

## 9. Changing the ground ring: splitting fields and the decomposition map

Suppose that  $A$  is an algebra  $A$  over a commutative ring  $R$  and that  $U$  is an  $A$ -module. If  $R \rightarrow S$  is a homomorphism to another commutative ring  $S$  we may form the  $S$ -algebra  $S \otimes_R A$ , and now  $S \otimes_R U$  becomes an  $S \otimes_R A$ -module in an evident way. In this section we study the relationship between  $U$  and  $S \otimes_R U$ . When we specialize to a group algebra  $A = RG$  we will identify  $S \otimes_R RG$  with  $SG$ .

We will pay special attention to two particular cases of this construction, the first being when  $R$  is a subring of  $S$ . If  $U$  is an  $A$ -module, we say that the module  $V = S \otimes_R U$  is obtained from  $U$  by *extending the scalars from  $R$  to  $S$* ; and if an  $S \otimes_R A$ -module  $V$  has the form  $S \otimes_R U$  we say it can be *written in  $R$* . In this situation, when  $U$  is free as an  $R$ -module we may identify  $U$  with the subset  $1_S \otimes_R U$  of  $S \otimes_R U$ , and an  $R$ -basis of  $U$  becomes an  $S$ -basis of  $S \otimes_R U$  under this identification. In case  $A = RG$  is a group ring, with respect to such a basis of  $V = S \otimes_R U$  the matrices which represent the action of elements  $g \in G$  on  $V$  have entries in  $R$ , and are the same as the matrices representing the action of these elements on  $U$  (with respect to the basis of  $U$ ). Equally, if we can find a basis for an  $SG$ -module  $V$  so that each  $g \in G$  acts by a matrix with elements in  $R$  then  $RG$  preserves the  $R$ -linear span of this basis, and this  $R$ -linear span is an  $RG$ -module  $U$  for which  $V = S \otimes_R U$ . Thus an  $S$ -free module  $V$  can be written in  $R$  if and only if  $V$  has an  $S$ -basis with respect to which  $G$  acts via matrices with entries in  $R$ .

The second situation to which we will pay particular attention arises when  $S = R/I$  for some ideal  $I$  in  $R$ . In this case applying  $S \otimes_R \_$  to a module  $U$  is the same as reducing  $U$  modulo  $I$ . If  $V$  is an  $S \otimes_R A$ -module of the form  $S \otimes_R U$  for some  $A$ -module  $U$  we say that  $V$  can be *lifted* to  $U$ , and that  $U$  is a *lift* of  $V$ . Most often we will perform this construction when  $R$  is a local ring and  $I$  is the maximal ideal of  $R$ .

We start by considering the behaviour of representations over a field. It is often a help to know that a representation can be written in a small field.

(9.1) PROPOSITION. *Let  $F \subseteq E$  be fields where  $E$  is algebraic over  $F$  and let  $A$  be a finite-dimensional  $F$ -algebra. Let  $V$  be a finite-dimensional  $E \otimes_F A$ -module. Then there exists a field  $K$  with  $F \subseteq K \subseteq E$ , of finite degree over  $F$ , so that  $V$  can be written in  $K$ .*

*Proof.* Let  $a^1, \dots, a^n$  be a basis for  $A$  and let  $a^t$  act on  $V$  with matrix  $(a_{ij}^t)$  with respect to some basis of  $V$ . Let  $K = F[a_{ij}^t, 1 \leq t \leq n, 1 \leq i, j \leq d]$ . Then  $[K : F]$  is finite since  $K$  is an extension of  $F$  by finitely many algebraic elements, and  $A$  acts by matrices with entries in  $K$ . □

Let  $A$  be a finite-dimensional  $F$ -algebra, where  $F$  is a field. A simple  $A$ -module  $U$  is said to be *absolutely simple* if and only if  $E \otimes_F U$  is a simple  $E \otimes_F A$ -module for all extension fields  $E$  of  $F$ . We say that  $E$  is a *splitting field* for  $A$  if and only if every simple  $E \otimes_F A$ -module is absolutely simple. If  $A$  is a group algebra, we say that  $E$  is a splitting field for  $G$ , by extension of the terminology.

The kind of phenomenon which these definitions are designed to address is exemplified by cyclic groups. If  $G = \langle g \rangle$  is cyclic of order  $n$  then  $g$  acts on  $\mathbb{C}G$  as a direct sum of 1-dimensional eigenspaces with eigenvalues  $e^{\frac{2\pi i}{n}}$ . Since these lie outside  $\mathbb{Q}$  (if  $n \geq 3$ ), the regular representation of  $\mathbb{Q}G$  is a direct sum of simple modules but some of them have dimension greater than 1. On extending scalars to a field containing  $e^{\frac{2\pi i}{n}}$  these simple modules decompose as direct sums of 1-dimensional modules. Thus  $\mathbb{Q}$  is not a splitting field for  $G$ , but any field containing  $\mathbb{Q}(e^{\frac{2\pi i}{n}})$  is a splitting field since the simple modules are now 1-dimensional and remain simple on extension of scalars.

We will use several times the fact that if we let  $F$  be any field, then  $F$  is a splitting field for the matrix algebra  $M_n(F)$ . In fact, if  $E \supseteq F$  is a field extension then  $E \otimes_F M_n(F) \cong M_n(E)$ , an isomorphism which is most easily seen by observing that  $M_n(F)$  has a basis consisting of the matrices  $E_{ij}$  which are non-zero only in position  $(i, j)$ , where the entry is 1. Thus  $E \otimes_F M_n(F)$  has a basis consisting of the elements  $1 \otimes_F E_{ij}$ . Since these multiply together in the same fashion as the corresponding basis elements of  $M_n(E)$  we obtain the claimed isomorphism. Every simple  $M_n(F)$ -module is isomorphic to the module of column vectors of length  $n$  over  $F$ , and on extending the scalars to  $E$  we obtain column vectors of length  $n$  over  $E$ , which is a simple module for  $E \otimes_F M_n(F)$ .

As another example, the prime field  $F_p$  is a splitting field for every  $p$ -group, since the only simple  $F_p G$ -module here is  $F_p$ , which is absolutely simple.

(9.2) PROPOSITION. *Let  $U$  be a simple module for a finite-dimensional algebra  $A$  over a field  $F$ . The following are equivalent.*

- (1)  $U$  is absolutely simple.
- (2)  $\text{End}_A(U) = F$ .
- (3) The matrix algebra summand of  $A/\text{Rad } A$  corresponding to  $U$  is  $M_n(F)$ , where  $n = \dim U$ .

*Proof.* (2)  $\Rightarrow$  (3): If the matrix summand of  $A/\text{Rad } A$  corresponding to  $U$  is  $M_n(D)$  for some division ring  $D$  then  $D = \text{End}_A(U)$ . The hypothesis is that  $D = F$  so the matrix summand is  $M_n(F)$  and since  $U$  identifies as column vectors of length  $n$  we have  $n = \dim U$ .

(3)  $\Rightarrow$  (1): The hypothesis is that  $A$  acts on  $U$  via a surjective ring homomorphism  $A \rightarrow M_n(F)$  where  $U$  is identified as  $F^n$ . Now if  $E \supseteq F$  is an extension field then  $E \otimes A$  acts on  $E \otimes U = E^n$  via the homomorphism  $E \otimes A \rightarrow E \otimes M_n(F) \cong M_n(E)$ , which is also surjective. Since  $E^n$  is a simple  $M_n(E)$ -module it follows that  $E \otimes_F U$  is a simple  $E \otimes_F A$ -module.

(1)  $\Rightarrow$  (2): We prove this implication here only in the situation where  $F$  is a perfect field, so that all irreducible polynomials with coefficients in  $F$  are separable. The result is true in general and is not difficult but requires some technicality which we wish to avoid (see [CR]). This implication will not be needed for our application of the result.

Suppose that  $\text{End}_A(U)$  is larger than  $F$ , so there exists an endomorphism  $\phi : U \rightarrow U$  which is not scalar multiplication by an element of  $F$ . Let  $\alpha$  be a root of the characteristic polynomial of  $\phi$  in some field extension  $E \supseteq F$ : in other words,  $\alpha$  is an eigenvalue of  $\phi$ . Then  $1_E \otimes \phi : E \otimes_F U \rightarrow E \otimes_F U$  is not scalar multiplication by  $\alpha$ , because if it were the minimal polynomial of  $\alpha$  over  $F$  would be a factor of  $(X - \alpha)^n$  where  $n = \dim_F U$  and by separability of the minimal polynomial we would deduce  $\alpha \in F$ . Now  $1_E \otimes \phi - \alpha \otimes 1_U \in \text{End}_{E \otimes A}(E \otimes_F U)$  is a non-zero endomorphism with non-zero kernel, and since  $E \otimes_F U$  is simple this cannot happen, by Schur's lemma.  $\square$

(9.3) COROLLARY. *Let  $A$  be a finite-dimensional algebra over a field  $F$ . Then  $A$  has a splitting field of finite degree over  $F$ .*

*Proof.* The algebraic closure  $\overline{F}$  of  $F$  is a splitting field for  $A$ , since by Schur's lemma condition (2) of Proposition 9.2 is satisfied for each simple  $\overline{F} \otimes_F A$ -module. By Proposition 9.1 there is a finite extension  $E \supseteq F$  so that every simple  $\overline{F} \otimes_F A$ -module can be written in  $E$ . The simple  $E \otimes_F A$ -modules  $U$  which arise like this are absolutely simple, because if  $K \supseteq F$  is an extension field for which  $K \otimes_F U$  is not simple then  $\overline{K} \otimes_F U$  is not simple, where  $\overline{K}$  is an algebraic closure of  $K$ , and since  $\overline{K}$  contains a copy of  $\overline{F}$ ,  $\overline{F} \otimes_F U$  cannot be simple since  $\overline{F}$  is a splitting field for  $A$ , a contradiction.

Finally, every simple  $E \otimes_F A$ -module is isomorphic to one of the simple modules  $U$  which arise in this way. For, if  $V$  is a simple  $E \otimes_F A$ -module let  $e^2 = e \in E \otimes_F A$  be an idempotent with the property that  $eV \neq 0$  but  $eV' = 0$  for all simple modules  $V'$  not isomorphic to  $V$ . Let  $W$  be a simple  $\overline{F} \otimes_F A$ -module which is not annihilated by  $e$ . We must have  $W \cong \overline{F} \otimes_F V$  since  $V$  is the only possible simple module which would give a result not annihilated by  $e$ .  $\square$

In the case of group algebras there is a finer result which was first conjectured by Schur and later proved by Brauer as a deduction from Brauer's induction theorem. We state the result, but will not use it and do not prove it. The *exponent* of a group  $G$  is the least common multiple of the orders of its elements.

(9.4) THEOREM (Brauer). *Let  $G$  be a finite group,  $F$  a field, and suppose that  $F$  contains a primitive  $m$ th root of unity, where  $m$  is the exponent of  $G$ . Then  $F$  is a splitting field for  $G$ .*

This theorem tells us that  $\mathbb{Q}(e^{\frac{2\pi i}{m}})$  and  $\mathbb{F}_p(\zeta)$  are splitting fields for  $G$ , where  $\zeta$  is a primitive  $m$ th root of unity in an extension of  $\mathbb{F}_p$ . Often smaller splitting fields than these

can be found, and the determination of minimal splitting fields must be done on a case-by-case basis. For example, we may see as a result of the calculations we have performed earlier in this text that in every characteristic the prime field is a splitting field for  $S_3$  — the same is in fact true for all the symmetric groups. However, if we require that a field be a splitting field not only for  $G$  but also for all of its subgroups, then  $\mathbb{Q}(e^{\frac{2\pi i}{m}})$  and  $\mathbb{F}_p(\zeta)$  are the smallest possibilities, since as we have seen earlier a cyclic group of order  $n$  requires the presence of a primitive  $n$ th root of 1 in a splitting field.

The reason for working with a splitting field is to get a complete picture of the composition factors of each module. When working with group representations in characteristic zero, if we did not take a splitting field the character table would not be square. When we do have a splitting field in characteristic zero, semisimplicity implies that knowing the behaviour of the simple modules tells us about all modules. In positive characteristic the situation is not so straightforward. Knowing that the simple modules do not break up further under extension of scalars implies the same thing for the indecomposable projective modules, and the Cartan matrix does not change. More specifically, if  $F$  is a splitting field for an algebra  $A$  and  $P$  is an indecomposable projective  $A$ -module then for every field extension  $E \supseteq F$  the  $E \otimes_F A$ -module  $E \otimes_F P$  remains indecomposable and projective, and if  $S$  is the simple quotient of  $P$  then  $E \otimes_F S$  is the simple quotient of  $E \otimes_F P$ . These statements appear in the exercises to this section.

An indecomposable  $A$ -module  $U$  which remains indecomposable under all field extensions  $E \supseteq F$  is termed *absolutely indecomposable*. In general if the ground field  $F$  is not algebraically closed we can expect that there will be indecomposable  $A$ -modules which are not absolutely indecomposable, even though  $F$  may be a splitting field.

We will not use it, but it is important to know that the statement of the following theorem is true. For a proof see [CRI, p. 139].

(9.5) THEOREM (Noether-Deuring). *Let  $A$  be a finite-dimensional algebra over a field  $F$  and let  $E \supseteq F$  be a field extension. Suppose that  $U$  and  $V$  are  $A$ -modules for which  $E \otimes_F U \cong E \otimes_F V$  as  $E \otimes_F A$ -modules. Then  $U \cong V$  as  $A$ -modules.*

Our next aim is to show that over a splitting field of characteristic  $p$ , the number of non-isomorphic simple representations of a group  $G$  equals the number of conjugacy classes of  $p$ -regular elements. Several proofs of this result are available, the first appearing in a paper of Brauer from 1932. The proof we shall present is also due to Brauer, coming from 1956. This proof is appealing because it is technically elementary, and could have appeared earlier in this text once we knew that the radical of a finite-dimensional algebra is nilpotent.

We start with some lemmas. These have to do with a finite-dimensional algebra  $A$  over a field of characteristic  $p$ , and we will write

$$S = \text{linear span in } A \text{ of } \{ab - ba \mid a, b \in A\}$$

$$T = \{r \in A \mid r^{p^n} \in S \text{ for some } n > 0\}.$$

(9.6) LEMMA.  $T$  is a linear subspace of  $A$  containing  $S$ .

*Proof.* Since  $ab \equiv ba \pmod{S}$  we have

$$(a + b)^p \equiv a^p + pa^{p-1}b + \cdots + b^p \equiv a^p + b^p \pmod{S}$$

and so if  $a^{p^n} \in S$ ,  $b^{p^m} \in S$  with  $m \geq n$  then

$$(\lambda a + \mu b)^{p^m} \equiv \lambda^{p^m} a^{p^m} + \mu^{p^m} b^{p^m} \equiv 0 \pmod{S}.$$

To show that  $S \subseteq T$  we show that  $(ab - ba)^p \in S$ . Now

$$(ab - ba)^p \equiv (ab)^p - (ba)^p \equiv a^p b^p - b^p a^p \equiv 0 \pmod{S}.$$

□

(9.7) LEMMA. If  $A = M_n(F)$  is a matrix algebra where  $F$  is a field then  $S = T =$  matrices of trace zero.

*Proof.* Since  $\text{tr}(ab - ba) = 0$  we see that  $S$  is a subset of the matrices of trace zero. On the other hand when  $i \neq j$  every matrix  $E_{ij}$  (zero everywhere except for a 1 in position  $(i, j)$ ) can be written as a commutator:  $E_{ij} = E_{ik}E_{kj} - E_{kj}E_{ik}$ , and also  $E_{ii} - E_{jj} = E_{ij}E_{ji} - E_{ji}E_{ij}$ . Since these matrices span the matrices of trace zero we deduce that  $S$  consists exactly of the matrices of trace 0. Now  $S \subseteq T \subseteq A$  and  $S$  has codimension 1 so either  $T = S$  or  $T = A$ . The matrix  $E_{11}$  is idempotent and does not lie in  $T$ , so  $T = S$ . □

(9.8) PROPOSITION. Let  $A$  be a finite-dimensional algebra over a field of characteristic  $p$  which is a splitting field for  $A$ . The number of non-isomorphic simple representations of  $A$  equals the codimension of  $T$  in  $A$ .

*Proof.* Let us write  $T(A)$ ,  $S(A)$ ,  $T(A/\text{Rad}(A))$ ,  $S(A/\text{Rad}(A))$  for the constructions  $S, T$  applied to  $A$  and  $A/\text{Rad}(A)$ . Since  $\text{Rad}(A)$  is nilpotent it is contained in  $T(A)$ . Also

$$(S(A) + \text{Rad}(A))/\text{Rad}(A) = S(A/\text{Rad}(A))$$

is easily verified. We claim that  $T(A)/\text{Rad}(A) = T(A/\text{Rad}(A))$ . For, if  $a^{p^n} \in S$  then  $(a + \text{Rad}(A))^{p^n} \in S + \text{Rad}(A)$  and this shows that the left-hand side is contained in the right. Conversely, if  $(a + \text{Rad}(A))^{p^n} \in S(A/\text{Rad}(A))$  then  $a^{p^n} \in S(A) + \text{Rad}(A) \subseteq T(A)$  so  $T(A/\text{Rad}(A)) \subseteq T(A)/\text{Rad}(A)$ .

Now  $A/\text{Rad}(A)$  is a direct sum of matrix algebras. It is apparent that both  $S$  and  $T$  preserve direct sums, so the codimension of  $T(A/\text{Rad}(A))$  in  $A/\text{Rad}(A)$  equals the number of simple  $A$ -modules, and this equals the codimension of  $T(A)$  in  $A$ . □

Let  $p$  be a prime. An element in a finite group is said to be  $p$ -regular if it has order prime to  $p$ , and  $p$ -singular if it has order a power of  $p$ . The only element which is both  $p$ -regular and  $p$ -singular is the identity.

(9.9) LEMMA. *Let  $G$  be a finite group and  $p$  a prime. Each element  $x \in G$  can be uniquely written  $x = st$  where  $s$  is  $p$ -regular,  $t$  is  $p$ -singular and  $st = ts$ . If  $x_1 = s_1t_1$  is such a decomposition of an element  $x_1$  which is conjugate to  $x$  then  $s$  is conjugate to  $s_1$ , and  $t$  is conjugate to  $t_1$ .*

*Proof.* If  $x$  has order  $n = \alpha\beta$  where  $\alpha$  is a power of  $p$  and  $\beta$  is prime to  $p$  then we may take  $s = x^\alpha$  and  $t = x^\beta$ . If  $x = st = s_1t_1$  is a second such decomposition then  $s_1$  commutes with  $x$  and hence commutes with  $s$  and  $t$  which are powers of  $x$ . Similarly  $t_1$  commutes with  $s$  and  $t$ . Thus  $s_1^{-1}s = t_1t^{-1}$  and now  $s_1^{-1}s$  is  $p$ -regular and  $t_1t^{-1}$  is  $p$ -singular, so these products equal 1, and  $s_1 = s$ ,  $t_1 = t$ . If  $x_1 = gxg^{-1}$  then  $x_1 = gsg^{-1}gtg^{-1}$  is a decomposition of  $x_1$  as a product of commuting  $p$ -regular and  $p$ -singular elements. Hence  $s_1 = gsg^{-1}$  and  $t_1 = gtg^{-1}$  by uniqueness of the decomposition.  $\square$

(9.10) LEMMA. *Let  $F$  be a field and  $G$  a group. Then  $S$  is the set of elements of  $FG$  with the property that the sum of coefficients from each conjugacy class of  $G$  is zero.*

*Proof.*  $S$  is spanned by elements  $ab - ba$  with  $a, b \in G$ . Now  $ab - ba = a(ba)a^{-1} - ba$  is the difference of an element and its conjugate. Such elements exactly span the elements of  $FG$  which have coefficient sum zero on conjugacy classes.  $\square$

We come now to the result which is the goal of these lemmas.

(9.11) THEOREM. *Let  $F$  be a splitting field of characteristic  $p$  for a finite group  $G$ . The number of non-isomorphic simple  $FG$  modules equals the number of conjugacy classes of  $p$ -regular elements of  $G$ .*

*Proof.* We know that the number of simple  $FG$  modules equals the codimension of  $T$  in  $FG$ . We show this equals the number of  $p$ -regular conjugacy classes by showing that if  $x_1, \dots, x_r$  is a set of representatives of the conjugacy classes of  $p$ -regular elements of  $G$  then  $x_1 + T, \dots, x_r + T$  is a basis of  $FG/T$ .

If we write  $x = st$  where  $s$  is  $p$ -regular and  $t$  is  $p$ -singular,  $s$  and  $t$  commute, then  $(st - s)^{p^n} = s^{p^n}t^{p^n} - s^{p^n} = s^{p^n} - s^{p^n} = 0$  for sufficiently large  $n$ , so that  $s + T = st + T$ . The elements  $g + T$ ,  $g \in G$  do span  $FG/T$ , and now it follows from the last observation that we may throw out all except the  $p$ -regular elements and still have a spanning set. We show that the set which remains is linearly independent.

Suppose that  $\sum \lambda_i x_i \in T$ . Then  $(\sum \lambda_i x_i)^{p^n} = \sum \lambda_i^{p^n} x_i^{p^n} \in S$  for sufficiently high  $p^n$ , and there is always a sufficiently large  $n$  so that  $x_i^{p^n} = x_i$  for all  $i$ , since the  $x_i$  are  $p$ -regular. Now  $\sum \lambda_i^{p^n} x_i \in S$ . But  $x_1, \dots, x_r$  are independent modulo  $S$  by Lemma 9.10

so  $\lambda_i^{p^n} = 0$  for all  $i$ , and hence  $\lambda_i = 0$  for all  $i$ . This shows that  $x_1 + T, \dots, x_r + T$  are linearly independent.  $\square$

### Reduction modulo $p$ and the decomposition map

We turn now to the theory of reducing modules from characteristic zero to characteristic  $p$ , for some prime  $p$ , a theory developed principally by Richard Brauer. There is inherent interest in studying the relationships between representations in different characteristics, but apart from this we will obtain a remarkable way to compute the Cartan matrix of a group algebra, as well as a second proof of its symmetry. After that we use it in a study of characters whose degree is divisible by the order of a Sylow  $p$ -subgroup of  $G$ , and in the next section it will be used in a proof that the Cartan matrix is non-singular.

There will be three rings in the set-up for reducing modules to characteristic  $p$ , and we list them as a triple  $(F, R, k)$ . Here  $F$  is a field of characteristic zero equipped with a discrete valuation,  $R$  is the valuation ring in  $F$  with maximal ideal  $(\pi)$ , and  $k = R/(\pi)$  is the residue field of  $R$ , which is required to have characteristic  $p$ . Such a triple is called a  *$p$ -modular system*. Given a finite group  $G$ , if both  $F$  and  $k$  are splitting fields for  $G$  we say that the triple is a *splitting  $p$ -modular system* for  $G$ . If we require that  $F$  contains a primitive  $m$ th root of unity (where  $m$  is the exponent of  $G$ ) then necessarily  $R$  and  $k$  also contain primitive  $m$ th roots of unity and according to Brauer's theorem both  $F$  and  $k$  are splitting fields. Without using Brauer's theorem we may still deduce from 9.3 the existence of splitting  $p$ -modular systems where  $F$  is a number field (a finite extension of  $\mathbb{Q}$ ), and  $k$  is a finite field.

We investigate some basic properties of representations of a finite group over a discrete valuation ring  $R$ . We comment that in this result and the next few results nothing specific to group representations is used, except that the group algebra of  $G$  is semisimple over a field of characteristic zero. The theory can be developed in the context of representations of an order in a finite-dimensional algebra, but this is a generality we do not pursue here.

(9.12) PROPOSITION. *Let  $R$  be a discrete valuation ring with maximal ideal  $(\pi)$  and residue field  $k = R/(\pi)$ . Let  $G$  be a finite group.*

- (1) *If  $S$  is a simple  $RG$ -module then  $\pi S = 0$ .*
- (2) *The simple  $RG$ -modules are exactly the simple  $kG$ -modules made into  $RG$ -modules via the surjection  $RG \rightarrow kG$ .*
- (3) *For each  $RG$ -module  $U$ ,  $\pi U \subseteq \text{Rad}(U)$ , and in particular  $(\pi)G \subseteq \text{Rad}(RG)$ .*
- (4) *For each  $RG$ -module  $U$  we have  $(\text{Rad } U)/\pi U = \text{Rad}(U/\pi U)$ .*

*Proof.* (1)  $\pi S$  is an  $RG$ -submodule of  $S$ , so  $\pi S = S$  or  $0$ . Since  $\text{Rad } R = (\pi)$  the  $R$ -module homomorphism  $S \rightarrow S/\pi S$  is essential by Nakayama's lemma, so that  $\pi S \neq S$ . Therefore  $\pi S = 0$ .

(2) This follows from (1) since  $kG = RG/(\pi)G$  and  $(\pi)G$  annihilates the simple  $RG$ -modules.

(3) This again follows from (1) since if  $V$  is a maximal submodule of  $U$  then  $U/V$  is simple so that  $\pi U \subseteq V$ , and it follows that  $\pi U$  is contained in all of the maximal submodules of  $U$  and hence in their intersection.

(4)  $\text{Rad } U$  is the intersection of kernels of all the homomorphisms from  $U$  to simple modules. These homomorphisms all factor through the quotient homomorphism  $U \rightarrow U/\pi U$ , and so  $\text{Rad } U$  is the preimage in  $U$  of the radical of  $U/\pi U$ , which is the statement we have to prove.  $\square$

(9.13) COROLLARY. *Let  $R$  be a discrete valuation ring with maximal ideal  $(\pi)$  and residue field  $k = R/(\pi)$ . Let  $G$  be a finite group. Let  $P$  and  $Q$  be projective  $RG$ -modules. Then  $P \cong Q$  as  $RG$ -modules if and only if  $P/\pi P \cong Q/\pi Q$  as  $kG$ -modules.*

*Proof.* If  $P/\pi P \cong Q/\pi Q$  as  $kG$ -modules then by 9.12 the radical quotients of  $P$  and  $Q$  are isomorphic,  $P/\text{Rad } P \cong Q/\text{Rad } Q$ . Now  $P$  and  $Q$  are projective covers of their radical quotients, by Nakayama's lemma, so  $P \cong Q$  by uniqueness of projective covers. The converse implication is trivial.  $\square$

In the next pair of results we see that some important properties of idempotents and projective modules which we have already studied in the case of representations over a field, continue to hold when we work over a complete discrete valuation ring. It is a crucial hypothesis that the discrete valuation ring be complete. The idea of the proofs is the same as for the corresponding results over a field.

(9.14) PROPOSITION. *Let  $R$  be a complete discrete valuation ring with maximal ideal  $(\pi)$  and residue field  $k = R/(\pi)$ . Let  $G$  be a finite group. Every expression  $1 = e_1 + \cdots + e_n$  as a sum of orthogonal idempotents in  $kG$  can be lifted to an expression  $1 = \hat{e}_1 + \cdots + \hat{e}_n$  in  $RG$ , where the  $\hat{e}_i \in RG$  are orthogonal idempotents with  $\hat{e}_i + (\pi) \cdot RG = e_i$ . Each idempotent  $e_i$  is primitive if and only if its lift  $\hat{e}_i$  is primitive.*

*Proof.* The proof is very like the proofs of 7.10, 7.11 and 7.12. We start by showing simply that each idempotent  $e \in kG$  can be lifted to an idempotent  $\hat{e} \in RG$ . Consider the surjections of group rings  $(R/(\pi^n))G \rightarrow (R/(\pi^{n-1}))G$  for each  $n \geq 2$ . Here  $(\pi^{n-1})G/(\pi^n)G$  is a nilpotent ideal in  $(R/(\pi^n))G$  and so by Theorem 7.9, any idempotent  $e_{n-1} + (\pi^{n-1})G \in (R/(\pi^{n-1}))G$  can be lifted to an idempotent  $e_n + (\pi^n)G \in (R/(\pi^n))G$ . Starting with an element  $e_1 \in kG$  for which  $e_1 + (\pi)G = e$  we obtain a sequence  $e_1, e_2, \dots$  of elements of  $RG$  which successively lift each other modulo increasing powers of  $(\pi)$ , and so is a Cauchy sequence in  $RG$ . (The metric on  $RG$  comes from the valuation on  $R$  by taking the distance between two elements to be the maximum of the distances in the coordinate places.) This Cauchy sequence represents an element  $\hat{e} \in RG$ , since  $R$  is complete.

Evidently  $\hat{e}$  is idempotent, because it is determined by its images modulo the powers of  $(\pi)$  and these are idempotent. It also lifts  $e$ .

The argument that sums of orthogonal idempotents can be lifted now proceeds by analogy with the proof of 7.11, and the assertion that  $e$  is primitive if and only if  $\hat{e}$  is primitive is proved as in 7.12.  $\square$

(9.15) PROPOSITION. *Let  $R$  be a complete discrete valuation ring with maximal ideal  $(\pi)$  and residue field  $k = R/(\pi)$ . Let  $G$  be a finite group.*

- (1) *For each simple  $RG$ -module  $S$  there is an indecomposable projective  $RG$ -module  $\hat{P}_S = RG\hat{e}_S$  with the property that  $\hat{P}_S/(\pi \cdot \hat{P}_S) \cong P_S$  is the projective cover of  $S$  as a  $kG$ -module. Here  $\hat{e}_S$  is a primitive idempotent in  $RG$  for which  $\hat{e}_S \cdot S \neq 0$ .*
- (2) *The composite homomorphism  $\hat{P}_S \rightarrow P_S \rightarrow S$  is a projective cover of  $S$  as an  $RG$ -module. Furthermore,  $S$  is the unique simple quotient of  $\hat{P}_S$ . Thus  $\hat{P}_S \cong \hat{P}_T$  if and only if  $S \cong T$ .*
- (3) *Every finitely-generated  $RG$  module has a projective cover.*
- (4) *Every finitely-generated indecomposable projective  $RG$ -module is isomorphic to  $\hat{P}_S$  for some simple module  $S$ .*

*Proof.* (1) Let  $e_S \in kG$  be a primitive idempotent for which  $e_S \cdot S \neq 0$  and let  $\hat{e}_S \in RG$  be an idempotent which lifts  $e_S$ , so that  $\hat{e}_S \cdot S = e + S \cdot S \neq 0$ . We define  $\hat{P}_S = RG\hat{e}_S$ . Then  $\hat{P}_S$  is projective, and it is indecomposable since  $\hat{e}_S$  is primitive. Furthermore  $\hat{P}_S/(\pi \cdot \hat{P}_S) = kGe_S$ , and defining this module to be  $P_S$  it is a projective cover of  $S$  as a  $kG$ -module.

(2) Now  $\hat{P}_S/\text{Rad}(\hat{P}_S) \cong P_S/\text{Rad}(P_S)$  by part (4) of 9.12, and this is isomorphic to  $S$ . Thus the composite epimorphism  $\hat{P}_S \rightarrow P_S \rightarrow S$  is essential, by Nakayama's lemma, and it is a projective cover. Since  $S$  is the radical quotient of  $\hat{P}_S$  it is the unique simple quotient of this module. This quotient determines the isomorphism type of  $\hat{P}_S$  by the uniqueness of projective covers.

(3) Let  $U$  be a finitely-generated  $RG$ -module. Then  $U/\text{Rad } U$  is a  $kG$ -module by 9.12, and it is semisimple, so  $U/\text{Rad } U \cong S_1 \oplus \cdots \oplus S_t$  for various simple modules  $S_i$ . Consider the diagram

$$\begin{array}{ccc}
 & \hat{P}_{S_1} \oplus \cdots \oplus \hat{P}_{S_t} & \\
 & \downarrow & \\
 U & \longrightarrow & U/\text{Rad } U
 \end{array}$$

where the vertical arrow is the projective cover of  $S_1 \oplus \cdots \oplus S_t$  as an  $RG$ -module. By projectivity we obtain a homomorphism  $\hat{P}_{S_1} \oplus \cdots \oplus \hat{P}_{S_t} \rightarrow U$  which completes the triangle and it is an essential epimorphism by Proposition 7.7. Thus it is a projective cover.

(4) Let  $P$  be a finitely-generated projective  $RG$ -module. By part (3) it has a projective cover, of the form  $\alpha : \hat{P}_{S_1} \oplus \cdots \oplus \hat{P}_{S_t} \rightarrow P$ . Since  $P$  is projective  $\alpha$  must split, and there is a monomorphism  $\beta : P \rightarrow \hat{P}_{S_1} \oplus \cdots \oplus \hat{P}_{S_t}$  with  $\alpha\beta = 1_P$ . Since  $\alpha$  is an essential

epimorphism  $\beta$  must be an epimorphism also, so it is an isomorphism. If we suppose that  $P$  is indecomposable, then  $t = 1$  and  $P \cong \hat{P}_{S_1}$ .  $\square$

Working over a principal ideal domain  $R$ , an  $RG$ -module  $L$  is called an  $RG$ -lattice if it is finitely-generated and free as an  $R$ -module. In more general contexts an  $RG$ -lattice is merely supposed to be projective as an  $R$ -module, but since projective modules are free over a principal ideal domain we do not need to phrase the definition that way here. We see, for example, that projective  $RG$ -modules are always lattices.

Given an  $RG$ -lattice  $L$  (where  $R$  is a principal ideal domain with field of fractions  $F$ ) we may regard  $L$  as a subset of  $F \otimes_R L$ . Conversely, if  $U$  is an  $FG$ -module, a full  $RG$ -lattice  $L$  in  $U$  is an  $RG$ -lattice  $L \subseteq U$  which has an  $R$  basis which is also an  $F$ -basis of  $U$ . In this situation  $U = FL \cong F \otimes_R L$ . We say also that  $L$  is an  $R$ -form of  $U$ . We will show, after an intermediate lemma, that every finitely-generated  $FG$ -module contains a full  $RG$ -lattice, or in other words that every finitely-generated  $FG$ -module has an  $R$ -form.

(9.16) LEMMA. *Let  $R$  be a principal ideal domain with field of fractions  $F$ , and let  $U$  be a finite-dimensional  $F$ -vector space. Any finitely-generated  $R$ -submodule of  $U$  which contains an  $F$ -basis of  $U$  is a full lattice in  $U$ .*

*Proof.* Let  $L$  be a finitely-generated  $R$ -submodule of  $U$  which contains an  $F$ -basis of  $U$ . Since  $L$  is a finitely-generated torsion-free  $R$ -module,  $L \cong R^n$  for some  $n$ , and it has an  $R$ -basis  $x_1, \dots, x_n$ . Since  $L$  contains an  $F$ -basis of  $U$  it follows that  $x_1, \dots, x_n$  span  $U$  over  $F$ . We show that  $x_1, \dots, x_n$  are independent over  $F$ . Suppose that  $\lambda_1 x_1 + \dots + \lambda_n x_n = 0$  for certain  $\lambda_i \in F$ . We may write  $\lambda_i = \frac{a_i}{b_i}$  where  $a_i, b_i \in R$ , since  $F$  is the field of fractions of  $R$ . Now clearing denominators we have  $(\prod b_i)(\lambda_1 x_1 + \dots + \lambda_n x_n) = 0$  which implies that  $(\prod b_i)\lambda_i = 0$  for each  $i$  since  $x_1, \dots, x_n$  is an  $R$ -basis. This implies that  $\lambda_i = 0$  for all  $i$  and hence that  $n = d$  and  $x_1, \dots, x_n$  is an  $F$ -basis of  $U$ .  $\square$

The kind of phenomenon which the last result is designed to exclude is exemplified by considering subgroups of  $\mathbb{R}$  generated by elements which are independent over  $\mathbb{Q}$ , such as the subgroup  $\langle 1, \sqrt{2} \rangle \cong \mathbb{Z}^2$ . This is a free abelian group, but its basis is not an  $\mathbb{R}$ -basis for  $\mathbb{R}$ . According to the last lemma, such a phenomenon would not occur if  $\mathbb{R}$  were the field of fractions of  $\mathbb{Z}$ ; indeed, the finitely-generated subgroups of  $\mathbb{Q}$  are all cyclic.

(9.17) PROPOSITION. *Let  $(F, R, k)$  be a  $p$ -modular system and  $U$  a finite-dimensional  $FG$ -module. Then  $U$  may be written in  $R$ .*  $\blacksquare$

*Proof.* Let  $u_1, \dots, u_n$  be any basis for  $U$  and let  $U_0$  be the  $R$ -submodule of  $U$  spanned by  $\{gu_i \mid i = 1, \dots, n, g \in G\}$ . This is a finitely-generated  $R$ -submodule of  $U$  which contains an  $F$ -basis of  $U$ . Since  $R$  is a principal ideal domain with field of fractions  $F$ , by the last result  $U_0$  is a full  $RG$ -lattice in  $U$ , which is what we need to prove.  $\square$

The reason we introduce lattices here is that we can reduce them modulo ideals of  $R$ . Given an ideal  $I$  of  $R$  and an  $RG$  lattice  $L$  evidently  $V = L/(I \cdot L)$  is an  $(R/I)G$ -module. We say that  $V$  is the *reduction modulo  $I$*  of the lattice  $L$ , and also that  $L$  is a *lift* from  $R/I$  to  $R$  of  $V$ . Not every  $(R/I)G$ -module need be liftable from  $R/I$  to  $R$ . For example, taking  $R = \mathbb{Z}$  and  $I = (p)$  with  $p \geq 3$ , the group  $GL(2, p)$  has a faithful 2-dimensional representation over  $\mathbb{F}_p$  which cannot be lifted to  $\mathbb{Z}$ , because such a representation would have to be faithful also, and on extending the scalars from  $\mathbb{Z}$  to  $\mathbb{R}$  would provide a 2-dimensional representation over  $\mathbb{R}$ . The only finite subgroups of  $2 \times 2$  real matrices are cyclic and dihedral. On the other hand the 2-dimensional faithful representation of  $GL(2, 2)$  over  $\mathbb{F}_2$  does lift to  $\mathbb{Z}$ .

The following result is crucial to the definition of the decomposition map, which will be given afterwards.

(9.18) THEOREM (Brauer-Nesbitt). *Let  $(F, R, k)$  be a  $p$ -modular system,  $G$  a finite group, and  $U$  a finitely-generated  $FG$ -module. Let  $L_1, L_2$  be full  $RG$ -lattices in  $U$ . Then  $L_1/\pi L_1$  and  $L_2/\pi L_2$  have the same composition factors with the same multiplicities, as  $kG$ -modules.*

*Proof.* We observe first that  $L_1 + L_2$  is also a full  $RG$ -lattice in  $U$ , by Lemma 9.16, so by proving the result first for the pair of lattices  $L_1$  and  $L_1 + L_2$  and then for  $L_2$  and  $L_1 + L_2$  we see that it suffices to consider the case of a pair of lattices, one contained in the other. We now assume that  $L_1 \subseteq L_2$ .

As  $R$ -modules,  $L_1$  and  $L_2$  are free of the same rank, and so  $L_2/L_1$  is a torsion module. Hence  $L_2/L_1$  has a composition series as an  $R$ -module, and hence also as an  $RG$ -module, because every series of  $RG$ -modules can be extended to give a composition series of  $R$ -modules. By working down the terms in a composition series, we see that it suffices to assume that  $L_1$  is a maximal  $RG$ -submodule of  $L_2$ , and we now make this assumption.

Since  $L_2/L_1$  is a simple  $RG$ -module we have  $\pi L_2 \subseteq L_1$ , by 9.12, and we consider the chain of sublattices  $L_2 \supseteq L_1 \supseteq \pi L_2 \supseteq \pi L_1$ . We must show that  $L_2/\pi L_2$  and  $L_1/\pi L_1$  have the same composition factors. The composition factors of  $L_1/\pi L_2$  are common to both  $L_2/\pi L_2$  and  $L_1/\pi L_1$ , and we will complete the proof by showing that  $L_2/L_1 \cong \pi L_2/\pi L_1$ . In fact, the map

$$\begin{aligned} L_2 &\rightarrow \pi L_2/\pi L_1 \\ x &\mapsto \pi x + \pi L_1 \end{aligned}$$

is a surjection with kernel  $L_1$ . □

We should expect that much of the time when  $p \mid |G|$  an  $FG$ -module  $U$  will contain non-isomorphic full sublattices. For example, if  $P$  is an indecomposable projective  $kG$ -module,  $F \otimes_R \hat{P}$  is very often not a simple module. Writing  $F \otimes_R P = S_1 \oplus \cdots \oplus S_t$  as a sum of simple modules and taking a full  $RG$ -lattice in each  $S_i$ , the direct sum of these lattices is not isomorphic to  $\hat{P}$ , since  $\hat{P}$  is indecomposable.

More concretely, consider a cyclic group  $G = \langle g \rangle$  of order 2 and let  $(F, R, k)$  be a 2-modular system. The regular representation  $FG$  contains the full lattice  $R \cdot 1 + R \cdot g$  which is indecomposable since its reduction  $kG$  is indecomposable. It also contains the full lattice  $R(1 + g) + R(1 - g)$ , which is a direct sum of  $RG$ -modules and hence is decomposable.

We now define the decomposition matrix for a group  $G$  in characteristic  $p$ . Suppose that  $(F, R, k)$  is a splitting  $p$ -modular system for  $G$ . The *decomposition matrix*  $D$  is the matrix with rows indexed by the simple  $FG$ -modules and columns indexed by the simple  $kG$ -modules whose entries are the numbers

$$d_{TS} = \text{multiplicity of } S \text{ as a composition factor of } L/\pi L$$

where  $S$  is a simple  $kG$ -module,  $T$  is a simple  $FG$ -module and  $L$  is a full  $RG$ -lattice in  $T$ . We note that it is possible to make the definition of a decomposition matrix without the assumption that the  $p$ -modular system should be splitting, but this is not usual.

*Examples.* 1. The decomposition matrices for  $S_3$  in characteristic 2 and characteristic 3 are:

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

2. When  $G$  is a  $p$ -group and  $k$  has characteristic  $p$ , the decomposition matrix has a single column and an entry for each ordinary simple character, that entry being the degree of the character.

3. The third example is sufficiently important that we state it as a separate result. This is the situation where both  $FG$ -modules and  $kG$ -modules are semisimple.

(9.19) THEOREM. *Let  $G$  be a group of order prime to  $p$  and let  $(F, R, k)$  be a  $p$ -modular system with  $R$  complete. With suitable ordering of the simple modules, the decomposition matrix is the identity matrix. In particular,  $FG$  and  $kG$  have the same number of simple modules, with the same dimensions.*

In fact more is true than this. Since the reduction modulo  $(\pi)$  of a tensor product is the tensor product of the reductions modulo  $(\pi)$ , the tensor products of  $FG$ -modules and of  $kG$ -modules decompose in the same way, as do the inductions and restrictions of modules.

*Proof.* Let  $T$  be a simple  $FG$ -module with full  $RG$ -lattice  $T_0$ . Then  $T_0/\pi T_0 \cong S_1 \oplus \cdots \oplus S_n$  for various simple  $kG$ -modules  $S_i$ . Since these are projective, they lift to projective  $RG$ -lattices  $\hat{S}_1, \dots, \hat{S}_n$  which are the projective covers of  $S_1, \dots, S_n$ . Thus the projective

cover of  $T_0$  is a homomorphism  $\hat{S}_1 \oplus \cdots \oplus \hat{S}_n \rightarrow T_0$ , and this is an isomorphism since the  $R$ -ranks of the two modules are the same. We deduce that  $T \cong F \otimes_R \hat{S}_1 \oplus \cdots \oplus F \otimes_R \hat{S}_n$ , and so  $n = 1$  since  $T$  is simple. Thus every reduction of a simple module is simple. Equally, every simple  $kG$ -module is a composition factor of the reduction of some simple  $FG$ -module, since it is a composition factor of the reduction of  $FG$ , and so every simple  $kG$ -module does appear as the reduction of a simple  $FG$ -module.  $\square$

We state without proof at this point a particularly fine result about the decomposition map in the case of  $p$ -solvable groups. A group  $G$  is said to be  $p$ -solvable if it has a chain of subgroups

$$1 = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$$

so that each factor  $G_i/G_{i+1}$  is either a  $p$ -group or a group of order prime to  $p$ .

(9.20) THEOREM (Fong, Swan, Rukolaine). *Let  $(F, R, k)$  be a splitting  $p$ -modular system for a  $p$ -solvable group  $G$ . Then every simple  $kG$ -module is the reduction modulo  $(\pi)$  of an  $RG$ -lattice.*

## The cde triangle

In order to express the decomposition matrix as the matrix of a linear map, we introduce three groups, which are instances of Grothendieck groups. Let  $(F, R, k)$  be a splitting  $p$ -modular system for a finite group  $G$ , and suppose that  $F$  and  $R$  are complete with respect to the valuation. We define

$G_0(FG)$  = free abelian group with the isomorphism types  
of simple  $FG$ -modules as a basis,

$G_0(kG)$  = free abelian group with the isomorphism types  
of simple  $kG$ -modules as a basis,

$K_0(kG)$  = free abelian group with the isomorphism types  
of indecomposable projective  $kG$ -modules as a basis.

Thus  $G_0(FG)$  has rank equal to the number of conjugacy classes of  $G$ , and both  $G_0(kG)$  and  $K_0(kG)$  have rank equal to the number of  $p$ -regular conjugacy classes of  $G$ . If  $S$  is a simple  $FG$ -module we write  $[S]$  for the corresponding basis element of  $G_0(FG)$ , similarly if  $S$  is a simple  $kG$ -module we write  $[S]$  for the corresponding basis element of  $G_0(kG)$ , and if  $P$  is an indecomposable projective  $kG$ -module we write  $[P]$  for the corresponding basis element of  $K_0(kG)$ . Extending this notation, if  $U$  is any  $kG$ -module with composition factors  $S_1, \dots, S_r$  occurring with multiplicities  $n_1, \dots, n_r$ , we write

$$[U] = n_1[S_1] + \cdots + n_r[S_r] \in G_0(kG).$$

There is a similar interpretation of  $[U] \in G_0(FG)$  if  $U$  happens to be an  $FG$ -module, and if  $P = P_1^{n_1} \oplus \cdots \oplus P_r^{n_r}$  where the  $P_i$  are indecomposable projective  $kG$ -modules we put

$$[P] = n_1[P_1] + \cdots + n_r[P_r] \in K_0(kG).$$

Since simple  $FG$ -modules biject with their characters, we may identify  $G_0(FG)$  with the subset of the space of class functions  $\mathbb{C}^{cc(G)}$  consisting of the  $\mathbb{Z}$ -linear combinations of the characters of the simple modules. Such  $\mathbb{Z}$ -linear combinations of characters are termed *virtual characters* of  $G$ , so  $G_0(FG)$  is the group of virtual characters of  $FG$ .

We now define the homomorphisms of the cde triangle, which are as follows:

$$\begin{array}{ccc}
 & G_0(FG) & \\
 e \nearrow & & \searrow d \\
 K_0(kG) & \xrightarrow{c} & G_0(kG)
 \end{array}$$

The definition of the homomorphism  $e$  on the basis elements of  $K_0(kG)$  is that if  $P_S$  is an indecomposable projective  $kG$ -module then  $e([P_S]) = [F \otimes_R \hat{P}_S]$ . As observed in 9.13 and 9.15 the lift  $\hat{P}_S$  is unique up to isomorphism, and so this map is well-defined. The *decomposition map*  $d$  is defined thus on basis elements: if  $U$  is a simple  $FG$ -module containing a full  $RG$ -lattice  $L$ , we put  $d([U]) = [L/\pi L]$ . By Theorem 9.18 this is well-defined, and in fact the formula works for arbitrary finite-dimensional  $FG$ -modules  $U$ , not just the simple ones. This definition means that the matrix of  $d$  is the transpose of the decomposition matrix. The homomorphism  $c$  is called the *Cartan map* and is defined by  $c([P_S]) = [P_S]$ , where on the left the symbol  $[P_S]$  means the basis element of  $K_0(kG)$  corresponding to the indecomposable projective  $P_S$ , and on the right  $[P_S]$  is an element of  $G_0(kG)$ . From the definitions we see that the matrix of  $c$  is the Cartan matrix:  $[P_T] = \sum_{\text{simple } S} c_{ST}[S]$  for each simple  $kG$ -module  $T$ .

(9.21) PROPOSITION.  $c = de$ .

*Proof.* It is simply a question of following through the definitions of these homomorphisms. If  $P_S$  is an indecomposable projective  $kG$ -module then  $e[P_S] = [F \otimes_R \hat{P}_S]$ . To compute  $d[F \otimes_R \hat{P}_S]$  we choose any full  $RG$ -sublattice of  $F \otimes_R \hat{P}_S$  and reduce it modulo  $(\pi)$ . Taking  $\hat{P}_S$  to be that lattice, its reduction is  $P_S$  and so  $de([P_S]) = [P_S] = c([P_S])$ .  $\square$

To investigate the properties of the cde triangle we study the relationship between homomorphisms between lattices and between their reductions modulo  $(\pi)$ .

(9.22) PROPOSITION. *Let  $(F, R, k)$  be a  $p$ -modular system. Let  $U, V$  be  $FG$ -modules containing full  $RG$ -lattices  $U_0$  and  $V_0$ .*

- (1)  $\text{Hom}_{RG}(U_0, V_0)$  is a full  $R$ -lattice in  $\text{Hom}_{FG}(U, V)$ .
- (2)  $\pi \cdot \text{Hom}_{RG}(U_0, V_0) = \text{Hom}_{RG}(U_0, \pi \cdot V_0)$  as a subset of  $\text{Hom}_{RG}(U_0, V_0)$
- (3) Suppose that  $U_0$  is a projective  $RG$ -lattice. Then

$$\begin{aligned} \text{Hom}_{RG}(U_0, V_0)/\pi \cdot \text{Hom}_{RG}(U_0, V_0) &\cong \text{Hom}_{RG}(U_0, V_0/\pi V_0) \\ &\cong \text{Hom}_{kG}(U_0/\pi U_0, V_0/\pi V_0). \end{aligned}$$

*Proof.* (1) We should explain how it is that  $\text{Hom}_{RG}(U_0, V_0)$  may be regarded as a subset of  $\text{Hom}_{FG}(U, V)$ . The most elementary approach is to take  $R$ -bases  $u_1, \dots, u_r$  for  $U_0$  and  $v_1, \dots, v_s$  for  $V_0$ . These are also  $F$ -bases for  $U$  and  $V$ . Any  $RG$ -homomorphism  $U_0 \rightarrow V_0$  can be represented with respect to these bases by a matrix with entries in  $R$ . Regarding it as a matrix with entries in  $F$ , it represents an  $FG$ -module homomorphism  $U \rightarrow V$ .

To see that  $\text{Hom}_{RG}(U_0, V_0)$  is in fact a sublattice of  $\text{Hom}_{FG}(U, V)$ , we observe that  $\text{Hom}_{RG}(U_0, V_0) \subseteq \text{Hom}_R(U_0, V_0) \cong R^{rs}$  where  $r = \dim U$ ,  $s = \dim V$ . The latter is a free  $R$ -module, so  $\text{Hom}_{RG}(U_0, V_0)$  is an  $R$ -lattice since  $R$  is a principal ideal domain. We show it is full in  $\text{Hom}_{FG}(U, V)$ . Using the bases for  $U_0, V_0$ , let  $\phi : U \rightarrow V$  be an  $FG$ -module homomorphism. Then  $\phi(u_i) = \sum \lambda_{ji} v_j$  with  $\lambda_{ji} \in F$ . Choose  $a \in R$  so that  $a\lambda_{ji} \in R$  for all  $i, j$ . Then  $a\phi : U_0 \rightarrow V_0$ , showing that  $\phi$  belongs to  $F \cdot \text{Hom}_{RG}(U_0, V_0)$ . Therefore  $\text{Hom}_{RG}(U_0, V_0)$  spans  $\text{Hom}_{FG}(U, V)$  over  $F$ .

(2) The map  $V_0 \rightarrow \pi \cdot V_0$  given by  $x \mapsto \pi x$  is an  $RG$ -isomorphism so the morphisms  $U_0 \rightarrow \pi \cdot V_0$  are precisely those which arise as composites  $U_0 \rightarrow V_0 \xrightarrow{\pi} \pi V_0$ , which are in turn the elements of  $\pi \cdot \text{Hom}_{RG}(U_0, V_0)$ .

(3) Consider  $\text{Hom}(U_0, V_0) \rightarrow \text{Hom}(U_0, V_0/\pi V_0)$ . Its kernel is  $\text{Hom}(U_0, \pi V_0)$ , which equals  $\pi \text{Hom}(U_0, V_0)$ . Since  $U_0$  is projective, the map is surjective, and it gives rise to the first isomorphism. For the second, all homomorphisms  $\alpha : U_0 \rightarrow V_0/\pi V_0$  contain  $\pi U_0$  in the kernel, and so factor as  $U_0 \rightarrow U_0/\pi U_0 \xrightarrow{\beta} V_0/\pi V_0$ . The correspondence of  $\alpha$  and  $\beta$  provides the isomorphism.  $\square$

(9.23) COROLLARY. *Suppose  $U_0$  and  $V_0$  are full  $RG$ -lattices in  $U$  and  $V$ , and  $U_0$  is projective. Then*

$$\dim_F \text{Hom}_{FG}(U, V) = \dim_k \text{Hom}_{kG}(U_0/\pi U_0, V_0/\pi V_0).$$

*Proof.* Both sides equal  $\text{rank}_R \text{Hom}_{RG}(U_0, V_0)$  by parts (1) and (3) of the last result.  $\square$

(9.24) THEOREM. *Let  $(F, R, k)$  be a splitting  $p$ -modular system for  $G$  and suppose that  $R$  is complete with respect to its valuation. Let  $S$  be a simple  $kG$ -module and let  $T$  be a simple  $FG$ -module containing a full  $RG$ -lattice  $T_0$ . The multiplicity of  $T$  in  $F \otimes_R \hat{P}_S$  equals the multiplicity of  $S$  as a composition factor of  $T_0/\pi T_0$ .*

*Proof.* Applying the last corollary to the full  $RG$ -lattice  $\hat{P}_S$  of  $F \otimes_R \hat{P}_S$  we obtain  $\dim_F \text{Hom}_{kG}(F \otimes_R \hat{P}_S, T) = \dim_k \text{Hom}_{kG}(P_S, T_0/\pi T_0)$ , which shows that the multiplicities are equal.  $\square$

We comment that this equality of dimensions gives a second proof of the Brauer-Nesbitt theorem that the decomposition numbers  $d_{TS} = \dim \text{Hom}_{kG}(P_S, T_0/\pi T_0)$  are defined independently of the choice of lattice  $T_0$ , since the left-hand side in the equality does not depend on this choice.

(9.25) COROLLARY. *Let  $(F, R, k)$  be a splitting  $p$ -modular system for  $G$  and suppose that  $R$  is complete with respect to its valuation. With respect to the bases of  $G_0(FG)$ ,  $G_0(kG)$  and  $K_0(kG)$  by which these groups were defined (namely the bases whose elements are the symbols  $[T]$ ,  $[S]$  and  $[P_S]$  where  $T$  is a simple  $FG$ -module and  $S$  is a simple  $kG$ -module) the matrix of  $e$  is  $D$  and the matrix of  $d$  is  $D^T$ , where  $D$  is the decomposition matrix.*

*Proof.* We have already observed that the matrix of  $d$  is  $D^T$ . The entries  $e_{TS}$  in the matrix of  $e$  are defined by

$$e([P_S]) = [F \otimes_R \hat{P}_S] = \sum_T e_{TS} T,$$

so that  $e_{TS}$  is the multiplicity of  $T$  in  $F \otimes_R \hat{P}_S$ . By the last result,  $e_{TS} = d_{TS}$ .  $\square$

*Example.* This result allows us to compute the characters of the indecomposable projective  $RG$ -modules  $\hat{P}_S$  (or more properly the characters of the  $FG$ -modules  $F \otimes_R \hat{P}_S$ ). Using the decomposition matrices for  $S_3$  which were previously computed we see that in characteristic 2,

$$\begin{aligned}\chi_{\hat{P}_1} &= \chi_1 + \chi_\epsilon \\ \chi_{\hat{P}_2} &= \chi_2,\end{aligned}$$

and in characteristic 3

$$\begin{aligned}\chi_{\hat{P}_1} &= \chi_1 + \chi_2 \\ \chi_{\hat{P}_\epsilon} &= \chi_\epsilon + \chi_2.\end{aligned}$$

We now have a second proof of the symmetry of the Cartan matrix, but perhaps more importantly an extremely good way to calculate it. The effectiveness of this approach will be increased once we know about Brauer characters, which are treated in the next section.

(9.26) COROLLARY. *Let  $(F, R, k)$  be a splitting  $p$ -modular system for  $G$ . Then the Cartan matrix  $C = D^T D$ . Thus  $C$  is symmetric.*

*Example.* When  $G = S_3$  the Cartan matrices in characteristic 2 and in characteristic 3 are

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

as we have seen already.

The equality of dimensions which played the key role in the proof of Theorem 9.24 can be nicely expressed in terms of certain bilinear pairings between the various Grothendieck groups. On the vector space of class functions on  $G$  we already have defined a Hermitian form and on the subgroup  $G_0(FG)$  it restricts to give a bilinear form

$$\langle \quad , \quad \rangle : G_0(FG) \times G_0(FG) \rightarrow \mathbb{Z}$$

specified by  $\langle [U], [V] \rangle = \dim \operatorname{Hom}_{FG}(U, V)$  when  $U$  and  $V$  are  $FG$ -modules. We also have a pairing

$$\langle \quad , \quad \rangle : K_0(FG) \times G_0(kG) \rightarrow \mathbb{Z}$$

specified by  $\langle [P], [V] \rangle = \dim \operatorname{Hom}_{kG}(P, V)$  when  $P$  is a projective  $kG$ -module and  $V$  is a  $kG$ -module. By Proposition 7.17 this quantity depends only on the composition factors of  $V$ , not on the actual module  $V$ , and so this pairing is well-defined. We readily see that each of these bilinear pairings is non-degenerate, in that in each case the free abelian groups have bases which are dual to each other. Thus if  $U$  and  $V$  are simple  $FG$ -modules we have  $\langle [U], [V] \rangle = \delta_{[U], [V]}$ , and if  $S$  and  $T$  are simple  $kG$ -modules we have  $\langle [P_S], [T] \rangle = \delta_{[S], [V]}$ . The equality of dimensions which appeared in the proof of 9.25 can now be expressed as follows. If  $x \in K_0(kG)$  and  $y \in G_0(FG)$  then  $\langle e(x), y \rangle = \langle x, d(y) \rangle$ . This formalism is an expression of the fact that  $e$  and  $d$  are the transpose of each other.

## Blocks of defect zero

We will use the relationship between representations in characteristic zero and in characteristic  $p$  to show that simple representations in characteristic zero whose degree is divisible by the order of a Sylow  $p$ -subgroup of  $G$  biject with simple representations in characteristic  $p$  which are projective. We study blocks more fully in a later section, and it turns out that representations with the special properties just described correspond to blocks of defect zero. We will deduce that each character of degree divisible by the order of a Sylow  $p$ -subgroup vanishes on elements of order divisible by  $p$ .

(9.27) PROPOSITION. *Let  $(F, R, k)$  be a  $p$ -modular system and  $G$  a finite group. Let  $\hat{P}$  be a projective  $RG$ -module and  $\chi$  the character of  $F \otimes_R \hat{P}$ . Then  $\chi(1)$  is divisible by the order of a Sylow  $p$ -subgroup of  $G$ , and if  $g \in G$  has order divisible by  $p$  then  $\chi(g) = 0$ .*

*Proof.* Since  $\hat{P}/\pi\hat{P}$  is a projective  $kG$ -module it has dimension divisible by the order of a Sylow  $p$ -subgroup of  $G$ , and this dimension equals the rank of  $\hat{P}$  and also  $\dim F \otimes_R \hat{P}$ , which equals  $\chi(1)$ .

Consider now an element  $g \in G$  of order divisible by  $p$ . To show that  $\chi(g) = 0$  it suffices to consider  $\hat{P}$  as an  $R\langle g \rangle$ -module, and as such it is still projective. We may suppose that  $\hat{P}$  is an indecomposable projective  $R\langle g \rangle$ -module.

Let us write  $g = st$  where  $s$  is  $p$ -regular,  $t$  is  $p$ -singular and  $st = ts$ , as in Lemma 9.9, so  $\langle g \rangle = \langle s \rangle \times \langle t \rangle$ . As in Example 8.6 we can write  $\hat{P}/\pi\hat{P} = S \otimes k\langle t \rangle$  where  $S$  is a simple  $k\langle s \rangle$ -module. Since  $k\langle s \rangle$  is semisimple and  $S$  is projective as a  $k\langle s \rangle$ -module, we can lift  $S$  to a projective  $R\langle s \rangle$ -module  $\hat{S}$  for which  $\hat{S}/\pi\hat{S} = S$ . Now  $\hat{P}/\pi\hat{P} = S \otimes k\langle t \rangle = S \otimes k \uparrow_{\langle s \rangle}^{\langle g \rangle} = S \uparrow_{\langle s \rangle}^{\langle g \rangle}$ . This lifts to  $\hat{S} \uparrow_{\langle s \rangle}^{\langle g \rangle}$ , which is a projective  $R\langle g \rangle$ -module. It is the projective cover of  $\hat{P}/\pi\hat{P}$ , so by uniqueness of projective covers  $\hat{P} \cong \hat{S} \uparrow_{\langle s \rangle}^{\langle g \rangle}$ . We deduce that  $\chi = \chi_{\hat{S}} \uparrow_{\langle s \rangle}^{\langle g \rangle}$ . It follows that  $\chi(g) = 0$  from the formula for an induced character, since no conjugate of  $g$  lies in  $\langle s \rangle$ .  $\square$

(9.28) THEOREM. *Let  $(F, R, k)$  be a splitting  $p$ -modular system in which  $R$  is complete, and let  $G$  be a group of order  $p^d q$  where  $q$  is prime to  $p$ . Let  $T$  be an  $FG$ -module of dimension  $n$ , containing a full  $RG$ -sublattice  $T_0$ . The following are equivalent.*

- (1)  $p^d \mid n$  and  $T$  is a simple  $FG$ -module.
- (2) The homomorphism  $RG \rightarrow \text{End}_R(T_0)$  which gives the action of  $RG$  on  $T_0$  identifies  $\text{End}_R(T_0) \cong M_n(R)$  with a ring direct summand of  $RG$ .
- (3)  $T$  is a simple  $FG$ -module and  $T_0$  is a projective  $RG$ -module.
- (4) The homomorphism  $kG \rightarrow \text{End}_k(T_0/\pi T_0)$  identifies  $\text{End}_k(T_0/\pi T_0) \cong M_n(k)$  with a ring direct summand of  $kG$ .

(5) As a  $kG$ -module,  $T_0/\pi T_0$  is simple and projective.

*Proof.* (1)  $\Rightarrow$  (2) Suppose that (1) holds. We will use the formula obtained in Theorem 3.23 for the primitive central idempotent  $e$  associated to  $T$ , namely

$$e = \frac{n}{|G|} \sum_{g \in G} \chi_T(g^{-1})g$$

where  $\chi_T$  is the character of  $T$ . The homomorphism  $\rho : FG \rightarrow \text{End}_F(T)$  which expresses the action of  $G$  on  $T$  identifies  $eFG$  with the matrix algebra  $\text{End}_F(T)$ , and has kernel  $(1 - e)FG$ .

Because  $p^d \mid n$  and the values of  $\chi_T$  are sums of roots of unity we have  $e \in RG$  so that  $RG = eRG \oplus (1 - e)RG$  as a sum of rings. Consider the homomorphism  $RG \rightarrow \text{End}_R(T_0)$  which expresses the action of  $RG$  on  $T_0$ . It is the restriction of  $\rho$  to  $RG$ , which takes values in  $\text{End}_R(T_0)$ , so has kernel  $(1 - e)FG \cap RG = (1 - e)RG$ . We will show that this homomorphism is surjective. From this it will follow that  $eRG \cong \text{End}_R(T_0) \cong M_n(R)$ , a direct summand of  $RG$ .

As an extension of the formula in Theorem 3.23 for the primitive central idempotent corresponding to  $T$ , we claim that if  $\phi \in \text{End}_F(T)$  then

$$\phi = \frac{n}{|G|} \sum_{g \in G} \text{tr}(\rho(g^{-1})\phi)\rho(g).$$

To demonstrate this it suffices to consider the case  $\phi = \rho(h)$  where  $h \in G$ , since these elements span  $\text{End}_F(T)$ . In this case

$$\begin{aligned} \frac{n}{|G|} \sum_{g \in G} \text{tr}(\rho(g^{-1})\rho(h))\rho(g) &= \rho(h) \frac{n}{|G|} \sum_{g \in G} \text{tr}(\rho(g^{-1}h))\rho(h^{-1}g) \\ &= \rho(h)\rho(e) \\ &= \rho(h) \end{aligned}$$

using the previously obtained formula for  $e$ . Now if  $\phi \in \text{End}_R(T_0)$ , which we regard as a subset of  $\text{End}_F(T)$ , we have  $\frac{n}{|G|} \sum_{g \in G} \text{tr}(\rho(g^{-1})\phi)g \in RG$ , which shows that  $RG \rightarrow \text{End}_R(T_0)$  is surjective. This completes the proof of this implication.

(2)  $\Rightarrow$  (3) Certainly  $T_0$  is projective as a module for  $\text{End}_R(T_0)$  since it identifies with the module of column vectors for this matrix algebra. Assuming (2), we have that  $T_0$  is a projective  $RG$ -module, since  $RG$  acts via its summand  $eRG$  which identifies with the matrix algebra. Furthermore,  $FG$  acts on  $T \cong F \otimes_R T_0$  as column vectors for a matrix algebra over  $F$ , so  $T$  is a simple  $FG$ -module.

(2)  $\Rightarrow$  (4) The decomposition  $RG = eRG \oplus (1 - e)RG$  with  $eRG \cong M_n(R)$  is preserved on reducing modulo  $(\pi)$ , and we obtain  $kG = \bar{e}kG \oplus (1 - \bar{e})kG$  where  $\bar{e}$  is the image  $e$  in  $kG$ . Here  $\bar{e}kG \cong M_n(k)$  and the action of  $kG$  on  $T_0/\pi T_0$  is via projection onto  $\bar{e}kG$ .

(3)  $\Rightarrow$  (5) Since  $T_0$  is a direct summand of a free  $RG$ -module it follows that  $T_0/\pi T_0$  is a direct summand of a free  $kG$ -module, and hence is projective. Furthermore, we claim that  $T_0/\pi T_0$  is indecomposable. For writing  $T_0/\pi T_0 = P_{S_1} \oplus \cdots \oplus P_{S_t}$  where the  $P_{S_i}$  are indecomposable projectives we have that  $T_0/\pi T_0$  is the projective cover of  $S_1 \oplus \cdots \oplus S_t$  as an  $RG$ -module. It follows that  $T_0 \cong \hat{P}_{S_1} \oplus \cdots \oplus \hat{P}_{S_t}$  and  $T \cong F \otimes_R \hat{P}_{S_1} \oplus \cdots \oplus F \otimes_R \hat{P}_{S_t}$ , so  $t = 1$  since  $T$  is simple. By Theorem 9.24 the column of the decomposition matrix corresponding to  $S_1$  consists of zeros except for an entry 1 in the row of  $T$ . Since  $C = D^T D$ , the multiplicity of  $S_1$  as a composition factor of  $P_{S_1}$  is 1. We know from Theorem 8.15 that  $\text{Soc } P_{S_1} \cong S_1$  and also  $P_{S_1}/\text{Rad } P_{S_1} \cong S_1$ , so that  $S_1$  occurs as a composition factor of  $P_{S_1}$  with multiplicity at least 2 unless  $P_{S_1} = S_1$ . This shows that  $T_0/\pi T_0$  is simple.

(4)  $\Rightarrow$  (5) This is analogous to the proof (2)  $\Rightarrow$  (3).

(5)  $\Rightarrow$  (1) Since  $T_0/\pi T_0$  is projective its dimension is divisible by  $p^d$  by Corollary 8.3, and this dimension equals  $\text{rank}_R T_0 = \dim T$ . If  $T$  were not simple as an  $FG$ -module we would be able to write  $T = U \oplus V$ , and taking full  $RG$ -lattices  $U_0, V_0$  the composition factors of  $T_0/\pi T_0$  are the same as those of  $U_0/\pi U_0 \oplus V_0/\pi V_0$ . Since  $T_0/\pi T_0$  is in fact simple, this situation cannot occur, and  $T$  is simple.  $\square$

Statement (5) of Theorem 9.28 appears to depend on the  $FG$ -module  $T$ , but this is not really the case. If  $P$  is any simple projective  $kG$ -module, it can be lifted to an  $RG$ -module  $\hat{P}$  and taking  $T = F \otimes_R \hat{P}$  we have a module with a full  $RG$ -lattice  $T_0$  for which  $T_0/\pi T_0 \cong P$ . Thus every simple projective  $kG$ -module is acted on by  $kG$  via projection onto a matrix algebra direct summand of  $kG$ , and the module  $T$  just constructed is always simple.

Notice in the statement of Theorem 9.28 that since the full  $RG$ -sublattice  $T_0$  is arbitrary, every full  $RG$ -sublattice of  $T$  is projective. Since such a full lattice  $T_0$  is the projective cover of  $T_0/\pi T_0$ , which is a simple module defined independently of the choice of  $T_0$ , all such lattices  $T_0$  are isomorphic as  $RG$ -modules.

Looking at the various equivalent statements of Theorem 9.28, one might be led to suspect that if  $k$  is a field of characteristic  $p$  and  $S$  is a simple  $kG$ -module of dimension divisible by the largest power of  $p$  which divides  $|G|$  then  $S$  is necessarily projective, but in fact this conclusion does not always hold.

(9.29) COROLLARY. *Let  $T$  be a simple  $FG$ -module, where  $F$  is a splitting field for  $G$  of characteristic 0, and let  $\chi_T$  be the character of  $T$ . Let  $p$  be a prime, and suppose that the highest power of  $p$  which divides  $|G|$  also divides the degree  $\chi_T(1)$ . Then if  $g$  is any element of  $G$  of order divisible by  $p$  we have  $\chi_T(g) = 0$ .*

*Proof.* This combines Proposition 9.27 with Theorem 9.28. If  $F$  does not initially appear as part of a  $p$ -modular system, we may replace  $F$  by a subfield which is a splitting field and which is a finite extension of  $\mathbb{Q}$ , since  $\mathbb{Q}G$  has a splitting field of this form and by the argument of 9.3 it may be chosen to be a subfield of  $F$ . We may write  $T$  in this subfield without changing its character  $\chi_T$  and the hypothesis about the power of  $p$  which

divides  $\chi_T(1)$  remains the same. Take the valuation on  $F$  determined by a maximal ideal  $\mathfrak{p}$  of the ring of integers for which  $\mathfrak{p} \cap \mathbb{Z} = (p)$ , and complete  $F$  with respect to this valuation to get a splitting, complete,  $p$ -modular system. We may now apply Theorem 9.28.  $\square$

The above corollary is a significant piece of information about the character table of a group, which can be observed in many examples. Thus the simple character of degree 2 of the symmetric group  $S_3$  is zero except on the 2-regular elements, and the simple characters of  $S_4$  of degree 3 are zero except on the 3-regular elements. It is notable that in order to prove this result, which is stated within a characteristic zero framework, we have used technical machinery from characteristic  $p$ .

*Exercises for Section 9.*

1. Let  $E = \mathbb{F}_p(t)$  be a transcendental extension of the field with  $p$  elements and let  $F$  be the subfield  $\mathbb{F}_p(t^p)$ . Write  $\alpha = t^p \in F$ , so that  $t^p - \alpha = 0$ . Let  $A = E$ , regarded as an  $F$ -algebra.

(a) Show that  $A$  has a simple module which is not absolutely simple.

(b) Show that  $E$  is a splitting field for  $A$ , and that the regular representation of  $E \otimes_F A$  is a uniserial module. Show that  $\text{Rad}(E \otimes_F A) \neq E \otimes_F \text{Rad}(A)$ .

[Notice that  $E \otimes_F \text{Rad}(A)$  is always contained in the radical of  $E \otimes_F A$  when  $A$  is a finite-dimensional algebra, being a nilpotent ideal.]

(c) Show that  $A$  is not isomorphic to  $FG$  for any group  $G$ .

2. Let  $G$  be a cyclic group,  $F$  a field and  $S$  a simple  $FG$ -module. Show that  $E = \text{End}_{FG}(S)$  is a field with the property that  $E \otimes_F S$  is a direct sum of modules which are all absolutely simple.

3. Let  $A$  be a finite-dimensional algebra over a field  $F$  and suppose that  $F$  is a splitting field for  $A$ . Let  $E \supseteq F$  be a field extension. Prove that  $\text{Rad}(E \otimes_F A) \cong E \otimes_F \text{Rad}(A)$ .

[The observation at the end of question 1 may help here.]

4. Let  $A$  be an  $F$ -algebra where  $F$  is a splitting field for  $A$ , and let  $E \supseteq F$  be a field extension. Show that every simple  $E \otimes_F A$ -module can be written in  $F$ .

[Bear in mind the result of question 3.]

5. Let  $A$  be a finite-dimensional  $F$ -algebra and let  $E \supseteq F$  be a field extension where  $E$  is a splitting field for  $A$ . Suppose that every simple  $A$ -module remains simple on extending scalars to  $E$ . Show that  $F$  is a splitting field for  $A$ .

6. Let  $A$  be a finite-dimensional  $F$ -algebra and  $E \supseteq F$  a field extension.

(a) Show that if  $U \rightarrow V$  is an essential epimorphism of  $A$ -modules then  $E \otimes_F U \rightarrow E \otimes_F V$  is an essential epimorphism of  $E \otimes_F A$ -modules.

(b) Show that if  $P \rightarrow U$  is a projective cover then so is  $E \otimes_F P \rightarrow E \otimes_F U$ .

7. Let  $A$  be a finite-dimensional  $F$ -algebra where  $F$  is a splitting field for  $A$ . Let  $P$  be an indecomposable projective  $A$ -module. Show that if  $E \supseteq F$  is any field extension then  $E \otimes_F P$  is indecomposable and projective as an  $E \otimes_F A$ -module. Show further that every indecomposable projective  $E \otimes_F A$ -module can be written in  $F$ .

8. Let  $G = C_2 \times C_2$  be generated by elements  $a$  and  $b$ , and let  $E$  be a field of characteristic 2. Let  $t \in E$  be any element, which may be algebraic or transcendental over  $\mathbb{F}_2$ . Let  $\rho : G \rightarrow GL(E^2)$  be the representation with

$$\rho(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho(b) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

Show that this representation is absolutely indecomposable, and that it cannot be written in any proper subfield of  $\mathbb{F}_2(t)$ .

9. Let  $(F, R, k)$  be a  $p$ -modular system and suppose that  $R$  is complete. Let  $L$  and  $M$  be  $RG$ -lattices, where  $G$  is a finite group.

(a) Show that  $L$  is a projective  $RG$ -module if and only if  $L/\pi L$  is a projective  $kG$ -module.

[Consider the projective cover of  $L$ .]

(b) Deduce that if  $L/\pi L \cong M/\pi M$  as  $kG$ -modules and that  $L/\pi L$  is a projective  $kG$ -module then  $L \cong M$  as  $RG$ -modules. In other words, projective  $kG$ -modules lift uniquely to  $RG$ -lattices.

10. Let  $(F, R, k)$  be a  $p$ -modular system and  $G$  a finite group. Show that if  $U = U_1 \oplus U_2$  is a finite-dimensional  $FG$ -module and  $L$  is a full  $RG$ -lattice in  $U$  then  $L \cap U_1$ ,  $L \cap U_2$  are full  $RG$ -lattices in  $U_1$  and  $U_2$ , but that it need not be true that  $L = (L \cap U_1) \oplus (L \cap U_2)$ .

[Consider the regular representation when  $G = C_2$ .]

11. Let  $U$  be the 2-dimensional representation of  $S_3$  over  $\mathbb{Q}$  which is defined by requiring that with respect to a basis  $u_1, u_2$  the elements  $(1, 2, 3)$  and  $(1, 2)$  act by matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}.$$

Let  $U_0$  be the  $\mathbb{Z}S_3$ -lattice which is the  $\mathbb{Z}$ -span of  $u_1$  and  $u_2$  in  $U$ . Show that  $U_0/3U_0$  has just 3 submodules as a module for  $(\mathbb{Z}/3\mathbb{Z})S_3$ , namely 0, the whole space, and a 1-dimensional submodule. Deduce that  $U_0/3U_0$  is not semisimple.

Now let  $U_1$  be the  $\mathbb{Z}$ -span of the vectors  $2u_1 + u_2$  and  $-u_1 + u_2$  in  $U$ . Show (for example, by drawing a picture in which the angle between  $u_1$  and  $u_2$  is  $120^\circ$ , or else algebraically) that  $U_1$  is a  $\mathbb{Z}S_3$ -lattice in  $U$ , and that it has index 3 in  $U_0$ . Write down matrices which give the action of  $(1, 2, 3)$  and  $(1, 2)$  on  $U_1$  with respect to the new basis. Show that  $U_1/3U_1$  also has just 3 submodules as a  $(\mathbb{Z}/3\mathbb{Z})S_3$ -module, but that it is not isomorphic to  $U_0/3U_0$ .

Identify  $U_0/U_1$  as a  $(\mathbb{Z}/3\mathbb{Z})S_3$ -module.

Prove that  $U_1$  is the unique  $\mathbb{Z}S_3$ -sublattice of  $U_0$  of index 3.

Show that  $\mathbb{Z}_3 \otimes_{\mathbb{S}} U_0$  is a uniserial  $\mathbb{Z}_3 S_3$ -lattice, where  $\mathbb{Z}_3$  denotes the 3-adic integers.

12. Let  $(F, R, k)$  be a splitting  $p$ -modular system and  $G$  a finite group. Let  $T$  be an  $FG$ -module with the property that every full  $RG$ -sublattice of  $T$  is indecomposable and projective. Show that  $T$  is simple of degree divisible by  $p^n$ , where  $p^n \mid |G|$ ,  $p^{n+1} \nmid |G|$ .

## 10. Brauer characters

To define Brauer characters for a finite group  $G$  we start with a  $p$ -modular system  $(F, R, k)$  and assume that both  $F$  and  $k$  contain a primitive  $a$ th root of unity, where  $a$  is the l.c.m. of the orders of the  $p$ -regular elements of  $G$ . If we wish to define the Brauer character of a  $kG$ -module  $U$  where  $k$  or  $F$  do not contain a primitive  $a$ th root of unity, we first extend the scalars so that the  $p$ -modular system does have this property. Let us put

$$\begin{aligned}\mu_F &= \{\text{ath roots of 1 in } F\} \\ \mu_k &= \{\text{ath roots of 1 in } k.\}\end{aligned}$$

The polynomial  $X^a - 1$  is separable both in  $F[X]$  and  $k[X]$  since its formal derivative  $\frac{d}{dX}(X^a - 1) = aX^{a-1}$  is not zero and has no factors in common with  $X^a - 1$ , so both  $\mu_F$  and  $\mu_k$  are cyclic groups of order  $a$ . Also  $\mu_F \subseteq R$  since roots of unity have value 1 under the valuation. We claim that the quotient homomorphism  $R \rightarrow R/(\pi) = k$  gives an isomorphism  $\mu_F \rightarrow \mu_k$ , which we write  $\hat{\lambda} \rightarrow \lambda$ . This is because  $X^a - 1$  reduces to the polynomial which is written the same way, and so its linear factors over  $F$  must map to the complete set of linear factors over  $k$ . These linear factors have the form  $X - \hat{\lambda}$  over  $F$  and  $X - \lambda$  over  $k$ , so we obtain a bijection between the two groups of roots of unity.

Let  $g \in G$  be a  $p$ -regular element (an element of order prime to  $p$ ), and let  $\rho : G \rightarrow GL(U)$  be a representation over  $k$ . Then  $\rho(g)$  is diagonalizable, since  $k\langle g \rangle$  is semisimple and all eigenvalues of  $\rho(g)$  lie in  $k$ , being  $a$ th roots of unity. If the eigenvalues of  $\rho(g)$  are  $\lambda_1, \dots, \lambda_n$  we put

$$\phi_U(g) = \hat{\lambda}_1 + \dots + \hat{\lambda}_n,$$

and this is the *Brauer character* of  $U$ . It is a function which is only defined on the  $p$ -regular elements of  $G$ , and takes values in a field of characteristic zero, which we may always take to be  $\mathbb{C}$ .

*Example.* Working over  $\mathbb{F}_2$ , the specification  $\rho(g) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$  provides a 2-dimensional representation  $U$  of the cyclic group  $\langle g \rangle$  of order 3. The characteristic polynomial of this matrix is  $t^2 + t + 1$  and its eigenvalues are the primitive cube roots of unity in  $\mathbb{F}_4$ . These lift to primitive cube roots of unity in  $\mathbb{C}$ , and so  $\phi_U(g) = e^{2\pi i/3} + e^{4\pi i/3} = -1$ . It is very tempting in this situation to observe that the trace of  $\rho(g)$  is 1, which can be lifted to  $1 \in \mathbb{C}$ , and to deduce that  $\phi_U(g) = 1$ ; however, this deduction is incorrect.

We list the immediate properties of Brauer characters.

(10.1) PROPOSITION. *Let  $(F, R, k)$  be a  $p$ -modular system, let  $G$  be a finite group, and let  $U, V, S$  be finite-dimensional  $kG$ -modules.*

- (1)  $\phi_U(1) = \dim_k U$ .
- (2)  $\phi_U$  is a class function on  $p$ -regular conjugacy classes.
- (3)  $\phi_U(g^{-1}) = \overline{\phi_U(g)} = \phi_{U^*}(g)$ .

- (4)  $\phi_{U \otimes V} = \phi_U \cdot \phi_V$ .
- (5) If  $0 \rightarrow U \rightarrow V \rightarrow W \rightarrow 0$  is a short exact sequence of  $kG$ -modules then  $\phi_V = \phi_U + \phi_W$ . In particular,  $\phi_U$  depends only on the isomorphism type of  $U$ . Furthermore, if  $U$  has composition factors  $S$ , each occuring with multiplicity  $n_S$ , then  $\phi_U = \sum_S n_S \phi_S$ .
- (6) If  $U$  is liftable to an  $RG$ -lattice  $\hat{U}$  (so  $U = \hat{U}/\pi\hat{U}$ ) and the ordinary character of  $\hat{U}$  is  $\chi_{\hat{U}}$ , then  $\phi_U(g) = \chi_{\hat{U}}(g)$  on  $p$ -regular elements  $g \in G$ .

*Proof.* (1) In its action on  $U$  the identity has  $\dim_k U$  eigenvalues all equal to 1. They all lift to 1 and the sum of the lifts is  $\dim_k U$ .

(2) This follows because  $g$  and  $xgx^{-1}$  have the same eigenvalues.

(3) The eigenvalues of  $g^{-1}$  on  $U$  are the inverses of the eigenvalues of  $g$  on  $U$ , as are the eigenvalues of  $g$  on  $U^*$  (since here  $g$  acts by the inverse transpose matrix). The lifting of roots of unity is a group homomorphism, so the result follows since if  $\hat{\lambda}$  lifts  $\lambda$  then  $\hat{\lambda}^{-1}$  lifts  $\lambda^{-1}$ .

(4) If  $g$  is a  $p$ -regular element then  $U$  and  $V$  have bases  $u_1, \dots, u_r$  and  $v_1, \dots, v_s$  consisting of eigenvectors of  $g$  with eigenvalues  $\lambda_1, \dots, \lambda_r$  and  $\mu_1, \dots, \mu_s$ , respectively. Now the tensors  $u_i \otimes v_j$  form a basis of eigenvectors of  $U \otimes V$  with eigenvalues  $\lambda_i \mu_j$ . Their lifts are  $\widehat{\lambda_i \mu_j} = \hat{\lambda}_i \hat{\mu}_j$  since lifting is a group homomorphism, and  $\sum_{i,j} \hat{\lambda}_i \hat{\mu}_j = (\sum_i \hat{\lambda}_i)(\sum_j \hat{\mu}_j)$  so that  $\phi_{U \otimes V}(g) = \phi_U(g)\phi_V(g)$ .

(5) If  $g$  is a  $p$ -regular element then  $k\langle g \rangle$  is semisimple so that  $V \cong U \oplus W$  as  $k\langle g \rangle$ -modules. It follows that the eigenvalues of  $g$  on  $V$  are the union of the eigenvalues on  $U$  and on  $W$  (taken with multiplicity), and from this  $\phi_V(g) = \phi_U(g) + \phi_W(g)$  follows. If  $U \cong U_1$  we may consider the sequence  $0 \rightarrow U_1 \rightarrow U \rightarrow 0 \rightarrow 0$  to see that  $\phi_U = \phi_{U_1}$ . The final sentence follows by an inductive argument.

(6) If  $g$  is  $p$ -regular and acts with eigenvalues  $\mu_1, \dots, \mu_n$  on  $\hat{U}$  then  $g$  acts on  $U = \hat{U}/\pi\hat{U}$  with eigenvalues  $\mu_1 + (\pi), \dots, \mu_n + (\pi)$ . Since  $\phi_U(g)$  is the sum of the lifts of these last quantities we have  $\phi(g) = \mu_1 + \dots + \mu_n = \chi_{\hat{U}}(g)$ . □

We may use these elementary properties to construct tables of Brauer characters. There are two significant tables which we might construct: the table of values of Brauer characters of simple modules, and the table of values of Brauer characters of indecomposable projective modules. By Theorem ? both these tables are square. We will eventually establish that they satisfy orthogonality relations which generalize those for ordinary characters, but we first present some examples.

*Examples.* 1. Let  $G = S_3$ . We have seen that in both characteristic 2 and characteristic 3 the simple representations of  $S_3$  lift to characteristic zero, and so the Brauer characters of the simple modules form tables which are part of the ordinary character table of  $S_3$ . The indecomposable projective modules for a group always lift to characteristic zero, but if we do not have some information such as the Cartan matrix or the decomposition matrix it is hard to know *a priori* what their characters might be. In the case of  $S_3$  we have already computed this information, and we now present the tables of Brauer characters of the simple and indecomposable projective modules.

()	(12)	(123)
1	1	1
1	-1	1
2	0	-1

()	(123)
1	1
2	-1

()	(123)
2	2
2	-1

TABLE: The character tables of  $S_3$ , ordinary and in characteristic 2.

()	(12)
1	1
1	-1

()	(12)
3	1
3	-1

TABLE: The character tables of  $S_3$  in characteristic 3.

2. When  $G = S_4$  the ordinary character table is

24	4	8	4	3
1	(12)	(12)(34)	(1234)	(123)
1	1	1	1	1
1	-1	1	-1	1
2	0	2	0	-1
3	-1	-1	1	0
3	1	-1	-1	0

as seen in Example 3.11. In characteristic 2,  $S_4$  has two simple modules, namely the trivial module and the 2-dimensional module of  $S_3$ , made into a module for  $S_4$  via the quotient homomorphism  $S_4 \rightarrow S_3$ . Both of these lift to characteristic zero, and so the Brauer characters of the 2-modular representations are

()	(123)
1	1
2	-1

which is the same as for  $S_3$ . The Brauer characters of the reductions modulo 2 of the ordinary characters of  $S_4$  are

()	(123)
1	1
1	1
2	-1
3	0
3	0

and we see from this that the sign representation reduces to the trivial representation, and reductions of the two 3-dimensional representations each have the 2-dimensional representation and the trivial representation as composition factors with multiplicity 1. This is because there is a unique way to express their Brauer characters as linear combinations of

the simple Brauer characters, and this determines the composition factors. It follows that the decomposition and Cartan matrices for  $S_4$  at the prime 2 are

$$D = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}.$$

In characteristic 3 the trivial representation and the sign representation are distinct 1-dimensional representations, and we also have two non-isomorphic 3-dimensional representations which are the reductions modulo 3 of the two 3-dimensional ordinary representations. This is because these 3-dimensional representations are blocks of defect zero by ?, and they remain simple on reduction modulo 3. This constructs four simple representations in characteristic 3, and this is the complete list by ? because  $S_4$  has four 3-regular conjugacy classes. Thus the table of Brauer characters of simple modules in characteristic 3 is

	1	(12)	(12)(34)	(1234)
1	1		1	1
1	-1		1	-1
3	-1		-1	1
3	1		-1	-1

and each is the reduction of a simple module from characteristic zero. The remaining 2-dimensional ordinary representation has Brauer character values 2, 0, 2, 0 and since this Brauer character is uniquely expressible as a linear combination of simple characters, namely the trivial Brauer character plus the sign Brauer character, these two 1-dimensional modules are the composition factors of any reduction modulo 3 of the 2-dimensional representation. We see that the decomposition and Cartan matrices for  $S_4$  in characteristic 3 are

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad C = D^T D = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

In these examples we have exploited the fact that the Brauer characters of the simple representations are independent to obtain the composition factors of the reductions of other modules, since there was a unique linear combination of the simple Brauer characters equal to the reduction of each ordinary simple character. As far as the examples were concerned it was possible to observe that the Brauer characters were independent after computing them, but it is reassuring to know that this is always the case. We prove this now, deducing it as a consequence of orthogonality relations for Brauer characters.

(10.2) PROPOSITION. *Let  $(F, R, k)$  be a  $p$ -modular system in which  $R$  is complete, and let  $G$  be a finite groups. Suppose that  $P$  and  $U$  are finite-dimensional  $kG$ -modules and that  $P$  is projective. Then*

$$\dim \operatorname{Hom}_{kG}(P, U) = \frac{1}{|G|} \sum_{p\text{-regular } g \in G} \phi_P(g^{-1})\phi_U(g).$$

*Proof.* We make use of the isomorphism  $\operatorname{Hom}_{kG}(U, V) \cong \operatorname{Hom}_{kG}(U \otimes_k V^*, k)$  whenever  $U$  and  $V$  are finite-dimensional  $kG$ -modules, which holds since both sides are isomorphic to  $(U^* \otimes_k V)^G$ , using results 3.3 and 3.4. Now  $\operatorname{Hom}_{kG}(P, U) \cong \operatorname{Hom}_{kG}(P \otimes U^*, k)$  and  $P \otimes U^*$  is a projective  $kG$ -module by 8.4. Thus it lifts to a projective  $RG$ -lattice  $P \widehat{\otimes}_k U^*$  and we have

$$\begin{aligned} \dim \operatorname{Hom}_{kG}(P, U) &= \dim \operatorname{Hom}_{kG}(P \otimes U^*, k) \\ &= \operatorname{rank} \operatorname{Hom}_{RG}(P \widehat{\otimes}_k U^*, R) \\ &= \dim \operatorname{Hom}_{FG}(F \otimes_R P \widehat{\otimes}_k U^*, F) \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{F \otimes_R P \widehat{\otimes}_k U^*}(g^{-1})\chi_k(g). \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{F \otimes_R P \widehat{\otimes}_k U^*}(g^{-1}). \end{aligned}$$

We claim that

$$\chi_{F \otimes_R P \widehat{\otimes}_k U^*}(g^{-1}) = \begin{cases} \phi_P(g^{-1})\phi_U(g) & \text{if } g \text{ is } p\text{-regular,} \\ 0 & \text{otherwise,} \end{cases}$$

and from this the result follows. If  $g$  is not  $p$ -regular it has order divisible by  $p$  and the character value is zero by Proposition 9.27, since  $P \widehat{\otimes}_k U^*$  is projective. When  $g$  is  $p$ -regular we calculate the character value by using the fact that it depends only on the structure of  $P$  and  $U$  as  $k\langle g \rangle$ -modules. Since  $k\langle g \rangle$  is a semisimple algebra both  $P$  and  $U^*$  are now projective, and they lift to  $R\langle g \rangle$ -lattices whose tensor product  $\hat{P} \otimes_R \hat{U}^*$  is isomorphic to  $P \widehat{\otimes}_k U^*$  as  $R\langle g \rangle$ -modules, since both of these are projective covers as  $R\langle g \rangle$ -modules of  $P \otimes_k U^*$ . From this we see that

$$\begin{aligned} \chi_{F \otimes_R P \widehat{\otimes}_k U^*}(g^{-1}) &= \chi_{(F \otimes \hat{P}) \otimes (F \otimes \hat{U}^*)}(g^{-1}) \\ &= \chi_{F \otimes \hat{P}}(g^{-1})\chi_{F \otimes \hat{U}^*}(g^{-1}) \\ &= \phi_P(g^{-1})\phi_U(g) \end{aligned}$$

as required. □

There is a similarity between the last result and Corollary ? in the last section, which related the dimensions of homomorphisms between modules in characteristic 0 and in characteristic  $p$ . The subtlety here is that the  $kG$ -module  $U$  might not be liftable to characteristic 0, whereas in ? this was an assumption.

It is convenient to interpret the formula of the last proposition in terms of an inner product on a space of functions, in a similar way to what we did with ordinary characters. Let  $p\text{-reg}(G)$  denote the set of conjugacy classes of  $p$ -regular elements of  $G$ , so that  $p\text{-reg}(G) \subseteq \text{cc}(G)$  where the latter denotes the set of all conjugacy classes of  $G$ . We may regard Brauer characters as elements of the vector space  $\mathbb{C}^{p\text{-reg}(G)}$  of functions

$$p\text{-reg}(G) \rightarrow \mathbb{C}.$$

We define a Hermitian bilinear form on this vector space by

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{p\text{-regular } g \in G} \overline{\phi(g)} \psi(g)$$

and just as with the similarly-defined bilinear form on  $\mathbb{C}^{\text{cc}(G)}$  we note that

$$\langle \phi\theta, \psi \rangle = \langle \phi, \theta^* \psi \rangle$$

where  $\theta^*(g) = \overline{\theta(g)}$ , the complex conjugate. With the notation of this bilinear form the last result now states that if  $P$  and  $U$  are finite-dimensional  $kG$ -modules with  $P$  projective then

$$\dim \text{Hom}_{kG}(P, U) = \langle \phi_P, \phi_U \rangle.$$

(10.3) THEOREM (Row orthogonality relations). *Let  $G$  be a finite group and  $k$  a splitting field for  $G$  of characteristic  $p$ . Let  $S_1, \dots, S_n$  be a complete list of non-isomorphic simple  $kG$ -modules, with projective covers  $P_{S_1}, \dots, P_{S_n}$ . Then the Brauer characters  $\phi_{S_1}, \dots, \phi_{S_n}$  of the simple modules form a basis for  $\mathbb{C}^{p\text{-reg}(G)}$ , as do also the Brauer characters  $\phi_{P_{S_1}}, \dots, \phi_{P_{S_n}}$  of the indecomposable projective modules. These two bases are dual to each other with respect to the bilinear form, in that*

$$\langle \phi_{P_{S_i}}, \phi_{S_j} \rangle = \delta_{i,j}.$$

The bilinear form on  $\mathbb{C}^{p\text{-reg}(G)}$  is non-degenerate.

*Proof.* Everything follows from the formula  $\langle \phi_{P_{S_i}}, \phi_{S_j} \rangle = \delta_{i,j}$  and the fact that the number of non-isomorphic simple modules equals the number of  $p$ -regular conjugacy classes of  $G$ . Thus if  $\sum_{i=1}^n \lambda_j \phi_{S_j} = 0$  we have  $0 = \langle \phi_{P_{S_i}}, \sum_{j=1}^n \lambda_j \phi_{S_j} \rangle = \lambda_j$ , which shows that the  $\phi_{S_j}$  are independent, and hence form a basis. By a similar argument the  $\phi_{P_{S_i}}$  also form a basis. The matrix of the bilinear form with respect to these bases is the identity matrix and it is non-degenerate.  $\square$

This result implies, of course, that the Brauer characters of the simple  $kG$ -modules are linearly independent as functions on the set of  $p$ -regular conjugacy classes of  $G$ , a fact we observed and used in the earlier examples. It means that they are sufficient to distinguish the composition factors of a module.

(10.4) COROLLARY. *Let  $U$  and  $V$  be finite-dimensional  $kG$ -modules, where  $k$  is a field of characteristic  $p$ . Then  $U$  and  $V$  have the same composition factors if and only if their Brauer characters  $\phi_U$  and  $\phi_V$  are equal.*

As an application we may deduce, for example, that if  $S$  is a simple  $kG$ -module then  $S \cong S^*$  if and only if  $\phi_S$  takes real values, since this is the condition that  $\phi_S = \overline{\phi_S} = \phi_{S^*}$ .

It is also true from the theorem that the Brauer characters of the indecomposable projective modules are independent functions on  $p$ -reg( $G$ ), and so Brauer characters enable us to distinguish between projective modules. Since the Brauer characters of a module are determined by its composition factors we have the following consequence.

(10.5) COROLLARY. *Let  $P$  and  $Q$  be projective  $kG$ -modules, where  $k$  is a splitting field of characteristic  $p$ . Then  $P$  and  $Q$  are isomorphic if and only if they have the same composition factors. The Cartan matrix is invertible. The decomposition matrix has maximum rank.*

*Proof.* Write  $P = P_{S_1}^{a_1} \oplus \cdots \oplus P_{S_n}^{a_n}$  and  $Q = P_{S_1}^{b_1} \oplus \cdots \oplus P_{S_n}^{b_n}$  so that  $\phi_P = \sum_{i=1}^n a_i \phi_{P_{S_i}}$  and  $\phi_Q = \sum_{i=1}^n b_i \phi_{P_{S_i}}$ . Then  $P \cong Q$  if and only if  $a_i = b_i$  for all  $i$ , if and only if  $\sum_{i=1}^n a_i \phi_{P_{S_i}} = \sum_{i=1}^n b_i \phi_{P_{S_i}}$  since the  $\phi_{P_{S_i}}$  are linearly independent, if and only if  $\phi_P = \phi_Q$ . By the last corollary this happens if and only if  $P$  and  $Q$  have the same composition factors.

We claim that the kernel of the Cartan homomorphism  $c : K_0(kG) \rightarrow G_0(kG)$  is zero. Any element of  $K_0(kG)$  can be written  $[P] - [Q]$  where  $P$  and  $Q$  are projective modules, and such an element lies in the kernel if and only if  $P$  and  $Q$  have the same composition factors. This forces  $P \cong Q$ , so that the kernel is zero. It now follows that the Cartan homomorphism is an isomorphism.

For the final statement about the decomposition matrix we use the fact that  $C = D^T D$ . Thus  $\text{rank } C \leq \text{rank } D$ . The number of columns of  $D$  equals the number of columns of  $C$ , and this number must be the rank of  $D$ .  $\square$

We may write the row orthogonality relations in various ways. The most rudimentary way is the statement that if  $S$  and  $T$  are simple  $kG$ -modules then

$$\frac{1}{|G|} \sum_{p\text{-regular } g \in G} \phi_{P_T}(g^{-1}) \phi_S(g) = \begin{cases} 1 & \text{if } S \cong T, \\ 0 & \text{otherwise.} \end{cases}$$

We can also express this as a matrix product. Let  $\Phi$  be the table of Brauer character values of simple  $kG$ -modules,  $\Pi$  the table of Brauer character values of indecomposable

projective modules, and let  $B$  be the diagonal matrix whose entries are  $\frac{1}{|C_G(g)|}$  as  $g$  ranges through the  $p$ -regular classes. The row orthogonality relations are

$$\overline{\Pi} B \Phi^T = I.$$

From this we obtain the column orthogonality relations.

(10.6) PROPOSITION (Column orthogonality relations). *With the above notation,*

$$\overline{\Phi}^T \Pi = \begin{pmatrix} |C_G(x_1)| & 0 & \cdots & 0 \\ 0 & |C_G(x_2)| & & \\ \vdots & & \ddots & \vdots \\ 0 & & \cdots & |C_G(x_n)| \end{pmatrix}$$

where  $x_1, \dots, x_n$  are representatives of the  $p$ -regular conjugacy classes of elements of  $G$ . Thus

$$\sum_{\text{simple } S} \phi_S(g^{-1}) \phi_{P_S}(h) = \begin{cases} |C_G(g)| & \text{if } g \text{ and } h \text{ are conjugate,} \\ 0 & \text{otherwise.} \end{cases}$$

The orthogonality relations can be used to determine the composition factors of a representation in a similar way to the procedure with ordinary characters. However this possibility is less useful than in characteristic zero because we need to know the Brauer characters of the indecomposable projectives to make it work. Usually we would only have this information once we have fairly complete information about the simple modules, whereas in characteristic zero we can test for simplicity of a character and subtract known character summands without complete character table information.

The orthogonality relations do allow us to deduce important theoretical information about the Cartan and decomposition matrices.

(10.7) COROLLARY. *Let  $k$  be a splitting field of characteristic  $p$  for the finite group  $G$ . Let  $\Phi$  be the table of values of Brauer characters of the simple  $kG$ -modules,  $\Pi$  the table of values of Brauer characters of the indecomposable projective  $kG$ -modules,  $C$  the Cartan matrix of  $G$  and  $D$  the decomposition matrix of  $G$ . Then*

- (1)  $\Pi = C\Phi$ , and
- (2)  $\Phi$ ,  $\Pi$  and  $C$  are invertible matrices.
- (3)  $D$  has maximum rank.

A finer result than this is true. The determinant of the Cartan matrix over a splitting field of characteristic  $p$  is known to be a power of  $p$ , and the decomposition map  $d : G_0(FG) \rightarrow G_0(kG)$  is a surjective homomorphism of abelian groups. Knowing that its matrix has maximum rank implies only that the cokernel is finite. These results may be proved by a line of argument which originates with the induction theorem of Brauer, a

result which we have skipped over. The surjectivity of  $d$  is in turn implied by the Fong-Swan theorem in the case of  $p$ -solvable groups.

We may interpret the cde triangle in terms of Brauer characters. As before, we let  $\text{cc}(G)$  denote the set of conjugacy classes of  $G$  and  $p\text{-reg}(G)$  the set of  $p$ -regular conjugacy classes of  $G$ . There are group homomorphisms

$$\begin{aligned} K_0(kG) &\rightarrow \mathbb{C}^{p\text{-reg}(G)} \\ G_0(kG) &\rightarrow \mathbb{C}^{p\text{-reg}(G)} \\ G_0(FG) &\rightarrow \mathbb{C}^{\text{cc}(G)} \end{aligned}$$

defined on the basis elements  $[P] \in K_0(kG)$ ,  $[S] \in G_0(kG)$  and  $[T] \in G_0(FG)$ , by

$$[P] \mapsto \phi_P, \quad [S] \mapsto \phi_S, \quad \text{and} \quad [T] \mapsto \chi_T.$$

In fact these same formulas hold whenever  $P$  is an arbitrary finitely-generated projective module and  $S, T$  are arbitrary finitely-generated modules. We may regard each of  $K_0(kG)$ ,  $G_0(kG)$  and  $G_0(FG)$  as lattices in complex vector spaces obtained by extending the scalars from  $\mathbb{Z}$  to  $\mathbb{C}$ . Because each of the above assignments is a correspondence of basis elements, the resulting linear maps they define are isomorphisms of vector spaces

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{Z}} K_0(kG) &\cong \mathbb{C}^{p\text{-reg}(G)} \\ \mathbb{C} \otimes_{\mathbb{Z}} G_0(kG) &\cong \mathbb{C}^{p\text{-reg}(G)} \\ \mathbb{C} \otimes_{\mathbb{Z}} G_0(FG) &\cong \mathbb{C}^{\text{cc}(G)}. \end{aligned}$$

Thus the cde triangle, on extending scalars to  $\mathbb{C}$ , yields a triangle of vector spaces

$$\begin{array}{ccc} & \mathbb{C}^{\text{cc}(G)} & \\ & \nearrow e & \searrow d \\ \mathbb{C}^{p\text{-reg}(G)} & \xrightarrow{c} & \mathbb{C}^{p\text{-reg}(G)} \end{array}$$

where, as before, the maps  $c, d, e$  have matrices  $C, D^T$  and  $D$ , respectively.

(10.8) PROPOSITION. *Let  $(F, R, k)$  be a splitting  $p$ -modular system for  $G$ . With this interpretation of the cde triangle, if  $\phi \in \mathbb{C}^{p\text{-reg}(G)}$  then  $e(\phi)$  is the function which is the same as  $\phi$  on  $p$ -regular conjugacy classes and is zero on the other conjugacy classes. If  $\chi \in \mathbb{C}^{\text{cc}(G)}$  then  $d(\chi)$  is the restriction of  $\chi$  to the  $p$ -regular conjugacy classes. The Cartan homomorphism  $c$  is an isomorphism, the decomposition map  $d$  is surjective, and  $e$  is injective. The image of  $e$  is the space of class functions which are non-zero only on  $p$ -regular classes.*

*Proof.* The description of  $e(\phi)$  follows from Proposition 9.27 and the definition of  $e$ , whereas the description of  $d$  comes from part (6) of Proposition 10.1. The Cartan

homomorphism is an isomorphism because the Cartan matrix is non-singular, and because the decomposition matrix  $D$  has maximal rank  $d$  is surjective and  $e$  is injective. The image of  $e$  is a space whose dimension is the number of  $p$ -regular conjugacy classes of  $G$ , and it is contained in the space of maps whose support is the set of  $p$ -regular conjugacy classes, so we must have equality.  $\square$

*Exercises for Section 10.*

1. If  $\theta \in \mathbb{C}^{p\text{-reg}(H)}$  is a function defined on the set of  $p$ -regular conjugacy classes we may define an *induced* function  $\theta \uparrow_H^G$  by means of the same formula in Proposition 4.10 which was used to define induction of ordinary class functions. Let  $H$  be a subgroup of  $G$  and let  $U$  be a finite-dimensional  $kH$ -module with Brauer character  $\phi_U$ , where  $k$  is a field of characteristic  $p$ . Prove that  $\phi_{U \uparrow_H^G} = \phi_U \uparrow_H^G$ , and that  $e(\theta \uparrow_H^G) = e(\theta) \uparrow_H^G$  and  $d(\chi \uparrow_H^G) = d(\chi) \uparrow_H^G$  if  $\chi$  is a class function.

Similarly define the restriction  $\psi \downarrow_H^G$  where  $\psi \in \mathbb{C}^{p\text{-reg}(G)}$  and show that similar formulas hold.

Show that  $\langle \theta \uparrow_H^G, \psi \rangle = \langle \theta, \psi \downarrow_H^G \rangle$  always holds.

2. Let  $(F, R, k)$  be a splitting  $p$ -modular system for  $G$ . Let  $P$  and  $Q$  be finitely-generated projective  $RG$ -modules such that  $F \otimes_R P \cong F \otimes_R Q$  as  $FG$ -modules. Show that  $P \cong Q$ .

3. The simple group  $GL(3, 2)$  has order  $168 = 8 \cdot 3 \cdot 7$ . The following is part of its ordinary character table (the first two rows list the orders of centralizers of elements, and then underneath the orders of elements in the conjugacy classes):

168	8	4	3	7	7
1	2	4	3	7A	7B
1	1	1	1	1	1
3	-1	1		$\alpha$	$\bar{\alpha}$
6	2	0		-1	-1
7	-1	-1	1		
8			-1	1	1

Here  $\alpha = \hat{\eta} + \hat{\eta}^2 + \hat{\eta}^4$  where  $\hat{\eta} = e^{2\pi i/7}$ . Note that  $\alpha^2 = \bar{\alpha} - 1$  and  $\alpha\bar{\alpha} = 2$ .

- (a) Obtain the complete character table of  $GL(3, 2)$ .
- (b) Compute the table of Brauer characters of simple  $\mathbb{F}_2[GL(3, 2)]$ -modules.
- (c) Find the decomposition matrix and Cartan matrix of  $GL(3, 2)$  at the prime 2.
- (d) Write down the table of Brauer characters of projective  $\mathbb{F}_2[GL(3, 2)]$ -modules.
- (e) Determine the direct sum decomposition of the module  $8 \otimes 3$  (where 8 and 3 denote  $\mathbb{F}_2[GL(3, 2)]$ -modules of those dimensions), as a direct sum of indecomposable modules.
- (f) Determine the composition factors of  $3 \otimes 3$  and  $3 \otimes 3^*$ , where 3 denotes the natural 3-dimensional  $\mathbb{F}_2[GL(3, 2)]$ -module.

[On approach is to use the orthogonality relations.]

4. Let  $p$  be an odd prime. The center of  $SL(2, p)$  consists of the two scalar matrices  $\{\pm I\}$  (do not prove this), and the group  $PSL(2, p)$  is defined to be  $SL(2, p)/\{\pm I\}$ . The simple  $\mathbb{F}_p[SL(2, p)]$ -modules thus consist of the simple  $\mathbb{F}_p[PSL(2, p)]$ -modules, together with those simple modules on which  $-I$  acts non-trivially.

The simple  $\mathbb{F}_p[SL(2, p)]$ -modules were constructed in Exercise 21 of Section 6 as the symmetric powers  $S^r(U_2)$  of the natural 2-dimensional representation  $U_2$  where  $0 \leq r \leq p - 1$ . Show that  $-I$  acts trivially on such a simple  $\mathbb{F}_p[SL(2, p)]$ -module if and only if the module has odd dimension. Deduce that the simple  $\mathbb{F}_p[PSL(2, p)]$ -modules have dimensions  $1, 3, 5, \dots, p$ , constructed as the even symmetric powers of the 2-dimensional  $\mathbb{F}_p[SL(2, p)]$ -module.

5. It so happens that  $GL(3, 2) \cong PSL(2, 7)$ .

(a) Construct the table of Brauer characters of simple  $\mathbb{F}_7[PSL(2, 7)]$ -modules.

[It will help to observe that an element of order 8 in  $SL(2, 7)$  represents an element of order 4 in  $PSL(2, 7)$ , and its square represents an element of order 2.]

(b) Compute the decomposition and Cartan matrices for  $PSL(2, 7)$  in characteristic 7. Show that the projective cover of the trivial module,  $P_1$ , has just four submodules, namely  $0$ ,  $P_1$  and two others.

## 11. Indecomposable modules

Until now the indecomposable modules we have considered have mostly been the simple and projective modules, and for these we have obtained straightforward descriptions in the case of an algebra which is finite-dimensional over a field, or of finite rank over a complete discrete valuation ring.

We now consider indecomposable modules in general and we start with some of their basic properties. We first present an extension of Proposition 7.4, combined with Lemma 2.2.

(11.1) PROPOSITION. *Let  $U$  be a module for a ring  $A$  with a 1. Expressions*

$$U = U_1 \oplus \cdots \oplus U_n$$

*as a direct sum of submodules biject with expressions  $1_U = e_1 + \cdots + e_n$  for the identity  $1_U \in \text{End}_A(U)$  as a sum of orthogonal idempotents. Here  $e_i$  is the composite of projection and inclusion  $U \rightarrow U_i \rightarrow U$ , and  $U_i = e_i(U)$ . The summand  $U_i$  is indecomposable if and only if  $e_i$  is primitive.*

*Proof.* We must check several things. Two constructions are indicated in the statement of the proposition, whereby given a direct sum decomposition of  $U$  we obtain an idempotent decomposition of  $1_U$ , and vice-versa. It is clear that the idempotents constructed from a module decomposition are orthogonal and sum to  $1_U$ . Conversely, given an expression  $1_U = e_1 + \cdots + e_n$  as a sum of orthogonal idempotents, every element  $u \in U$  can be written  $u = e_1u + \cdots + e_nu$  where  $e_iu \in e_iU = U_i$ . In any expression  $u = u_1 + \cdots + u_n$  with  $u_i \in e_iU$  we have  $e_ju_i \in e_je_iU = 0$  if  $i \neq j$  so  $e_iu = e_iu_i = u_i$ , and this expression is uniquely determined. Thus the expression  $1_U = e_1 + \cdots + e_n$  gives rise to a direct sum decomposition.

We see that  $U_i$  decomposes as  $U_i = V \oplus W$  if and only if  $e_i = e_V + e_W$  can be written as a sum of orthogonal idempotents, and so  $U_i$  is indecomposable if and only if  $e_i$  is primitive.  $\square$

(11.2) COROLLARY. *An  $A$ -module  $U$  is indecomposable if and only if the only non-zero idempotent in  $\text{End}_A(U)$  is  $1_U$ .*

*Proof.* From the proposition,  $U$  is indecomposable if and only if  $1_U$  is primitive, and this happens if and only if  $1_U$  and  $0$  are the only idempotents in  $\text{End}_A(U)$ . This last implication in the forward direction follows since any idempotent  $e$  gives rise to an expression  $1_U = e + (1_U - e)$  as a sum of orthogonal idempotents.  $\square$

Our next step is to pin down the structure of the endomorphism ring of an indecomposable module.

(11.3) PROPOSITION. *Let  $B$  be a ring with 1. The following are equivalent.*

- (1)  $B$  has a unique maximal left ideal.
- (2)  $B$  has a unique maximal right ideal.
- (3)  $B/\text{Rad}(B)$  is a division ring.
- (4) The set of elements in  $B$  which are not invertible forms a left ideal.
- (5) The set of elements in  $B$  which are not invertible forms a right ideal.
- (6) The set of elements in  $B$  which are not invertible forms a 2-sided ideal.

*Proof.* (1)  $\Rightarrow$  (3) Let  $I$  be the unique maximal left ideal of  $B$ . Since  $\text{Rad}(B)$  is the intersection of the maximal left ideals, it follows that  $I = \text{Rad}(B)$ . If  $a \in B - I$  then  $Ba$  is a left ideal not contained in  $I$ , so  $Ba = B$ . Thus there exists  $x \in B$  with  $xa = 1$ . Furthermore  $x \notin I$ , so  $Bx = B$  also and there exists  $y \in B$  with  $yx = 1$ . Now  $yx a = a = y$  so  $a$  and  $x$  are 2-sided inverses of one another. This implies that  $B/I$  is a division ring.

(1)  $\Rightarrow$  (6) The argument just presented shows that the unique maximal left ideal  $I$  is in fact a 2-sided ideal, and every element not in  $I$  is invertible. This implies that every non-invertible element is contained in  $I$ . Equally, no element of  $I$  can be invertible, so  $I$  consists of the non-invertible elements, and they form a 2-sided ideal.

(3)  $\Rightarrow$  (1) If  $I$  is a maximal left ideal of  $B$  then  $I \supseteq \text{Rad}(B)$  and so corresponds to a left ideal of  $B/\text{Rad}(B)$ , which is a division ring. It follows that either  $I = \text{Rad}(B)$  or  $I = B$ , and so  $\text{Rad}(B)$  is the unique maximal left ideal of  $B$ .

(4)  $\Rightarrow$  (1) Let  $J$  be the set of non-invertible elements of  $B$  and  $I$  a maximal left ideal. Then no element of  $I$  is invertible, so  $I \subseteq J$ . Since  $J$  is an ideal, we have equality, and  $I$  is unique.

(6)  $\Rightarrow$  (4) This implication is immediate, and so we have established the equivalence of conditions (1), (3), (4) and (6).

Since conditions (3) and (6) are left-right symmetric, it follows that they are also equivalent to conditions (2) and (5), by analogy with the equivalence with (1) and (4).  $\square$

We will call a ring  $B$  satisfying any of the equivalent conditions of the last proposition a *local ring*. Any commutative ring which is local in the usual sense (i.e. it has a unique maximal ideal) is evidently local in the non-commutative sense. We see also that if  $G$  is a  $p$ -group and  $k$  is a field of characteristic  $p$  then the group algebra  $kG$  is a local ring, because its radical is the augmentation ideal and the quotient by the radical is  $k$ , which is a division ring.

In our application of 11.3 to the proof of the Krull-Schmidt theorem we will want to know that in a local ring every element outside the radical is invertible. We point out also that if  $B$  is a ring with a 2-sided ideal  $I$  which is nilpotent and for which  $B/I$  is a division ring, then necessarily  $B$  is local. This will, at one point, be a useful way of showing that a ring is local. We also see that in a local ring  $B$ , the only idempotents are 0 and 1. (Any

other idempotent would give a direct sum decomposition of  $B$ , and hence more than one maximal left ideal.) Combining this with Corollary 11.2, any module which has a local endomorphism ring must necessarily be indecomposable, without restriction on the ring for which this is a module. In special circumstances we obtain also the converse implication, as will now be shown.

(11.4) PROPOSITION. *Suppose that  $B$  is an  $R$ -algebra which is finitely generated as an  $R$ -module, where  $R$  is a complete discrete valuation ring or a field. Then  $B$  is a local ring if and only if the only non-zero idempotent in  $B$  is 1.*

*Proof.* We have just observed that if  $B$  is a local ring then the only idempotents are 0 and 1. Conversely, suppose that 0 and 1 are the only idempotents in  $B$ , and let  $(\pi)$  be the maximal ideal of  $R$ . Just as in the proof of part (1) of Proposition 9.12 we see that  $\pi$  annihilates every simple  $B$ -module, and so  $\pi B \subseteq \text{Rad}(B)$ . This implies that  $B/\text{Rad}(B)$  is a finite-dimensional  $R/(\pi)$ -algebra. If  $e \in B/\text{Rad}(B)$  is idempotent then by the argument of Proposition 9.14 it lifts to an idempotent of  $B$ , which must be 0 or 1. Since  $e$  is the image of this lifting, it must also be 0 or 1. Now  $B/\text{Rad}(B) \cong M_{n_1}(\Delta_1) \oplus \cdots \oplus M_{n_t}(\Delta_t)$  for certain division rings  $\Delta_i$ , since this is a semisimple algebra, and the only way this algebra would have just one non-zero idempotent is if  $t = 1$  and  $n_1 = 1$ . This shows that condition (3) of the last proposition is satisfied.  $\square$

(11.5) COROLLARY. *Let  $U$  be a finitely-generated  $RG$ -module where  $R$  is a complete discrete valuation ring or a field and  $G$  is a finite group. Then  $U$  is indecomposable if and only if  $\text{End}_{RG}(U)$  is a local ring.*

*Proof.* Putting together the last results, all we need to do is to show that  $\text{End}_{RG}(U)$  is finitely-generated as an  $R$ -module. Let  $R^m \rightarrow U$  be a surjection of  $R$ -modules. Composition with this surjection gives a homomorphism  $\text{End}_{RG}(U) \rightarrow \text{Hom}_R(R^m, U)$ , and it is an injection since  $R^m \rightarrow U$  is surjective. Thus  $\text{End}_{RG}(U)$  is realized as an  $R$ -submodule of  $\text{Hom}_R(R^m, U) \cong U^m$ , which is a finitely generated  $R$ -module. Since  $R$  is Noetherian, the submodule is also finitely-generated.  $\square$

(11.6) THEOREM (Krull-Schmidt). *Let  $A$  be a ring with a 1, and suppose that  $U$  is an  $A$ -module which has two  $A$ -module decompositions*

$$U = U_1 \oplus \cdots \oplus U_r = V_1 \oplus \cdots \oplus V_s$$

*where for each  $i$ ,  $\text{End}_A(U_i)$  and  $\text{End}_A(V_i)$  are local rings. Then  $r = s$  and the summands  $U_i$  and  $V_j$  are isomorphic in pairs when taken in a suitable order.*

*Proof.* The proof is by induction on  $\max\{r, s\}$ . When this number is 1 we have  $U = U_1 = V_1$ , and this starts the induction.

Now suppose  $\max\{r, s\} > 1$  and the result is true for smaller values of  $\max\{r, s\}$ . For each  $j$  let  $\pi_j : U \rightarrow V_j$  be projection onto the  $j$ th summand with respect to the decomposition  $U = V_1 \oplus \cdots \oplus V_s$ , and let  $\iota_j : V_j \hookrightarrow U$  be inclusion. Then  $\sum_{j=1}^s \iota_j \pi_j = 1_U$ . Now let  $\beta : U \rightarrow U_1$  be projection with respect to the decomposition  $U = U_1 \oplus \cdots \oplus U_r$  and  $\alpha : U_1 \hookrightarrow U$  be inclusion so that  $\beta\alpha = 1_{U_1}$ . We have

$$1_{U_1} = \beta \left( \sum_{j=1}^s \iota_j \pi_j \right) \alpha = \sum_{j=1}^s \beta \iota_j \pi_j \alpha$$

and since  $\text{End}_A(U_1)$  is a local ring it follows that at least one term  $\beta \iota_j \pi_j \alpha$  must be invertible. By renumbering the  $V_j$  if necessary we may suppose that  $j = 1$ , and we write  $\phi = \beta \iota_1 \pi_1 \alpha$ . Now  $(\phi^{-1} \beta \iota_1)(\pi_1 \alpha) = 1_{U_1}$  and so  $\pi_1 \alpha : U_1 \rightarrow V_1$  is split mono and  $\phi^{-1} \beta \iota_1 : V_1 \rightarrow U_1$  is split epi. It follows that  $\pi_1 \alpha(U_1)$  is a direct summand of  $V_1$ . Since  $\text{End}_A(V_1)$  is local,  $V_1$  is indecomposable and so  $\pi_1 \alpha(U_1) = V_1$ . Thus  $\pi_1 \alpha : U_1 \rightarrow V_1$  is an isomorphism.

We now show that  $U = U_1 \oplus V_2 \oplus \cdots \oplus V_s$ . Because  $\pi_1 \alpha$  is an isomorphism,  $\pi_1$  is one-to-one on the elements of  $U_1$ . Also  $\pi_1$  is zero on  $V_2 \oplus \cdots \oplus V_s$  and it follows that  $U_1 \cap (V_2 \oplus \cdots \oplus V_s) = 0$ , since any element of the intersection is detected by its image under  $\pi_1$ , and this must be zero. The submodule  $U_1 + V_2 + \cdots + V_s$  contains  $V_2 + \cdots + V_s = \text{Ker } \pi_1$  and so corresponds via the first isomorphism theorem for modules to a submodule of  $\pi_1(U) = V_1$ . In fact  $\pi_1$  is surjective and so  $U_1 + V_2 + \cdots + V_s = U$ . It follows that  $U = U_1 \oplus V_2 \oplus \cdots \oplus V_s$ .

We now deduce that  $U/U_1 \cong U_2 \oplus \cdots \oplus U_r \cong V_2 \oplus \cdots \oplus V_s$ . It follows by induction that  $r = s$  and the summands are isomorphic in pairs, which completes the proof.  $\square$

(11.7) COROLLARY. *Let  $R$  be a complete discrete valuation ring or a field and  $G$  a finite group. Suppose that  $U$  is a finitely-generated  $RG$ -module which has two decompositions*

$$U = U_1 \oplus \cdots \oplus U_r = V_1 \oplus \cdots \oplus V_s$$

*where the  $U_i$  and  $V_j$  are indecomposable  $RG$ -modules. Then  $r = s$  and the summands  $U_i$  and  $V_j$  are isomorphic in pairs when taken in a suitable order.*

### Relative projectivity

Let  $H$  be a subgroup of  $G$  and  $R$  a commutative ring with 1. An  $RG$ -module is said to be  $H$ -free if it has the form  $V \uparrow_H^G$  for some  $RH$ -module  $V$ . It is  $H$ -projective, or *projective relative to  $H$* , if it is a direct summand of a module of the form  $V \uparrow_H^G$  for some  $RH$ -module  $V$ .

For example, the regular representation  $RG \cong R \uparrow_1^G$  is 1-free, and projective modules are 1-projective. If  $R$  is a field then every 1-projective module is projective, but if  $R$  is not a field and  $V$  is an  $R$ -module which is not projective as an  $R$ -module, then  $V \uparrow_1^G$  is 1-free but not projective as an  $RG$ -module. Every  $RG$ -module is  $G$ -projective.

In order to investigate relative projectivity we first deal with some technicalities. We have seen the pervasive importance of the group ring element  $\sum_{g \in G} g$  at every stage of the development of representation theory. As an operator on any representation of  $G$  it has image contained in the  $G$ -fixed points. We now consider something more general, and for a subgroup  $H$  of  $G$  and an  $RG$ -module  $U$  we define the *relative trace map*  $\text{tr}_H^G : U^H \rightarrow U^G$ . To define this we choose a set of representatives  $g_1, \dots, g_t$  of the left cosets of  $H$  in  $G$ , so  $G = g_1H \cup \dots \cup g_tH$ . If  $u \in U^H$  we define  $\text{tr}_H^G(u) = \sum_{i=1}^t g_i u$ .

(11.8) LEMMA. *The homomorphism  $\text{tr}_H^G$  is well-defined, and if  $K \leq H \leq G$  are subgroups then  $\text{tr}_H^G \text{tr}_K^H = \text{tr}_K^G$ .*

(11.9) LEMMA. *Suppose that  $\alpha : U \rightarrow V$  and  $\gamma : W \rightarrow X$  are homomorphisms of  $RG$ -modules and that  $\beta : V \downarrow_H^G \rightarrow W \downarrow_H^G$  is an  $RH$ -module homomorphism. Then  $(\text{tr}_H^G \beta) \circ \alpha = \text{tr}_H^G(\beta \circ \alpha)$  and  $\gamma \circ (\text{tr}_H^G \beta) = \text{tr}_H^G(\gamma \circ \beta)$ .*

*Proof.* Let  $g_1, \dots, g_n$  be a set of left coset representatives for  $H$  in  $G$  and  $u \in U$ . Then  $(\text{tr}_H^G \beta)\alpha(u) = \sum_{i=1}^n g_i \beta(g_i^{-1} \alpha u) = \sum_{i=1}^n g_i \beta \alpha(g_i^{-1} u) = \text{tr}_H^G(\beta \alpha)(u)$ . Similarly  $\gamma(\text{tr}_H^G \beta)(u) = \gamma \sum_{i=1}^n g_i \beta(g_i^{-1} u) = \sum_{i=1}^n g_i \gamma \beta(g_i^{-1} u) = \text{tr}_H^G(\gamma \beta)(u)$ .  $\square$

(11.10) COROLLARY. *The image of  $\text{tr}_H^G : \text{End}_{RH}(U) \rightarrow \text{End}_{RG}(U)$  is an ideal.*

It will help us to consider the adjoint properties of induction and restriction of modules in detail. We have seen in result 4.12 that when  $U$  is an  $RH$ -module and  $V$  is an  $RG$ -module, where  $H \leq G$ , we have  $\text{Hom}_{RG}(U \uparrow_H^G, V) \cong \text{Hom}_{RH}(U, V \downarrow_H^G)$ . There may be many such isomorphisms, but there is a choice which is *natural* in  $U$  and  $V$ . This means that whenever  $U_1 \rightarrow U_2$  is an  $RG$ -module homomorphism the resulting square

$$\begin{array}{ccc} \text{Hom}_{RG}(U_1 \uparrow_H^G, V) & \longrightarrow & \text{Hom}_{RH}(U_1, V \downarrow_H^G) \\ \uparrow & & \uparrow \\ \text{Hom}_{RG}(U_2 \uparrow_H^G, V) & \longrightarrow & \text{Hom}_{RH}(U_2, V \downarrow_H^G) \end{array}$$

commutes, as does the square

$$\begin{array}{ccc} \mathrm{Hom}_{RG}(U \uparrow_H^G, V_1) & \longrightarrow & \mathrm{Hom}_{RH}(U, V_1 \downarrow_H^G) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{RG}(U \uparrow_H^G, V_2) & \longrightarrow & \mathrm{Hom}_{RH}(U, V_2 \downarrow_H^G) \end{array}$$

whenever  $V_1 \rightarrow V_2$  is a homomorphism of  $RG$ -modules. In this situation we say that the operation  $\uparrow_H^G: RH\text{-modules} \rightarrow RG\text{-modules}$  is *left adjoint* to  $\downarrow_H^G: RG\text{-modules} \rightarrow RH\text{-modules}$ . (These ‘operations’ are in fact *functors*.) We say also that  $\downarrow_H^G$  is *right adjoint* to  $\uparrow_H^G$ .

We now describe explicitly a natural isomorphism between these groups of homomorphisms. For convenience we take a set of left coset representatives of  $H$  in  $G$  with  $g_1 = 1$ . For each  $RH$ -module  $U$  let  $\mu: U \rightarrow U \uparrow_H^G \downarrow_H^G = \bigoplus_{i=1}^n g_i \otimes U$  be the inclusion into the summand  $1 \otimes U$ , so  $\mu(u) = 1 \otimes u$ , and let  $\nu: U \uparrow_H^G \downarrow_H^G \rightarrow U$  be projection onto this summand. If  $V$  is an  $RG$ -module we define  $RG$ -module homomorphisms  $\eta: V \rightarrow V \downarrow_H^G \uparrow_H^G$  and  $\epsilon: V \downarrow_H^G \uparrow_H^G \rightarrow V$  by  $\eta(v) = \sum_{i=1}^n g_i \otimes g_i^{-1}v$  and  $\epsilon(\sum \lambda_x x \otimes u) = \sum \lambda_x x u$ . In fact, regarding  $\mathrm{tr}_H^G: \mathrm{Hom}_{RH}(V, V \downarrow_H^G \uparrow_H^G) \rightarrow \mathrm{Hom}_{RG}(V, V \downarrow_H^G \uparrow_H^G)$  we have  $\eta = \mathrm{tr}_H^G \mu$  where  $\mu$  has domain  $V$  regarded as an  $RH$ -module. Similarly  $\epsilon = \mathrm{tr}_H^G \nu$ , and this shows that  $\eta$  and  $\epsilon$  are defined independently of the choice of coset representatives. We see that  $\eta$  is a monomorphism,  $\epsilon$  is an epimorphism and their composite is multiplication by  $|G:H|$ .

Given an  $RG$ -module homomorphism  $U \uparrow_H^G \rightarrow V$  we obtain an  $RG$ -module homomorphism  $U \xrightarrow{\mu} U \uparrow_H^G \downarrow_H^G \xrightarrow{\alpha} V \downarrow_H^G$ , and given an  $RH$ -module homomorphism  $\beta: U \rightarrow V \downarrow_H^G$  we obtain an  $RG$ -module homomorphism  $U \uparrow_H^G \xrightarrow{\beta \uparrow_H^G} V \downarrow_H^G \uparrow_H^G \xrightarrow{\epsilon} V$ . We may check that these two constructions are mutually inverse, and are natural in  $U$  and  $V$ .

Group rings of finite groups have the special property that not only is induction left adjoint to restriction, it is also right adjoint. This coincidence of the left and right adjoint of restriction is related to other phenomena we have studied, such as the fact that over a field projective and injective modules are the same thing. We construct a natural isomorphism

$$\mathrm{Hom}_{RG}(V, U \uparrow_H^G) \cong \mathrm{Hom}_{RH}(V \downarrow_H^G, U)$$

whenever  $U$  is an  $RH$ -module and  $V$  is an  $RG$ -module. Given an  $RG$ -module homomorphism  $\alpha: V \rightarrow U \uparrow_H^G$  we obtain an  $RH$ -module homomorphism

$$V \downarrow_H^G \xrightarrow{\alpha} U \uparrow_H^G \downarrow_H^G \xrightarrow{\nu} U$$

and given an  $RH$ -module homomorphism  $\beta: V \downarrow_H^G \rightarrow U$  we obtain an  $RG$ -module homomorphism

$$V \xrightarrow{\eta} V \downarrow_H^G \uparrow_H^G \xrightarrow{\beta \uparrow_H^G} U \uparrow_H^G.$$

Again we check that these operations are natural and mutually inverse.

(11.11) PROPOSITION. *Let  $G$  be a finite group with a subgroup  $H$ . The following are equivalent for an  $RG$ -module  $U$ .*

- (1)  $U$  is  $H$ -projective.
- (2) Whenever we have homomorphisms

$$\begin{array}{ccc} & & U \\ & & \downarrow \psi \\ V & \xrightarrow{\phi} & W \end{array}$$

where  $\phi$  is an epimorphism and for which there exists an  $RH$ -module homomorphism  $U \downarrow_H^G \rightarrow V \downarrow_H^G$  making the diagram commute, then there exists an  $RG$ -module homomorphism  $U \rightarrow V$  making the diagram commute.

- (3) Whenever  $\phi : V \rightarrow U$  is a homomorphism of  $RG$ -modules such that  $\phi \downarrow_H^G : V \downarrow_H^G \rightarrow U \downarrow_H^G$  is a split epimorphism of  $RH$ -modules, then  $\phi$  is a split epimorphism of  $RG$ -modules.
- (4) The surjective homomorphism of  $RG$ -modules

$$\begin{aligned} U \downarrow_H^G \uparrow_H^G = RG \otimes_{RH} U &\rightarrow U \\ x \otimes u &\mapsto xu \end{aligned}$$

is split.

- (5)  $U$  is a direct summand of  $U \downarrow_H^G \uparrow_H^G$ .
- (6) (Higman's criterion)  $1_U$  lies in the image of  $\text{tr}_H^G : \text{End}_{RH}(U) \rightarrow \text{End}_{RG}(U)$ .

*Proof.* (1)  $\Rightarrow$  (2) We first prove this implication in the special case when  $U$  is an induced module  $T \uparrow_H^G$ . Suppose we have a diagram of  $RG$ -modules

$$\begin{array}{ccc} & & T \uparrow_H^G \\ & & \downarrow \psi \\ V & \xrightarrow{\phi} & W \end{array}$$

and a homomorphism of  $RH$ -modules  $\alpha : T \uparrow_H^G \downarrow_H^G \rightarrow V \downarrow_H^G$  so that  $\psi = \phi\alpha$ . Under the adjoint correspondence  $\psi$  corresponds to the composite  $T \xrightarrow{\mu} T \uparrow_H^G \downarrow_H^G \xrightarrow{\psi} W \downarrow_H^G$  and we have a commutative triangle of  $RH$ -module homomorphisms

$$\begin{array}{ccc} & & T \\ & \swarrow \alpha\mu & \downarrow \psi\mu \\ V \downarrow_H^G & \xrightarrow{\phi \downarrow_H^G} & W \downarrow_H^G \end{array}$$

By the adjoint correspondence (and its naturality) this corresponds to a commutative triangle of  $RG$ -module homomorphisms

$$\begin{array}{ccc}
 & & T \uparrow_H^G \\
 & \epsilon(\alpha\mu) \uparrow_H^G & \downarrow \psi \\
 V & \xrightarrow{\phi} & W
 \end{array}$$

which proves this implication for the module  $T \uparrow_H^G$ .

Now consider a module  $U$  which is a summand of  $T \uparrow_H^G$ , and let  $U \xrightarrow{\iota} T \uparrow_H^G \xrightarrow{\pi} U$  be inclusion and projection. We suppose there is a homomorphism  $\alpha : U \downarrow_H^G \rightarrow V \downarrow_H^G$  so that  $\phi\alpha = \psi$ . The homomorphism  $\psi\pi : T \uparrow_H^G \rightarrow W$  has the property that  $\psi\pi = \phi(\alpha\pi)$  and so by what we proved there is a homomorphism of  $RG$ -modules  $\beta : T \uparrow_H^G \rightarrow V$  so that  $\phi\beta = \psi\pi$ . Now  $\phi\beta\iota = \psi\pi\iota = \psi$  so that  $\beta\iota : U \rightarrow V$  is an  $RG$ -module homomorphism which makes the triangle commute.

(2)  $\Rightarrow$  (3) This follows immediately on applying (2) to the diagram

$$\begin{array}{ccc}
 & & U \\
 & & \downarrow 1_U \\
 V & \longrightarrow & U
 \end{array}$$

(3)  $\Rightarrow$  (4) We know that  $\epsilon : U \downarrow_H^G \uparrow_H^G \rightarrow U$  is split as an  $RH$ -module homomorphism by  $\mu : U \rightarrow U \downarrow_H^G \uparrow_H^G$ . Applying condition (3) it splits as an  $RG$ -module homomorphism.

(4)  $\Rightarrow$  (5) and (5)  $\Rightarrow$  (1) are immediate.

(5)  $\Rightarrow$  (6) We may prove that  $1_U \downarrow_H^G \uparrow_H^G = \text{tr}_H^G(\mu\nu)$  by direct computation. Writing  $U \downarrow_H^G \uparrow_H^G = V_1 \oplus V_2$  where  $V_1 = U$ , we can represent  $\mu\nu$  as a matrix

$$\mu\nu = \begin{pmatrix} f_{11} & f_{21} \\ f_{12} & f_{22} \end{pmatrix}$$

where  $f_{ij} : V_i \rightarrow V_j$ . Then

$$\text{tr}_H^G(\mu\nu) = \begin{pmatrix} \text{tr}_H^G f_{11} & \text{tr}_H^G f_{21} \\ \text{tr}_H^G f_{12} & \text{tr}_H^G f_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and from this we see that for every summand of  $U \downarrow_H^G \uparrow_H^G$  (and in particular for  $U$ ) the identity map on that summand is in the image of  $\text{tr}_H^G$ .

(6)  $\Rightarrow$  (5) Write  $1_U = \text{tr}_H^G \alpha$  for some morphism  $\alpha : U \downarrow_H^G \rightarrow U \downarrow_H^G$ . Now  $\alpha$  corresponds by the adjoint correspondence to the composite homomorphism

$$U \xrightarrow{\eta} U \downarrow_H^G \uparrow_H^G \xrightarrow{\alpha \uparrow_H^G} U \downarrow_H^G \uparrow_H^G.$$

We claim that  $\alpha \uparrow_H^G \eta$  splits  $\epsilon$ : for

$$\epsilon \alpha \uparrow_H^G \eta = \text{tr}_H^G(\nu) \alpha \uparrow_H^G \eta = \text{tr}_H^G(\nu \alpha \uparrow_H^G \eta) = \text{tr}_H^G(\alpha) = 1_U.$$

□

Condition (6) is in fact equivalent to the statement that  $\text{tr}_H^G : \text{End}_{RH}(U) \rightarrow \text{End}_{RG}(U)$  is surjective. This is because the image of  $\text{tr}_H^G$  is an ideal in  $\text{End}_{RG}(U)$ , and so it equals  $\text{End}_{RG}(U)$  if and only if it contains  $1_U$ . Conditions (2), (3) and (4) are modeled on conditions associated with the notion of projectivity. There are dual conditions associated with the notion of an injective module, obtained by reversing the arrows and interchanging the words ‘epimorphism’ and ‘monomorphism’. These conditions are also equivalent to the ones stated in this result. In fact, the notion of relative projectivity in the context of group algebras of finite groups might have been termed relative injectivity with equal validity.

(11.12) PROPOSITION. *Suppose that  $H$  is a subgroup of  $G$  and that  $|G : H|$  is invertible in the ring  $R$ . Then every  $RG$ -module is  $H$ -projective.*

*Proof.* For any  $RG$ -module  $U$  we may write  $1_U = \frac{1}{|G:H|} \text{tr}_H^G 1_U$ , thus verifying condition (6) of the last result.  $\square$

(11.13) COROLLARY. *Suppose that  $H$  is a subgroup of  $G$  for which  $|G : H|$  is invertible in the ring  $R$ , and let  $U$  be an  $RG$ -module. Then  $U$  is projective as an  $RG$ -module if and only if  $U \downarrow_H^G$  is projective as an  $RG$ -module.*

*Proof.* We already know that if  $U$  is projective then  $U \downarrow_H^G$  is projective, no matter what subgroup  $H$  is. conversely, if  $U \downarrow_H^G$  is projective it is a summand of a free module  $RH^n$ . Since  $U$  is  $H$ -projective it is a summand of  $U \downarrow_H^G \uparrow_H^G$ , which is a summand of  $RH^n \uparrow_H^G \cong RG^n$ . Therefore  $U$  is projective.  $\square$

This criterion for projectivity would have simplified matters when we were considering the projective modules for groups of the form  $G = H \rtimes K$  in Section 8. In this situation we saw that  $RG$  becomes an  $RG$ -module where  $H$  acts by left multiplication and  $K$  acts by conjugation. If  $K$  has order prime to  $p$  and  $R$  is a field of characteristic  $p$  (or a discrete valuation ring with residue field of characteristic  $p$ ) it follows from the corollary that  $RH$  is projective as an  $RG$ -module, because on restriction to  $H$  it is projective and the index of  $H$  in  $G$  is invertible. On the other hand, we may also regard  $RK$  as an  $RG$ -module via the homomorphism  $G \rightarrow K$ , and if now  $H$  has order prime to  $p$  then  $RK$  is a projective  $RG$ -module, because it is projective on restriction to  $RK$  and the index of  $K$  in  $G$  is prime to  $p$ .

In the exercises to Section 6 the simple  $\mathbb{F}_p SL_2(p)$ -modules were considered. The goal of Exercise 21 of Section 6 was to show that the symmetric powers  $S^r(U_2)$  are all simple  $\mathbb{F}_p SL_2(p)$ -modules when  $0 \leq r \leq p - 1$ , where  $U_2$  is the 2-dimensional space on which  $SL_2(p)$  acts as invertible transformations of determinant 1. The order of  $SL_2(p)$  is  $p(p^2 - 1)$  and so a Sylow  $p$ -subgroup of this group is cyclic of order  $p$ . In Exercise 20 of Section 6 one shows that on restriction to a certain Sylow  $p$ -subgroup,  $S^r(U_2)$  is indecomposable of dimension  $r + 1$  when  $0 \leq r \leq p - 1$ . From the classification of indecomposable modules for a cyclic group of order  $p$  we deduce that  $S^{p-1}(U_2)$  is projective as a module for the

Sylow  $p$ -subgroup. It follows from the last corollary that  $S^{p-1}(U_2)$  is projective as an  $\mathbb{F}_p SL_2(p)$ -module. This module is thus a simple projective  $\mathbb{F}_p SL_2(p)$ -module, or in other words a block of defect zero.

## Representation type of algebras

In trying to understand the representation theory of a ring one hopes, where possible, to be able to describe all the indecomposable modules. The possibility of such a description depends on there being in some sense sufficiently few indecomposable modules for a classification to be a reasonable goal, or for a description of the indecomposable modules to make any sense or have any utility. Unfortunately for the majority of rings one encounters both a classification of the indecomposable modules and a way of organizing the classification so that it can be understood seem to be unreasonable expectations.

On the other hand, in special cases the indecomposable modules can indeed be classified. With this in mind, we say that a ring  $A$  has *finite representation type* if and only if there are only finitely many isomorphism classes of indecomposable  $A$ -modules, and otherwise we say that  $R$  has *infinite representation type*. We have seen in Theorem 6.2 that if  $G$  is a cyclic  $p$ -group and  $k$  is a field of characteristic  $p$ , then  $kG$  has finite representation type.

(11.14) PROPOSITION. *Let  $R$  be a discrete valuation ring with residue field of characteristic  $p$  or a field of characteristic  $p$ , and let  $P$  be a Sylow  $p$ -subgroup of a finite group  $G$ . Then  $RG$  has finite representation type if and only if  $RP$  has finite representation type.*

*Proof.* Since  $|G : P|$  is invertible in  $R$ , by Proposition ? every indecomposable  $RG$ -module is a summand of some module  $T \uparrow_P^G$ , and we may assume that  $T$  is indecomposable, since if  $T = T_1 \oplus T_2$  then  $T \uparrow_P^G = T_1 \uparrow_P^G \oplus T_2 \uparrow_P^G$ , and by the Krull-Schmidt theorem the indecomposable summands of  $T \uparrow_P^G$  are the indecomposable summands of  $T_1 \uparrow_P^G$  together with the indecomposable summands of  $T_2 \uparrow_P^G$ . If  $RP$  has finite representation type then there are only finitely many modules  $T \uparrow_P^G$  with  $T$  indecomposable, and these have only finitely many summands by the Krull-Schmidt theorem. Conversely, every  $RP$ -module  $U$  is a direct summand of  $U \uparrow_P^G \downarrow_P^G$  and hence is a direct summand of some module  $V \downarrow_P^G$ . If  $U$  is indecomposable, we may assume  $V$  is indecomposable. Now if  $RG$  has finite representation type there are only finitely many isomorphism types of summands of modules  $V \downarrow_P^G$ , by the Krull-Schmidt theorem, and hence  $RP$  has finite representation type.  $\square$

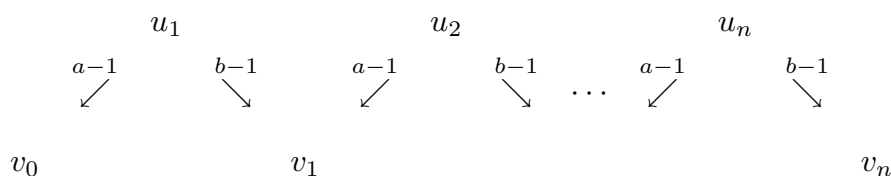
In preparation for a characterization of group algebras of finite representation type we now show that  $k[C_p \times C_p]$  has infinitely many non-isomorphic indecomposable modules, where  $k$  is a field of characteristic  $p$ . We will first describe infinitely many modules, and after that we will prove that they are indecomposable. Let  $G = C_p \times C_p = \langle a \rangle \times \langle b \rangle$  and let  $k$  be a field of characteristic  $p$ . We define a module  $M_{2n+1}$  of dimension  $2n + 1$  with basis  $u_1, \dots, u_n, v_0, \dots, v_n$  and an action of  $G$  given as follows:

$$\begin{aligned} a(u_i) &= u_i + v_{i-1}, & b(u_i) &= u_i + v_i & \text{where } 1 \leq i \leq n \\ a(v_i) &= v_i, & b(v_i) &= v_i & \text{where } 0 \leq i \leq n. \end{aligned}$$

It is perhaps easier to write this as

$$\begin{aligned} (a - 1)u_i &= v_{i-1}, & (b - 1)u_i &= v_i & \text{where } 1 \leq i \leq n \\ (a - 1)v_i &= 0, & (b - 1)v_i &= 0 & \text{where } 0 \leq i \leq n \end{aligned}$$

and to describe  $M_{2n+1}$  diagrammatically



We may check that this is indeed a representation of  $G$  by verifying that

$$(a - 1)(b - 1)x = (b - 1)(a - 1)x = 0$$

and

$$(a - 1)^p x = (b - 1)^p x = 0$$

for all  $x \in M_{2n+1}$ , which is immediate.

Let us now show that  $M_{2n+1}$  is indecomposable. We will do this by showing that  $\text{End}_k M_{2n+1} / I$  has dimension 1 for a certain nilpotent ideal  $I$ . Observe that

$$\text{Soc}(M_{2n+1}) = \text{Rad}(M_{2n+1}) = kv_0 + \dots + kv_n.$$

The ideal  $I$  in question is  $\text{Hom}_k M_{2n+1} / \text{Soc}(M_{2n+1})$ , and this squares to zero since if  $\phi : M_{2n+1} \rightarrow \text{Soc}(M_{2n+1})$  then  $\text{Rad}(M_{2n+1}) \subseteq \text{Ker } \phi$  and so  $\phi \text{Soc}(M_{2n+1}) = 0$ .

If  $\phi$  is any endomorphism of  $M_{2n+1}$  then  $\phi(\text{Soc}(M_{2n+1})) \subseteq \text{Soc } M_{2n+1}$  so  $\phi$  induces an endomorphism  $\bar{\phi}$  of  $M_{2n+1} / \text{Soc}(M_{2n+1})$ . We show that  $\bar{\phi}$  is necessarily a scalar multiple of the identity. To establish this we will exploit the equations

$$(a - 1)u_i = (b - 1)u_{i-1} \quad \text{when } 2 \leq i \leq n$$

and also the fact that  $(a - 1)$  and  $(b - 1)$  both map  $ku_1 + \cdots + ku_n$  injectively into  $\text{Soc}(M_{2n+1})$ . We have

$$\phi((a - 1)u_i) = (a - 1)\phi(u_i) = \phi((b - 1)u_{i-1}) = (b - 1)\phi(u_{i-1})$$

and it follows from this that  $\bar{\phi}$  is completely determined once we know  $\phi(u_1)$ , since then  $(a - 1)\phi(u_2) = (b - 1)\phi(u_1)$  determines  $\bar{\phi}(u_2)$ ,  $(a - 1)\phi(u_3) = (b - 1)\phi(u_2)$  determines  $\bar{\phi}(u_3)$ , and so on.

Suppose that

$$\phi(u_1) \equiv \lambda_1 u_1 + \cdots + \lambda_r u_r \pmod{\text{Soc}(M_{2n+1})}$$

where the  $\lambda_i$  are scalars and  $\lambda_r \neq 0$ . The equations imply that

$$\phi(u_2) \equiv \lambda_1 u_2 + \cdots + \lambda_r u_{r+1} \pmod{\text{Soc}(M_{2n+1})}$$

and inductively

$$\phi(u_{n-r+1}) \equiv \lambda_1 u_{n-r+1} + \cdots + \lambda_r u_n \pmod{\text{Soc}(M_{2n+1})}.$$

If it were the case that  $r > 1$  then the equation

$$(b - 1)\phi(u_{n-r+1}) = (a - 1)\phi(u_{n-r+2}) = \lambda_1 v_{n-r+1} + \cdots + \lambda_r v_n$$

would have no solution, since no such vector where the coefficient of  $v_n$  is non-zero lies in the image of  $a - 1$ .

We conclude that  $r = 1$  and  $\phi(u_i) \equiv \lambda_1 u_i \pmod{\text{Soc}(M_{2n+1})}$  for some scalar  $\lambda_1$ , for all  $i$  with  $1 \leq i \leq n$ . Thus

$$\phi - \lambda_1 1_{M_{2n+1}} : M_{2n+1} \rightarrow \text{Soc}(M_{2n+1})$$

and so  $\text{End}_{kG}(M_{2n+1}) / \text{Hom}_{kG}(M_{2n+1}, \text{Soc}(M_{2n+1}))$  has dimension 1.

We have proved

(11.15) PROPOSITION. *The quotient  $\text{End}_{kG}(M_{2n+1}) / \text{Rad } \text{End}_{kG}(M_{2n+1})$  has dimension 1. Thus  $\text{End}_{kG}(M_{2n+1})$  is a local ring and  $M_{2n+1}$  is indecomposable.*

(11.16) THEOREM (D.G. Higman). *Let  $k$  be a field of characteristic  $p$ . Then  $kG$  has finite representation type if and only if Sylow  $p$ -subgroups of  $G$  are cyclic.*

*Proof.* By Proposition 11.14 it suffices to show that if  $P$  is a  $p$ -group then  $kP$  has finite representation type if and only if  $P$  is cyclic. We have seen in ? that  $kP$  has finite representation type when  $P$  is cyclic. If  $P$  is not cyclic then  $P$  has the group  $C_p \times C_p$  as a homomorphic image. (This may be proved using the fact that if  $\Phi(P)$  is the Frattini subgroup of  $P$  then  $P/\Phi(P) \cong (C_p)^d$  for some  $d$  and that  $P$  can be generated by  $d$  elements. Since  $P$  cannot be generated by a single element,  $d \geq 2$  and so  $(C_p)^2$  is an image of  $P$ .) The infinitely-many non-isomorphic indecomposable  $k[C_p \times C_p]$ -modules become non-isomorphic indecomposable  $kP$ -modules via the quotient homomorphism, and this establishes the result.  $\square$

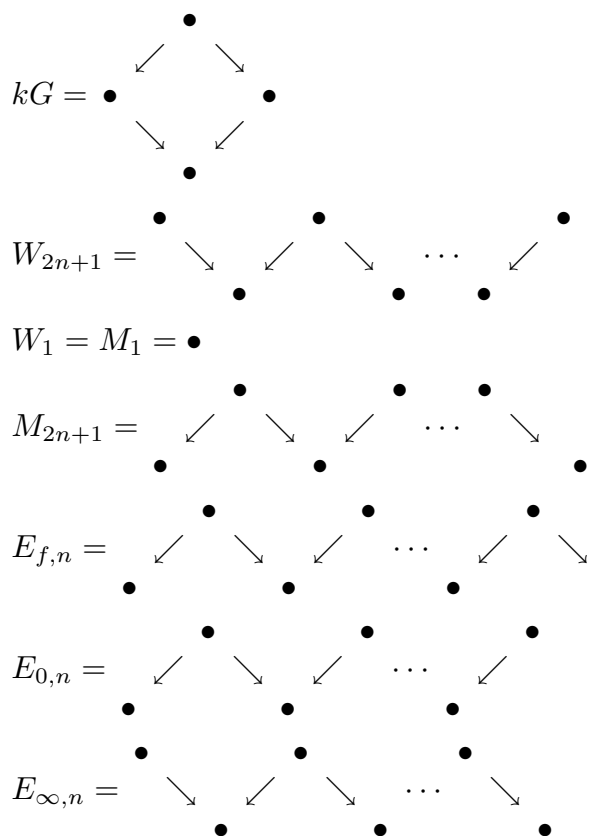
Even when the representation type is infinite, the arguments that we have been using still yield the following result.

(11.17) THEOREM. *Let  $k$  be a field of characteristic  $p$ . For any finite group  $G$ , the number of isomorphism classes of indecomposable modules which are projective relative to a cyclic subgroup is finite.*

We now consider the kinds of phenomena that can occur with indecomposable  $kG$ -modules. We will indicate for which groups we can expect a reasonable classification of indecomposable modules and point out some of the techniques which are available to describe them.

An understanding of the indecomposable modules for a finite group in characteristic  $p$  is very much connected with an understanding of the modules for a Sylow  $p$ -subgroup. We generally expect there to be more modules for  $G$  than for its Sylow  $p$ -subgroup, and a description of modules for the Sylow  $p$ -subgroup tends to be easier than for  $G$ .

We start with the easiest example of a description of indecomposable modules for a group algebra of infinite representation type, which is the modules for  $k[C_2 \times C_2]$  where  $k$  is a field of characteristic 2. In constructing infinitely many indecomposable modules for  $C_p \times C_p$  we already constructed some of the indecomposable  $k[C_2 \times C_2]$ -modules, but now we complete the picture. As before we let  $G = C_2 \times C_2 = \langle a \rangle \times \langle b \rangle$  and exhibit the modules diagrammatically by the action of  $a - 1$  and  $b - 1$  on a basis. Here are the indecomposable modules:



In these diagrams each node represents a basis element of a vector space, a southwest arrow  $\swarrow$  emanating from a node indicates that  $a - 1$  sends that basis element to the basis element at its tip, and similarly a southeast arrow  $\searrow$  indicates the action of  $b - 1$  on a basis element. Where no arrow in some direction emanates from a node, the corresponding element  $a - 1$  or  $b - 1$  acts as zero.

The even-dimensional indecomposable representations  $E_{f,n}$  require some further explanation. They are parametrized by pairs  $(f, n)$  where  $f \in k[X]$  is an irreducible monic polynomial and  $n \geq 1$  is an integer. Let the top row of nodes in the diagram correspond to basis elements  $u_1, \dots, u_n$ , and the bottom row to basis elements  $v_1, \dots, v_n$ . Let

$$(f(X))^n = X^{mn} + a_{mn-1}X^{mn-1} + \dots + a_0.$$

The right-most arrow  $\searrow$  starting at  $u_{mn}$  which has no terminal node is supposed to indicate that  $(b - 1)u_{mn} = v_{mn+1}$  where

$$v_{mn+1} = -a_{mn-1}v_{mn-1} - \dots - a_1v_2 - a_0v_1,$$

so that with respect to the given bases  $b - 1$  has matrix

$$\begin{pmatrix} 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & & 0 & 1 \\ -a_0 & & \dots & -a_{mn-1} \end{pmatrix}$$

which is an indecomposable matrix in rational canonical form with characteristic polynomial  $f^n$ .

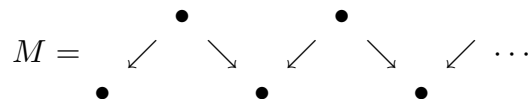
(11.18) THEOREM. *Let  $k$  be a field of characteristic 2. The  $k[C_2 \times C_2]$ -modules shown are a complete list of indecomposable modules.*

*Proof.* We describe only the strategy of the proof, and refer to the exercises at the end of this section and [Ben] for more details. The first step is to use the fact that the regular representation is injective, with simple socle spanned by  $\sum_{g \in G} g$ . If  $U$  is an indecomposable module for which  $(\sum_{g \in G} g)U \neq 0$  then there is a vector  $u \in U$  with  $(\sum_{g \in G} g)u \neq 0$ . The homomorphism  $kG \rightarrow U$  specified by  $x \mapsto xu$  is a monomorphism, since if its kernel were non-zero it would contain  $\sum_{g \in G} g$ , but this element does not lie in the kernel. Since  $kG$  is injective, the submodule  $kGu$  is a direct summand of  $U$ , and hence  $U \cong kG$  since  $U$  is indecomposable. From this we deduce that apart from the regular representation, every indecomposable module is annihilated by  $\sum_{g \in G} g$ , and hence is a module for the ring  $kG/(\sum_{g \in G} g)$ , which has dimension 3 and is isomorphic to  $k[\alpha, \beta]/(\alpha^2, \alpha\beta, \beta^2)$ , where  $\alpha$  corresponds to  $a - 1 \in kG$  and  $\beta$  to  $b - 1 \in kG$ .

Representations of this ring are the same thing as the specification of a vector space  $U$  with a pair of linear endomorphisms  $\alpha, \beta : U \rightarrow U$  which annihilate each other and square to zero. The classification of such pairs of matrices up to simultaneous conjugacy of the matrices (which is the same as isomorphism of the module) was achieved by Kronecker in the 19th century, and he obtained the indecomposable forms which we have listed.  $\square$

The modules  $M_{2n+1}$  and  $W_{2n+1}$  have become known as *string modules* and the  $E_{f,n}$  as *band modules*, in view of the form taken by the diagrams which describe them. More complicated classifications, but with a similar flavor, have been achieved for representations of the dihedral, semidihedral and generalized quaternion 2-groups in characteristic 2. For dihedral 2-groups, all the modules apart from the regular representation are string modules or band modules (see ?).

Provided the field  $k$  is infinite,  $k[C_2 \times C_2]$  has infinitely many isomorphism types of indecomposable modules in each dimension larger than 1. They can nevertheless be grouped into finitely many families, as we have seen intuitively in their diagrammatic description. As a more precise version of this idea, consider the infinite-dimensional  $k[C_2 \times C_2]$ -module  $M$  with diagram



and basis  $u_1, u_2, \dots, u_1, v_2, \dots$ . This module has an endomorphism  $\eta$  which shifts each of the two rows one place to the right, specified by  $\eta(u_i) = u_{i+1}$  and  $\eta(v_i) = v_{i+1}$ , so that  $M$  becomes a  $(k[C_2 \times C_2], k[X])$ -bimodule, where the indeterminate  $X$  acts via  $\eta$ . As  $k[X]$ -modules we have  $M \cong k[X] \oplus k[X]$ . Given an irreducible polynomial  $f \in k[X]$  and

an integer  $n \geq 1$  we may construct the  $k[C_2 \times C_2]$ -module  $M \otimes_{k[X]} k[X]/(f^n)$ , which is a module isomorphic to  $(k[X]/(f^n))^2$  as a  $k[X]$ -module, and which is acted on by  $k[C_2 \times C_2]$  as a module isomorphic to  $Ef, n$ . This construction accounts for all but finitely many of the indecomposable  $k[C_2 \times C_2]$ -modules in each dimension.

With our understanding improved by the last example, we now divide infinite representation type into two kinds: tame and wild. Let  $A$  be a finite-dimensional algebra over an infinite field  $k$ . We say  $A$  has *tame representation type* if it has infinite type and for each dimension  $d$  there are finitely many  $(A, k[X])$ -bimodules  $M_i$  which are free as  $k[X]$ -modules so that all but finitely many of the indecomposable  $A$ -modules of dimension  $d$  have the form  $M_i \otimes_{k[X]} k[X]/(f^n)$  for some irreducible polynomial  $f$  and integer  $n$ . If the bimodules  $M_i$  can be chosen independently of  $d$  (as happens with representations of  $C_2 \times C_2$ ) we say that  $A$  has *domestic representation type*, and otherwise it is *non-domestic*.

We say that the finite-dimensional algebra  $A$  has *wild representation type* if there is a finitely-generated  $(A, k\langle X, Y \rangle)$ -bimodule  $M$  which is free as a right  $k\langle X, Y \rangle$ -module, such that the functor  $M \otimes_{k\langle X, Y \rangle} \_$  from finite-dimensional  $k\langle X, Y \rangle$ -modules to finite-dimensional  $A$ -modules preserves indecomposability and isomorphism type. Here  $k\langle X, Y \rangle$  is the free algebra on two non-commuting variables, having as basis the non-commutative monomials  $X^{a_1} Y^{b_1} X^{a_2} Y^{b_2} \dots$  where  $a_i, b_i \geq 0$ .

In view of the following theorem it would have been possible, over an algebraically closed field, to define wild to be everything which is not finite or tame.

(11.19) THEOREM (Drozd [Dro]; Crawley-Boevey [CB]). *Let  $A$  be a finite-dimensional algebra over an algebraically-closed field. Then  $A$  has either finite, tame or wild representation type.* ■

When  $A$  has wild representation type, the idea is that phenomena which occur with representations of  $k\langle X, Y \rangle$  also appear with  $A$ -modules. Thus  $A$  has at least as many isomorphism types indecomposable modules as  $k\langle X, Y \rangle$  does. The indecomposable  $k\langle X, Y \rangle$ -modules are quite diverse, and in some sense it is a hopeless task to try to classify them. Thus, it is known that the theory of finite-dimensional  $k\langle X, Y \rangle$ -modules is undecidable, meaning that there exists a sentence in the language of finite-dimensional  $k\langle X, Y \rangle$ -modules which cannot be decided by any Turing machine (an account of this result can be found in [Prest]). It is also the case in a heuristic sense that the  $k\langle X, Y \rangle$ -modules are as badly behaved as those of any algebra: it is possible to embed the category of  $A$ -modules and their homomorphisms, for any algebra  $A$ , into the category of  $k\langle X, Y \rangle$ -modules (see [Brenner, Gabriel]).

In the context of group algebras the division into finite, tame and wild representation type is given by the following theorem, in which we include the result of D.G. Higman already proven.

(11.20) THEOREM (Bondarenko, Brenner, Drozd, Higman, Ringel). *Let  $k$  be an infinite field of characteristic  $p$  and let  $G$  be a finite group with Sylow  $p$ -subgroup  $P$ . Then  $kG$  has finite representation type if and only if  $P$  is cyclic, tame representation type if and only if  $p = 2$  and  $P$  is dihedral, semidihedral or generalized quaternion. In all other cases  $kG$  has wild representation type.*

We include  $C_2 \times C_2$  as a dihedral group in the statement of this theorem

The first step in the proof of this theorem we have already seen, and it is to identify the group algebras of finite representation type. Next, certain group algebras were established as being wild. This is implied ? by the following result, which also serves as an example of the kind of phenomenon we may expect with wild algebras.

(11.21) THEOREM (Brenner [Bre1]). *Let  $P$  be a finite  $p$ -group having either  $C_p \times C_p$  ( $p$  odd),  $C_2 \times C_4$  or  $C_2 \times C_2 \times C_2$  as a homomorphic image, let  $k$  be a field of characteristic  $p$ , and let  $E$  be a finite-dimensional algebra over  $k$ . Then there exists a finite-dimensional  $kP$ -module  $M$  such that  $\text{End}_{kP}(M)$  has a nilpotent ideal  $J$  and a subalgebra  $E'$  isomorphic to  $E$ , with the property that the quotient map sends  $E'$  isomorphically to  $\text{End}_{kP}(M)/J$ .*

A theorem of Blackburn implies that if  $P$  is a 2-group which is not cyclic and does not have  $C_2 \times C_4$  or  $C_2 \times C_2 \times C_2$  as a homomorphic image, then  $P$  is dihedral, semidihedral or generalized quaternion. Groups with these as Sylow 2-subgroups were the only groups whose representation type was in question at this point. It was decided by classifying explicitly the indecomposable modules in these cases, and it was done by Bondarenko, Drozd and Ringel. A later approach can be found in the work of Crawley-Boevey [CB].

### Vertices, sources and Green correspondence

Having just given an impression of the difficult of classifying indecomposable modules, we now explain some positive techniques which are available for understanding them better.

(11.22) THEOREM. *Let  $R$  be a field or a complete discrete valuation ring, and let  $U$  be an indecomposable  $RG$ -module.*

- (1) *There is a unique conjugacy class of subgroups  $Q$  of  $G$  which are minimal subject to the property that  $U$  is  $Q$ -projective.*
- (2) *Let  $Q$  be a minimal subgroup of  $G$  such that  $U$  is  $Q$ -projective. There is an indecomposable  $RQ$ -module  $T$  which is unique up to conjugacy by elements of  $N_G(Q)$  such that  $U$  is a summand of  $T \uparrow_Q^G$ .*

*Proof.* (1) We offer two proofs of this result, one employing module-theoretic techniques, and the other a ring-theoretic approach. Both proofs exploit similar ideas, in which the Mackey formula is a key ingredient.

First proof: we start by supposing that  $U$  is both  $H$ -projective and  $K$ -projective where  $H$  and  $K$  are subgroups of  $G$ . Then  $U$  is a summand of  $U \downarrow_H^G \uparrow_H^G$  and also of  $U \downarrow_K^G \uparrow_K^G$ , so it is also a summand of

$$\begin{aligned} U \downarrow_H^G \uparrow_H^G \downarrow_K^G \uparrow_K^G &= \bigoplus_{g \in [K \backslash G/H]} ({}^g((U \downarrow_H^G) \downarrow_{K \cap {}^g H}^H)) \uparrow_{K \cap {}^g H}^K \uparrow_K^G \\ &= \bigoplus_{g \in [K \backslash G/H]} ({}^g(U \downarrow_{K \cap {}^g H}^G)) \uparrow_{K \cap {}^g H}^G \end{aligned}$$

using transitivity of restriction and induction, and now  $U$  must be a summand of some module induced from one of the groups  $K \cap {}^g H$ . If both  $H$  and  $K$  happen to be minimal subject to the condition that  $U$  is projective relative to these groups, we deduce that  $K \cap {}^g H = K$ , so  $K \subseteq {}^g H$ . Similarly  $H \subseteq {}^{g'} K$  for some  $g'$  and so  $H$  and  $K$  are conjugate.

Second proof: we start the same way and suppose that  $U$  is both  $H$ -projective and  $K$ -projective. We may write  $1_U = \text{tr}_H^G \alpha = \text{tr}_K^G \beta$  for certain  $\alpha \in \text{End}_{RH}(U)$  and  $\beta \in \text{End}_{RK}(U)$ . Now

$$1_U = (\text{tr}_H^G \alpha)(\text{tr}_K^G \beta) = \text{tr}_K^G((\text{tr}_H^G \alpha)\beta) = \text{tr}_K^G(\text{tr}_H^G(\alpha\beta)) = \sum_{g \in [K \backslash G/H]} \text{tr}_{K \cap {}^g H}^G(c_g \alpha \beta).$$

Since  $U$  is indecomposable its endomorphism ring is local and so some term  $\text{tr}_{K \cap {}^g H}^G(c_g \alpha \beta)$  must lie outside the unique maximal ideal of  $\text{End}_{RG}(U)$  and must be an automorphism. This implies that  $\text{tr}_{K \cap {}^g H}^G : \text{End}_{R[K \cap {}^g H]}(U) \rightarrow \text{End}_{RG}(U)$  is surjective, since the image of  $\text{tr}_{K \cap {}^g H}^G$  is an ideal, and so  $U$  is  $K \cap {}^g H$ -projective.

We now deduce as in the first proof that if  $K$  and  $H$  are minimal subgroups relative to which  $U$  is projective, then  $H$  and  $K$  are conjugate.

(2) Let  $Q$  be a minimal subgroup relative to which  $U$  is projective. We know that  $U$  is a summand of  $U \downarrow_Q^G \uparrow_Q^G$  and hence it is a summand of  $T \uparrow_Q^G$  for some indecomposable summand  $T$  of  $U \downarrow_Q^G$ . Suppose that  $T'$  is another indecomposable module for which  $U$  is a summand of  $T' \uparrow_Q^G$ . Now  $T$  is a summand of  $T' \uparrow_Q^G \downarrow_Q^G = \bigoplus_{g \in [Q \backslash G / Q]} ({}^g(T' \downarrow_{Q \cap {}^g Q})) \uparrow_{Q \cap {}^g Q}^Q$  and hence a summand of some  $({}^g(T' \downarrow_{Q \cap {}^g Q})) \uparrow_{Q \cap {}^g Q}^Q$ . For this element  $g$  we deduce that  $U$  is  $Q \cap {}^g Q$ -projective and by minimality of  $Q$  we have  $Q = Q \cap {}^g Q$  and  $g \in N_G(Q)$ . Now  $T$  is a summand of  ${}^g T'$ , and since both modules are indecomposable we have  $T = {}^g T'$ .  $\square$

A minimal subgroup  $Q$  of  $G$  relative to which the indecomposable module  $U$  is projective is called a *vertex* of  $U$ , and it is defined up to conjugacy in  $G$ . An  $RQ$ -module  $T$  for which  $U$  is a summand of  $T \uparrow_Q^G$  is called a *source* of  $U$ , and given the vertex  $Q$  it is defined up to conjugacy by elements of  $N_G(Q)$ . We write  $\text{vtx}(U)$  to denote some vertex of  $U$ .

(11.23) COROLLARY. *Let  $R$  be a field or a complete discrete valuation ring, and let  $U$  be an indecomposable  $RG$ -module. If  $T$  is an indecomposable module for which  $U$  is a summand of  $T \uparrow_Q^G$  where  $Q$  is a vertex of  $U$ , then  $T$  is a summand of  $U \downarrow_Q^G$ .*

We record some immediate properties of the vertex of a module.

(11.24) PROPOSITION. *Let  $R$  be a field of characteristic  $p$  or a complete discrete valuation ring with residue field of characteristic  $p$ .*

- (1) *The vertex of every indecomposable module is a  $p$ -group.*
- (2) *An indecomposable module is projective if and only if its vertex is 1.*
- (3) *A vertex of the trivial module  $R$  is a Sylow  $p$ -subgroup of  $G$ .*

*Proof.* (1) We know from ? that every module is projective relative to a Sylow  $p$ -subgroup, and so vertices must be  $p$ -groups.

(2) A module is projective if and only if it is projective relative to 1, which is the case for an indecomposable module if and only if 1 is a vertex.

(3) Let  $Q$  be a vertex of  $R$  and  $P$  a Sylow  $p$ -subgroup of  $G$  containing  $Q$ . Then  $R$  is a summand of  $R \uparrow_Q^G$ , so  $R \downarrow_P^G$  is a summand of  $R \uparrow_Q^G \downarrow_P^G = \bigoplus_{g \in [P \backslash G / Q]} R \uparrow_{P \cap {}^g Q}^P$  and hence is a summand of  $R \uparrow_{P \cap {}^g Q}^P$  for some  $g \in G$ . We claim that for every subgroup  $H \leq P$ ,  $R \uparrow_H^P$  is an indecomposable  $RP$ -module. From this it will follow that  $R = R \uparrow_{P \cap {}^g Q}^P$  and that  $Q = P$ . The only simple  $RP$ -module is the residue field  $k$  with the trivial action (in case  $R$  is a field already,  $R = k$ ), and  $\text{Hom}_{RP}(R \uparrow_H^P, k) = \text{Hom}_{RH}(R, k) \cong k$  is a space of dimension 1. This means that  $R \uparrow_H^P$  has a unique simple quotient, and hence is indecomposable.  $\square$

(11.25) LEMMA. *Let  $Q$  be a subgroup of  $G$  and  $L$  a subgroup with  $L \supseteq N_G(Q)$ . Let  $g \in G - L$ . Then  $L \cap {}^gQ$  is not conjugate in  $L$  to  $Q$ .*

*Proof.* Suppose that  ${}^x(L \cap {}^gQ) = Q$  for some  $x \in L$ . Then  ${}^{xg}Q = Q$  so that  $xg \in N_G(Q) \subseteq L$ . Since  $x \in L$  it follows that  $g \in L$ .  $\square$

(11.26) THEOREM (Green correspondence). *Let  $R$  be a field of characteristic  $p$  or a complete discrete valuation ring with residue field of characteristic  $p$ . Let  $Q$  be a  $p$ -subgroup of  $G$  and  $L$  a subgroup of  $G$  which contains the normalizer  $N_G(Q)$ .*

- (1) *Let  $U$  be an indecomposable  $RG$ -module with vertex  $Q$ . Then in any decomposition of  $U \downarrow_L^G$  as a direct sum of indecomposable modules there is a unique indecomposable summand  $f(U)$  with vertex  $Q$ . Writing  $U \downarrow_L^G = f(U) \oplus X$ , each summand of  $X$  is projective relative to a subgroup of the form  $L \cap {}^gQ$  where  $g \in G - L$ .*
- (2) *Let  $V$  be an indecomposable  $RL$ -module with vertex  $Q$ . Then in any decomposition of  $V \uparrow_L^G$  as a direct sum of indecomposable modules there is a unique indecomposable summand  $g(V)$  with vertex  $Q$ . Writing  $V \uparrow_L^G = g(V) \oplus Y$ , each summand of  $Y$  is projective relative to a subgroup of the form  $Q \cap {}^gQ$  where  $g \in G - L$ .*
- (3) *In the notation of parts (1) and (2) we have  $gf(U) \cong U$  and  $fg(V) \cong V$ .*

*Proof.* We will prove statement (2) before statement (1). Let  $V$  be an indecomposable  $RL$ -module with vertex  $Q$ .

Step 1. We show that in any decomposition as a direct sum of indecomposable modules,  $V \uparrow_L^G \downarrow_L^G$  has a unique summand with vertex  $Q$ , the other summands being projective relative to subgroups of the form  $L \cap {}^gQ$  with  $g \notin L$ . To show this, let  $T$  be a source for  $V$ , so that  $T \uparrow_Q^L \cong V \oplus Z$  for some  $RL$ -module  $Z$ . Put

$$\begin{aligned} V \uparrow_L^G \downarrow_L^G &= V \oplus V', \\ Z \uparrow_L^G \downarrow_L^G &= Z \oplus Z' \end{aligned}$$

for certain  $RL$ -modules  $V'$  and  $Z'$ . Then

$$\begin{aligned} T \uparrow_Q^G \downarrow_L^G &= V \uparrow_L^G \downarrow_L^G \oplus Z \uparrow_L^G \downarrow_L^G \\ &= V \oplus V' \oplus Z \oplus Z' \\ &= \bigoplus_{g \in [L \backslash G / Q]} ({}^g(T \downarrow_{L^g \cap Q})) \uparrow_{L \cap {}^gQ}^L. \end{aligned}$$

There is one summand in the last direct sum with  $g \in L$  and it is isomorphic to  $T \uparrow_Q^L = V \oplus Z$ . The remaining summands are all induced from subgroups  $L \cap {}^gQ$  with  $g \notin L$ , and it follows that all indecomposable summands of  $V'$  and  $Z'$  are projective relative to these subgroups. This in particular implies the assertion we have to prove in this step.

Step 2. We show that in any decomposition as a direct sum of indecomposable modules,  $V \uparrow_L^G$  has a unique indecomposable summand with vertex  $Q$  and that the remaining

summands are projective relative to subgroups of the form  $L \cap {}^gQ$  where  $g \notin L$ . To show this, write  $V \uparrow_L^G$  as a direct sum of indecomposable modules and pick an indecomposable summand  $U$  for which  $U \downarrow_L^G$  has  $V$  as a summand. This summand  $U$  must have vertex  $Q$ ; for it is projective relative to  $Q$ , since  $V$  is, and if  $U$  were projective relative to a smaller group then  $V$  would be also, contradicting the fact that  $Q$  is a vertex of  $V$ . This shows that the direct sum decomposition of  $V \uparrow_L^G$  has at least one summand with vertex  $Q$ .

Let  $U'$  be another summand of  $V \uparrow_L^G$ . Then  $U' \downarrow_L^G$  must be a summand of  $V'$ , in the notation of Step 1, and every indecomposable summand of  $U' \downarrow_L^G$  is projective relative to a subgroup  $L \cap {}^yQ$  with  $y \notin L$ . Since  $U'$  is a summand of  $T \uparrow_Q^G$  it is projective relative to  $Q$ , and hence has a vertex  $Q'$  which is a subgroup of  $Q$ . Since  $L \supseteq Q'$  it follows that  $U' \downarrow_L^G$  has an indecomposable summand which on restriction to  $Q'$  has a source of  $U'$  as a summand, and so  $Q'$  is a vertex of this summand. It follows that some  $L$ -conjugate of  $Q'$  must be contained in one of the subgroups  $L \cap {}^yQ$  with  $y \notin L$ . In other words  ${}^xQ' \subseteq L \cap {}^yQ$  for some  $x \in L$ . Thus  $Q' \subseteq {}^{x^{-1}y}Q$  where  $g = x^{-1}y \notin L$ . This shows that  $Q' \subseteq Q \cap {}^gQ$  and completes the proof of assertion (2) of this theorem.

Step 3. We establish assertion (1). Suppose that  $U$  is an indecomposable  $RG$ -module with vertex  $Q$ . Letting  $T$  be a source of  $U$ , there is an indecomposable summand  $V$  of  $T \uparrow_Q^L$  for which  $U$  is a summand of  $V \uparrow_L^G$ . This is because  $U$  is a summand of  $T \uparrow_Q^G = (T \uparrow_Q^L) \uparrow_L^G$ . This  $RG$ -module  $V$  must have vertex  $Q$ , since it is projective relative to  $Q$ , and if it were projective relative to a smaller subgroup then so would  $U$  be. Now  $U \downarrow_L^G$  is a direct summand of  $V \uparrow_L^G \downarrow_L^G$ , and by Step 1 this has just one direct summand with vertex  $Q$ , namely  $V$ . In fact  $U \downarrow_L^G$  must have an indecomposable summand which on further restriction to  $Q$  has  $T$  as a summand, and this summand has vertex  $Q$ . It follows that this summand must be isomorphic to  $V$ , and in any expression for  $U \downarrow_L^G$  as a direct sum of indecomposable modules, one summand is isomorphic to  $V$  and the rest are projective relative to subgroups of the form  $L \cap {}^gQ$  with  $g \notin L$ . This completes the proof of assertion (1) of the theorem.

Step 4. The final assertion of the theorem follows from the first two and the fact that  $U$  is isomorphic to a summand of  $U \downarrow_L^G \uparrow_L^G$  and  $V$  is isomorphic to a summand of  $V \uparrow_L^G \downarrow_L^G$ .  
 □

**THEOREM** (Burry-Carlson-Puig).

**THEOREM.** *Maps.*

Reiten's construction of the indecomposable modules. Green Peacock.

Examples of Green correspondence in action.

Green's indecomposability theorem.

Green correspondence is one of the main tools available to us in understanding the indecomposable representations of a group algebra. It shows that to some degree these representations are determined by the representations of the normalizers of  $p$ -subgroups.

This approach has been the principal area of development in modular representation theory of finite groups in recent times. We will see it in action in the next chapter, which has to do with blocks.

We mention also another technique which has been used to give positive information about indecomposable representations of finite-dimensional algebras, namely the theory of almost split sequences. This has its context in the representation theory of finite-dimensional algebras in general, not just group algebras, and is described in [Ben], and in more detail in [ARS]. In the context of group algebras this approach was used by Erdmann [Erd] in classifying the structure of (blocks of) group algebras of tame representation type.

*Exercises for Section 11.*

We will assume throughout these exercises that the ground ring  $R$  is either a complete discrete valuation ring, or a field  $k$ , so that the Krull-Schmidt theorem holds.

1. Write out proofs of the following assertions. They refer to  $RG$ -modules  $U$  and  $W$ , subgroups  $H \leq K \leq G$  and  $J \leq G$ , and a  $RK$ -module  $V$ .

- (a) If  $U$  is  $H$ -projective then  $U$  is  $K$ -projective.
- (b) If  $U$  is  $H$ -projective and  $W$  is an indecomposable summand of  $U \downarrow_J^G$  then  $W$  is  $J \cap {}^g H$ -projective for some element  $g \in G$ . Deduce that there is a vertex of  $W$  which is contained in a subgroup  $J \cap {}^g H$ .
- (c) If  $U$  is a summand of  $V \uparrow_K^G$  and  $V$  is  $H$ -projective then  $U$  is  $H$ -projective.
- (d) For any  $g \in G$ ,  $U$  is  $H$ -projective if and only if  ${}^g U$  is  ${}^g H$ -projective.
- (e) If  $U$  is  $H$ -projective and  $W$  is any  $RG$ -module then  $U \otimes W$  is  $H$ -projective.

2. Consider an even-dimensional indecomposable  $k[C_2 \times C_2]$ -module  $E_{f,n}$  where  $k$  is a field of characteristic 2, and suppose that  $f \neq 0, \infty$ . Define  $u_{mn+1} = -a_{mn-1}u_{mn-1} - \cdots - a_1u_2 - a_0u_1$  and let  $\eta : E_{f,n} \rightarrow E_{f,n}$  be the linear map specified by  $\eta(u_i) = u_{i+1}$ ,  $\eta(v_i) = v_{i+1}$  where  $1 \leq i \leq mn$ .

- (1) Show that  $\eta \in \text{End}_{k[C_2 \times C_2]}(E_{f,n})$ .
- (2) Show that the subalgebra  $k\langle \eta \rangle$  of  $\text{End}_{k[C_2 \times C_2]}(E_{f,n})$  generated by  $\eta$  is isomorphic to  $k[X]/(f^n)$ .
- (3) Show that

$$k\langle \eta \rangle + \text{Hom}_{k[C_2 \times C_2]}(E_{f,n}, \text{Soc}(E_{f,n})) = \text{End}_{k[C_2 \times C_2]}(E_{f,n}).$$

- (4) Deduce that  $E_{f,n}$  is an indecomposable  $k[C_2 \times C_2]$ -module.

3. Let  $G = \langle a \rangle \times \langle b \rangle = C_2 \times C_2$  and let  $U$  be an even-dimensional indecomposable  $kG$ -module where  $k$  is a field of characteristic 2.

- (1) Prove that if  $U \not\cong kG$  and  $G \not\cong k$  then  $\text{Rad}(U) = \text{Soc}(U)$ .

Throughout the rest of this question, suppose that multiplication by  $a - 1$  induces an isomorphism  $U/\text{Rad}(U) \rightarrow \text{Soc}(U)$ .

- (2) Show that there is an action of the polynomial ring  $k[X]$  on  $U$  so that  $X(a-1)u = (b-1)u = (a-1)Xu$  for all  $u \in U$ . Show that  $U \cong k\langle a \rangle \otimes_k (U/\text{Rad}(U))$  as  $k\langle a \rangle \otimes_k k[X]$ -modules.

(3) Show that invariant subspaces of  $U$  as a  $k\langle a \rangle \otimes_k K[X]$ -module are also invariant subspaces of  $U$  as a  $kG$ -module. Show that  $U/\text{Rad}(U)$  is an indecomposable  $k[X]$ -module and deduce that  $U/\text{Rad}(U) \cong k[X]/(f^n)$  as  $k[X]$ -modules for some irreducible polynomial  $f$  and integer  $n$ .

(4) Prove that  $U \cong E_{f,n}$  as  $kG$ -modules.

4. Let  $k$  be a field of characteristic  $p$  and suppose that  $U$  is a  $kG$ -module with the property that for every proper subgroup  $H < G$ ,  $U \downarrow_H^G$  is a projective  $kH$ -module.

(1) Show that if  $G$  is a cyclic  $p$ -group then  $U$  must be a projective  $kG$ -module.

(2) Show by example that if  $G = C_2 \times C_2$  is the Klein four-group and  $p = 2$  then  $U$  need not be a projective  $kG$ -module.

5. Suppose that  $U$  is an  $RG$ -module which is  $Q$ -projective and that  $U \downarrow_Q^G$  has a summand which is not projective relative to any proper subgroup of  $Q$ . Show that  $Q$  is a vertex of  $U$ .

6. Let  $H$  be a subgroup of  $G$  and  $U$  an indecomposable  $RG$ -module which is a direct summand of  $R \uparrow_H^G$ . Show that the source of  $U$  is the trivial module (for the subgroup which is the vertex of  $U$ ).

[Because of this, the indecomposable summands of permutation modules (over a field) are sometimes called *trivial source modules*.]

7. Suppose that  $Q$  is a vertex of an indecomposable  $RG$ -module  $U$  and that  $H$  is a subgroup of  $G$  which contains  $Q$ .

(a) For each subgroup  $Q' \subseteq H$  which is conjugate in  $G$  to  $Q$ , show that  $U \downarrow_H^G$  has an indecomposable summand with vertex  $Q'$ . Deduce that if  $U \downarrow_H^G$  is indecomposable then subgroups of  $H$  which are conjugate in  $G$  to  $Q$  are all conjugate in  $H$ .

(b) Show that there is an indecomposable  $RH$  module  $V$  with vertex  $Q$  so that  $U$  is a direct summand of  $V \uparrow_H^G$ .

8. Suppose that  $H$  is a subgroup of  $G$  and that  $V$  is an indecomposable  $RH$ -module with vertex  $Q$ , where  $Q \leq H$ . Show that  $V \uparrow_H^G$  has an indecomposable direct summand with vertex  $Q$ . Show that for every  $p$ -subgroup  $Q$  of  $G$  there is an indecomposable  $RG$ -module with vertex  $Q$ .

## 12. Blocks

Let  $(F, R, k)$  be a  $p$ -modular system and  $G$  a finite group. Thus  $R$  is a discrete valuation ring with field of fractions  $F$  of characteristic zero and residue field  $k$  of characteristic  $p$ . We will define a  $p$ -block of  $G$  in a moment, but whatever it is, it determines and is determined by any of the following data:

- an equivalence class of  $kG$ -modules,
- an equivalence class of indecomposable  $kG$ -modules,
- an equivalence class of simple  $kG$ -modules,
- an equivalence class of  $RG$ -modules,
- a primitive central idempotent in  $kG$  or  $RG$ ,
- an equivalence class of primitive idempotents in  $kG$  or  $RG$ ,
- an equivalence class of  $FG$ -modules,
- an indecomposable 2-sided direct summand of  $kG$ ,
- an indecomposable 2-sided direct summand of  $RG$ ,
- a division of the Cartan matrix of  $kG$  into block diagonal form obtained by permuting rows and permuting columns, with as many diagonal blocks as possible.

In view of this, a block can be defined by specifying any of these data, and there are many possible definitions of a block. People who work with blocks often seem to have many of these definitions in mind at the same time.

To fix things, we will define a *block* of a ring  $A$  with identity to be a primitive idempotent in the center  $Z(A)$ . We start by exploring some of the equivalent properties of blocks. First we recall without proof the statement of Proposition 3.22.

(12.1) PROPOSITION. *Let  $A$  be a ring with identity. Decompositions*

$$A = A_1 \oplus \cdots \oplus A_r$$

*as direct sums of 2-sided ideals  $A_i$  biject with expressions*

$$1 = e_1 + \cdots + e_r$$

*as a sum of orthogonal central idempotent elements, where  $e_i$  is the identity element of  $A_i$  and  $A_i = Ae_i$ . The  $A_i$  are indecomposable as rings if and only if the  $e_i$  are primitive central idempotent elements. If every  $A_i$  is indecomposable as a ring then the  $A_i$ , and also the primitive central idempotents  $e_i$ , are uniquely determined as subsets of  $A$ , and every central idempotent can be written as a sum of certain of the  $e_i$ .*

It makes sense to consider blocks for arbitrary algebras with identity, but the notion is particularly relevant for group algebras because here we are naturally presented with an algebra which may not be indecomposable. In a more abstract study of algebras in general we would probably make the assumption at the start that the algebra we are studying is indecomposable, and if we were to do this the notion of a block would be irrelevant.

(12.2) PROPOSITION. *Let  $A$  be a ring with identity, let  $1 = e_1 + \cdots + e_n$  be a sum of orthogonal idempotents of  $Z(A)$  and let  $U$  be an  $A$ -module. Then  $U = e_1U \oplus \cdots \oplus e_nU$  as  $A$ -modules. Thus if  $U$  is indecomposable we have  $e_iU = U$  for precisely one  $i$ , and  $e_jU = 0$  for  $j \neq i$ . These summands of  $U$  satisfy  $\text{Hom}_A(e_iU, e_jU) = 0$  if  $i \neq j$ .*

This result means that each indecomposable  $A$ -module  $U$  belongs to a unique block, or lies in a unique block, namely the unique primitive central idempotent  $e$  for which  $eU \neq 0$ , and this  $e$  acts as the identity on  $U$ . More generally, we say that an  $A$ -module  $U$  belongs to  $e$  if each of its indecomposable summands belongs to  $e$ , and this is the same as requiring that  $eU = U$ . The modules which belong to a block determine that block, since in any expression for  $A$  as a direct sum of indecomposable modules the sum of the summands belonging to  $e$  is necessarily the 2-sided ideal  $eA$ . When  $A = RG$  is a group algebra, the block to which the trivial module  $R$  belongs is called the *principal block*.

(12.3) PROPOSITION. *Let  $G$  be a finite group and  $(F, R, k)$  a  $p$ -modular system in which  $R$  is complete.*

- (1) *Reduction modulo  $(\pi)$  gives a surjective ring homomorphism  $Z(RG) \rightarrow Z(kG)$ .*
- (2) *Each idempotent of  $Z(kG)$  lifts uniquely to an idempotent of  $Z(RG)$ , with primitive idempotents corresponding to primitive idempotents under the lifting process.*

*Proof.* (1) The conjugacy class sums  $\sum_{g \sim x} g$  (i.e. the sum of all elements  $g$  conjugate to  $x$ ) form a basis for  $Z(RG)$  over  $R$ , and over  $k$  they form a basis for  $Z(kG)$ . Reduction modulo  $(\pi)$  sends one basis to the other, which proves surjectivity.

(2) We have seen the lifting argument before. Since  $\pi^{n-1}Z(RG)/\pi^nZ(RG)$  is a nilpotent ideal in  $Z(RG)/\pi^nZ(RG)$  we may lift any idempotent  $e_{n-1} + \pi^{n-1}Z(RG)$  to an idempotent  $e_n + \pi^nZ(RG)$ , thereby obtaining from any idempotent  $e_1 + \pi Z(RG) \in Z(kG)$  a Cauchy sequence  $e_1, e_2, \dots$  of elements of  $Z(RG)$  whose limit is the required lift. We have also seen before that primitive idempotents correspond to primitive idempotents. In the present situation the lift of each primitive idempotent is unique since the primitive central idempotents of  $RG$  themselves are unique, so that there is only one primitive idempotent of  $Z(RG)$  which reduces to each primitive idempotent of  $Z(kG)$ .  $\square$

Because of this, it is the same thing to study the blocks of  $RG$  and of  $kG$  since they correspond to each other under reduction modulo  $\pi$ . If  $U$  is a  $kG$ -module we may regard it also as an  $RG$ -module via the surjection  $RG \rightarrow kG$  and if  $e$  is a block of  $RG$  with image the block  $\bar{e} \in Z(kG)$  there is no difference between the statements that  $U$  belongs to  $e$  or that  $U$  belongs to  $\bar{e}$ . We may also partition the simple  $FG$ -modules into blocks in a way consistent with the blocks for  $RG$  and  $kG$ . Regarding  $RG$  as a subset of  $FG$ , a primitive central idempotent  $e$  of  $RG$  is also a central idempotent of  $FG$ . We say that an  $FG$  module  $U$  belongs to  $e$  if  $eU = U$ . Evidently each simple  $FG$ -module belongs to a unique block. We see that if  $U$  is an  $RG$ -module and  $U_0 \subset U$  is any  $R$ -form of  $U$  (i.e. a full  $RG$ -lattice in  $U$ ) then  $U_0$  belongs to  $e$  if and only if  $U$  belongs to  $e$ .

*Examples.* 1. When  $A$  is a finite-dimensional semisimple algebra over a field, the blocks correspond to the matrix summands of  $A$ , each block being the idempotent which is the identity element of a matrix summand. Each simple module lies in its own block, and so there is only one indecomposable module in each block. We saw in Theorem 3.23 a formula in terms of characters for the primitive central idempotent in  $\mathbb{C}G$  corresponding to each simple complex representation.

2. When  $G$  is a  $p$ -group and  $k$  is a field of characteristic  $p$  the regular representation  $kG$  is indecomposable and the identity element is a block. There is only one block in this situation and block theory does nothing for us if we are interested only in representations of  $p$ -groups in characteristic  $p$ .

3. We have seen at the end of Section 9 that when we have a block of defect zero for  $G$  over a splitting  $p$ -modular system  $(F, R, k)$  there is a 2-sided direct summand of  $RG$  which is isomorphic to a matrix algebra  $M_n(R)$ , and also a matrix summand  $M_n(k)$  of  $kG$  which is the reduction modulo  $\pi$  of the summand of  $RG$ . There is a unique simple  $kG$ -module in this block, and it is projective. It lifts to a unique  $RG$ -lattice, and all  $RG$ -sublattices of it are isomorphic to it. A key fact which we used in identifying the features of this situation is that the primitive central idempotent of  $\mathbb{C}G$  corresponding to the matrix summand in fact lies in  $RG$ . All this explains why we made reference to a ‘block’ in that situation, but not why we used the term ‘defect zero’. This too will soon be explained.

4. When  $G = S_3$  in characteristic 2 there are two blocks, since the simple module of degree 2 is a block of defect zero, and the only other simple module is the trivial module, which lies in the principal block. The projective cover of the trivial module as an  $RG$ -module has character equal to the sum of the characters of the trivial representation and the sign representation, and so the principal block idempotent in  $RG$  acts as the identity on this, meaning that they are the ordinary characters in the principal block. The other ordinary character, of degree 2, lies in the other block.

In characteristic 3,  $S_3$  has only one block since there are two simple modules (trivial and sign) and the sign representation appears as a composition factor of the projective cover of the trivial module. This means that it belongs to the principal block.

(12.4) LEMMA. *Let  $e$  be a block of a ring  $A$  with identity. If  $0 \rightarrow U \rightarrow V \rightarrow W \rightarrow 0$  is a short exact sequence of  $A$ -modules then  $V$  belongs to  $e$  if and only if  $U$  and  $W$  belong to  $e$ .*

In other words, every submodule and factor module of a module which belongs to  $e$  also belong to  $e$ , and an extension of two modules which belong to  $e$  also belongs to  $e$ .

*Proof.* A module belongs to  $e$  if and only if multiplication by  $e$  is an isomorphism of that module, and this property holds for  $V$  if and only if it holds for  $U$  and  $W$ .  $\square$

In what follows we characterize blocks in terms of a relation on the simple modules. We could work with modules for an algebra over a complete discrete valuation ring  $R$ , but since the simple modules are naturally defined over the residue field  $k$  we will assume that  $A$  is a finite-dimensional  $k$ -algebra. The next result is an elaboration of the observation from the last lemma that each indecomposable projective module  $P_S$  lies in the same block as the simple module  $S$ , and in fact all of the composition factors of  $P_S$  lie in this block.

(12.5) PROPOSITION. *Let  $A$  be a finite-dimensional algebra over a field  $k$ . The following are equivalent for simple  $A$ -modules  $S$  and  $T$ .*

- (1)  $S$  and  $T$  lie in the same block.
- (2) There is a list of simple  $A$ -modules  $S = S_1, S_2, \dots, S_n = T$  so that  $S_i$  and  $S_{i+1}$  are both composition factors of the same indecomposable projective module, for each  $i = 1, \dots, n - 1$ .
- (3) There is a list of simple  $A$ -modules  $S = S_1, S_2, \dots, S_n = T$  so that for each  $i = 1, \dots, n - 1$ ,  $S_i$  and  $S_{i+1}$  appear in a non-split short exact sequence of  $A$ -modules  $0 \rightarrow U \rightarrow V \rightarrow W \rightarrow 0$  with  $\{U, W\} = \{S_i, S_{i+1}\}$ .

*Proof.* The implications (3)  $\Rightarrow$  (2)  $\Rightarrow$  (1) are straightforward in that all the composition factors of any indecomposable module necessarily belong to the same block, and whenever we have a non-split extension of the kind which appears in condition (3), the middle module is uniserial and hence indecomposable.

To show that (1)  $\Rightarrow$  (2) we will write  $S \sim T$  to mean that the simple modules  $S$  and  $T$  satisfy the condition of (2), which is an equivalence relation. All the composition factors of any particular indecomposable projective module are equivalent in this sense. Suppose that  $S$  and  $T$  lie in the same block. We need to show that  $S \sim T$ . We may write the regular representation as  $A = P_1 \oplus \dots \oplus P_r \oplus Q_1 \oplus \dots \oplus Q_s$  where the composition factors of every  $P_i$  are equivalent to  $S$ , and none of the composition factors of the  $Q_j$  are equivalent to  $S$ . Let  $P = P_1 \oplus \dots \oplus P_r$  and  $Q = Q_1 \oplus \dots \oplus Q_s$  so that  $A = P \oplus Q$ . In fact every submodule of  $A$  whose composition factors are all equivalent to  $S$  is contained in  $P$ , for if  $U$  is such a submodule then  $P + U$  has the same property, and  $(P + U) \cap Q = 0$  since composition factors of the intersection are both equivalent and not equivalent to  $S$ . Thus  $A = (P + U) \oplus A$ , and it follows that  $P + U = P$  so  $U \subseteq P$ .

We show that  $P$  and  $Q$  are 2-sided ideals of  $A$ . Since they are already left ideals we only need to show that they are closed under right multiplication by elements of  $A$ . Each element  $x \in A$  determines a module endomorphism  $\phi : A \rightarrow A$  which is  $\phi(a) = ax$ . Now  $\phi(P)$  is a submodule of  $A$  all of whose composition factors are equivalent to  $S$ , so  $\phi(P) \subseteq P$ . This means that  $Px \subseteq P$ , so that  $P$  is a right ideal, as we were trying to show. Similarly  $Q$  is a right ideal of  $A$ , and hence a 2-sided ideal.

It follows that  $P$  is a direct sum of block ideals. The block ideal determined by  $S$  is a direct summand of  $P$ , and hence every simple module in this block is equivalent to  $S$  in the sense of condition (2).

(2)  $\Rightarrow$  (3)

□

The effect of this result is that the division of the simple  $A$ -modules into blocks can be achieved in a purely combinatorial fashion, knowing the Cartan matrix of  $A$ . The statement of the next result seems confusing because the term ‘block’ is used in two different ways. It is probably the origin of the use of the term in representation theory.

(12.6) COROLLARY. *Let  $A$  be a finite-dimensional algebra over a field  $k$ . On listing the simple  $A$ -modules so that modules in each block occur together, the Cartan matrix of  $A$  has a block diagonal form, with one block matrix for each block of the group. Up to permutation of simple modules within blocks and permutation of the blocks, this is the unique decomposition of the Cartan matrix into block diagonal form with the maximum number of block matrices.*

*Proof.* Given any matrix we may define an equivalence relation on the set of rows and columns of the matrix by requiring that a row be equivalent to a column if and only if the entry in that row and column is non-zero, and extending this by transitivity to an equivalence relation. Now if we order the rows and columns so that the rows and columns in each equivalence class come together, the matrix is in block form, and this is the unique expression with the maximal number of blocks (up to permutation of the blocks and permutation of rows and columns within a block). The last result implies that this equivalence relation coincides with the division of modules into blocks.  $\square$

*Example.* Suppose that  $G = K \rtimes H$  where  $K$  has order prime to  $p$  and  $H$  is a  $p$ -group. In other words,  $G$  has a normal  $p$ -complement and is termed  $p$ -nilpotent. We saw in Theorem 8.10 that this is precisely the situation in which each indecomposable projective module has only one isomorphism type of composition factor. Another way of expressing this is to say that the Cartan matrix is diagonal. In view of the last results we see that we have characterized the groups for which each  $p$ -block contains just one simple module over a field of characteristic  $p$  as being the  $p$ -nilpotent groups.

We can describe the primitive central idempotents explicitly in this situation.

(12.7) PROPOSITION. *Let  $G = K \rtimes H$  be a  $p$ -nilpotent group, where  $K$  has order prime to  $p$  and  $H$  is a  $p$ -group. Let  $k$  be a field of characteristic  $p$ . Each block of  $kG$  lies in  $kK$ , and is the sum of a  $G$ -conjugacy class of blocks of  $kK$ .*

*Proof.* Observe that if  $1 = e_1 + \cdots + e_n$  is the sum of blocks of  $kK$  then for each  $i$  and  $g \in G$  the conjugate  $ge_i g^{-1}$  is also a block of  $kK$ . For this we verify that this element is idempotent, and also that it is central in  $kK$ , which is so since if  $x \in K$  then  $xge_i g^{-1} = g(g^{-1}xg)e_i g^{-1} = ge_i(g^{-1}xg)g^{-1} = ge_i g^{-1}x$ . Furthermore  $ge_i g^{-1}$  is primitive in  $Z(kK)$  since if it were the sum of two orthogonal central idempotents, on conjugating back by  $g^{-1}$  we would be able to deduce that  $e_i$  is not primitive either.

The blocks of  $kK$  are uniquely determined, and it follows that  $ge_i g^{-1} = e_j$  for some  $j$ . Thus  $G$  permutes the blocks of  $kK$ .

For each fixed  $i$  the element  $f = \sum_{e=ge_i g^{-1}} e \in Z(kK)$  is idempotent. It is in fact central in  $kG$  since if  $x \in G$  then  $xfx^{-1} = \sum_{e=ge_i g^{-1}} xex^{-1} = f$ , the sum again being over the elements in the  $G$ -orbit of  $e_i$ . We now show that  $f$  is primitive in  $Z(kG)$ . Suppose instead that  $f = f_1 + f_2$  is a sum of orthogonal idempotents in  $Z(kG)$ . Then there are non-isomorphic simple  $kG$ -modules  $U_1$  and  $U_2$  with  $f_1 U_1 = U_1$  and  $f_2 U_2 = U_2$ . Since  $f f_1 = f_1$  and  $f f_2 = f_2$  we have  $f U_1 = U_1$  and  $f U_2 = U_2$ .

By Clifford's theorem  $U_1 \downarrow_K^G \cong S_1^a \oplus \cdots \oplus S_t^a$  for some integer  $a$ , where  $S_1, \dots, S_t$  are  $G$ -conjugate simple  $kK$ -modules. Since  $f \in kK$  we have  $f S_i = S_i$  for all  $i$ , and this identifies these modules exactly as the  $G$ -orbit of simple  $kK$  modules associated to  $f$ . By a similar argument  $U_2 \downarrow_K^G \cong S_1^b \oplus \cdots \oplus S_t^b$  for some integer  $b$ , where the  $S_i$  are the same modules. Since  $K$  consists of the  $p$ -regular elements of  $G$  it follows that the Brauer characters of  $U_1$  and  $U_2$  are scalar multiples of one another. Since Brauer characters of non-isomorphic simple modules are linearly independent we deduce that  $U_1 \cong U_2$ , a contradiction. This shows that  $f$  is primitive in  $Z(kG)$ . □

We may see the phenomenon described in the last result in many examples, of which the smallest non-trivial one is  $G = S_3 = K \rtimes H$  where  $K = \langle(1, 2, 3)\rangle$  and  $H = \langle(1, 2)\rangle$ . Let  $k = \mathbb{F}_4$ . The blocks of  $kK$  are  $e_1 = () + (1, 2, 3) + (1, 3, 2)$ ,  $e_2 = () + \omega(1, 2, 3) + \omega^2(1, 3, 2)$  and  $e_3 = () + \omega^2(1, 2, 3) + \omega(1, 3, 2)$  where  $\omega$  is a primitive cube root of 1 in  $\mathbb{F}_4$ . In the action of  $G$  on these there are two orbits, namely  $\{e_1\}$  and  $\{e_2, e_3\}$ . The blocks of  $kG$  are  $e_1$  and  $e_2 + e_3 = (1, 2, 3) + (1, 3, 2)$ .

### The defect of a block

There is more than one approach to the definition of a defect group of a block. We will start with a module-theoretic approach, and after that relate it to a ring-theoretic approach.

There are two ways to obtain the regular representation from the group ring  $RG$ . One is to regard  $RG$  as a left  $RG$ -module via multiplication from the left, but there is another left action of  $G$  in which an element  $g \in G$  acts by multiplication from the right by  $g^{-1}$ . The module we obtain in this way is isomorphic to the regular representation obtained via left multiplication. Because these two actions commute with each other we may combine them, and regard  $kG$  as a representation of  $G \times G$  with an action given by

$$(g_1, g_2)x = g_1 x g_2^{-1} \quad \text{where } g_1, g_2 \in G, x \in kG.$$

It will be important to consider the diagonal embedding of  $\delta : G \rightarrow G \times G$  specified by  $\delta(g) = (g, g)$ . Via this embedding we obtain yet another action of  $G$  on  $RG$ , which is the action given by conjugation:  $g \cdot x = gxg^{-1}$ .

PROPOSITION.

- (1) The submodules of  $RG$ , regarded as a module for  $R[G \times G]$ , are precisely the 2-sided ideals of  $RG$ .
- (2) Any decomposition of  $RG$  as a direct sum of indecomposable  $R[G \times G]$ -modules is a decomposition as a direct sum of blocks.
- (3) Regarded as a representation of  $G \times G$ ,  $RG$  is a permutation module in which the stabilizer of 1 is  $\delta(G)$ . Thus  $RG \cong R \uparrow_{\delta(G)}^{G \times G}$ .

COROLLARY. Let  $R$  be a discrete valuation ring with residue field of characteristic  $p$  (or a field of characteristic  $p$ ) and let  $G$  be a finite group. Let  $e$  be a block of  $RG$ . Then regarded as a  $R[G \times G]$ -module the summand  $eRG$  has a vertex of the form  $\delta(D)$  where  $D$  is a  $p$ -subgroup of  $G$ . Such a subgroup  $D$  is defined up to conjugacy in  $G$ .

We define a subgroup  $D$  of  $G$  to be a *defect group* of the block  $e$  if  $\delta(D)$  is a vertex of  $eRG$ . It is defined up to conjugacy in  $G$ . If  $|D| = p^d$  we say that  $d$  is the *defect* of  $e$ , but often we abuse this terminology and say simply that the defect of the block is  $D$ . According to these definitions, a block of defect 0 is one whose defect group is the identity subgroup. It is not immediately apparent that this definition of a block of defect zero coincides with the previous one, and this will have to be proved.

The module-theoretic approach to the defect group of a block, which was pioneered by J.A. Green, allows us to obtain more specific information about the kinds of groups which can be defect groups.

THEOREM (Green). Let  $e$  be a  $p$ -block of  $G$  with defect group  $D$ , and let  $P$  be a Sylow  $p$ -subgroup of  $G$  which contains  $D$ . Then  $D = P \cap {}^gP$  for some element  $g \in C_G(D)$ .

*Proof.* Let  $P$  be a Sylow  $p$ -subgroup containing  $D$ . We consider

$$\begin{aligned}
 RG \downarrow_{P \times P}^{G \times G} &= \uparrow_{\delta(G)}^{G \times G} \downarrow_{P \times P}^{G \times G} \\
 &= \bigoplus_{y \in [P \times P \backslash G \times G / \delta(G)]} ({}^y(R \downarrow_{(P \times P) \cap {}^y\delta(G)}^{\delta(G)})) \uparrow_{(P \times P) \cap {}^y\delta(G)}^{P \times P} \\
 &= \bigoplus_{y \in [P \times P \backslash G \times G / \delta(G)]} R \uparrow_{(P \times P) \cap {}^y\delta(G)}^{P \times P} .
 \end{aligned}$$

Now each  $R \uparrow_{(P \times P) \cap {}^y\delta(G)}^{P \times P}$  is indecomposable since  $P \times P$  is a  $p$ -group, as shown in the proof of part (3) of Proposition 11.24. The summand  $eRG$  of  $RG$  on restriction to  $P \times P$  has a summand which on further restriction to  $\delta(D)$  has a source of  $eRG$  as a summand. This summand of  $eRG \downarrow_{P \times P}^{G \times G}$  also has vertex  $\delta(D)$  (an argument which is familiar from the proof of the Green correspondence 11.26), and must have the form  $R \uparrow_{(P \times P) \cap {}^y\delta(G)}^{P \times P}$  for some  $y \in G \times G$ . Thus  $\delta(D)$  is conjugate in  $P \times P$  to  $(P \times P) \cap {}^y\delta(G)$ , so  $\delta(D) = {}^z((P \times P) \cap {}^y\delta(G))$  for some  $z \in P \times P$ .

The elements  $1 \times G = \{(1, t) \mid t \in G\}$  form a set of coset representatives for  $\delta(G)$  in  $G \times G$ , and so we may assume  $y = (1, t)$  for some  $t \in G$ . Write  $z = (r, s)$ , where  $r, s \in P$ . Now

$$\begin{aligned} (P \times P) \cap {}^{(1,t)}\delta(G) &= \{(x, {}^t x) \mid x \in P \text{ and } {}^t x \in P\} \\ &= \{(x, {}^t x) \mid x \in P \cap P^t\} \\ &= {}^{(1,t)}\delta(P \cap P^t) \end{aligned}$$

and  $\delta(D) = {}^{(r,s)}\delta(P \cap P^t)$ . The projection onto the first coordinate here equals  $D = r(P \cap P^t) = rP \cap {}^{rt^{-1}}P = P \cap {}^{rt^{-1}}P$  since  $r \in P$ . At this point it almost looks as though the proof is complete, apart from the fact that  $rt^{-1}$  might not centralize  $D$ . Now  ${}^{(1,t^{-1})(r^{-1},s^{-1})}\delta(D) \subseteq \delta(G)$ , so that  $r^{-1}x = {}^{t^{-1}s^{-1}}x$  for all  $x \in D$ , and  $rt^{-1}s^{-1} \in C_G(D)$ . Since  $s \in P$  we have  $D = P \cap {}^{rt^{-1}s^{-1}}P$  and this completes the proof.  $\square$

**COROLLARY.** *If  $e$  is a  $p$ -block of  $G$  with defect group  $D$  then  $D = O_p(N_G(D)) \supseteq O_p(G)$ , where  $O_p(G)$  denotes the largest normal  $p$ -subgroup of  $G$ .*

*Proof.* We start by observing that  $O_p(G)$  is the intersection of the Sylow  $p$ -subgroups of  $G$ ; for the intersection of the Sylow  $p$ -subgroups is a normal  $p$ -subgroup since the Sylow  $p$ -subgroups are closed under conjugation, and on the other hand  $O_p(G) \subseteq P$  for some Sylow  $p$ -subgroup  $P$ , and hence  ${}^g(O_p(G)) = O_p(G) \subseteq {}^gP$  for each element  $g \in G$ . Since  ${}^gP$  accounts for all Sylow  $p$ -subgroups by Sylow's theorem it follows that  $O_p(G)$  is contained in their intersection.

It follows immediately that  $D \supseteq O_p(G)$  since  $D$  is the intersection of two Sylow  $p$ -subgroups and hence contains the intersection of all Sylow  $p$ -subgroups.

To prove that  $D = O_p(N_G(D))$ , let  $P$  be a Sylow  $p$ -subgroup of  $G$  which contains a Sylow  $p$ -subgroup of  $N_G(D)$ . Such a  $P$  necessarily has the property that  $P \cap N_G(D)$  is a Sylow  $p$ -subgroup of  $N_G(D)$ . Now  $D = P \cap {}^gP$  for some  $g \in C_G(D)$  and so in particular  $g \in N_G(D)$ . Thus  ${}^gP \cap N_G(D) = {}^g(P \cap N_G(D))$  is also a Sylow  $p$ -subgroup of  $N_G(D)$ , and  $D = (P \cap N_G(D)) \cap {}^g(P \cap N_G(D))$  is the intersection of two Sylow  $p$ -subgroups of  $N_G(D)$ . Thus  $D \supseteq O_p(N_G(D))$ . But on the other hand  $D$  is a normal  $p$ -subgroup of  $N_G(D)$ , and so is contained in  $O_p(N_G(D))$ . Thus we have equality.  $\square$

The condition on a subgroup  $D$  of  $G$  that  $D = O_p N_G(D)$  is quite restrictive. Such subgroups have been called  *$p$ -radical subgroups* by some authors in recent years, and they are also called  *$p$ -stubborn subgroups*. They play an important role in many questions about groups to do with topology, for example in studying the properties of classifying spaces and in studying the topological properties of the partially-ordered set of  $p$ -subgroups of  $G$ . The terminology  *$p$ -radical* comes from the fact that when  $G$  is a finite group of Lie type in characteristic  $p$  the  $p$ -radical subgroups are precisely the unipotent radicals of parabolic subgroups. Thus the definition of  *$p$ -radical subgroup* extends this notion to all finite groups. The name  *$p$ -stubborn* refers to the fact that in certain calculations with the partially-ordered set of  $p$ -subgroups of  $G$ , many subgroups can be ignored, but the

$p$ -stubborn ones cannot. The reader should be warned that the term ‘ $p$ -radical’ has also been used in some different senses, one of which is described in the book by Feit [Fei].

It is immediate that Sylow  $p$ -subgroups of a group are  $p$ -radical, as is  $O_p(G)$ . An exercise in group theory (presented at the end of this section) shows that other  $p$ -radical subgroups must lie between these two extremes. It is always the case that  $G$  has a  $p$ -block with defect group a Sylow  $p$ -subgroup (the principal block, for example) but it need not happen that  $O_p(G)$  is the defect group of any block.

We now describe another context where  $p$ -radical subgroups arise, namely Alperin’s weight conjecture. This conjecture and its refinements due to Dade have been a principal motivating force behind much research in modular representatin theory of finite groups in recent years. Let  $k$  be a splitting field for  $G$  in characteristic  $p$ . Alperin defines a *weight* to be a pair  $(H, V)$  where  $H$  is a  $p$ -subgroup of  $G$  and  $V$  is a simple projective  $k[N_G(H)/H]$ -module, that is, a block of defect zero for  $N_G(H)/H$ . We identify two pairs  $(H, V)$ ,  $(H_1, V_1)$  if  $H$  and  $H_1$  are conjugate, and after transporting the action on  $V$  via conjugation,  $V$  and  $V_1$  are isomorphic. Thus the condition that  $(H, V) = (H_1, V_1)$  is that  $H_1 = {}^gH$ , and  $V_1 \cong {}^gV$ .

CONJECTURE (Alperin). *For every finite group  $G$ , the number of weights for  $G$  in characteristic  $p$  equals the number of simple  $kG$ -modules.*

This number is also equal to the number of  $p$ -regular conjugacy classes of  $G$ , and from this point of view is easy to determine. What is more mysterious is the number of blocks of a group, and one of the remarkable things about this conjecture is that it makes a connection between two apparently different sets of objects, one of them easy to compute, the other more difficult.

When  $(H, V)$  is a weight the fact that  $V$  is a block of defect zero for  $N(H)/H$  implies that  $O_p(N_G(H)/H) = 1$ . Since  $O_p(N_G(H)/H) = O_p(N_G(H))/H$  this is equivalent to  $O_p(N_G(H)) = H$ , and so  $H$  must be a  $p$ -radical subgroup. This property enables us to list the weights for various groups. For example, when  $G = S_4$  and  $p = 2$  the 2-radical subgroups are the normal subgroup  $V \cong C_2 \times C_2$  and the Sylow 2-subgroup  $D_8$  only. Since  $N_G(V)/V \cong S_3$  has a 2-dimensional module which is a block of defect zero and  $N_G(D_8)/D_8 = 1$  has the trivial module as a block of defect zero, there are two weights:  $(V, 2)$  and  $(D_8, 1)$ . There are also two 2-regular conjugacy classes in  $G$ , as predicted by Alperin’s conjecture.

When  $G = A_5$  a Sylow 2-subgroup is  $C_2 \times C_2$  and it is 2-radical, as is the identity subgroup. There remains one conjugacy class of 2-subgroups, which are cyclic of order 2, but since  $N_G(C_2) = C_2 \times C_2$  these are not 2-radical. Since  $N_G(C_2 \times C_2) = A_4$  and  $A_4/C_2 \times C_2 \cong C_3$  has order prime to 2, there are 3 weights of the form  $(C_2 \times C_2, \lambda)$  where  $\lambda$  is a 1-dimensional representation of  $C_3$ . The remaining weights must have the form  $(1, V)$  where  $V$  is a block of defect zero for  $G$ . In fact  $G$  has four 2-regular conjugacy classes and there is indeed a block of defect zero for  $A_5$ , a representation of degree 4: by ? the

permutation representation with stabilizer  $A_4$  decomposes as  $\mathbb{C} \uparrow_{A_4}^{A_5} = \mathbb{C} \oplus U$  where  $U$  is a simple representation of degree 4.

## Ring-theoretic methods

The advantage of the module-theoretic approach we have just taken is that it immediately establishes the notion of a defect group of a block and its uniqueness up to conjugacy, using the theory of vertices and sources we have already developed. However, it is more convenient in many situations to adopt a ring-theoretic approach, which is not surprising in view of the fact that blocks are rings. We make some definitions which are appropriate to this context.

Let  $R$  be a commutative ring with a 1 and  $G$  a group. We define an *interior  $G$ -algebra over  $R$*  to be an  $R$ -algebra  $A$  together with a group homomorphism  $u : G \rightarrow A^\times$  where  $A^\times$  denotes the group of units of  $A$ . Several examples of interior  $G$ -algebras are immediately available to us. The group algebra  $RG$  is itself an interior  $G$ -algebra where  $u$  is the inclusion of  $G$  as a subset of  $RG$ . Whenever  $A$  is an interior  $G$ -algebra and  $\phi : A \rightarrow B$  is an algebra homomorphism (sending  $1_A$  to  $1_B$ ) then  $B$  becomes an interior  $G$ -algebra via the homomorphism  $\phi u : G \rightarrow B^\times$ . Thus if  $B$  is a block of  $G$  the algebra homomorphism  $RG \rightarrow B$  makes  $B$  into an interior  $G$ -algebra. Each  $RG$ -module  $U$  is determined by an algebra homomorphism  $RG \rightarrow \text{End}_R(U)$  which expresses the action of  $RG$ . In fact, to specify an action of  $G$  on  $U$  is the same as specifying the structure of an interior  $G$ -algebra on  $\text{End}_R(U)$ .

Whenever we have an interior  $G$ -algebra  $A$  there arise three module actions of  $G$  on  $A$ , namely an element  $g \in G$  can act as left multiplication by  $u(g)$ , as right multiplication by  $u(g^{-1})$ , and also  $g$  can act as  $a \mapsto {}^g a = u(g) a u(g^{-1})$ . This last action is particularly important since the action is via algebra automorphisms, satisfying  ${}^g(ab) = {}^g a {}^g b$ . We have seen this action before when  $A = \text{End}_R(U)$  is the endomorphism algebra of an  $RG$ -module  $U$ , and whenever we have an action of  $G$  on an interior  $G$ -algebra, this will be the action we mean. Thus fixed points  $A^H$  where  $H \leq G$  will be taken with respect to this action, as will the relative trace map  $\text{tr}_H^G(a) = \sum_{g \in [G/H]} {}^g a$  when  $a \in A^H$ .

**PROPOSITION.** *Let  $A$  be an interior  $G$ -algebra over  $R$  in which  $1_A = \text{tr}_H^G a$  for some element  $a \in A^H$ . Let  $U$  be an  $A$ -module. Then regarded as an  $RG$ -module,  $U$  is  $H$ -projective.*

*Proof.* The representation of  $A$  on  $U$  is given by an algebra homomorphism  $\phi : A \rightarrow \text{End}_R(U)$  and now  $1_U = \phi(1_A) = \phi(\text{tr}_H^G a) = \text{tr}_H^G \phi(a)$ . Thus by Higman's criterion  $U$  is  $H$ -projective.  $\square$

LEMMA. Let  $U$  be an  $R[G \times G]$ -module which is  $\delta(H)$ -projective. Then  $U \downarrow_{\delta(G)}^{G \times G}$  is  $\delta(H)$ -projective.

*Proof.*  $U$  is a summand of some module  $V \uparrow_{\delta(H)}^{G \times G}$  so  $U \downarrow_{\delta(G)}^{G \times G}$  is a summand of

$$V \uparrow_{\delta(H)}^{G \times G} \downarrow_{\delta(G)}^{G \times G} = \bigoplus_{x \in [\delta(G) \backslash G \times G / \delta(H)]} ({}^x(V \downarrow_{\delta(G)^x \cap \delta(H)}^{\delta(H)}) \uparrow_{\delta(G) \cap {}^x \delta(H)}^{\delta(G)}).$$

In this formula we may write each  $x \in G \times G$  as  $x = (a, b) = (a, a)(1, a^{-1}b)$  and now

$$\begin{aligned} \delta(G) \cap {}^x \delta(H) &= ({}^{a,a}(\delta(G) \cap ({}^{1,a^{-1}b} \delta(H))) \\ &= ({}^{a,a}\{(H, a^{-1}bh) \mid h = a^{-1}bh\}) \\ &= ({}^{a,a}\delta(C_H(a^{-1}b)) \leq ({}^{a,a}\delta(H). \end{aligned}$$

It follows that every summand of the decomposition of  $V \uparrow_{\delta(H)}^{G \times G} \downarrow_{\delta(G)}^{G \times G}$  is projective relative to a  $\delta(G)$ -conjugate of  $\delta(H)$ , which is the same as being  $\delta(H)$ -projective. Thus  $U \downarrow_{\delta(G)}^{G \times G}$  is  $\delta(H)$ -projective.  $\square$

PROPOSITION. Let  $e \in Z(RG)$  be a central idempotent of  $RG$  and  $H \leq G$ . Then  $eRG$  is projective relative to  $\delta(H)$  as an  $R[G \times G]$ -module if and only if  $e = \text{tr}_{\delta(H)}^{\delta(G)} \alpha$  for some element  $\alpha \in (eRG)^H$ .

*Proof.* Suppose first that  $eRG$  is  $\delta(H)$ -projective as an  $R[G \times G]$ -module. then by Lemma ?  $(eRG) \downarrow_{\delta(G)}^{G \times G}$  is  $\delta(H)$ -projective. By Higman's criterion there is an endomorphism  $\alpha$  of  $eRG$  as a  $R[\delta(H)]$ -module so that the identity morphism  $1_{eRG} = \text{tr}_{\delta(H)}^{\delta(G)} \alpha$ . Now

$$\begin{aligned} e &= 1_{eRG}(e) \\ &= (\text{tr}_{\delta(H)}^{\delta(G)} \alpha)(e) \\ &= \sum_{g \in [G/H]} {}^g \alpha(e) \\ &= \sum_{g \in [G/H]} (g, g)(\alpha(g^{-1}, g^{-1})e) \\ &= \sum_{g \in [G/H]} g(\alpha(g^{-1}eg))g^{-1} \\ &= \sum_{g \in [G/H]} g\alpha(e)g^{-1} \\ &= \text{tr}_H^G(\alpha(e)). \end{aligned}$$

Conversely, suppose  $e = \text{tr}_{\delta(H)}^{\delta(G)} \alpha$  for some  $\alpha \in (eRG)^{\delta(H)}$ . Thus  $h\alpha h^{-1} = \alpha$  and  $e = \sum_{g \in [G/H]} g\alpha g^{-1}$ . Now  $\phi : eRG \rightarrow eRG$  specified by  $\phi(x) = \alpha x$  is an endomorphism of  $R[\delta(H)]$ -modules, since

$$\phi((h, h)x) = \alpha h x h^{-1} = h(h^{-1}\alpha h)x h^{-1} = h\alpha x h^{-1} = (h, h)\phi(x).$$

We claim that  $\text{tr}_{\delta(H)}^{\delta(G)} \phi = 1_{eRG}$ . For

$$\begin{aligned} (\text{tr}_{\delta(H)}^{\delta(G)} \phi)(x) &= \sum_{g \in [G/H]} (g, g), \phi((g^{-1}, g^{-1})x) \\ &= \sum_{g \in [G/H]} (g, g)\phi(g^{-1}xg) \\ &= \sum_{g \in [G/H]} (g, g)\alpha g^{-1}xg \\ &= \sum_{g \in [G/H]} g\alpha g^{-1}xgg^{-1} \\ &= \sum_{g \in [G/H]} g\alpha g^{-1}x \\ &= ex \\ &= x. \end{aligned}$$

This shows that  $eRG \downarrow_{\delta} (G)^{G \times G}$  is  $\delta(H)$ -projective, and hence since  $eRG$  is  $\delta(G)$ -projective this implies that  $eRG$  is in fact  $\delta(H)$ -projective.  $\square$

Putting the last results together we obtain a proof of the following characterization of the defect group in terms of the effect of the relative trace map on the interior  $G$  algebra  $ekG$ . This characterization could have been used as the definition of the defect group.

**THEOREM.** *Let  $e$  be a block of  $kG$  and  $D$  a  $p$ -subgroup of  $G$ . Then  $D$  is a defect group of  $e$  if and only if  $D$  is a minimal subgroup with the property that  $\text{tr}_D^G : (ekG)^D \rightarrow (ekG)^G$  is surjective.*

**COROLLARY.** *Let  $e$  be a block of  $RG$  with defect group  $D$ . Then every  $ekG$ -module is projective relative to  $D$ .*

It is a fact (which we will not prove?) that every block has an indecomposable module with vertex exactly the defect group  $D$ , so that the defect group may be characterized as the unique maximal vertex of modules in the block.

**COROLLARY.** *The defect groups of the principal block are the Sylow  $p$ -subgroups of  $G$ .*

*Proof.* A defect group is a  $p$ -subgroup of  $G$ , and it must contain a vertex of the trivial module, which is a Sylow  $p$ -subgroup.  $\square$

We are now in a position to show that our previous use of the term ‘block of defect 0’ is consistent with the definitions of this section.

**COROLLARY.** *Assume that  $k$  is a splitting field for  $G$ . A block of  $kG$  has defect zero in the sense of this section if and only if it has defect zero in the sense of Section 9, which can be characterized as saying that the block is a matrix algebra over  $k$ .*

*Proof.* If the block has defect zero in the sense of this section its defect group is 1 and every module in the block is 1-projective, or in other words projective. Thus the block has a simple projective module and from the characterizations of Section 9 the block has defect zero in the sense of that Section.

Conversely, suppose the block has defect zero in the sense of Section 9, so that  $ekG$  is a matrix algebra over  $k$ . We will show that  $ekG$  is projective as a  $k[G \times G]$ -module, and will make use of the isomorphism  $k[G \times G] \cong kG \otimes_k kG$ . Let  $*$  :  $kG \rightarrow kG$  be the algebra anti-isomorphism which sends each group element  $g$  to its inverse, so that  $(\sum \lambda_g g)^* = \sum \lambda_g g^{-1}$ . An element  $x$  in the second  $kG$  factor in the tensor product acts on  $ekG$  as right multiplication by  $x^*$ , and it follows that  $e \otimes e^*$  acts as the identity on  $ekG$ . Now  $e \otimes e^*$  is a central idempotent in  $kG \otimes_k kG$  which generates the 2-sided ideal  $ekG \otimes_k e^*kG = ekG \otimes_k (ekG)^*$ . This is the tensor product of two matrix algebras, since the image of a matrix algebra under an anti-isomorphism is a matrix algebra. Such a tensor product is again a matrix algebra, for if  $E_{ij}$  and  $F_{kl}$  are two matrix algebra bases (consisting of the matrices which are non-zero in only one place, where the entry is 1), then the tensors  $E_{ij} \otimes_k F_{kl}$  are a basis for the tensor product which multiply together in the manner of a matrix algebra basis. We see that the block  $ekG \otimes_k e^*kG$  of  $kG \otimes_k kG$  is semisimple, and so  $ekG$  is a projective  $k[G \times G]$ -module.  $\square$

## The Brauer morphism and correspondence of blocks

In this section we will work over a field  $k$  of characteristic  $p$ .

LEMMA. *Let  $e$  be an idempotent in a ring  $A$ .*

- (1) (Rosenberg's lemma) *Suppose that  $eAe$  is a local ring and that  $e \in \sum_j I_j$  where the  $I_j$  are members of a family of ideals of  $A$  (right, left or 2-sided). Then  $e \in I_j$  for some  $j$ .*
- (2) *The idempotent  $e$  is primitive in  $A$  if and only if  $e$  is the only idempotent in  $eAe$ . Thus if  $A$  is a finite-dimensional algebra over a field,  $eAe$  is a local ring if and only if  $e$  is a primitive idempotent.*

*Proof.* (1) If  $e \notin I_j$  for all  $j$  then every  $I_j$  is contained in the maximal ideal of  $eAe$  and so  $e \notin \sum_j I_j$  since  $e$  does not lie in the maximal ideal.

(2) If  $e = e_1 + e_2$  is a sum of orthogonal idempotents then  $ee_i = e_i$  for each  $i$  and so  $e_i \in eAe$ . Thus  $e$  is not the only idempotent of  $eAe$ . Conversely, if  $e' \in eAe$  then  $e = e' + (e - e')$  is a sum of orthogonal idempotents, and  $e$  is not primitive. The final statement about the situation for a finite-dimensional algebra is Proposition 11.4.  $\square$

When  $U$  is a  $kG$ -module and  $K \leq H$  are subgroups of  $G$  we have the inclusion of fixed points  $\text{res}_K^H : U^H \rightarrow U^K$  and the relative trace map  $\text{tr}_K^H : U^K \rightarrow U^H$ . There is also a map  $c_g : U^H \rightarrow U^{gH}$  for each  $g \in G$  specified by  $c_g(x) = gx$ .

LEMMA.

- (1) *Let  $A$  be a  $G$ -algebra and  $H$  a subgroup of  $G$ . Let  $a \in A^G$  and  $x \in A^H$ . Then  $(\text{tr}_H^G x)a = \text{tr}_H^G(xa)$  and  $a(\text{tr}_H^G x) = \text{tr}_H^G(ax)$ . It follows that the image of  $\text{tr}_H^G : A^H \rightarrow A^G$  is a 2-sided ideal.*
- (2) *Let  $H, K$  be subgroups of  $G$  and  $U$  a  $kG$ -module. Then*

$$\text{res}_H^G \text{tr}_K^G = \sum_{g \in [H \backslash G / K]} \text{tr}_{H \cap gK}^H c_g \text{res}_{H \cap gK}^K.$$

*Equivalently, if  $x \in U^K$  then*

$$\text{tr}_K^G(x) = \sum_{g \in [H \backslash G / K]} \text{tr}_{H \cap gK}^H(gx).$$

*Proof.* (1)

$$\begin{aligned}
 (\mathrm{tr}_H^G x)a &= \left( \sum_{g \in [G/H]} {}^g x \right) a \\
 &= \sum_{g \in [G/H]} {}^g x a \\
 &= \sum_{g \in [G/H]} {}^g x {}^g a \\
 &= \sum_{g \in [G/H]} {}^g(xa) \\
 &= \mathrm{tr}_H^G(xa).
 \end{aligned}$$

The rest of the argument is clear from this.

(2) Writing  $G = Hg_1K \cup \cdots \cup Hg_nK$  as a disjoint union of double cosets, so that  $g_1, \dots, g_n$  are double coset representatives, we have  $G/K = Hg_1K/K \cup \cdots \cup Hg_nK/K$ . Regarding this as an equality of  $H$ -sets, each  $Hg_iK/K$  is permuted transitively by  $H$ , and  $\mathrm{Stab}_H(g_iK) = H \cap {}^{g_i}K$ . Thus  $Hg_iK/K \cong H/(H \cap {}^{g_i}K)$  as  $H$ -sets, so that as  $h$  ranges through a set of left coset representatives for  $H \cap {}^{g_i}K$  in  $H$ , so  $hg_i$  ranges through a set of left coset representatives for  $K$  in  $Hg_iK$ . Applying the sum of these to  $x$  gives  $\sum_{h \in [H/(H \cap {}^{g_i}K)]} hg_i x = \mathrm{tr}_{H \cap {}^{g_i}K}^H(g_i x)$ . Summing over the  $(H, K)$ -double cosets in  $G$  gives the right side of the equation to be established, and it equals the left side because each left coset representative of  $K$  in  $G$  is applied to  $x$  just once in this sum.  $\square$

We now combine these constructions and define the *Brauer quotient*

$$\bar{U}(H) = U^H / \sum_{K < H} \mathrm{tr}_K^H(U^K).$$

We also define the *Brauer morphism*  $\mathrm{Br}_H^G : U^G \rightarrow \bar{U}(H)$  to be the composite

$$U^G \xrightarrow{\mathrm{res}_H^G} U^H \rightarrow \bar{U}(H)$$

where the latter map is the quotient homomorphism. In this generality  $U^G$  is simply a vector space and  $\bar{U}(H)$  has the structure of a  $k[N_G(H)]$ -module. The image of  $\mathrm{Br}_H^G$  lies in the fixed points under the action of  $N_G(H)$ . If  $U$  happens also to be a  $G$ -algebra then  $\sum_{K < H} \mathrm{tr}_K^H(U^K)$  is an ideal of  $U^H$  by the above lemma, the Brauer quotient  $\bar{U}(H)$  is an  $N_G(H)$ -algebra, and the Brauer morphism is a ring homomorphism.

We will eventually apply these constructions to  $kG$  regarded as an interior  $G$ -algebra, in which case we regard  $kG$  as a representation of  $G$  via the conjugation action.

**LEMMA.** *Let  $U$  be a  $kG$ -module where  $k$  is a field of characteristic  $p$ . Let  $H$  be a subgroup of  $G$ . If  $\bar{U}(H) \neq 0$  then  $H$  is a  $p$ -group.*

*Proof.* For any group  $H$ , if  $K$  is a Sylow  $p$ -subgroup of  $H$  then  $\mathrm{tr}_K^H : U^K \rightarrow U^H$  is surjective, and if  $H$  is not a  $p$ -group then  $K$  is a proper subgroup of  $H$ . This shows that  $\sum_{K < H} \mathrm{tr}_K^H(U^K) = U^H$  if  $H$  is not a  $p$ -group, and  $\bar{U}(H) = 0$ .  $\square$

LEMMA. Let  $H$  and  $J$  be subgroups of  $G$ , let  $U$  be a  $kG$ -module and let  $a \in U^J$ . If  $\text{Br}_H(\text{tr}_J^G(a)) \neq 0$  then  $H$  is conjugate to a subgroup of  $J$ .

*Proof.*  $\text{Br}_H(\text{tr}_J^G(a))$  is the image in  $\overline{U}(J)$  of  $\text{res}_H^G \text{tr}_J^G(a) = \sum_{g \in [H \backslash G / J]} \text{tr}_{H \cap {}^g J}^H(ga)$ . If this is not zero in  $\overline{U}(J)$  then for some term in the sum,  $H \cap {}^g J$  must not be a proper subgroup of  $H$ , or in other words  $H \subseteq {}^g J$ .  $\square$

The next result provides two more characterizations of the defect group of a block.

PROPOSITION. Let  $e$  be a block of  $kG$ . The following are equivalent.

- (1)  $e$  has defect group  $D$ .
- (2)  $e = \text{tr}_D^G(a)$  for some element  $a \in (kG)^D$  and  $\text{Br}_D^G(e) \neq 0$ .
- (3)  $D$  is up to conjugacy the unique maximal subgroup of  $G$  such that  $\text{Br}_D^G(e) \neq 0$ .

*Proof.* (1)  $\Rightarrow$  (2) If  $e$  has defect group  $D$  then  $D$  is minimal among groups for which  $e = \text{tr}_D^G(a)$  for some  $a \in (kG)^D$ . Thus certainly  $e = \text{tr}_D^G(a)$ . Suppose that  $\text{Br}_D(e) = 0$ . then  $e \in \sum_{K < D} \text{tr}_K^D(kG)^K$  and we may write  $e = \sum_{K < D} \text{tr}_K^D(u_K)$  where  $u_K \in (kG)^K$ . Note that although this expression only suggests that  $e \in (kG)^D$ , in fact  $e \in (kG)^G$ . Now

$$\begin{aligned} e &= ee \\ &= (\text{tr}_D^G(a)) \left( \sum_{K < D} \text{tr}_K^D(u_K) \right) \\ &= \text{tr}_D^G \left( a \sum_{K < D} \text{tr}_K^D(u_K) \right) \\ &= \text{tr}_D^G \sum_{K < D} \text{tr}_K^D(au_K) \\ &= \sum_{K < D} \text{tr}_K^G(au_K). \end{aligned}$$

Thus  $e \in \sum_{K < D} \text{tr}_K^G(kG)^K$  and since  $e$  is a primitive idempotent,  $e \in \text{tr}_K^G(kG)^K$  for some  $K < D$ , by Rosenberg's lemma. This contradicts the minimal property of  $D$  and so the supposition  $\text{Br}_D(e) = 0$  was false.

(2)  $\Rightarrow$  (3) Suppose that  $e = \text{tr}_D^G(a)$  for some  $a \in (kG)^D$  and  $\text{Br}_D(e) \neq 0$ . By the lemma, if  $K$  is any subgroup for which  $\text{Br}_K(e) \neq 0$  then  $K$  is a subgroup of a conjugate of  $D$ , and this shows that  $D$  is up to conjugacy the unique maximal subgroup with  $\text{Br}_D(e) \neq 0$ .

(3)  $\Rightarrow$  (1) Suppose that condition (3) holds and let  $D_1$  be a defect group of  $e$ . By the implication (1)  $\Rightarrow$  (3) we know that  $D_1$  is up to conjugacy the unique maximal subgroup for which  $\text{Br}_{D_1}(e) \neq 0$ . Since  $D$  has this property,  $D$  and  $D_1$  are conjugate, and  $D$  is a defect group.  $\square$

LEMMA. Let  $\Omega$  be an  $H$ -set and  $k\Omega$  the corresponding permutation module. Then  $(k\Omega)^H$  has as a basis the elements which are sums of  $H$ -orbits on  $\Omega$ . When  $H$  is a  $p$ -group  $\sum_{K < H} \text{tr}_K^H((k\Omega)^K)$  is spanned by the orbit sums where the orbit has size larger than 1. Thus  $k\Omega = k[\Omega^H] \oplus \sum_{K < H} \text{tr}_K^H((k\Omega)^K)$  when  $H$  is a  $p$ -group and in this case the Brauer quotient  $\overline{U}(H)$  may be identified with  $k[\Omega^H]$ .

*Proof.* If  $\Omega$  is permuted transitively by  $H$  we know that  $(k\Omega)^H = \sum_{\omega \in \Omega} \omega$ , and from this it follows that in general if  $\Omega = \Omega_1 \cup \dots \cup \Omega_n$  where the  $\Omega_i$  are the orbits of  $H$  on  $\Omega$  then  $(k\Omega)^H = (k\Omega_1)^H \oplus \dots \oplus (k\Omega_n)^H$  has as a basis the orbit sums.

Suppose  $H$  is a  $p$ -group. It suffices to assume that  $H$  acts transitively on  $\Omega$ , so  $\Omega \cong H/J$  for some subgroup  $J$ . We have  $\sum_{\omega \in \Omega} \omega = \text{tr}_J^H(\omega_0)$  for any fixed  $\omega_0 \in \Omega$ . Thus  $\sum_{K < H} \text{tr}_K^H(k\Omega)^K$  contains the orbit sums for orbits of size larger than 1. On the other hand, if  $\Omega = \{\omega\}$  has size 1 and  $K < H$  then  $\text{tr}_K^H \omega = |H : K|\omega = 0$  since  $|H : K| = 0$  in  $k$ . □

COROLLARY. Let  $G$  act on  $kG$  via conjugation and let  $H$  be a  $p$ -subgroup of  $G$ . Then  $\overline{kG}(H) \cong k[C_G(H)]$ . With this identification the Brauer morphism is a ring homomorphism  $\text{Br}_H^G : Z(kG) \rightarrow k[C_G(H)]^{N_G(H)}$  which truncates a group ring element  $\sum_{g \in G} \lambda_g g$  to  $\sum_{g \in C_G(H)} \lambda_g g$ .

*Proof.* In the conjugation action  $kG$  is a permutation module and the set of fixed points of  $H$  on  $G$  is  $C_G(H)$ . Thus the Brauer morphism may be identified as projection onto the first factor in the decomposition  $kG = k[C_G(H)] \oplus \sum_{K < H} \text{tr}_K^H((kG)^K)$ , which is what we refer to as truncation to have support on  $C_G(H)$ . □

It would have been possible to define the Brauer morphism in this context as the map  $Z(kG) \rightarrow k[C_G(H)]$  which truncates a group ring element to have support on  $C_G(H)$ , but with this direct approach it is less obvious that the Brauer morphism is a ring homomorphism. The interpretation of  $\text{Br}_H^G$  as truncation of the support of a group ring element to  $C_G(H)$  provides a concrete picture of this homomorphism in the context of blocks. Notice that, as with Galois correspondence, for each containment of subgroups  $K \leq H$  we have the reverse containment of fixed points  $(kG)^K \supseteq (kG)^H$  and also a containment of centralizers  $C_G(K) \supseteq C_G(H)$ . This means that we obtain a commutative diagram

$$\begin{array}{ccccc} \text{Br}_H^G : & (kG)^G & \xrightarrow{\text{res}_H^G} & (kG)^H & \longrightarrow & \overline{kG}(H) & = & kC_G(H) \\ & & & \parallel & & \downarrow \iota & & \\ & & & \downarrow \text{res}_K^H & & & & \\ \text{Br}_K^G : & (kG)^G & \xrightarrow{\text{res}_K^G} & (kG)^K & \longrightarrow & \overline{kG}(K) & = & kC_G(K) \end{array}$$

where  $\iota$  is the inclusion of the centralizer group rings, so that  $\text{Br}_K^G$  is the composite  $\iota \circ \text{Br}_H^G$ . We see from this that if  $\text{Br}_H^G(x) \neq 0$  for some  $x \in (kG)^G$  then  $\text{Br}_K^G(x) \neq 0$  for every  $K \leq H$ , since  $\text{Br}_H^G(x)$  equals  $\text{Br}_K^G(x)$  with its support truncated to  $C_G(H)$ . This observation

provides a strengthening of part of Proposition ?, that if  $K$  is any subgroup of a defect group  $D$  of a block  $e$  of  $kG$ , then  $\text{Br}_K(e) \neq 0$ .

We illustrate with  $G = S_3$  and  $k = \mathbb{F}_2$  where we have blocks  $e_1 = () + (1, 2, 3) + (1, 3, 2)$  and  $e_2 = (1, 2, 3) + (1, 3, 2)$ . When  $H = \langle (1, 2) \rangle$  we have  $C_G(H) = H$  and  $\text{Br}_H^G(e_1) = ()$ ,  $\text{Br}_H^G(e_2) = 0$ . We also have  $\text{Br}_1^G(e_1) = e_1$  and  $\text{Br}_1^G(e_2) = e_2$  showing that  $\langle (1, 2) \rangle$  and  $1$  are (respectively) the largest subgroups  $H$  (up to conjugacy) for which  $\text{Br}_H(e_1) \neq 0$  and  $\text{Br}_H(e_2) \neq 0$ . These subgroups are the defect groups of the blocks, as asserted by Proposition ?.

**COROLLARY.** *Let  $e$  be a block of  $kG$  with defect group  $D$ , and suppose  $g \in G$  is an element which centralizes a  $p$ -power element of  $G$  which does not lie in any conjugate of  $D$ . Then  $g$  does not lie in the support of  $e$ .*

*Proof.* Let  $x$  be a  $p$ -power element of  $G$  not in any conjugate of  $D$ . Then  $\text{Br}_{\langle x \rangle}(e) = 0$  since  $\langle x \rangle$  is not contained in any conjugate of  $D$ . Since the coefficients of  $g$  in  $e$  and  $\text{Br}_{\langle x \rangle}(e)$  are the same, the result follows.  $\square$

For example, if  $e$  is a block of defect zero corresponding to a character  $\chi$ , then  $\chi(g) \in (\pi)$ , the maximal ideal of the discrete valuation ring in a  $p$ -modular system  $(F, R, k)$ , if  $g$  commutes with any element of order  $p$ .

We now define the Brauer correspondence of blocks. Since

$$k[C_G(H)]^{N_G(H)} \subseteq k[C_G(H)]^{C_G(H)} = Z(k[C_G(H)])$$

the Brauer morphism may be regarded as a map  $\text{Br}_H^G : Z(kG) \rightarrow Z(k[C_G(H)])$  which is a ring homomorphism, and since it is obtained by truncating the support of group ring elements outside  $C_G(H)$  it sends  $1$  to  $1$ . It follows that if  $e$  is any central idempotent of  $kG$  then  $\text{Br}_H^G(e)$  is a central idempotent of  $k[C_G(H)]$  in the center of  $N_G(H)$ , and if  $1 = e_1 + \dots + e_n$  is the sum of blocks of  $kG$  then  $1 = \text{Br}_H^G(e_1) + \dots + \text{Br}_H^G(e_n)$  is a sum of orthogonal central idempotents of  $k[N_G(H)]$ . If  $J$  is a subgroup of  $G$  with  $C_G(H) \subseteq J \subseteq N_G(H)$  and  $b$  is a block of  $kJ$  then there is a unique block  $e$  of  $G$  so that  $b$  is a summand of  $\text{Br}_H^G(e)$ , in the sense that  $b \text{Br}_H^G(e) = b$ . We write  $b^G$  for this block  $e$ , and call it the *Brauer correspondent* of  $b$ . Notice that the choice of subgroup  $H$  does not matter in the definition, since the Brauer homomorphism truncates a group ring element outside  $C_G(H)$ , and if  $H_1$  were another subgroup of  $G$  with the same centralizer the Brauer homomorphism with respect to  $H_1$  would be the same.

**PROPOSITION.** *Suppose that  $Q$  is a normal  $p$ -subgroup of  $G$ . Then every block of  $G$  lies in  $k[C_G(Q)]$  and is the sum of a  $G$ -orbit of blocks of  $C_G(Q)$ .*

*Proof.* We show first that  $\sum_{K < Q} \text{tr}_K^Q(kG)^K \subseteq \text{Rad}((kG)^Q)$ . This will follow from the fact that if  $S$  is a simple  $kG$ -module then  $Q$  acts trivially on  $S$  (since by Clifford's theorem

$S \downarrow_Q^G$  is semisimple and the trivial module is the only simple  $kQ$ -module). Thus if  $a \in (kG)^K$  and  $u \in S$  we have  $\text{tr}_K^Q(a) \cdot u = \sum_{g \in [Q/K]} gag^{-1}u = \sum_{g \in [Q/K]} au = |Q : K|au = 0$ . Thus  $\sum_{K < Q} \text{tr}_K^Q(kG)^K$  annihilates every simple  $kG$ -module and so is contained in the radical of  $kG$ . It follows that  $\sum_{K < Q} \text{tr}_K^Q(kG)^K$  is a nilpotent ideal, and so is contained in  $\text{Rad}((kG)^Q)$ .

If  $e$  is a central idempotent of  $kG$  then both  $e$  and  $\text{Br}_Q(e)$  are idempotents of  $(kG)^Q$  which map under the quotient homomorphism  $(kG)^Q \rightarrow \overline{kG}(Q)$  to  $\text{Br}_Q(e)$ . Since the kernel of this homomorphism is nilpotent it follows that  $e$  and  $\text{Br}_Q(e)$  are conjugate in  $(kG)^Q$ , by ?. PROVE THIS SOMEWHERE. However  $e$  is central and so the only conjugate of  $e$  is  $e$ . Thus  $e = \text{Br}_Q(e)$ , and this lies in  $k[C_G(Q)]$ .

We can now write  $e = f_1 + \cdots + f_n$  as a sum of primitive central idempotents  $f_i$  of  $k[C_G(Q)]$ , and since  $e$  is stable under conjugation by  $G$  the  $f_1, \dots, f_n$  must be a union of  $G$  orbits in the conjugation action on the blocks of  $k[C_G(Q)]$ . However the sum of a single  $G$  orbit of the  $f_i$  is already a central idempotent of  $kG$  and  $e$  is the sum of such sums, so if  $e$  is a block it must be the sum of a single  $G$ -orbit of the  $f_i$ .  $\square$

**COROLLARY.** *If  $Q$  is a normal  $p$ -subgroup of  $G$  for which  $C_G(Q)$  is a  $p$ -group (for example, if  $C_G(Q) \subseteq Q$ ) then  $G$  has only one  $p$ -block.*

*Proof.* Any block of  $kG$  must lie in  $k[C_G(Q)]$ ; but this is the group ring of a  $p$ -group which has only one block, so  $kG$  also has only one block.  $\square$

The above corollary implies, for example, that if  $K$  is a subgroup of  $\text{Aut}(Q)$  where  $Q$  is a  $p$ -group then the semidirect product  $Q \rtimes K$  has only one  $p$ -block. Such is the case with the symmetric group  $S_4$  at  $p = 2$  on taking  $Q$  to be the normal Klein four-group, and we have seen also many other examples of this phenomenon.

**PROPOSITION.** *Let  $H$  be a  $p$ -subgroup of  $G$ ,  $J$  a subgroup of  $G$  with  $HC_G(H) \subseteq J \subseteq N_G(H)$  and  $b$  a block of  $kJ$ . Then  $b^G$  has a defect group which contains a defect group of  $b$ .*

*Proof.* If  $D \subseteq J$  is a defect group of  $b$  then  $D \supseteq H$  since  $H$  is a normal  $p$ -subgroup of  $J$ , and so  $C_G(H) \supseteq C_G(D) = C_J(D)$ . Now  $\text{Br}_H(b^G) = b + b_1$  where  $b$  and  $b_1$  are orthogonal central idempotents of  $kJ$ , and so  $\text{Br}_D^G(b^G) = \text{Br}_D^J(\text{Br}_H^G(b^G)) = \text{Br}_D^J(b) + \text{Br}_D^J(b_1)$  is a sum of orthogonal idempotents. Since  $\text{Br}_D^J(b) \neq 0$  it follows that  $\text{Br}_D^G(b^G) \neq 0$ , and hence  $D$  is contained in a defect group of  $b^G$ .  $\square$

LEMMA. Let  $H$  be a subgroup of  $G$  and  $U$  a  $kG$ -module. Then  $\text{Br}_H^G \text{tr}_H^G = \text{tr}_H^{N_G(H)} \text{Br}_H^H : U^H \rightarrow \overline{U}(H)^{N_G(H)}$ .

*Proof.*  $\text{Br}_H^G \text{tr}_H^G(x)$  is the image in  $\overline{U}(H)$  of  $\text{res}_H^G \text{tr}_H^G(x) = \sum_{g \in [H \backslash G / H]} \text{tr}_{H \cap {}^g H}^H(gx)$ . The only terms which contribute have  $H \cap {}^g H = H$ , or in other words  $g \in N_G(H)$ , so the image equals the image of  $\sum_{g \in [N_G(H) / H]} gx = \text{tr}_H^{N_G(H)} x$ .  $\square$

The following is a basic version of Brauer’s ‘first main theorem’.

THEOREM (Brauer’s first main theorem). Let  $D$  be a  $p$ -subgroup of  $G$ . The Brauer morphism induces a bijection between blocks of  $kG$  with defect group  $D$  and blocks of  $N_G(D)$  with defect group  $D$ .

*Proof.* Let us write  $N$  for  $N_G(D)$  and let  $b \in Z(kN)$  have defect  $D$ . Then  $b = \text{tr}_D^N(a)$  for some  $a \in (kN)^D = k[C_G(D)] \oplus \sum_{K < D} \text{tr}_K^D(kN)^K$ . Since  $\text{tr}_D^N$  preserves both of the two last summands and  $b \in k[C_G(D)]$  we may assume  $a \in k[C_G(D)]$  and so  $\text{Br}_D(a) = a$ . Thus  $b = \text{tr}_D^N \text{Br}_D(a) = \text{Br}_D \text{tr}_D^G(a)$  by the last lemma.

Let  $e = b^G \in Z(kG)$  be the Brauer correspondent of  $b$ , so that  $b$  is a summand of  $\text{Br}_D(b)$  and  $e$  has a defect group  $D_1 \supseteq D$ . We will show that  $D_1 = D$ . Now  $\text{Br}_D(\text{tr}_D^G((kG)^D)) \subseteq \text{tr}_D^N(k[C_G(D)]^D)$  and so  $\text{Br}_D(e \text{tr}_D^G((kG)^D)) \subseteq \text{Br}_D(e) \text{tr}_D^N(k[C_G(D)]^D)$  which contains  $b$ . Thus the ideal  $e \text{tr}_D^G((kG)^D)$  of  $eZ(kG)$  is not nilpotent, since it has an image under a ring homomorphism which contains a non-zero idempotent. It follows that  $e \text{tr}_D^G((kG)^D) = eZ(kG)$ , since  $eZ(kG)$  is local. This implies that  $e$  lies in the image of  $\text{tr}_D^G$ , and so has defect group contained in  $D$ . This completes the argument that the defect group of  $e$  equals  $D$ .

Next  $\text{Br}_D(eZ(kG))$  is an image of a local ring and hence is local and contains only one idempotent. It contains the idempotents  $b$  and  $\text{Br}_D(e)$ , and so we deduce that  $b = \text{Br}_D(e)$ .

We have seen so far that  $b \mapsto b^G$  is a one-to-one mapping from blocks of  $kN$  with defect group  $D$  to blocks of  $kG$  with defect group  $D$ . We conclude by observing that this mapping is surjective. For if  $e \in Z(kG)$  is a block with defect group  $D$  then  $\text{Br}_D(e)$  is a sum of blocks  $b$  of  $kN$  for which  $e = b^G$ , and the blocks  $b$  have defect groups which are subgroups of  $D$ , by ?. On the other hand every block of  $kN$  has defect group containing  $D$ , since  $D$  is a normal  $p$ -subgroup of  $N$ .  $\square$

*Examples.* 1. When  $G = S_3$  and  $k = \mathbb{F}_2$  we have seen that  $e_1 = () + (1, 2, 3) + (1, 3, 2)$  has defect group  $\langle (1, 2) \rangle$  and  $e_2 = (1, 2, 3) + (1, 3, 2)$  has defect group 1. Here  $\text{Br}_{\langle (1, 2) \rangle}^G(e_1) = () \in k\langle (1, 2) \rangle$ , so that the Brauer correspondent  $()^G$  of the only idempotent in  $k\langle (1, 2) \rangle$  is  $e_1$ , this giving a bijection between the idempotents of  $S_3$  and  $k\langle (1, 2) \rangle$  with defect group  $\langle (1, 2) \rangle$ .

2. Let  $G = A_5$  and let  $k$  be a splitting field of characteristic 2. A Sylow 2-subgroup  $P \cong C_2 \times C_2$  has  $N_G(P) \cong A_4$ , and we have seen in Section ? that  $kA_4$  has only one block. Thus there is only one block of  $kG$  with defect group  $P$ : it is the principal block.

The subgroups  $C_2$  have Sylow  $p$ -subgroups  $P$  as their normalizers and there are no blocks of  $kP$  with  $C_2$  as defect group, since  $P$  is a 2-group. Hence there are no blocks of  $kG$  with this defect group. This duplicates information we know from a different source, to the effect that  $C_2$  cannot be a defect group by ? because it is not  $O_2$  of its normalizer. Finally there remain the blocks of defect zero of  $kA_5$ , which have defect group 1. There is in fact just one of these, as may be seen by inspecting the character table of  $A_5$  for characters of degree divisible by 4.

*Exercises for Section 12.*

1. Prove that if a module  $U$  lies in the principal block then so does  $U^*$ .
2. Use the results of Section 10 Exercises 3 5 to show that the simple group  $GL(3, 2)$  of order 168 has two blocks in characteristic 2 and two blocks in characteristic 7.
3. Suppose that  $Q_1$  and  $Q_2$  are subgroups of  $G$  which satisfy  $Q_i = O_p(N_G(Q_i))$  for  $i = 1, 2$ , and let  $N_i = N_G(Q_i)$  for each  $i$ . Prove that if  $N_1 \supseteq N_2$  then  $Q_1 \subseteq Q_2$ . Deduce that  $Q_i \supseteq O_p(G)$  for each  $i$ .

LEMMA. *Let  $U$  and  $V$  be  $A$ -modules which lie in different blocks of an algebra  $A$ . Then*

- (1)  $\text{Hom}_A(U, V) = 0$ , and
- (2) every short exact sequence of  $A$ -modules  $0 \rightarrow U \rightarrow W \rightarrow V \rightarrow 0$  is split.

PROPOSITION. *Let  $(F, R, k)$  be a complete  $p$ -modular system and  $G$  a finite group. Let the decomposition number  $d_{TS}$  be the multiplicity of the simple  $kG$ -module  $S$  as a composition factor of the reduction modulo  $\pi$  of the simple  $FG$ -module  $T$ .*

- (1) *The simple  $FG$ -modules  $T$  for which  $d_{TS} \neq 0$  for some simple module  $S$  in a fixed block of  $kG$  constitute the simple modules in a  $p$ -block of  $FG$ -modules.*
- (2) *The simple  $kG$ -modules  $S$  for which  $d_{TS} \neq 0$  for some simple module  $T$  in a fixed block of  $FG$  constitute the simple modules in a block of  $kG$ -modules.*

## Appendix: Discrete valuation rings

Let  $F$  be a field. A *valuation* on  $F$  is a mapping  $\phi : F \rightarrow \mathbb{R}_{\geq 0}$  such that

- $\phi(a) = 0$  if and only if  $a = 0$ ,
- $\phi(ab) = \phi(a)\phi(b)$  for all  $a, b \in F$ , and
- $\phi(a + b) \leq \phi(a) + \phi(b)$  for all  $a, b \in F$ .

(A.1) *Examples.* 1. No matter what the field  $F$  is, we always have the valuation

$$\phi(a) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{otherwise.} \end{cases}$$

This valuation is the *trivial valuation*, and we generally exclude it.

2. If  $F$  is any subfield of the complex numbers we may take  $\phi(a) = |a|$ , the absolute value of  $a$ .

3. Let  $F = \mathbb{Q}$  and pick a prime  $p$ . Every rational number  $a \in \mathbb{Q}$  may be written  $a = \frac{r}{s}$  where  $(r, s) = 1$ . We set

$$\nu_p(a) = \begin{cases} \infty & \text{if } a = 0, \\ \text{power to which } p \text{ divides } r & \text{if } p \mid r, \\ -\text{power to which } p \text{ divides } s & \text{otherwise,} \end{cases}$$

so that

$$a = p^{\nu_p(a)} \frac{r'}{s'}$$

where  $(r', p) = 1 = (s', p)$ . Now let  $\lambda$  be any real number with  $0 < \lambda < 1$  and put  $\phi(a) = \lambda^{\nu_p(a)}$ . Often  $\lambda$  is taken to be  $\frac{1}{p}$ , but the precise choice of  $\lambda$  does not affect the properties of the valuation. This valuation is called the *p-adic valuation* on  $\mathbb{Q}$ .

This last  $\phi$  is an example of a valuation which satisfies the so-called *ultrametric inequality*

$$\phi(a + b) \leq \max\{\phi(a), \phi(b)\},$$

which in the case of this example comes down to the fact that if  $p^n \mid a$  and  $p^n \mid b$  where  $a, b \in \mathbb{Z}$ , then  $p^n \mid (a + b)$ . We say that  $\phi$  is *non-archimedean* if it satisfies the ultrametric inequality. The valuations in the third example are also *discrete*, meaning that  $\{\phi(a) \mid a \in K, a \neq 0\}$  is an infinite cyclic group under multiplication. It is the case that discrete valuations are necessarily non-archimedean.

We deduce from the axioms for a valuation that  $\phi(1) = \phi(-1) = 1$ . Using this we see that every valuation  $\phi$  gives rise to a metric  $d(a, b) = \phi(a - b)$  on the field  $F$ . We say that two valuations are *equivalent* if and only if the metric spaces they determine are equivalent, i.e. they give rise to the same topologies. In Example 3 above, changing the value of  $\lambda$  between 0 and 1 gives an equivalent valuation.

(A.1) THEOREM (Ostrowski). *Up to equivalence, the non-trivial valuations on  $\mathbb{Q}$  are the ones just described, namely the usual absolute value and for each prime number a non-archimedean valuation.*

More generally, if  $R$  is a ring of algebraic integers (or more generally a Dedekind domain) with quotient field  $F$ , the non-archimedean valuations on  $R$ , up to equivalence, biject with the maximal ideals (which are the same as the non-zero prime ideals) of  $R$ .

Let  $\phi$  be a non-archimedean valuation on a field  $F$ . We rapidly verify that the set  $R_\phi = \{a \in F \mid \phi(a) \leq 1\}$  is a ring, called the *valuation ring* of  $\phi$ . Any ring arising in this way is called a *valuation ring*, and if the valuation is discrete the ring is called a *discrete valuation ring*. We set  $P_\phi = \{a \in F \mid \phi(a) < 1\}$ , and this is evidently an ideal of  $R_\phi$ . For example, if  $F = \mathbb{Q}$  and  $\phi$  is the non-archimedean valuation corresponding to the prime  $p$  then  $R_\phi$  is the localization of  $\mathbb{Z}$  at  $p$ , and  $P_\phi$  is its unique maximal ideal.

(A.2) PROPOSITION. *Let  $\phi$  be a discrete valuation on a field  $F$  with valuation ring  $R_\phi$  and valuation ideal  $P_\phi$ .*

- (1) *An element  $a \in R_\phi$  is invertible if and only if  $\phi(a) = 1$ .*
- (2)  *$P_\phi$  is the unique maximal ideal of  $R_\phi$ , consisting of the non-invertible elements.*
- (3)  *$P_\phi = (\pi)$  where  $\pi$  is any element such that  $\phi(\pi)$  generates the value group of  $\phi$ .*
- (4) *Every element of  $R_\phi$  is uniquely expressible  $a = \pi^\nu a'$  where  $a'$  is a unit in  $R_\phi$ . In this situation  $\phi(a) = \phi(\pi)^\nu$ .*
- (5) *The ideals of  $R_\phi$  are precisely the powers  $P_\phi^n = (\pi^n)$ . Thus  $R_\phi$  is a principal ideal domain.*
- (6)  *$F$  is the field of fractions of  $R_\phi$ .*

*Proof.* The proofs are all rather straightforward. If  $ab = 1$  where  $a, b \in R_\phi$  then  $\phi(ab) = \phi(a)\phi(b) = \phi(1) = 1$  and since  $\phi(a)$  and  $\phi(b)$  are real numbers between 0 and 1 it follows that they equal 1. Conversely, if  $\phi(a) = 1$  let  $b$  be the inverse of  $a$  in  $F$ . Since  $\phi(b) = 1$  also it follows that  $b \in R_\phi$  and  $a$  is invertible in  $R_\phi$ . This proves statement (1).

Now  $P_\phi$  is seen to consist of the non-invertible elements of  $R_\phi$ . It is an ideal, and it follows that it is the unique maximal ideal. Defining  $\pi$  to be an element for which  $\phi(\pi)$  generates the value group of  $\phi$  we see that  $\pi \in P_\phi$ . If  $a \in P_\phi$  is any element then  $\phi(a) = \phi(\pi)^\nu$  for some  $\nu$  and so  $\phi(\pi^{-\nu}a) = 1$ . Thus  $\pi^{-\nu}a = a'$  for some element  $a' \in R_\phi$  which is a unit, and so  $a = \pi^\nu a'$ . This proves that  $P_\phi = (\pi)$ , and also the first statement of (4). The uniqueness of the expression in (4) comes from the fact that in any expression  $a = \pi^\nu a'$  with  $a'$  a unit, necessarily  $\nu$  is defined by  $\phi(a) = \phi(\pi)^\nu$ , and then  $a'$  is forced to be  $\pi^{-\nu}a$ .

To prove (5), if  $I$  is any ideal of  $R_\phi$  we let  $n$  be minimal so that  $I$  contains a non-zero element  $a$  with  $\phi(a) = \phi(\pi)^n$ . Then by (4) we have  $(a) = (\pi^n) \supseteq I$ , and it follows that  $I = (\pi^n)$ .

As for (6), given any element  $a \in F$ , either  $a \in R_\phi$  or  $\phi(a) = \phi(\pi)^{-n}$  for some  $n > 0$ . In the second case the element  $a' = \pi^n a$  has  $\phi(a') = 1$  so  $a' \in R_\phi$  and now  $a = \frac{a'}{\pi^n}$ , showing that  $a$  lies in the field of fractions of  $R_\phi$  in both cases.  $\square$

When we reduce representations from characteristic zero to positive characteristic we need to work with algebraic number fields, that is, field extensions of  $\mathbb{Q}$  of finite degree. Let  $F$  be an algebraic number field, and  $R$  its ring of integers. We quote without proof some facts about this situation. A full account may be found in [Cas] or [FT]. A *fractional ideal* in  $F$  is a finitely-generated  $R$ -submodule  $I$  of  $F$ . For any such  $I$  we put  $I^{-1} = \{x \in F \mid xI \subseteq R\}$ . With this definition of inverse and with a multiplication defined the same way as the multiplication of ideals, the fractional ideals form a group, whose identity is  $R$ . Every fractional ideal may be written uniquely as a product  $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}$  where  $\mathfrak{p}_1, \dots, \mathfrak{p}_t$  are maximal ideals of  $R$  and the  $a_i$  are non-zero integers (which may be positive or negative). Let us write  $\nu_{\mathfrak{p}_i}(I) = a_i$ , and let  $0 < \lambda < 1$ . Then for each maximal ideal  $\mathfrak{p}$  of  $R$  we obtain a discrete valuation on  $F$  by putting  $\phi(a) = \lambda^{\nu_{\mathfrak{p}}(Ra)}$ , which is called the  *$\mathfrak{p}$ -adic valuation* on  $F$ .

(A.3) PROPOSITION. *Let  $F$  be an algebraic number field with ring of algebraic integers  $R$ , and let  $\phi$  be the discrete valuation on  $F$  associated to a maximal ideal  $\mathfrak{p}$  of  $R$ . Let  $R_{\mathfrak{p}}$  be the valuation ring of  $\phi$  with maximal ideal  $P_{\mathfrak{p}}$ . Then  $R_{\mathfrak{p}}$  is the localization of  $R$  at  $\mathfrak{p}$ , and the inclusion  $R \rightarrow R_{\mathfrak{p}}$  induces an isomorphism  $R/\mathfrak{p} \cong R_{\mathfrak{p}}/P_{\mathfrak{p}}$ .*

*Proof.* We assume the group structure of the set of fractional ideals. The localization of  $R$  at  $\mathfrak{p}$  is

$$\left\{ \frac{a}{b} \mid a, b \in R, b \notin \mathfrak{p} \right\}$$

and this is clearly contained in  $R_{\mathfrak{p}}$ . Conversely, if  $\frac{a}{b} \in R_{\mathfrak{p}}$  then  $\nu_{\mathfrak{p}}(a) \geq \nu_{\mathfrak{p}}(b)$  and if we choose  $x \in \mathfrak{p}^{-\nu_{\mathfrak{p}}(b)} - \mathfrak{p}^{-\nu_{\mathfrak{p}}(b)+1}$  then  $\frac{a}{b} = \frac{ax}{bx}$ . Now  $bx \notin \mathfrak{p}$ , showing that  $\frac{a}{b}$  lies in the localization.

The kernel of the composite  $R \rightarrow R_{\mathfrak{p}} \rightarrow R_{\mathfrak{p}}/P_{\mathfrak{p}}$  is  $R \cap P_{\mathfrak{p}} = \mathfrak{p}$ . We show that this composite is surjective. We can write any element of  $R_{\mathfrak{p}}/P_{\mathfrak{p}}$  as  $\frac{a}{b} + P_{\mathfrak{p}}$  where  $a, b \in R$  and  $b \notin \mathfrak{p}$ . Since  $\mathfrak{p}$  is maximal in  $R$ ,  $R/\mathfrak{p}$  is a field and so there exists  $c \in R$  with  $bc - 1 \in \mathfrak{p}$ . Now  $\frac{a}{b} - ac = \frac{a}{b}(1 - bc) \in P_{\mathfrak{p}}$  and  $\frac{a}{b} + P_{\mathfrak{p}} = ac + P_{\mathfrak{p}}$  is the image of  $ac \in R$ . These observations show that we have an isomorphism  $R/\mathfrak{p} \cong R_{\mathfrak{p}}/P_{\mathfrak{p}}$ .  $\square$

Given a valuation  $\phi$  on  $F$  we may form the completion  $\hat{F}$  as a metric space, which contains  $F$  in a canonical way. The completion  $\hat{F}$  acquires a ring structure extending that of  $F$ , and in fact  $\hat{F}$  is a field. The valuation  $\phi$  extends uniquely to a valuation  $\hat{\phi}$  on  $\hat{F}$ , and  $\hat{F}$  is complete in the metric given by  $\hat{\phi}$ . If  $\phi$  is non-archimedean then so is  $\hat{\phi}$ , and if  $\phi$  is discrete then so is  $\hat{\phi}$ , with the same value group. Thus in the case of a discrete valuation we have a valuation ring  $\hat{R}_\phi = \{a \in \hat{F} \mid \hat{\phi}(a) \leq 1\}$  with unique maximal ideal  $\hat{P}_\phi = \{a \in \hat{F} \mid \hat{\phi}(a) < 1\}$ , and  $\hat{P}_\phi = \hat{R}_\phi(\pi)$  since  $\hat{\phi}(\pi) = \phi(\pi)$  generates the value group. (We should properly write  $\hat{R}_{\hat{\phi}}$  etc, but this seems excessive.) The ideals of  $\hat{R}_\phi$  are exactly the powers  $\hat{P}_\phi^n$ .

(A.4) LEMMA. *Let  $\phi$  be a discrete valuation on a field  $F$  with valuation ring  $R_\phi$ . The inclusion  $R_\phi \hookrightarrow \hat{R}_\phi$  induces an isomorphism  $R_\phi/P_\phi^n \cong \hat{R}_\phi/\hat{P}_\phi^n$  for all  $n$ .*

*Proof.* Consider the composite homomorphism  $R_\phi \rightarrow \hat{R}_\phi \rightarrow \hat{R}_\phi/\hat{P}_\phi^n$ . Its kernel is  $P_\phi^n$  and the desired isomorphism will follow if we can show that this homomorphism is surjective. To show this, given  $a \in \hat{R}_\phi$  we know from the construction of the completion that there exists  $b \in R_\phi$  with  $\phi(b - a) < \phi(\pi)^n$ , that is,  $b - a \in \hat{P}_\phi^n$ . Now  $b$  maps to  $a + \hat{P}_\phi^n$ .  $\square$

The completion  $\hat{R}_\phi$  is by definition the set of equivalence classes of Cauchy sequences in  $R_\phi$ . We comment that a sequence  $(a_i)$  of elements of  $R_\phi$  is a Cauchy sequence if and only if for every  $n$  there exists a number  $N$  so that whenever  $i, j > N$  we have  $a_i - a_j \in P_\phi^n$ , that is,  $a_i \equiv a_j \pmod{P_\phi^n}$ .

(A.5) LEMMA. *Let  $\phi$  be a discrete valuation on a field  $F$  with valuation ring  $R_\phi$ , maximal ideal  $P_\phi$  and completion  $\hat{R}_\phi$ . Any element of  $\hat{R}_\phi$  is uniquely expressible as a series*

$$a = a_0 + a_1\pi + a_2\pi^2 + \cdots$$

where the  $a_i$  lie in a set of representatives  $\mathcal{S}$  for  $R_\phi/P_\phi$ .

*Proof.* Let  $a \in \hat{R}_\phi$ . Since  $\hat{R}_\phi/\hat{P}_\phi \cong R_\phi/P_\phi$ , we have  $a + \hat{P}_\phi = a_0 + \hat{P}_\phi$  for some uniquely determined  $a_0 \in \mathcal{S}$ . Now  $a - a_0 \in \hat{P}_\phi$  so  $a = a_0 + \pi b_1$  for some  $b_1 \in \hat{R}_\phi$ . Repeating this construction we write  $b_1 = a_1 + \pi b_2$  with  $a_1 \in \mathcal{S}$  uniquely determined, and in general  $b_n = a_n + \pi b_{n+1}$  with  $a_n \in \mathcal{S}$  uniquely determined. Now  $a_0, a_0 + a_1\pi, a_0 + a_1\pi + a_2\pi^2, \dots$  is a Cauchy sequence in  $R_\phi$  whose limit is  $a$ , and we write this limit as the infinite series.  $\square$

The last result, combined with Proposition A.3, provides a very good way to realize the completion  $\hat{R}_\phi$ . For example, in the case of the  $p$ -adic valuation on  $\mathbb{Q}$  we may take  $\mathcal{S} = \{0, 1, \dots, p - 1\}$ . The completion  $\hat{\mathbb{Z}} = \mathbb{Z}_p$  may be realized as the set of infinite sequences  $\cdots a_3 a_2 a_1 a_0$  of elements from  $\mathcal{S}$  presented in positions to the left of a ‘point’, analogous to the decimal point (which we write on the line following American convention). Thus  $a_0$  is in the 1s position,  $a_1$  is in the  $ps$  position,  $a_2$  is in the  $p^2s$  position, and so on. Unlike decimal numbers these strings are potentially infinite to the left of the point, whereas decimal numbers are potentially infinite to the right of the point. Addition and multiplication of these strings is performed by means of the same algorithms (carrying values from one position to the next when  $p$  is exceeded, etc.) that are used with infinite decimals. Note that  $p$ -adic integers have the advantage over decimals that certain real numbers have more than one decimal representation, whereas distinct  $p$ -adic expansions always represent distinct elements of  $\mathbb{Z}_p$ .

*Exercises.*

1. With the description of the  $p$ -adic integers as the set of infinite sequences

$$\cdots a_3 a_2 a_1 a_0.$$

in positions to the left of a ‘point’, where  $a_i \in \{0, \dots, p-1\}$ , show that when  $p = 2$  we have

$$-1 = \cdots \overline{1}111. \quad \text{and}$$

$$\frac{1}{3} = \cdots \overline{1}0101011.$$

Find the representation of the fraction  $1/5$  in the 2-adic integers. What fraction does  $\cdots \overline{1}100110011.$  represent?

2. Show that the  $p$ -adic rationals  $\mathbb{Q}_p$  (i.e. the completion  $\hat{\mathbb{Q}}$  of  $\mathbb{Q}$  in the  $p$ -adic valuation) may be constructed as the set of sequences  $\cdots a_3 a_2 a_1 a_0 . a_{-1} a_{-2} \cdots a_{-n}$  which may be infinite to the left of the point, but must be finite to the right of the point, where  $a_i \in \{0, \dots, p-1\}$  for all  $i$ . Show that the rational numbers  $\mathbb{Q}$  is the subset of these sequences which eventually recur.