde -triangle. These constitute the bulk of the results on modular representations that Serre proves in [12], and the interested reader should now turn to studying that book. We quote from chapter 16 of Serre:

Theorem 55 *Let G be a finite group.*

1. *The homomorphism $d : R_K(G) \rightarrow R_k(G)$ is surjective.*
2. *The homomorphism $e : P_k(G) \rightarrow R_K(G)$ is a split injection.*
3. *Let p^n be the largest power of p dividing the order of G . Then every element of $R_k(G)$ divisible by p^n belongs to the image of the map $c : P_k(G) \rightarrow R_k(G)$.*
4. *The image of $e : P_k(G) \rightarrow R_K(G)$ consists of those elements of $R_K(G)$ whose character is zero on the elements of G whose order is divisible by p .*

References

- [1] Alperin, J. L. *Local representation theory*. Cambridge: Cambridge University Press, 1986.
- [2] Atiyah, M. F. and I. G. MacDONald. *Introduction to Commutative Algebra*. Reading: Addison-Wesley, 1969.
- [3] Burrow, Martin. *Representation Theory of Finite Groups*. New York: Dover, 1993.
- [4] Curtis, Charles W. and Irving Reiner. *Representation Theory of Finite Groups and Associative Algebras*. New York: John Wiley & Sons, 1962.
- [5] Dummit, David S. and Richard M. Foote. *Abstract Algebra*. Englewood Cliffs: Prentice-Hall, 1991.
- [6] Hungerford, Thomas W. *Algebra*. New York: Springer-Verlag, 1974.
- [7] Jacobson, Nathan. *Basic Algebra II*. San Francisco: W. H. Freeman and Company, 1980.
- [8] Lam, T. Y. *A First Course in Noncommutative Rings*. New York: Springer-Verlag, 1991.
- [9] Mac Lane, Saunders. *Homology*. Berlin: Springer-Verlag, 1995.
- [10] Matsumura, Hideyuki. *Commutative Ring Theory*. Cambridge: Cambridge University Press, 1986.
- [11] Nagao, Hiroshi and Yukio Tsushima. *Representations of Finite Groups*. San Diego: Academic Press, 1989.
- [12] Serre, J.-P. *Linear Representations of Finite Groups*. New York: Springer-Verlag, 1977.