12. Projective modules [s:projective]

The blanket assumptions about the base ring k, the k-algebra A, and A-modules enumerated at the start of §11 continue to hold.

[ss:localendam]

12.1. **Indecomposability of M and the localness of $\mathrm{End}_A M$.** In analogy with the terminology 'local' in the commutative case, the algebra A is called *local* if $A/\mathfrak{Rad}\,A \simeq k$.

[l:local]

Lemma 12.1. *A is local if and only if every element of A is either invertible or nilpotent.*

Proof. The latter condition goes down to quotients. In particular it is true for $A/\mathfrak{Rad}\,A$ which by Wedderburn is a product of matrix algebras over k. If there is more than one factor, then the element that corresponds to the identity in one factor and zero elsewhere is neither invertible not nilpotent. So there is only one factor. Moreover, if this factor is an $n \times n$ matrix algebra where $n \geq 2$, then it too has a non-nilpotent non-invertible element, e.g., a diaganal matrix where one of the diagonal entries is 1 and all others zero.

We claim that the latter condition if it holds for a quotient by a nilpotent two sided ideal holds also for A. It suffices to prove the claim for the condition holds for $A/\mathfrak{Rad}\,A$ if A is local, and $\mathfrak{Rad}\,A$ is nilpotent.

To prove the claim, suppose that $\mathfrak{n}$ is nilpotent and that every element of $A/\mathfrak{n}$ is either nilpotent or invertible. Let a be an non-nilpotent element of A. Then $\bar{a}$ is non-nilpotent in $A/\mathfrak{n}$. Thus we can find b in A such that $ba \equiv ab \equiv 1 \pmod{\mathfrak{n}}$. Writing $ab = 1 + x$ with $x \in \mathfrak{n}$, we see that ab and therefore a itself has a right inverse (because x is nilpotent). Similary ba and so a itself has a left inverse. Since a has both a left inverse and a right inverse, it is invertible. □

[t:local]

Theorem 12.2. *A module M is indecomposable if and only if $\mathrm{End}_A M$ is local.*

Proof. If $M = N \oplus P$, then the projection to N followed by the inclusion of N in M is an element of $\mathrm{End}_A M$ which is neither invertible nor nilpotent. Conversely, suppose that M is indecomposable and let φ be an element of $\mathrm{End}_A M$. For large enough n, by the Fitting Lemma (see §6.2), $\ker \varphi^n \oplus \mathrm{Im}\,\varphi^n = M$. If $\mathrm{Im}\,\varphi^n = M$, then φ^n and therefore φ is surjective, and M being Noetherian, this means φ is invertible (see (6.1)). If $\mathrm{Im}\,\varphi^n = 0$, then $\varphi^n = 0$, which means that φ is nilpotent. □

[p:cancel]

Proposition 12.3. *If M, U, V are A-modules such that $M \oplus U \simeq M \oplus V$, then $U \simeq V$.*

Proof. This follows from the Krull-Remak-Schmidt theorem (Theorem 6.2). □

[ss:uniserial]

12.2. **Uniserial modules.**

[p:uniserial]

Proposition 12.4. *For a module U, the following are equivalent* (U is called *uniserial* if these hold)*:*

1. *U has a unique composition series*
2. *the successive quotients in the radical series of U are simple.*
3. *the successive quotients in the socle series of U are simple.*

Proof. We make a few observations in aid of the proof. Let $0 \subsetneq U_1 \subsetneq \ldots \subsetneq U_{n-1} \subsetneq U$ be a composition series. Then $U_1 \subseteq \mathrm{soc}\,U$ and $\mathfrak{Rad}\,U \subseteq U_{n-1}$. Moreover, $\mathrm{soc}\,U$

is the sum of the U_1 and $\mathfrak{Rad}\, U$ the intersection of the U_{n-1}, as we vary over all composition series of U.

Let us now prove that (2) implies (1) by induction on the radical length. Since $U/\mathfrak{Rad}\, U$ is simple, $\mathfrak{Rad}\, U = U_{n-1}$. By induction, (1) holds for $\mathfrak{Rad}\, U$ and so also for U. The argument that (3) implies (1) is similar. Since $\operatorname{soc} U$ is simple, $U_1 = \operatorname{soc} U$. By induction on the socle length, (1) holds for U/U_1. So (1) holds also for U.

Suppose (1) holds. Then, from the observations at the start of this proof, $\mathfrak{Rad}\, U = U_{n-1}$, so $U/\mathfrak{Rad}\, U$ is simple. By induction on the length of U, we see that the quotients in the radical series for $U_{n-1} = \mathfrak{Rad}\, U$ are all simple. Therefore the same holds for U, and (2) is proved.

The proof that (1) implies (3) is similar to that of (1) implies (2). $\square$

[ss:fp]

12.3. **Free modules and projective modules.**

[p:free]

Proposition 12.5. *An A-module F is free if and only if it has a k-subspace S such that any linear map from S to an A-module M can be extended to an A-module morphism from F to M.*

Proof. Suppose that F is free with basis $\{x_i\}$. Take S to be the k-subspace generated by the x_i. Any (set) map from $\{x_i\}$ to M extends uniquely to a k-linear map of S to M, and to an A-module map from F to M. Conversely, if there exists such a subspace, then choosing $\{x_i\}$ to be k-basis of S, it is verified readily that F is freely generated by $\{x_i\}$. $\square$

[p:projective]

Proposition 12.6. *The following conditions are equivalent for an A-module P.*[12] (We call P *projective* if these hold.)

1. *Any short exact sequence of A-modules $0 \to L \to M \to P \to 0$ splits.*
2. *The functor $M \mapsto \operatorname{Hom}_A(P, M)$ is exact (on finite type A-modules).*
3. *If $\varphi : M \to N$ is a surjection of A-modules and $\vartheta : P \to N$ any A-module map, then there exists a lift $\tilde{\vartheta} : P \to M$ of ϑ, i,e., $\varphi\tilde{\vartheta} = \vartheta$.*
4. *P is a direct summand of a free module.*

Proof. (1) $\Rightarrow$ (4) Any module is a quotient of a free module. Write $F \twoheadrightarrow P$ where F is free. Now by (1) this splits. Therefore P is a direct summand of F.

(4) $\Rightarrow$ (3) Let $P \oplus Q$ be free. Extend ϑ to $\vartheta' : P \oplus Q \to N$ by defining it to be 0 on Q. Since (3) holds for a free module, we get $\tilde{\vartheta}' : P \oplus Q \to M$ such that $\varphi\tilde{\vartheta}' = \vartheta'$. Set $\tilde{\vartheta} := \tilde{\vartheta}'|_P$.

(3) $\Rightarrow$ (2) Let $0 \to L \to M \to N \to 0$ be exact. Then $0 \to \operatorname{Hom}_A(P, L) \to \operatorname{Hom}_A(P, M) \to \operatorname{Hom}_A(P, N)$ is exact in general. Since (3) holds the last map is also onto.

(2) $\Rightarrow$ (1) $0 \to \operatorname{Hom}_A(P, L) \to \operatorname{Hom}_A(P, M) \to \operatorname{Hom}_A(P, P) \to 0$ is exact. But this means that $\operatorname{Hom}_A(P, M) \to \operatorname{Hom}_A(P, P)$ is onto. If $\varphi : P \to M$ is a preimage of the identity morphism on P, then φ is a splitting. $\square$

[ss:pims]

12.4. **Projective indecomposable modules.**

We will write *PIM* for a projective indecomposable A-module.

[t:pimsimple]

Theorem 12.7. *Let P be a PIM.*

[12] It is to be understood that all modules appearing are finite dimensional k-vector spaces (equivalently finite type A-modules), for it is in that context that we will need the proposition.

(1) *P is a direct summand of A.*
(2) *The quotient $P/\mathfrak{Rad}\, P$ is simple.*
(3) *The association $P \mapsto P/\mathfrak{Rad}\, P$ is a bijection from PIMs to simples.*
(4) *The multiplicity of P in A equals $\dim_k P/\mathfrak{Rad}\, P$.*

Proof. (1) This follows by an application of the Krull-Remak-Schmidt theorem (Theorem 6.2) to the decomposition into indecomposables of $P \oplus N \simeq A^{\oplus n}$. (Why can we take n to be finite? Because a finitely generated projective module can be realized as a direct summand of a free module of finite rank.)
(2) $P/\mathfrak{Rad}\, P$ being semisimple, it suffices to show that it is indecomposable, for which it in turn suffices to show that the ring $\mathrm{End}_A(P/\mathfrak{Rad}\, P)$ contains no non-invertible non-nilpotent elements (the projection to a component in a non-trivial decomposition, if one were to exist, being such an element). In turn it suffices to find a ring with the above property that maps onto $\mathrm{End}_A\,(P/\mathfrak{Rad}\, P)$. We show that $\mathrm{End}_A\, P$ is such a ring.

Since P is indecomposable, the ring $\mathrm{End}_A\, P$ has the above property (this follows from Fitting's lemma: see Theorem 12.2). On the other hand, since $\mathfrak{Rad}\, P$ is a characteristic submodule, there is a natural map $\mathrm{End}_A\, P \to \mathrm{End}_A\,(P/\mathfrak{Rad}\, P)$. Since P is projective, this map is surjective.
(3) Let $A = P_1 \oplus \cdots \oplus P_m$ be a decomposition of A into indecomposables. Each P_i occurring here is a PIM, and each PIM must occur here as a P_i by (1). Since radicals of direct sums are direct sums of radicals, $\mathfrak{Rad}\, A = \mathfrak{Rad}\, P_1 \oplus \cdots \oplus \mathfrak{Rad}\, P_m$ and $A/\mathfrak{Rad}\, A = P_1/\mathfrak{Rad}\, P_1 \oplus \cdots \oplus P_m/\mathfrak{Rad}\, P_m$. By (2) this is a decomposition into simples of $A/\mathfrak{Rad}\, A$. Since every simple module must occur in this decomposition, it follows that every simple module arises as $Q/\mathfrak{Rad}\, Q$ for some PIM Q.

Suppose that $\pi : P/\mathfrak{Rad}\, P \to Q/\mathfrak{Rad}\, Q$ is an isomorphism for some PIM Q. Let $\sigma : Q/\mathfrak{Rad}\, Q \to P/\mathfrak{Rad}\, P$ be its inverse. By the projectivity of P (respectively Q), we get a lift $\tilde{\pi} : P \to Q$ of π (respectively $\tilde{\sigma} : Q \to P$ of σ). Consider the elements $\tilde{\sigma}\tilde{\pi}$ and $\tilde{\pi}\tilde{\sigma}$ of $\mathrm{End}_A\, P$ and $\mathrm{End}_A\, Q$. By the indecomposability of P (respectively Q), the former (respectively the latter) is either invertible or nilpotent (Theorem 12.2). But since their images in $\mathrm{End}_A\,(P/\mathfrak{Rad}\, P)$ and $\mathrm{End}_A\,(Q/\mathfrak{Rad}\, Q)$ respectively are invertible, they are both invertible. Thus $\tilde{\pi}$ is an injection (since $\tilde{\sigma}\tilde{\pi}$ is) and a surjection (since $\tilde{\pi}\tilde{\sigma}$ is), so a bijection.
(4) Write $A = \oplus Q^{m(Q)}$ be a decomposition of A into PIMs, the sum being over distinct isomorphism classes and $m(Q)$ being the mulitplicities. By (3), $A/\mathfrak{Rad}\, A = \oplus (Q/\mathfrak{Rad}\, Q)^{m(Q)}$ is a decomposition into simples, $(Q/\mathfrak{Rad}\, Q)^{m(Q)}$ being the isotypic components. The multiplicity $m(Q)$ thus equals $\dim_k\,(Q/\mathfrak{Rad}\, Q)$ (Theorem 9.4 (1)). ☐

[l:pimind]

Lemma 12.8. *Let P be a PIM and U be any module such that $U/\mathfrak{Rad}\, U \simeq P/\mathfrak{Rad}\, P$. Then U is a homomorphic image of P.*

Proof. Let $\pi : P/\mathfrak{Rad}\, P \to U/\mathfrak{Rad}\, U$ be an isomorphism. By the projectivity of P, we can get a lift $\tilde{\pi} : P \to U$ of π. Since π is a surjection, we have $\tilde{\pi}P + \mathfrak{Rad}\, U = U$, which by Nakayama (§10.2) implies $\tilde{\pi}P = U$. ☐

[ss:indecompkg]

12.5. **The case of group algebras.** We make two observations:

- The restriction to kH of a projective kG-module P is kH-projective. (It is enough to show that kG is a free kH-module. But this is obvious: a set of right coset representatives of H form a basis for kG over kH.)

- If P is a projective kG-module, then $\dim_k P \geq p^a$, where p^a is the order of a p-sylow subgroup of G. (By the preivous item, the restriction to a sylow p-subgroup H of a projective module is projective. So the restriction is a direct sum of indecomposable projectives. But there is only one PIM for kH (Theorem 12.7), for the trivial module is its only simple module: namely, kH itself.)

[l:npsylow]

Lemma 12.9. *Let R be a normal p-sylow subgroup of G. For a kG-module U, its radical equals the radical of its restriction to R: $\mathfrak{Rad}\, U = \mathfrak{Rad}\,(U|_R)$. If R is cyclic with generator x, then $\mathfrak{Rad}\, U = (1-x)U$.*

Proof. The restriction of $U/\,\mathfrak{Rad}\, U$ to kR is semisimple by Clifford (Theorem 11.5), so $\mathfrak{Rad}\,(U|_R) \subseteq \mathfrak{Rad}\, U$. On the other hand, $\mathfrak{Rad}\,(U|_R)$ is a kG-module. Indeed, for $u \in U$, $r \in R$, and $g \in G$, we have $rgu = g(g^{-1}rg)u$, so that $(gU)|_R$ is the twist of $U|_R$ by the automorphism $r \mapsto g^{-1}rg$. Since the radical is invariant under twists, we conclude that $g\,\mathfrak{Rad}\,(U|_R) = \mathfrak{Rad}\,(U|_R)$, so $\mathfrak{Rad}\,(U|_R)$ is a kG-module.

The restriction to kR of the kG-module $U/\,\mathfrak{Rad}\,(U|_R)$ is semisimple. Since R is a p-group, and simple modules for p-groups are trivial, the action of G on $U/\,\mathfrak{Rad}\,(U|_R)$ descends to G/R. Since G/R is a group of order coprime to p, $U/\,\mathfrak{Rad}\,(U|_R)$ is semisimple as a kG-module. So $\mathfrak{Rad}\, U \subseteq \mathfrak{Rad}\,(U|_R)$.

As for the second assertion, $\mathfrak{Rad}\, U = \mathfrak{Rad}\,(U|_R)$ by the first part. We have $\mathfrak{Rad}\,(U|_R) = (\mathfrak{Rad}\, kR)U$ (see §11), and $\mathfrak{Rad}\, kR = (1-x)kR$. ☐

[ss:duality]

12.6. **Duality.** We take $A = kG$ throughout this section. The dual (as a k-vector space) of a kG-module V is a kG-module: $({}^g f)(v) := f(g^{-1}v)$. We have a natural isomorphism $V \simeq V^{**}$ since, by our blanket assumptions on modules, V is finite dimensional over k. Dualization commutes with the operation of taking finite direct sums.

[l:dualsimple]

Lemma 12.10. *V is simple if and only if so is V^*.*

Proof. If $W \subseteq V$, then there is a natural surjection $W^* \twoheadleftarrow V^*$. So V is simple if V^* is. Conversely, if V simple, then so is V^{**} (because $V \simeq V^{**}$), and, V^{**} being the same as $(V^*)^*$, it follows from the first part that V^* simple. ☐

[i:simpledual]

(1) Duals of semisimple modules are semisimple, of indecomposables indecomposable. We have:

$$\operatorname{soc}(M^*) = (M/\,\mathfrak{Rad}\, M)^* \qquad M^*/\,\mathfrak{Rad}\,(M^*) = (\operatorname{soc} M)^*.$$

(2) Duality induces an involution $S \mapsto S^*$ (possibly the identity) on simple modules.

We will presently show that duals of free modules are free (Lemma 12.11). It will follow that duals of projectives are projective (Corollary 12.12). Assuming this for the moment, we have:

[i:pimdual]

(3) The dual of a PIM is a PIM. Duality induces an involution $P \mapsto P^*$ on PIMs.
(4) The socle of a PIM P is simple. Indeed $\operatorname{soc} P \simeq (P^*/\,\mathfrak{Rad}\, P^*)^*$, and P^* is a PIM. Now use Theorem 12.7 (2).

[i:pimsoc]

(5) The mapping $P \mapsto \operatorname{soc} P$ from PIMs to simples is a bijection. Indeed it is the composition $P \mapsto P^* \mapsto P^*/\,\mathfrak{Rad}\, P^* \mapsto (P^*/\,\mathfrak{Rad}\, P^*)^*$ of the bijections in (3), Theorem 12.7, and (1).

(6) The two bijections $P \mapsto P/\mathfrak{Rad}\,P$ and $P \mapsto \operatorname{soc} P$ from PIMs to simples (of Theorem 12.7 (2) and item (5) above) are the same, for as we will show $P/\mathfrak{Rad}\,P \simeq \operatorname{soc} P$ for a PIM P (Theorem 12.15). [i:multsoc]

(7) The number m of times a PIM P appears in the decomposition into indecomposables of kG equals $\dim \operatorname{soc} P$. This follows from the bijection $P/\mathfrak{Rad}\,P \simeq \operatorname{soc} P$ of Theorem 12.15 below, but it can be deduced more easily as follows. Since $kG \simeq kG^*$ by Lemma 12.11 below, m equals the corresponding the number for the PIM P^*. Now, by Theorem 12.7 (4), $m = \dim(P^*/\mathfrak{Rad}\,P^*)$. But $P^*/\mathfrak{Rad}\,P^* \simeq (\operatorname{soc} P)^*$. [l:dualkG]

Lemma 12.11. *$kG \simeq kG^*$ as a kG-module.*

Proof. Let δ_g be the element of kG^* defined by $\delta_g(h) := \delta_{g,h}$ for $h \in G \subseteq kG$, where $\delta_{g,h}$ is the Kronecker-delta function. Extend the association $g \leftrightarrow \delta_g$ to a linear isomorphism $kG \leftrightarrow kG^*$. We claim that this is a kG-module isomorphism. Indeed, $\delta_{xg}(h) = \delta_{xg,h} = \delta_{g,x^{-1}h} = \delta_g(x^{-1}h) = (x\delta_g)(h)$. □ [c:dualkG]

Corollary 12.12. *Let M be a kG-module.*

(1) *It is free if and only if its dual is free.*
(2) *It can be imbedded in a free module.*
(3) *It is projective if and only if its dual is projective.*

Proof. (1): Since any module is naturally identified with its double dual, $M \simeq (kG)^{\oplus n} \Leftrightarrow M^* \simeq (kG^{\oplus n})^*$. Since dualization commutes with taking (finite) direct sums, $M^* \simeq (kG^{\oplus n})^* \Leftrightarrow M^* \simeq (kG^*)^{\oplus n}$. By the lemma, $M^* \simeq (kG^*)^{\oplus n} \Leftrightarrow M \simeq kG^{\oplus n}$.

(2): Choose a surjection $F \twoheadrightarrow M^*$ with F free. Dualizing we get $M \hookrightarrow F^*$. But F^* is free by (1).

(3): If $M \oplus N$ is free then, by (1), so is its dual $M^* \oplus N^*$. This proves the 'only if' part, applying which we get: M^{**} is projective if M^* is so. But $M^{**} \simeq M$ naturally, which proves the 'if' part too. □ [c:injective]

Corollary 12.13. *The following conditions are equivalent for a kG-module I. A projective module satisfies these conditions and any module satisfying these conditions is projective.*

(1) *Any short exact sequence of A-modules $0 \to I \to M \to N \to 0$ splits.*
(2) *The functor $M \mapsto \operatorname{Hom}_A(M, I)$ is exact.*
(3) *If $\varphi : L \to M$ is a injection of A-modules and $\vartheta : L \to I$ any A-module map, then there exists an extension $\tilde{\vartheta} : M \to I$ of ϑ, i,e., $\tilde{\vartheta}\varphi = \vartheta$.*

Proof. (3) $\Rightarrow$ (2): Let $0 \to L \to M \to N \to 0$ be exact. Then $0 \to \operatorname{Hom}_A(N, I) \to \operatorname{Hom}_A(M, I) \to \operatorname{Hom}_A(L, I)$ is exact in general. Since (3) holds the last map is also onto.

(2) $\Rightarrow$ (1): $0 \to \operatorname{Hom}_A(N, I) \to \operatorname{Hom}_A(M, I) \to \operatorname{Hom}_A(I, I) \to 0$ is exact. But this means that $\operatorname{Hom}_A(M, I) \to \operatorname{Hom}_A(I, I)$ is onto. If $\varphi : M \to I$ is a preimage of the identity morphism on I, then φ is a splitting.

(1) $\Rightarrow$ I is projective: By item (2) of the previous Corollary 12.12, we can choose $I \hookrightarrow F$ with F free. Since this splits, I is a direct summand of F, and so projective.

I is projective $\Rightarrow$ (3): By (3) of the previous Corollary 12.12, I^* is projective. Dualizing φ and ϑ, we get $\varphi^* : L^* \leftarrow M^*$ a surjection and $\vartheta^* : L^* \leftarrow I^*$. Since I^* is projective, there exist $\tilde{\vartheta^*} : M^* \leftarrow I^*$ such that $\varphi^*\tilde{\vartheta^*} = \vartheta^*$. The dual $\tilde{\vartheta^*}^*$ of $\tilde{\vartheta^*}$ has the desired property. □

[sss:form] 12.6.1. The bilinear form. On kG we have a bilinear form: for g, h in G we define (g,h) to be 1 if $gh=1$ and 0 otherwise. This form is *symmetric*, i.e., $(a,b)=(b,a)$ (for, clearly, $(g,h)=(h,g)$), and *associative*, i.e., $(a,bc)=(ab,c)$ (for, clearly $(g,hk)=(gh,k)$).

Another description of the form is as follows: (a,b) is the coefficient of the identity element of G when the product ab is expressed as a linear combination of elements of G with coefficients in k. The symmetry of the form now says that this coefficient is the same for ab and ba.

As a corollary of the existence of this form, we have:

[p:form]

Proposition 12.14. *Let $\mathfrak{r}$ be a right ideal and a an element of the group ring kG. If $\mathfrak{r}a=0$, then $a\mathfrak{r}=0$.*

Proof. Suppose that $ar\neq 0$ for some $r\in\mathfrak{r}$. Then $ar=\sum\alpha_g g$ with $\alpha_g\neq 0$ for some g in G. Then $(a,rg^{-1})\neq 0$, and by symmetry $(rg^{-1},a)\neq 0$. But, on the other hand, $rg^{-1}a$ belongs to $\mathfrak{r}a$ and is therefore 0. □

[t:pimradsoc]

Theorem 12.15. *For P a PIM for kG, we have $P/\mathfrak{Rad}\,P\simeq\operatorname{soc}P$.*

Proof. Set $S:=P/\mathfrak{Rad}\,P$, $T:=\operatorname{soc}P$, and assume, by way of contradiction, that $S\not\simeq T$. We know that S is simple (Theorem 12.7 (1)), and so is T (see the itemized list at the beginning of this subsection).

Let $\mathfrak{s}$ be the S-isotypic component of $\operatorname{soc}kG$. Decomposing kG into indecomposables, write $kG=Q\oplus R$, where Q is the sum of all PIMs isomorphic to P, and R the sum of the rest. We make some observations about $\mathfrak{s}$ and its relation to Q and R. Given the observations, it will be easy to derive a contradiction using Proposition 12.14.

- $\mathfrak{s}\neq 0$: Indeed, S occurs as the socle of some PIM: see (5) of the itemized list at the beginning of this subsection.[13]
- $\mathfrak{s}$ is a two sided ideal: Indeed, it is a characteristic left ideal of kG.
- $\mathfrak{s}\subseteq R$: Indeed, $\operatorname{soc}kG=\operatorname{soc}Q\oplus\operatorname{soc}R$, and $\operatorname{soc}Q$ is isotypic of type T.
- $\mathfrak{s}Q=0$: Indeed, on the one hand, by the previous two observations, $\mathfrak{s}Q\subseteq\mathfrak{s}\subseteq R$; on the other, $\mathfrak{s}Q\subseteq Q$ since Q is a left ideal. But $Q\cap R=0$.
- $R\mathfrak{s}=0$: Indeed, kG-endomporphisms of kG with images in $\mathfrak{s}$ are precisely right multiplications by elements of $\mathfrak{s}$. Any such endomorphism restricted to R factors through $R/\mathfrak{Rad}\,R$ (since $\mathfrak{s}$ is semisimple), but the S-length of $R/\mathfrak{Rad}\,R$ is 0 (for P is the only PIM such that $P/\mathfrak{Rad}\,P\simeq S$).

Now, Proposition 12.14 together with the fact $\mathfrak{s}Q=0$ yields $Q\mathfrak{s}=0$. In turn, this together with the fact $R\mathfrak{s}=0$ yields $\mathfrak{s}=(kG)\mathfrak{s}=(Q+R)\mathfrak{s}=0$, a contradiction. □

[ss:tensor]

12.7. **Tensor Products.** As in §12.6 we take $A=kG$ throughout this subsection. The tensor product (over k) of two kG-modules is defined: $g(v\otimes w):=gv\otimes gw$. The standard natural isomorphisms as k-vector spaces hold also as kG-modules: e.g., $U\otimes(V\otimes W)=(U\otimes V)\otimes W$. Some of these, e.g., $\operatorname{Hom}(V,W)\simeq V^*\otimes W$, require the assumption that V is finite dimensional over k, which anyway we are imposing blanketly.

[13] In fact, although we don't need this stronger statement for the proof, the length of $\mathfrak{s}$ equals $\dim S$: see (7) of the itemized list at the beginning of this subsection.

A kG-module V is *G-faithful* if the defining group homomorphism $G \to \mathrm{GL}_k V$ is an injection. (Caution: The algebra map $kG \to \mathrm{End}_k(V)$ could have non-trivial kernel for a G-faithful V.)

[t:galois]

Theorem 12.16. *Let V be a G-faithful kG-module. Then given a PIM P there exists an n such that P occurs as an indecomposable component of $V^{\otimes n}$.*

Proof. Let $k[V]$ denote the symmetric algebra of V. Its graded components $k[V]_j$ are kG-modules. We claim that there is a copy of the left regular representation kG in $\sum_{0\leq j\leq d} k[V]_j$ for d large enough. Let us first finish the proof of the theorem assuming the claim.

Since $P \subseteq kG$, we have $P \subseteq \sum_{0\leq j\leq d} k[V]_j$. Since P is 'injective' (see Corollary 12.13), it follows that P is a direct summand of $\sum_{0\leq j\leq d} k[V]_j$. By Krull-Remak-Schmidt, P occurs an indecomposable summand of $k[V]_j$ for some j, $0 \leq j \leq d$. Since $k[V]_j$ is a quotient of $V^{\otimes n}$, it follows that $V^{\otimes n}$ surjects onto P. Since P is projective, it follows that P is a direct summand of $V^{\otimes n}$, proving the theorem.

It remains therefore only to prove the claim. Consider the quotient field $k(V)$ of $k[V]$. The group G acts on $k(V)$ by field automorphisms. Let F denote the fixed field: $F := \{f \in k(V) \mid {}^g f = f \ \forall\ g \in G\}$. The extension $F \subseteq k(V)$ is Galois with Galois group G. By the normal basis theorem, there exists an element f in $k(V)$ such that its orbit under G forms a basis of $k(V)$ over F. Writing $f = p/q$ with p, q in $k[V]$ and taking $f' = f \cdot \prod_{g\in G} {}^g q$, we see that the orbit under G of f' too forms a basis for $k(V)$ over F.

$\square$ [ex:lrtwo]

12.8. **Exercises.** Our blanket assumptions about k, A, and A-modules are in force (unless explicitly relaxed).

12.8.1. Prove or disprove: any quotient of an indecomposable module is indecomposable.

[sss:simproj]

12.8.2. Let S be a simple A-module and P the corresponding PIM. For any A-module M, the multiplicity of S in a composition series of M equals the dimension (as a k-vector space) of $\mathrm{Hom}_A(P, M)$.

[sss:pformcounter]

12.8.3. Show by means of an example that Proposition 12.14 does not hold in general for a finite dimensional algebra over k.

12.8.4. Let P be a projective A-module. Set $M := P/\mathfrak{Rad}\, P$. Then the following are equivalent:

(1) M is simple.
(2) M is indecomposable.
(3) P is indecomposable.