Thesis for Doctorate of Philosophy

UNITS IN GROUP RINGS

Graham Higman

Balliol College

UNITS IN GROUP RINGS

Abstract of Thesis

If G is any group, written multiplicatively, and K is any ring, then the finite formal sums

$$k_1 g_1 + k_2 g_2 + \cdots + k_\tau g_\tau, \qquad k_i \in K, \; g_i \in G, \; (i = 1, \ldots, \tau),$$

form a ring, when addition and multiplication is defined in the obvious way. This ring we call the group ring of G over K, and we write it as R(G,K). More precisely, R(G,K) may be defined as a ring which is a linear set over K, and has a basis which is a multiplicative group isomorphic to G. If K has the unity element 1, and if g_0 is the identity of G, then $1.g_0$ is a unity element of R(G,K). We shall identify, when confusion cannot arise thereby, elements k of K with the elements of $k.g_0$ of R(G,K). The object of this thesis is to establish certain theorems on the units of R(G,K).

An element e_1 in a ring with unity element 1 will be called a left unit if there exists also an element e_2 such that $e_1 e_2 = 1$; and e_2 will then be called a right unit, and a right inverse of e_1. If e_1 is also a right unit, then it has a uniquely defined inverse which we write as e_1^{-1}, and e_1 is then called a unit, simply. We shall deal always with rings R(G,K) in which the coefficient ring K has no right units which are not left units. Whether it is even

so possible for R(G,K) to have right units which are not left units, I do not know. Certainly it is not in the most important cases, - for instance if K can be embedded in a field, and G is of finite order. Any group ring has units of the form e.g, where e is a unit in K, and g is an element of G, for e.g has the inverse $e^{-1}.g^{-1}$. Such a unit we shall call trivial. One of the questions that naturally arises is, for what group rings these are the only units.

This thesis is chiefly concerned with the case in which G is a group of finite order, and K is the ring C of integers in an algebraic field k. We shall then speak of R(G,C) as an integral group ring. R(G,C) is then an order, but not in general a maximal order, of the linear associative algebra R(G,k). Accordingly, after an introductory section, and one ~~are~~ on definitions, we discuss in Section 3 the group algebra R(G,k). This section is an exposition of well-known facts concerning the decomposition of the semi-simple algebra R(G,k) into simple components, and is based on the classical theory of representations of finite groups in algebraic fields, as developed by I. Schur.

In Section 4 we pass on to the consideration of integral groupings, and more particularly, to a determination of what such rings have only trivial units. The result is, that R(G,C), where C is the integer ring of the field k, has only trivial units in the following four cases, and these only:

(i) G is Abelian, and the orders of its elements all divide two; k is the rational field or an imaginary quadratic extension of it;

(ii) G is Abelian, and the orders of its elements all divide six; k is the rational field, or the extension of it by a complex cube root of unity;

(iii) G is Abelian, and the orders of its elements all divide four; k is the rational field, or the extension of it by a complex fourth root of unity (that is, by $i = \sqrt{-1}$);

(iv) G is the direct product of a quaternion group and an Abelian group the orders of whose elements all divide two; k is the rational field.

To establish this theorem, we prove first a theorem which is a particular case of a result due to O. Schilling, namely, that if k is of finite degree over the rational field the unit group of R(G,C) has a finite index in the unit group of any maximal order of R(G,k) containing it. Secondly, we show that the group of trivial units in R(G,C) is not contained as a proper sub-group of finite index in any group of units of R(G,C). From these two theorems together, it follows that R(G,C) has only trivial units if and only if a maximal order of R(G,k) containing it has a finite unit group. This imposes severe restrictions on the possible simple components of R(G,k), which give rise to our main result.

In the following section, we turn our attention to the units of finite order in R(G,C). We find it convenient to treat normalised units only, - that is to say, units in which the sum of the coefficients is unity. This involves no essential loss, since any unit of finite order is the product of a normalised unit of finite order and a root of unity in C; and any group of units of finite order is isomorphic to the direct product of the corresponding group of normalised units and a group of roots of unity in C. In terms of normalised units, a theorem from section 4 becomes: The group G is not contained as a proper sub-group of finite index in any group of normalised units of R(G,C). In particular this implies that a unit of finite order in the centrum of R(G,C) must be trivial. If G is Abelian, therefore, all the units of finite order in R(G,C) are trivial. This is of course no longer true if G is not Abelian. In fact, a unit of finite order in R(G,C) need not necessarily even be conjugate to a trivial unit. We are able, however, to prove two results on units of finite order. The first states that the elements of any group of normalised units of finite order in R(G,C) are linearly independent, and even linearly independent modulo m, for any integer m, and that therefore the order of such a group cannot exceed the order of G. The second states that the prime factors of the order of a normalised unit of R(G,C)

divide the order of G. If we add the assumption that G is soluble, we can show that the order of the unit divides the order of G. Lastly, we show for the very special class of groups whose lower central series terminates in the identity and whose second derived group consists of the identity, that a group of normalised units of finite order in R(G,C) is isomorphic to a subgroup of G. This implies that R(G,C) is not isomorphic to any other group ring R(H,C) unless G is isomorphic to H. These last theorems are proved by methods different from those of the rest of the section, and our chief tools are the two-sided ideals λ_H, where H is a self conjugate subgroup of G, generated by the elements h-1, for all h in H. It should be added, that throughout this section the coefficient ring C is an arbitrary ring of algebraic integers, and may be taken to be ring of all algebraic integers.

In section 6, we apply the theorems we have proved to the detailed investigation of the ring R(G,C) where G is generated by two elements a, b subject to the relations:-

$$a^p = b^{p-1} = 1 \quad , \quad b^{-1} a b = a^r$$

where p is an odd prime, and r a primitive number modulo p. Here, too, we show that a group of normalised units in R(G,C) is isomorphic to a subgroup of G.

Finally, in section 7, we consider group rings of groups without elements of finite order. Naturally, the theorems proved are of an entirely different character. Notably, they do not depend at all on the coefficient ring K, provided that it has no zero divisors. We show, in fact, that if G satisfy the condition that every subgroup generated by a finite number of elements of G has a homomorphism on the free cyclic group, then if K has no zero divisors neither has R(G,K), and the units of R(G,K) are all trivial. The condition is satisfied by free groups and by free Abelian groups; and generally, by the direct product and the free product of any two groups that satisfy it.

As we have said, section 3 is a repetition of well-known facts; and the first theorems of section 4 are a particular case of a theorem due to Schilling. The rest of the thesis is original, though some of it has been published previously.

Thesis for Doctorate of Philosophy

UNITS IN GROUP RINGS

Graham Higman

Balliol College

UNITS IN GROUP-RINGS

1. Introduction and summary of results

If G is any group, which is written multiplicatively, and K is any ring, then the finite formal sums

$$k_1 g_1 + k_2 g_2 + \cdots + k_\tau g_\tau, \qquad k_i \in K,\ g_i \in G,\ (i = 1, \ldots, \tau),$$

form a ring when addition and multiplication are defined in the obvious way. This ring we call the group ring of G over K, and write R(G,K). (A precise definition is given at the beginning of the next section). If g_o is the identity in G, and K possesses the unity element (or modulus) 1, then $1.g_o$ is a modulus of R(G,K). We can without risk of confusion, and shall identify elements k of K with $k.g_o$ of R(G,K), and elements g_i of G with $1.g_i$ of R(G,K). The object of this thesis is to study units in group rings, - that is, elements E having an inverse E^{-1} satisfying $EE^{-1} = 1$ and $E^{-1}E = 1$. Every group-ring possesses the units $e.g_i$, where e is a unit in K and g_i is an element of G; for $e.g_i$ has the inverse $e^{-1}.g_i^{-1}$. A unit of this form will be called trivial.

Most of the present work is concerned with the special case in which G is a finite group and K is the integer ring C of an algebraic field k. Then R(G,C) is an order, though not generally a maximal order, of R(G,k), the group algebra of G over k. Naturally, therefore, in considering the properties of R(G,C) the methods of the theory of Algebras

play an important part. However, the study belongs more particularly to the Theory of Groups, because from the algebraic point of view there is nothing distinctive about the particular non-maximal order R(G,C) - indeed it is quite possible for two distinct groups G, G^1 to have isomorphic algebras, even over the rational field, though their group rings over C are not isomorphic. We shall speak of a group ring R(G,C) where C is a ring of algebraic integers, as an integral group ring.

The first question that it is natural to ask is whether a group ring has units other than the trivial ones. In the case of integral group rings of finite groups, the answer is generally affirmative. The exceptions, - group rings having only trivial units - are the rings R(G,C), where C is the integer ring of the field k, and either:-

(i) G is Abelian, and the orders of its elements all divide two; k is the rational field or a quadratic imaginary extention of it:

or (ii) G is Abelian, and the orders of its elements all divide six; k is the rational field or the extension of it by a complex cube root of unity:

or (iii) G is Abelian, and the orders of its elements all divide four; k is the rational field or the extension of it by a complex fourth root of unity (that is, by $i = \sqrt{-1}$):

or (iv) G is the direct product of a quaternion group and an Abelian group the orders of whose elements all divide two; k is the rational field.

This we prove in Section 4 below. We then turn our attention to units of finite order. It is convenient to consider only normalised units, - that is, units the sum of whose coefficients is unity. This is no loss of generality, as every unit in R(G,C) is the product of a normalised unit and a unit of C. It emerges from the proof of the results previously mentioned, that G is not contained as a proper subgroup of finite index in any group of normalised units. In particular, this implies that a unit of the centrum of R(G,C) cannot be of finite order unless it is trivial. If G is Abelian, therefore, all the units of finite order in R(G,C) are trivial. This, of course, is no longer true if G is not Abelian. It is not even necessary for a unit of finite order in R(G,C) to be conjugate to a trivial unit, as we shew by means of an example. However, we shew that the prime factors of the order of a normalised unit of finite order in R(G,C) all divide the order of G; and that a group of normalised units of finite order of R(G,C) has an order not greater than that of G. For a soluble group, we improve the ~~final~~ first statement to: The order of a normalised unit of finite order in R(G,C) divides the order of G. For the special case of a group G whose upper central series ends in

the whole group G, and whose second derived group consists of the identity, we are able to show that a group of normalised units of finite order is isomorphic to a subgroup of G. In all these theorems we may take the ring C to be the ring of all algebraic integers.

In the last section we turn to the case in which G is a group without elements of finite order. As might be expected the theorems provable here are of a quite different character. In fact, they all state that if G satisfies given conditions, then, whatever be the coefficient ring K, provided only that it has no zero divisors, R(G,K) has no zero-divisors and only trivial units. Of these conditions, the most manageable is that any subgroup H of G generated by a finite number of elements, has a homomorphism on a free cyclic group. This condition is satisfied in particular by free groups, and by free Abelian groups.

There is very little to be said concerning previous work on the same or similar subjects. The group algebra of a finite group is, of course, well known, and affords one of the most convenient examples of a semi-simple algebra. In particular, the results of section 3 are well known, and no originality is claimed for them. Considerably less attention has hitherto been paid to integral group rings, or to the group rings of infinite groups. Certain particular problems in connection with integral group rings have been studied

with a view to applications to topology, notably by K. Reidermeister[1] and W. Franz[2], but these have no relevance to the problems with which we are concerned. More relevant is the work on units in maximal orders in semi-simple algebras which has been done by O. Schilling[3] and M. Eichler[4]. In particular, Theorem 4 of section 4, is a particular case of a theorem of Schilling's. However, in a maximal order of a general semi-simple algebra there is clearly no analogue of a trivial unit, so that the remainder of section 4 does not overlap with Schilling's work. Sections 5, 6 and 7, too, are entirely original, though I have to thank my successive supervisors, Mr J.H.C. Whitehead and Mr P. Hall, for many suggestions. Some of the results in these sections I have previously published[5].

---

(1) Journal fur die reine und angewandte Mathematik, 173, 164-173, (1935).
(2) Journal fur die reine und angewandte Mathematik, 173, 174-184 and 245-254, (1935).
(3) Journal fur die reine und angewandte Mathematik, 175, 246-251 (1936).
(4) Mathematisches Annalen, 114, 635-654, (1937).
(5) Proceedings of the London Mathematical Society, (2), 46, 231-248 (1940).

2. Definitions and Preliminary Considerations

Let K be any ring. Then a set L will be called a linear set over K if:-

(i) its elements form an Abelian group with respect to an operation of addition;

(ii) there is defined a multiplication of elements of L by elements of K, satisfying

$$\left.\begin{aligned} k.(a+b) &= k.a + k.b, \\ (k_1+k_2).a &= k_1.a + k_2.a, \\ k_1.(k_2\,a) &= (k_1 k_2).a, \end{aligned}\right\} \quad k, k_1, k_2, \text{ in } K;\ a, b \text{ in } L.$$

The set of elements $e_1, e_2, e_3 \ldots$ of L will be called a basis of L if every element of L can be written in the form:-

$$k_1 e_{i_1} + k_2 e_{i_2} + \cdots + k_r e_{i_r}\ ; \quad k_1, \ldots, k_r \text{ in } K,\ i_1 < i_2 < \cdots < i_r;$$

and if this element is zero only if $k_1 = k_2 = \ldots = k_r = 0$.

Henceforward we shall further suppose that the ring K has a unity element 1, and that 1 is an identity operator on L, - that is, that $1.a = a$ for all a in L.

If a ring R is also a linear set over K, with a basis, and furthermore

$$a.kb = k.ab, \quad k \text{ in } K,\ a, b \text{ in } R,$$

then R may be called a hyper-complex system over K. The structure of R is determined by the multiplication table of the elements of its basis. For if the products

$$e_i\, e_j = k_{ij1}\, e_1 + k_{ij2}\, e_2 + \cdots$$

(where, of course, only a finite number of coefficients k_{ij} are different from zero), are known, we can find the product of any two elements of R by the distributive laws. If, in particular, these basis elements form a multiplicative group G, then R is called the group ring of G over K, and we write R = R(G,K). We make, that is to say, the definition:

The group ring R(G,K) of a group G over a ring K is a hyper-complex system over K having a basis which is a multiplicative group isomorphic to G.

If G is a group of finite order, and K is a field, then R(G,K) is, of course, a linear algebra over K, and is usually called the group algebra of G over K.

If e_o is the identity of G, the quantities $k\,e_o$ of R(G,K) form a sub-ring isomorphic to K; and moreover for any element P in R(G,K) we have $k_o e_o . P = kP$. It is therefore possible to identify the element $k.e_o$ of R(G,K) with the element of k of K, and whenever it is convenient to do so, we shall. In particular, the element $1.e_o$, which is a unity element in R(G,K), will be written as 1.

In any ring with a unity element 1, if elements E_1, E_2 exist satisfying $E_1E_2 = 1$, we say that E_1 is a left unit, and E_2 is a right unit. An element E that is both a left unit and a right unit will be described amply as a unit. Then the element E^{-1} satisfying $EE^{-1} = 1$ is unique, and

$E^{-1}E = 1$. The units of a ring therefore form a group. A group ring always possesses units of the form $k.e_i$, where k is any unit in the coefficient ring k. For we have $k\,e_i \,.\, k^{-1}e_i^{-1} = 1$. Such a unit will be described as trivial. If the coefficient ring has right units which are not left units, the same is true of the group ring. For if, say, $k_1k_2 = 1$, $k_2k_1 \neq 1$, we have $k_1\,e_o \,.\, k_2\,e_o = 1$; and $k_2\,e_o \,.\, E = 1$, E in $R(G,K)$, would imply $E = k_1e_o$, whereas $k_2\,e_o \,.\, k_1\,e_o = k_2\,k_1\,e_o \neq 1$. Thus $k_2\,e_o$ is a right unit but not a left unit in $R(G,K)$. Whether this is possible in case every right unit in K is also a left unit, I do not know. Obviously, if both the ring K and the group G are commutative, so is $R(G,K)$; and every right unit in $R(G,K)$ is therefore also a left unit. Moreover, if G is of finite order, and K is a subring of a (not necessarily commutative) field k, then every right unit in $R(G,K)$ is also a left unit. For the regular representation of G can then be extended to $R(G,K)$, and gives an isomorphism of that ring onto a ring of finite matrices with elements in k. In such a ring of matrices, however, the equation $E_1E_2 = 1$ certainly implies $E_2E_1 = 1$. For, as in the theory of matrices whose elements are numbers, we can reduce any matrix whose element lie in a field to the form $\begin{Vmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 0 \end{Vmatrix}$ by a series of elementary transformations - interchanging two rows, adding a right multiple of one column to

another, etc. - each of which is equivalent to multiplication on the right or the left by a matrix with a right and left inverse. A matrix is clearly both a right and a left unit if there are no zeros in its diagonal when it is so reduced, and neither a right nor a left unit if there are such zeros. However, it is quite possible for a hypercomplex system with an infinite basis over a field to have right units which are not left units - we may simply take as basis all products $a^{\alpha}b^{\beta}$, α, β non-negative integers, with the multiplication table implied by $ba = 1$ - and there seems nothing to suggest that this is impossible in a group ring.

Before we proceed to the study of units under more particular assumptions on G and K, let us consider the relations between the units in the group rings R(G,K) and R(H,K) when H is a subgroup, or a factor group of G.

First, let H be a subgroup of G. Then R(H,K) may be regarded as a subring of R(G,K). If E in R(H,K) is a unit in R(H,K) it is obviously also a unit in R(G,K). The converse, however, is also true: If E in R(H,K) is a unit in R(G,K) it is also a unit in R(H,K). For let $E F = 1$, F in R(G,K). Let $e_0 = 1, e_1, \ldots$, etc. be a set of representatives of the right hand residue classes H x of H in G. Then we have $F = F_0 e_0 + F_1 e_1 + \ldots$; where $F_0, F_1, \ldots$ are in R(H,K).

Therefore $E F = E F_0 e_0 + E F_1 e_1 + \ldots = 1.$

Comparing the coefficients on the right hand and on the left hand of elements in H, we obtain $E\,F_0 = 1$, as required.

Next, let F be a self-conjugate subgroup of G, and let H be the factor group G/F. Since $g \to g\,F$ is a homomorphism of G on H, the correspondence

$$u = k_1.e_1 + \cdots + k_r.e_r \to uF = k_1.e_1F + \cdots + k_r.e_rF$$

is a homomorphism of R(G,K) on R(H,K). If u is a unit in R(G,K), u F is a unit in R(H,K), and if u is trivial, uF is trivial. If in particular we take F = G, we have a homomorphism of R(G,K) onto $R(G/G, K)$ - that is onto K itself - in which each element of R(G,K) is mapped onto the sum of its coefficients. Thus if u is a unit in R(G,K), the sum of its coefficients is a unit in K. Let us describe u as normalised if that sum is 1. Then every unit in R(G,K) is the product of a unit in K and a normalised unit. The normalised units form a group, and the whole group of units of R(G,K) is the direct product of the group of normalised units and the unit group of K.

3. The Group Algebra of a Finite Group

Let G be a finite group of order n, having the elements $g^{(1)}, g^{(2)}, \ldots, g^{(n)}$; and let k be any algebraic extension of the rational field. We are concerned in this section with the group algebra A = R(G,k) of G over k.

The algebra A is semi-simple. This is equivalent to the theorem of Maschke, that every representation of a finite group by matrices in k is completely reducible to a sum of representations irreducible in k. A is therefore a direct sum of simple algebras, each of which is a total matric algebra over some division algebra over k. There is, moreover, a well-known connection between the decomposition of a semi-simple algebra A into simple components, and its representations by matrices with elements in the ground field k. Suppose, in fact, that $\Gamma_1, \Gamma_2, \ldots, \Gamma_\alpha$ are a complete set of mutually inequivalent representations of A, by matrices in k, that are irreducible in k. Then firstly the only element of A represented by zero in each of the representations $\Gamma_1, \ldots, \Gamma_\alpha$ is zero; and secondly, the representations are independent, in the sense that if an element x of A is represented in Γ_ρ by X, then there exists x^1 in A such that x^1 is represented in Γ_ρ by X, and in Γ_σ by zero, if $\sigma \neq \rho$.

Let A_ρ denote the sub-algebra of A consisting of all elements represented by zero in each representation Γ_σ, $\sigma \neq \rho$. Then A is the direct sum of $A_1, \ldots, A_\alpha$; each of which is

simple, and isomorphic to the algebra of matrices by which Γ_ρ represents A. We shall not here make use of these theorems from the theory of algebras, but shall base ourselves instead on the classical theory of representations of finite groups. This seems more in keeping with the nature of the subject, for the ring R(G,C), where C is the integer ring of k, in which we are more particularly interested, is only defined in terms of the special basis of R(G,k) which consists of the elements of G. We should therefore in any case need the explicit formulae connecting that basis with the basis that exhibits the decomposition of R(G,k) into simple components, and such formulae are provided by the classical theory[1].

The simplest case, naturally, arises when every representation of G that is irreducible in k is absolutely irreducible. Then the simple components of A are total matric algebras over k of the degrees of the representations. Suppose in fact that Γ_ρ is the representation:-

$$(1)\quad \Gamma_\rho : g^{(a)} \to \| g^{(a)}_{\rho ij} \| , \quad i,j = 1,\dots,n_\rho ; \quad a = 1,\dots,n ; \quad \rho = 1,\dots,\alpha .$$

Then if we write $\| \bar{x}_{ij} \|$ for the inverse of the matrix $\| x_{ij} \|$ we have the relations between the representations[2]:-

---

(1) For the theorems quoted in this paragraph cf. B.L. van der Waerden, Moderne Algebra, vol. II, ch. XVII or A.A. Albert, Structure of Algebras, ch. VIII.

(2) Compare A. Speiser, Theorie der Grappen von Endliche Ordnung, Ch. 11, § 53.

$$(a)\quad \sum_{a=1}^{n} g^{(a)}_{\rho ij}\, \bar{g}^{(a)}_{\sigma kl} = 0\,, \quad \rho \neq \sigma,\ \rho,\sigma = 1,\dots,\alpha;\ i,j = 1,\dots,n_\rho;\ k,l = 1,\dots,n_\sigma$$

(2)

$$(b)\quad \sum_{a=1}^{n} g^{(a)}_{\rho ij}\, \bar{g}^{(a)}_{\rho kl} = \frac{n}{n_\rho}\,\delta_{il}\,\delta_{jk}, \quad \rho = 1,\dots,\alpha;\ i,j,k,l = 1,\dots n_\rho;$$

which can be written in the equivalent form:-

$$(a)\quad \sum_{\rho,i,j} n_\rho\, g^{(a)}_{\rho ij}\, \bar{g}^{(b)}_{\rho ji} = 0\,, \quad b \neq a,\ a,b = 1,\dots,n;$$

(3)

$$(b)\quad \sum_{\rho,i,j} n_\rho\, g^{(a)}_{\rho ij}\, \bar{g}^{(a)}_{\rho ji} = n\,, \quad a = 1,\dots,n.$$

Define elements $\eta_{\rho ij}$ in A by:

$n g/n$

$$(4)\quad \eta_{\rho ij} = \frac{1}{n}\sum_{a=1}^{n} \bar{g}^{(a)}_{\rho ji}\cdot g^{(a)}\,; \quad i,j = 1,\dots,n_\rho\,;\ \rho = 1,\dots,\alpha.$$

Then using (1) and (2) we see that $\eta_{\rho ij}$ is represented by zero in Γ_σ if $\sigma \neq \rho$, and in Γ_ρ by E_{ij}, the matrix having 1 at the junction of the i-th row and the j-th column, and zeros elsewhere. By direct multiplication we have

$$\eta_{\rho ij}\,\eta_{\sigma kl} = \frac{n_\rho\, n_\sigma}{n^2}\sum_{a=1}^{n}\sum_{b=1}^{n} \bar{g}^{(a)}_{\rho ji}\,\bar{g}^{(b)}_{\sigma lk}\cdot g^{(a)} g^{(b)}\,.$$

Then setting $g^{(a)}\, g^{(b)} = g^{(c)}$, we have $g^{(b)-1} = g^{(c)-1}\, g^{(a)}$, which implies

$$\bar{g}^{(b)}_{\sigma lk} = \sum_{p=1}^{n_\rho} \bar{g}^{(c)}_{\sigma lp}\, g^{(a)}_{\sigma pk}\,.$$

Substituting, we obtain

$$\eta_{\rho ij}\,\eta_{\sigma kl} = \frac{n_\rho n_\sigma}{n^2}\sum_{p=1}^{n_\sigma}\Big(\sum_{a=1}^{\hat{n}} \bar{g}^{(a)}_{\rho ji}\, g^{(a)}_{\sigma pk}\Big)\Big(\sum_{c=1}^{\hat{n}} \bar{g}^{(c)}_{\sigma lp}\, g^{(c)}\Big).$$

Using (2), we have, therefore, the multiplication table:-

(5) (a) $\eta_{\rho ij}\,\eta_{\sigma kl} = 0, \quad \rho \neq \sigma;$

(b) $\eta_{\rho ij}\,\eta_{\rho kl} = \delta_{ik}\,\eta_{\rho il}\,;$

which expresses the fact that for fixed ρ, $\eta_{\rho ij}$ are a normal matric basis of a matric subalgebra, A_ρ of A, and that the sum $A_1 + \ldots + A_a$ is direct. That this sum is the whole algebra A follows from the solution of equations (4) for $g^{(a)}$, which are obtained by the use of (3):-

(6) $$g^{(a)} = \sum_{\rho,i,j} g^{(a)}_{\rho ij}\,\eta_{\rho ij}\,.$$

That the group algebra A is semi-simple emerges, of course, as a corollary.

If the absolutely irreducible representations of G are not all equivalent to representations in k, the state of affairs is more complicated. Let Γ_1 be an absolutely irreducible representation of G, of order n_1, and let k_1 be the extension of k determined by the characters of Γ_1, k_1 being of degree r over k. Then Γ_1 determines representations

$\Gamma_2, \Gamma_3, \ldots, \Gamma_r$ of G whose characters are conjugate with respect to k to those of Γ_1[1]. The characters of the representation $\Gamma_1 + \Gamma_2 + \ldots + \Gamma_r$ are in k, and therefore some multiple of it is equivalent to a representation in k. Let s be the least number such that $s(\Gamma_1 + \ldots + \Gamma_r)$ is equivalent to a representation in k, and let Γ, with elements in k, be equivalent to it. Then Γ is irreducible in k, and it is the only representation of G irreducible in k that has Γ_1 among its absolutely irreducible components. The number s might equally well have been defined as the least number such that $s\Gamma_1$ is equivalent to a representation in k_1, the field of its characters. Moreover there exists a field k_2 of degree s over k_1 such that Γ_1 is equivalent to a representation in k_2; and s divides n_1. Thus every absolutely irreducible representation of G is a component of just one irreducible representation of G in k. If, now, x in $A = R(G,k)$ is represented by zero in Γ, it is likewise represented by zero in Γ_1, so that if x is represented by zero in every representation irreducible over k, it is represented by zero in every absolutely irreducible representation, and is therefore zero. To demonstrate that Γ is independent of the other irreducible representations of G in k, it is sufficient to show that

---

(1) For the results quoted in this paragraph, see I. Schur, Berliner Sitzungsberichte, 1906, 164-184.

there is an element in R(G,k) represented in Γ by $\|1\|$ and in every other representation by zero. If, however, we suppose $\Gamma_1, \ldots, \Gamma_r$ given by (1), and $\eta_{\rho ij}$ in some extension ring R(G,k') defined by (4), then the element E has the desired property, where

$$E = \sum_{\rho=1}^{r} \sum_{i=1}^{n_\rho} \eta_{\rho ii},$$

or, by (4)

$$E = \frac{n_1}{n} \sum_{a=1}^{n} \cdot \sum_{\rho=1}^{r} \sum_{i=1}^{n_\rho} \bar{g}^{(a)}_{\rho ii} \cdot g^{(a)}.$$

Here the coefficient of $g^{(a)}$ is equal to $\frac{n_1}{n}[\chi_1(g^{(a)-1}) + \cdots + \chi_r(g^{(a)-1})]$ and is therefore in k; so that E is in R(G,k) as required.

Thus A is the direct sum of the algebras A_ρ by which it is represented in its irreducible representations. Let Γ, as above, be irreducible in k, but have the absolutely irreducible components $\Gamma_1, \ldots, \Gamma_r$ each taken s times. Let A_1 be the corresponding component of A. If x is in A, the representing matrix $\Gamma(x)$ plainly determines $\Gamma_1(x)$; but conversely, the representations $\Gamma_1, \ldots, \Gamma_r$ being conjugate with respect to k, $\Gamma_1(x)$ determines $\Gamma_2(x), \ldots, \Gamma_r(x)$, and therefore $\Gamma(x)$. Thus A_1, which is isomorphic to the algebra of matrices $\Gamma(x)$ is equally isomorphic to the algebra over k of matrices $\Gamma_1(x)$. In this algebra, the centrum is generated by all matrices $\Gamma_1(y)$ where $y = \sum g^{(a)}$ is the sum of a set of conjugate elements in G. Such a matrix, however, is a

scalar matrix $\frac{c}{n_1}\chi_1(g^{(a)}) \times \|1\|$, c being the number of elements conjugate to $g^{(a)}$. These together generate the field k_1 of the characters of Γ_1. Thus A_1 is a simple algebra. Since Γ_1 can be realised in a field k_2 of degree s over k_1, the algebra $A_1(k_2)$, formed by extending the centrum k_1 of A_1 to k_2, is a direct sum of total matric algebras. Since s is also the least number for which this is so, A_1 is a total matric algebra over a division algebra having index s over k_1, the field of characters of Γ_1. Summing up our results:-

Theorem 1. The group algebra A of a finite group G over a field k is the direct sum of as many simple components as there are inequivalent irreducible representations of G in k. If Γ is a representation of G ~~of order n~~, irreducible in k, but the sum of r absolutely irreducible components of order n_0 each taken s times, then the corresponding simple component of A is a total matric algebra of ~~order~~ index $\frac{n}{s}$ over a division algebra of index s over its centrum. That centrum is the field of the characters of an absolutely irreducible component of Γ, and is of degree r over k.

If G is Abelian, every absolutely irreducible representation of G is of order 1. The characters of such a representation are just those numbers x for which $\|x\|$ represents an element of G. There can thus be no question of a

representation of G not being realisable in the field of its characters. Now if h is the maximum order of any element in G, each of these characters must be an h-th root of unity, since the order of any element of G divides h. Moreover, G can be written as the direct product of a cyclic group $\{g\}$ of order h, and a subgroup G^1. Thus there is a representation of G in which g is represented by $\|w\|$, where w is a primitive h-th root of unity, and whose characters therefore generate the field k(w). Thus Theorem 1 yields, for the particular case in which G is Abelian:-

Theorem 2. If G is Abelian, and the maximum order of any element in G is h, then R(G,k) is isomorphic to a direct sum of fields $k(w_\rho)$, $\rho = 1,\ldots,a$; where w_ρ is an h-th root of unity, and for at least one value of ρ a primitive h-th root of unity.

In dealing with particular examples, it is frequently convenient to treat R(G,k) as a direct sum not of its simple components, but of components formed by uniting some of these. This is especially so if G has a self conjugate sub-group H. Among the irreducible representations of G there will then be some, say $\Gamma_1,\ldots,\Gamma_s$ in which all the elements of H are represented by the identity. These will therefore form a complete set of irreducible representations of the factor

group G/H. Hence the simple components of R(G,k) corresponding to these representations can be united into a single ring isomorphic to the group ring of this factor group, R(G/H, k). In particular, the simple components corresponding to the representations of G whose absolutely irreducible components are of order 1, can be united into a single component isomorph to $R(G/G^1, k)$ where G^1 is the derived group of G.

Before we turn to the application of these results to integral group rings, we must make good our earlier statement that it is possible for two distinct groups to have isomorphic group algebras. An obvious case of this is that of any two Abelian groups G, G^1, of the same order n, the coefficient field k being any field containing the n-th roots of unity. For then both R(G,k) and $R(G^1,k)$ are direct sums of n fields isomorphic to k. We can, however, give an example in which R(G,k) and $R(G^1,k)$ are isomorphic when k is the rational field, and therefore when k is any field. Let in fact G, G^1 be two non-Abelian groups of order p^3, where p is any odd prime, given by the generators and relation systems:-

G: generators:- a, b ; relations:- $a^{p^2} = b^p = 1$; $a b a^{-1} b^{-1} = a^p$.

G': generators:- x, y, z; relations:- $x^p = y^p = z^p = 1$;

$x y x^{-1} y^{-1} = z$, $x z x^{-1} z^{-1} = y z y^{-1} z^{-1} = 1$.

G and G^1 are not isomorphic because G has an element of order p^2, and G^1 has not. In either case, there are p^2 representations of order 1, whose corresponding simple components can be united into a group ring of an Abelian group of order p^2 and type (1,1). The remaining absolutely irreducible components are p-1 in number, and of order p; and each is realisable in the field k(w) of its characters, where w is a primitive p-th root of unity. We have in fact the representations:-

G: $a \to \begin{Vmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & & & 1 \\ w & 0 & & \cdots & 0 \end{Vmatrix}$, $b \to \begin{Vmatrix} 1 & & & & 0 \\ & w & & & \\ & & w^2 & & \\ & & & \ddots & \\ 0 & & & & w^{p-1} \end{Vmatrix}$.

G^1: $x \to \begin{Vmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & & & 1 \\ 1 & 0 & & \cdots & 0 \end{Vmatrix}$, $y \to \begin{Vmatrix} 1 & & & & 0 \\ & w & & & \\ & & w^2 & & \\ & & & \ddots & \\ 0 & & & & w^{p-1} \end{Vmatrix}$, $z \to \begin{Vmatrix} w & & & & 0 \\ & w & & & \\ & & w & & \\ & & & \ddots & \\ 0 & & & & w \end{Vmatrix}$.

By Theorem 1, R(G,k) and R(G',k), if k is the rational field, are both a direct sum of the group ring of an Abelian group of order p^2 and type (1,1), and the total matric algebra of index p over k(w).

In neither of the above two cases are the corresponding integral group rings R(G,C) and $R(G^1,C)$ isomorphic, by the 1st corollary to Theorem 13 in section 5. Whether it is possible for two non-isomorphic groups to have isomorphic integral group rings I do not know; but the results of section 5 suggest that it is unlikely.

4. Integral Group Rings of Finite Groups

We now turn our attention to the integral group ring R(G,C), where G is a finite group and C is the ring of integers in an algebraic extension k of the rational field. The particular object of the present section is to determine under what conditions all the units of such a group ring are trivial.

The elements of R(G,C), are integers of R(G,k); that is to say, they satisfy polynomial equations with coefficients in C and leading coefficient unity. For let t be any element in R(G,C) and T its image in the regular representation of R(G,C). That is, let $T = \| \tau_{ij} \|$, where $g^{(i)} . t = \sum_{j=1}^{n} \tau_{ij} g^{(j)}$. Then T has integral elements, and its characteristic function $\varphi(x)$ therefore has integral coefficients, and leading coefficient unity. But $\varphi(T) = 0$, and therefore $\varphi(t) = 0$; so that t is an integer of R(G,k), as required. Moreover, R(G,C) contains the unity of R(G,k), and the product of any element in R(G,C) by an element of C is in R(G,C). That ring is therefore an order in R(G,k). It is not, however, a maximal order in R(G,k), except in the trivial case in which G consists of the identity alone. For the element $\frac{1}{n} \sum_{i=1}^{n} g^{(i)}$ is an idempotent of the centrum of R(G,k) and is therefore in every maximal order of R(G,k), but it is not in R(G,C). We have, however, the following Theorem:-

Theorem 3. If k is a finite extension of the rational field, and O is any order of R(G,k) containing R(G,C), then R(G,C) contains the set n O of all multiples of elements in O by the order n of G.

Suppose that a complete set of irreducible representations of G can be so chosen that in each representation all the elements of O are represented by matrices whose elements are integers. Let these representations be $\Gamma_1, \ldots, \Gamma_\alpha$ given by equation (1) of the previous section. Let k^1 be the extension of k determined by $g^{(a)}_{\rho ij}$, $(i,j = 1,\ldots,n_\rho; \rho = 1,\ldots,\alpha; a = 1,\ldots,n)$ and define $\eta_{\rho ij}$ in $R(G,k^1)$ by equation (4) of the previous section. An element in O is of the form $\sum_{\rho ij} b_{\rho ij}\,\eta_{\rho ij}$, with $b_{\rho ij}$ integral, since by assumption the matrix $\| b_{\rho ij} \|$ representing it in Γ_ρ has integral elements. Thus an element in nO can be written $\sum_{\rho,i,j} b_{\rho ij} \cdot n\,\eta_{\rho ij}$ with $b_{\rho ij}$ integral, and it suffices to show that $n\,\eta_{\rho ij}$ is in $R(G,C^1)$ where C^1 is the integer ring of k^1. However, since R(G,C) is contained in O, elements in G are represented in Γ_ρ by matrices with integer elements, so that $\bar{g}^{(a)}_{\rho ij}$ is integral, and so by equation (4), $n\,\eta_{\rho ij}$ is in $R(G,C^1)$.

It remains, therefore, to show that given the irreducible representation Γ we can find Γ' equivalent to it, such that the elements of O are represented in Γ' by matrices

whose elements are integers[1]. We may suppose Γ to be a representation in some finite algebraic field k' containing k. Let O' be the order in $R(G,k')$ consisting of all elements $\sum_i c_i O_i$ where c_i are integers in k', and O_i are elements in O. Let $e_1,\ldots e_s$ be the unit vectors of the vector space in which the matrices of $\Gamma(G)$ act, and consider the vectors

$$(1) \qquad X e_1 = x_{11} e_1 + x_{12} e_2 + \cdots + x_{1s} e_s ,$$

for all matrices X representing elements of O'. Call a vector (1) of length r if $x_{1t} = 0$ for $t > r$ and consider the set I_r of all r-th coefficients x_{1r} of vectors of length r. For each r, I_r is fractional ideal in k' distinct from the zero ideal. For I_r plainly contains the difference of any two of its elements, and the product of any one of them by an integer in k'. Moreover we can find a number m_r such that any element of $m_r I_r$ is an integer. If r = 1, we have $X e_1 = x_{11} e_1$ so that $x - x_{11}$ is a factor of the characteristic function of X. Since O' is an order, this function has integral coefficients, and therefore x_{11} is an integer, so that we may take $m_1 = 1$. Now since Γ is irreducible, we can, by Burnside's Theorem[2] choose an element E_r in $R(G,C^F)$, and therefore in O', such that its image in Γ is $m_r E_{1r}$, for

---

(1) Cf. Speiser, op.cit. Ch. 14, § 65.
(2) Cf. van der Waerden, op.cit. Ch. XVII, § 121.

some number m_r, where $E_{1r}\, e_r = e_1$, $E_{1r}\, e_k = 0$, $k \neq r$.

Then by (1) we have

$$m_r E_{1r} \cdot X e_1 = m_r x_{1r} e_1 ,$$

so that $m_r x_{1r}$ must be integral, as required. Thus I_r is an ideal in k^1. If it were the zero ideal, there would be less than s linearly independent vectors in (1), contrary to the hypothesis that Γ is irreducible. Since k^1 is a finite extension of the rational field, we can find an extension k'' of k', such that the ideals I_r^1 in k'', having the elements of I_r as basis, are principal ideals (α_r). Extending the order O' again to O" in R(G,k") and supposing X in (1) to be chosen now from the matrices representing elements of O", we have that there are vectors $f_1, f_2, \ldots, f_s$ in the set (1) such that

$$f_r = f_{r1} e_1 + \cdots + f_{r,r-1} e_{r-1} + \alpha_r e_r .$$

Then every vector of (1) can be written as $\sum_r y_r f_r$ with integral coefficients y_r. Choosing $f_1, f_2, \ldots, f_s$ as a new basis for the vector space, we obtain an equivalent representation Γ' with the desired properties. Our next theorem is almost a corollary of Theorem 3.

Theorem 4. If C is the integer ring of a finite extension k of the rational field, then the unit group of R(G,C) has a

---

(1) See Hilbert, Jahresberichte der Deutschen Mathematiker-Vereinigung, 4, p.224, (1897).

finite index in the unit group of any order O of R(G,k) containing R(G,C).[1]

Let X, Y be any two units in O such that $X = Y + nZ$, where Z is in O. Then we have $X Y^{-1} = 1 + nZY^{-1}$, which by Theorem 3 is an element of R(G,C). That is to say, X and Y are in the same left residue class with respect to the unit group of R(G,C). The index of this group in the unit group of O cannot therefore exceed the maximum number of elements of O that are incongruent modulo n, and this number is the finite integer n^{nm} where m is the degree of k over the rational field.

It follows that the units of R(G,C) cannot all be trivial unless the unit group of a maximal order O containing R(G,C) is finite. Suppose in the first place that the unit group of C is of finite order. Then the group of trivial units of R(G,C) is of finite order, and if it is the whole unit group of R(G,C), must be contained as a subgroup of finite index in the unit group of O. This group must therefore be of finite order. If, on the other hand, the unit group of C is infinite, then its rank is a finite integer r.[2] That is to say, the unit group has a subgroup which is a free Abelian group on r generators, but not for any greater number. Then clearly the

---

(1) Cf. Schilling, loc.cit.
(2) See Hilbert, op.cit., p.214.

same is true of the group of trivial units in R(G,C). However, the centrum of R(G,k) is a direct sum of α fields, where α is the number of simple components of R(G,k), and each of these is isomorphic to k or an extension of k. Every maximal order of R(G,k) and O in particular contains the integer ring of this centrum, and the unit group of this integer ring has a free Abelian subgroup on αr generators. Since $\alpha > 1$ and $r > 0$, we have $\alpha^r > r$. Thus the trivial unit group of R(G,C) cannot have finite index in the unit group of O, and therefore cannot be the whole unit group of R(G,C). This gives the necessity of the following condition:-

Theorem 5. A necessary and sufficient condition that all the units of R(G,C) be trivial, is that a maximal order of R(G,k) containing R(G,C) have a unit group of finite order.

To show that this condition is sufficient, we rely on:-

Theorem 6. The group of trivial units in R(G,C) is not contained as a proper subgroup of finite index in any group of units of R(G,C).

If O has a finite unit group, as has R(G,C). The unit group of R(G,C) must then contain the trivial group as a subgroup of finite index. By Theorem 6, it must therefore coincide with it.

If the group of trivial units were contained as a proper subgroup of finite index in a group G_1, of units of $R(G,C)$, then G_1 would contain a non-trivial unit of finite order, in which the coefficient of the identity of G differs from zero. However, we shall show that this is impossible, and therefore that Theorem 6 holds.

Lemma. The coefficient of the identity in a non-trivial unit of finite order in $R(G,C)$ is zero.

Let E be a unit of finite order in $R(G,C)$, in which the coefficient of the identity is the non-zero integer a. Let $\bar{E}$ be the image of E in the regular representation of G. We have trace $\bar{E} = na$, where n is the order of G. The characteristic roots of $\bar{E}$ are roots of unity, $w_1, \ldots, w_n$, and therefore

$$(1) \qquad |\text{trace } \bar{E}| = |w_1 + w_2 + \cdots + w_n| \leq |w_1| + |w_2| + \cdots + |w_n| = n$$

and the same is true for all the conjugates of trace $\bar{E}$. Therefore $|N(a)| \leq 1$, where N(a) stands for the norm of a, and is therefore a non-zero rational integer. Thus equality must hold here, and therefore also in (1). That is to say

$$|w_1 + w_2 + \cdots + w_n| = |w_1| + |w_2| + \cdots + |w_n|,$$

which can only happen if $w_1 = \ldots = w_n$. Then, however, the matrix $\bar{E}$, being of finite order, must be scalar, so that $E = w.1$, and therefore E is trivial, which proves the Lemma.

We now seek to use Theorem 5 in order to determine all group rings having only trivial units. By Theorem 5, the corresponding group algebra must have a maximal order of highest rank with a finite unit group. Now if an algebra A is a direct sum of subalgebras $A_1,\ldots,A_\alpha$, and O is an order in A, then the set O_i, $(i = 1,\ldots,\alpha)$, of elements of A_i in O is an order in A_i. Conversely, if O_i, $i = 1,\ldots,\alpha$, is an order in A_i, then the set O of all sums $\sigma_1 + \sigma_2 \ldots + \sigma_\alpha$, ($\sigma_i$ in O_i) is an order in A. Moreover, if u is a unit in O, then if we write $u = u_1 + u_2 + \ldots + u_\alpha$, u_i in A_i, then u_i is a unit of O_i; and conversely if for $i = 1,\ldots,\alpha$, u_i is a unit in O_i, then $u = u_1 + u_2 + \ldots + u_\alpha$ is a unit in O. The unit group of O is therefore the direct product of the unit groups of O_1, O_2, ..., O_α. It follows that a semi-simple algebra has a maximal order of highest rank with a finite unit group, if and only if the same is true of each of its simple components. Such a simple component is, of course, a total matric algebra over some division algebra over the ground field k. If the component is to have the desired property, then in the first place the matric algebra must be of index one. For otherwise an order of highest rank must contain for some x not equal to 0 the matrix $\begin{Vmatrix} 1 & x & 0 & 0 \\ 0 & 1 & & \\ 0 & & \ddots & \\ & & & 1 \end{Vmatrix}$ which is a unit of infinite order. The simple component must therefore be either a field or a division algebra. In the former case,

by Dirichlet's theorem on units in algebraic fields, the unique maximal order has a finite unit group only if the field is the field of rationals, or a quadratic imaginary extension of it[1]. In the case of a division algebra D, let k_1 be a maximal subfield of D, and C_1 its integer ring. An order of highest rank in D contains all elements of m C_1 for some integer m, and hence all units of C_1 of the form $1 + m X$, X in C_1. But if the unit group of C_1 is infinite, these latter units are also infinite in number. Thus if D satisfies our condition, C_1 must be an imaginary quadratic field, and therefore D a definite quaternion algebra[2].

Thus if a group ring R(G,C) has only trivial units, its group algebra R(G,k) must be the direct sum of fields isomorphic to the rational field or to quadratic imaginary fields, and definite quaternion algebras.

In the case in which there are no quaternion summands, G must be Abelian. By Theorem 2 if h is the maximum order of any element in G, and w a primitive h-th root of unity, R(G,k) has a summand isomorphic to k(W), and all its summands are isomorphic to subfields of k(w). Now w can be contained in a quadratic field only if h = 2,3,4 or 6. Taking these cases in turn, it is easy to see that the distinct possibilities are:-

---

(1) See Hilbert, op.cit. p.214.
(2) Cf. Albert, op.cit., Ch.5, § 10.

I. G is an Abelian group, and the orders of its elements all divide two; k is the rational field or a quadratic imaginary extension of it.

II. G is an Abelian group, and the orders of its elements all divide six; k is the rational field, or the field of the cube roots of unity.

III. G is an Abelian group, and the orders of its elements all divide four; k is the rational field, or the field of the fourth roots of unity.

If there are quaternion algebras among the direct summands of R(G,k), then we have the fourth possibility:-

IV. G is the direct product of a quaternion algebra and on Abelian group the orders of whose elements all divide two; k is the rational field.

For we have that G must be Hamiltonian. That is to say every subgroup of G must be self conjugate. For if x, y, in an algebra that is a direct sum of division algebras satisfy xy = 0, they must also satisfy yx = 0. Take, then $x = a_1(1-a_2)$, $y = 1 + a_2 + \dots + a_2^{m-1}$, where a_2 is an element in G of order m. We have

$$(1 + a_2 + \dots + a_2^{m-1})\, a_1 (1 - a_2) = 0,$$

$$a_1 + a_2 a_1 + \dots + a_2^{m-1} a_1 = a_1 a_2 + a_2 a_1 a_2 + \dots + a_2^{m-1} a_1 a_2 .$$

For some value of r, therefore, $a_2^r a_1 = a_1 a_2$, $a_1 a_2 a_1^{-1} = a_2^r$ so that $\{a_2\}$ is self-conjugate, and G is Hamiltonian, as required. Now a Hamiltonian group must be a direct product of a group of the kind defined in IV, by an Abelian group of odd order[1]. However, if this latter group is not the identity alone, the simple components of R(G,k) will include a quaternion algebra over a field k(w), w a root of unity other than ± 1, which is excluded. By the same reasoning, the coefficient field must be the field of rationals. Conversely, the group algebra R(G,k), G and k as under IV, is a direct sum of fields isomorphic to the rational field, and ordinary quaternion algebras. Its maximal orders of highest rank have therefore finite unit groups. We have therefore:-

Theorem 8. The group ring R(G,C) of a finite group G over a ring of algebraic integers C has only trivial units if and only if G and k, the quotient field of C, have one of the forms I, II, III, IV, listed above.

It is easy to generalise Theorem 8 to the case of a group ring R(G,C) in which G is no longer a group of finite order, but is a group all of whose elements have finite order. Firstly if G,k, are of any of the forms I, II, III, IV, then R(G,C) cannot have non-trivial units. For if $E = a_1 g_1 + \cdots + a_r g_r$

---

(1) See, for instance, H. Hilton, Finite Groups, p.178.

were such a unit, $g_1,\ldots,g_r$ would generate a finite subgroup G^* of the form I, II, III or IV, and E would be a unit in $R(G^*,C)$ contrary to Theorem 8. Secondly, let G be a group whose group ring R(G,C) has only trivial units. Then we may show directly that in R(G,C), xy = 0 implies yx = 0. For we have $(1 - 3yx)(1 + 3yx) = 0$, and $1 + 3yx$ cannot be a trivial unit unless yx = 0. It follows as above that G is either Abelian or Hamiltonian; and as it must not contain a finite subgroup not of the form I, II, III or IV, it itself must be of one of those forms.

Theorem 9. The statement of Theorem 8 remains true if for the words "a finite group G" we substitute "a group G all of whose elements have finite order."

5. Units of Finite Order in Integral Group Rings

We are concerned in this section with units of finite order in the integral group ring R(G,C) of a finite group G over a ring C of algebraic integers. The theorems that we prove are all partial cases of the plausible theorem:- A group of units of finite order in R(G,C) is isomorphic to a group of trivial units. It is convenient to treat only normalised units - that is, units in which the sum of the coefficients is equal to 1. Any unit is the product of a normalised unit and a unit in C, and any unit of finite order is the product of a normalised unit of finite order and a root of unity. The trivial normalised units, are of course simply the elements of G.

Our starting point is in all cases the Lemma used in the proof of Theorem 6 in the last section, which for convenience of reference we repeat as a Theorem.

Theorem 10 The coefficient of the identity of G in a non-trivial unit of finite order in G is zero.

Two results can be proved immediately from this theorem concerning the order of a group of normalised units of finite order in R(G,C), one quantitative and the other qualitative.

Theorem 11 The elements of a group of normalised units of finite order in R(G,C) are linearly independent. The order of such a group is at most equal to the order of G.

Let $E_0 = 1, E_1, \ldots, E_k$, be the elements of a group of normalised units of finite order in R(G,C), and suppose that

$$\lambda_0 E_0 + \lambda_1 E_1 + \cdots + \lambda_k E_k = 0$$

The coefficient of 1 in E_i, $i \neq 0$, is zero, by Theorem 10, unless E_i is trivial, in which case it is obviously zero. Thus we must have $\lambda_0 = 0$. Applying the same procedure after multiplying through by E_i^{-1} gives $\lambda_i = 0$, $i = 1, \ldots k$, so that the elements of the group are linearly independent, as required. The second half of the theorem is then obvious, as there cannot be more than n linearly independent elements in R(G,C) if n is the order of G. Theorem 6 is, of course, a particular case of Theorem 11.

The same argument shows that the elements of the group of normalised units remain linearly independent modules any ideal λ in C. If, in particular,

$$\lambda_0 E_0 + \lambda_1 E_1 + \cdots + \lambda_k E_k = mP$$

where P is in R(G,C) then each of $\lambda_0, \ldots, \lambda_k$ is divisible by m, so that P is expressible as a linear form in $E_0, \ldots, E_k$ with integral coefficients. That is to say:-

Corollary. If a linear form in the elements of a group of normalised units of finite order in R(G,C) expresses an element of R(G,C), its coefficients are integers.

Next let us proceed to our qualitative theorem concerning the order of a group of normalised units.

Theorem 12. The prime factors of the order of a group of normalised units of finite order in R(G,C) divide the order of G.

Let E be a normalised unit of prime order p in R(G,C). Then Theorem 12 will follow if we can shew that p divides n, the order of G. We may assume E to be non-trivial. Let $\bar{E}$ be the matrix representing E in the regular representation of G. Its trace, by Theorem 10, is zero. If $w_1,\ldots,w_n$ are its characteristic roots, therefore, we have

$$w_1 + w_2 + \cdots + w_n = 0 .$$

Each of $w_1,\ldots,w_n$ is a p-th root of unity; and therefore a power w^k of the primitive p-th root w. We have therefore $w_i \equiv 1$ modulo λ, the ideal (1-w). Therefore

$$n \equiv w_1 + w_2 + \cdots + w_n = 0 \mod \lambda .$$

But $\lambda^{p-1} = p$; so that $n^{p-1} \equiv 0\ (p)$, or p divides n, as required.

This theorem is essentially dependent on the fact that our coefficient ring C is a ring of integers, but it is independent of the field k out of which they chosen, - C may indeed be taken to be the ring of all algebraic integers. The theorem is therefore in direct contrast to the restrictions on the orders of elements in R(G,k) obtainable from the

fact that such elements must satisfy an equation with coefficients in k, and degree less than n. These latter restrictions are much less closely bound up with the nature of the group than are those on units of finite order in R(G,C). For instance, in the group ring of the quaternion group, of order 8, generated by x, y, z, subject to the relations $x^2 = y^2 = z^2 = xyz$, we have the unit of order 3,

$$1 - \tfrac{1}{4}(1-xyz)(3+x+y+z).$$

It is a corollary of Theorem 10, that if the coefficient of an element of the centrum of G in a unit of finite order in R(G,C) is not zero, then the unit is trivial. In particular, if G is Abelian, the units of finite order in R(G,C) are all trivial. It might be supposed that in any integral group ring a unit of finite order is conjugate to a trivial unit, but this is not so. Consider, for instance, the non-Abelian group of order 6, generated by elements x, y, subject to the relations $x^3 = y^2 = (xy)^2 = 1$. We can show by direct multiplication that if

$$A(k) = y + k(x - x^2)(1+y),$$

then for all integral values of k, $[A(k)]^2 = 1$. But A(k) is not conjugate to a trivial unit unless k is even. For under the representation of G:-

$$x \to \begin{Vmatrix} 1 & -3 \\ 1 & -2 \end{Vmatrix}, \quad y \to \begin{Vmatrix} 1 & 0 \\ 1 & -1 \end{Vmatrix}; \quad \left(\text{whence, } xy \to \begin{Vmatrix} -2 & 3 \\ -1 & 2 \end{Vmatrix}, x^2y \to \begin{Vmatrix} 1 & -3 \\ 0 & -1 \end{Vmatrix}\right),$$

we have

$$A(k) \to \begin{Vmatrix} 1 & 0 \\ k+1 & -1 \end{Vmatrix}.$$

Now if k is odd, this matrix is of the form 1 + 2 X, where X is a matrix with integral elements. However the matrices representing the trivial units of order two, - y, xy, and x^2y, - are not of this form; so that A(k) cannot be conjugate to one of them.

The remainder of this section is concerned with theorems probable under special assumptions concerning the nature of the group G.

Theorem 13. If the group G is soluble and of order n, then the order of any normalised unit of finite order in R(G,C) divides n.

We require first two lemmas on matrices whose elements are algebraic integers.

Lemma 1. The algebraic integers $p_1, p_2, \ldots, p_n$, form the first row of a matrix whose elements are algebraic integers and whose determinant is unity, if and only if the ideal $(p_1, p_2, \ldots, p_n)$ is the unit ideal (1), it being supposed that $n > 1$.

The necessity of the condition is obvious. The sufficiency can be proved by induction on n, as it is plainly true for n = 2.

Every ideal with a finite basis in the ring C, of all algebraic integers, is a principal ideal. For the elements $\alpha_1, \ldots \alpha_r$, of the basis determine a finite extension of the

rational field. In this field some power, say I^s, of the ideal I having $(\alpha_1, \ldots, \alpha_r)$ as basis is a principal ideal (β)[1]. In any field containing $\beta^{\frac{1}{s}}$, and in particular in C, the ideal having $\alpha_1, \ldots, \alpha_r$ as basis is therefore the principal ideal $(\beta^{\frac{1}{s}})$. In particular, the ideal $(p_1, \ldots, p_{n-1})$ is a principal ideal, say (q), and therefore $p_i = q\, p_i^1$, $i = 1, \ldots, n-1$, where p_i^1 is an integer, and $(p_1^1, \ldots, p_{n-1}^1)$ is (1). By the hypothesis of the induction we can find a matrix $\left\| \begin{matrix} p_1^1, \ldots, p_{n-1}^1 \\ X \end{matrix} \right\|$ with integral elements and determinant unity. Now $(p_1, \ldots, p_{n-1}, p_n) = (q, p_n) = (1)$, so that we can find integers ρ, σ, such that $\rho q + \sigma p_n = 1$. Then the matrix $\left\| \begin{matrix} p_1, \ldots, p_{n-1}, p_n \\ X \\ \sigma p_1^1, \ldots, \sigma p_{n-1}^1, \rho \end{matrix} \right\|$ has integral elements and determinant unity as required.

Lemma 2. If X is a matrix whose elements are algebraic integers, we can find a matrix Y of determinant unity and with integer elements, such that the elements of the transform $Y^{-1} X Y$ below the main diagonal are all zero.

Let Θ be a characteristic root of X, and let $v = (p_1, \ldots, p_r)$ be a vector such that $Xv = \Theta v$ where of course r is the index of the matrix X. We may without loss of generality suppose that $p_1, \ldots, p_r$ are integers, and that the ideal they generate is the unit ideal. For it would in any event be a

---

(1) See Hilbert, loc.cit., p.224.

principal ideal (q), and we could divide through by q. By the previous lemma, then, we can find a matrix Y_1 with integral elements and of determinant unity such that $Y_1 e_1 = v$, where e_1 is the first unit vector, $(1, 0, \ldots, 0)$. Then we have $Y_1^{-1} X Y_1 . e_1 = \theta e_1$ so that $Y_1^{-1} X Y_1$ has the form $\left\| \begin{matrix} \theta & * & \cdots & * \\ 0 & & & \\ \vdots & & X^1 & \\ 0 & & & \end{matrix} \right\|$. Repeating the process for the matrix X^1, we eventually arrive at the desired transform.

We now prove our main theorem. Since every unit of finite order in the group ring of an Abelian group is trivial, we can proceed by induction on the order of G. Since G is soluble, it possesses an Abelian self-conjugate subgroup H of prime power order, p^α. Then the factor group G/H is soluble and its order m is less than the order $p^\alpha m = n$ of G. By the hypothesis of the induction therefore, the theorem is true of G/H. If E is a normalised unit of finite order in R(G,C), its image $\bar{E}$ in the natural homomorphism of R(G,C) on R(G/H,C) will be a normalised unit of finite order in R(G/H,C) and therefore $\bar{E}^m = 1$. Therefore

$$(1) \qquad E_0 = E^m = 1 + \sum_i F_i (h_i - 1), \quad h_i \text{ in } H.$$

It suffices therefore to show that a unit of this form has an order dividing p^α. And for that it suffices in turn, to show that the image of E_0 in any irreducible representation of G has an order dividing p^α.

Let Γ, then, be an irreducible representation of G. We can suppose that the elements of H are represented by diagonal matrices, and at the same time that all the elements of G are represented by matrices whose elements are integers[1]. For, let $\Gamma_1,\ldots,\Gamma_r$ be the distinct irreducible components of Γ considered as a representation of H; let X be the vector space in which the matrices of $\Gamma(G)$ operate; and let X_α, $\alpha = 1,\ldots,r$, be the subspaces of X in which $\Gamma(h)$, for all elements h in H, acts as a multiplier by the scalar $\Gamma_\alpha(h)$. Then any matrix of $\Gamma(G)$ permutes the subspaces $X_1,\ldots,X_r$. For if v is in X_α, g in G, then for any element h in H,

$$\Gamma(h)\cdot\Gamma(g)\,v = \Gamma(g)\cdot\Gamma(g^{-1}hg)\,v = \Gamma(g)\cdot\Gamma_\alpha(g^{-1}hg)\,v, \text{ since } g^{-1}hg \text{ is in H}$$
$$= \Gamma_\beta(h)\cdot\Gamma(g)\,v, \text{ for some value of } \beta,$$

so that $\Gamma(g).v$ is in X_β. Since Γ is irreducible, the permutation group so formed must be transitive. Hence $X_1,\ldots X_r$ must all have the same rank, say m. Now let G_0 be the maximal subgroup of G such that $\Gamma(G_0)$ leaves X_1 invariant, and choose a basis $x_1,\ldots,x_m$ of X_1 so that the matrices of the representation of G_0 induced by Γ in X_1 have integral elements. Furthermore, for $\alpha = 2,\ldots,r$, let g_α be an element of G such that $\Gamma(g_\alpha)\,X_1 = X_\alpha$, and ~~that~~ choose $\Gamma(g_\alpha)\,x_1,\ldots,\Gamma(g_\alpha)\,x_m$ as a basis $x_{m(\alpha-1)+1},\ldots,x_{m(\alpha-1)+m}$ of X_α. Uniting these bases into a

(1) Cf. Speiser, op.cit., ch. 13, § 51.

basis of the whole space X, we find that Γ has the desired form.

Then, if $\Gamma(E_0) = E_0^*$ we have by (1)

$$(2) \qquad E_0^* = 1 + \sum_i X_i (H_i - 1),$$

where X_i represent matrices with integral elements, H_i matrices of the form $\left\| \begin{matrix} w_1 & & 0 \\ & \ddots & \\ 0 & & w_s \end{matrix} \right\|$. If p^β is the maximum order of any element in H, we have $\beta \leq \alpha$ and w_j in H_i is a p^β-th root of unity. Let w be a primitive p^β-th rooth of unity. Then (2) can be written

$$(3) \qquad E_0^* = 1 + (w-1) X_0, \text{ where } X_0 \text{ is a matrix with integer elements.}$$

But by lemma 2, we can find a matrix Y such that both Y and Y^{-1} have integral elements, and the elements below the main diagonal in $Y^{-1} E_0^* Y$ are zero. Then the elements in the main diagonal of $Y^{-1} E_0^* Y$ will be the characteristic roots $\theta_1, \ldots, \theta_s$ of E_0^*. But by (3)

$$Y^{-1} E_0^* Y = 1 + Y^{-1} X_0 Y \cdot (w-1),$$

so that, if λ denotes the ideal (w-1),

$$(4) \qquad \theta_\rho - 1 \equiv 0 \quad (\lambda), \qquad \rho = 1, \ldots, s.$$

Since E_0 is a unit of finite order, θ_ρ is a root of unity, say of order q_ρ, and the order of E_0^* is the least common multiple of $q_1, \ldots, q_s$. Now $(\lambda)^\pi = (p)$ where $\pi = p^{\beta-1}(p-1)$ (1).

---

(1) Hilbert, op.cit., p.331.

But if q_ρ were divisible by two primes, $\theta_\rho - 1$ would be a unit, making (4) impossible. If on the other hand $q_\rho = t^\gamma$ where t is a prime, then the ideal $(\theta_\rho - 1)$, raised to the power $\tau = t^{\gamma-1}(t-1)$, is equal to t. Raising (4) to the power $\pi\tau$, we obtain

$$t^\pi \equiv 0 \quad (p^\tau),$$

whence $t = p$, $\pi \geqslant \tau$, or $\beta \geqslant \gamma$. That is to say, the order of θ_ρ for $\rho = 1, \ldots, s$ divides p^β as required.

We have, actually, proved more than is stated in the theorem, namely:-

Corollary. If G is a soluble group; $G = G_1 \supset G_2 \supset \cdots \supset G_r = E$ any series of self conjugate subgroups of G such that G_i / G_{i+1} is Abelian; and n_i is the maximum order of any element in G_i / G_{i+1}; then the order of a normalised unit of finite order in R(G,C) divides $n_1 n_2 \ldots n_{r-1}$.

We stated at the beginning of this section that our Theorem were all partial cases of the statement that "A group of units of finite order in R(G,C) is isomorphic to a group of trivial units." We shall only succeed in proving this statement for the particular case in which G is a group of prime-power order whose second derived group is the identity, or a direct product of such groups. These groups have the property that their upper central series terminates in the

whole group G.[1] The upper central series $Z_0, Z_1, \ldots$ is defined by (i) Z_0 consists of the identity alone, (ii) ~~$Z_{i+1} \; X_i$~~ Z_{i+1}/Z_i is the centrum of G/Z_i.

The theorem is proved by the use of rather different methods from those used in proving the previous theorem. We define, in the group ring R(G,C) of any group G, the two-sided ideal λ_H, where H is any self-conjugate subgroup of G, as that generated by the elements $(h-1)$ for all h in H. This ideal consists of all elements in R(G,C) whose image in the natural homomorphism of R(G,C) on R(G/H,C) is zero. Let us observe that according to our definition a unit is normalised if it is congruent to 1 modulo λ_G. We prove first two lemmas concerning these ideals.

Lemma 1. If $x_1, \ldots, x_r$, of orders $n_1, \ldots, n_r$ are a basis of the Abelian group G, then

$$X = \mu_1(x_1-1) + \mu_2(x_2-1) + \cdots + \mu_r(x_r-1) \equiv 0 \quad (\lambda_G^2) \qquad (\mu_\alpha \text{ integers})$$

if and only if μ_α is divisible by n_α, $\alpha = 1, \ldots, r$.

We have

$$n_\alpha(x_\alpha - 1) \equiv (1 + x_\alpha + \cdots + x_\alpha^{n_\alpha - 1})(x_\alpha - 1) \equiv 0 \quad (\lambda_G^2),$$

so that the condition is sufficient.

Suppose on the other hand that $X \equiv 0 \; (\lambda_G^2)$. X must then be expressible in the form

$$X = \varphi_{11}(x_1-1)^2 + \varphi_{12}(x_1-1)(x_2-1) + \cdots + \varphi_{rr}(x_r-1)^2.$$

---

(1) W. Burnside, Theory of Groups (2nd Edition), ch. VIII, § 93.

Setting $x_2 = \ldots = x_3 = 1$ gives a homomorphism of G on to the cyclic group $\{x_1\}$ of order n_1, and the above relation must of course remain true under it. That is to say

$$\mu_1 (x_1 - 1) = \varphi_{11}' (x_1 - 1)^2,$$

or $$(\mu_1 - \varphi_{11} (x_1 - 1))(x_1 - 1) = 0.$$

However, in the group ring of the cyclic group $\{X_1\}$, $\psi (x_1 - 1) = 0$ only if $\psi = m(1 + x_1 + \ldots + x_1^{n_1 - 1})$. Therefore

$$\mu_1 - \varphi_{11}' (x_1 - 1) = m(1 + x_1 + \ldots + x_1^{n_1 - 1});$$

whence, setting $x_1 = 1$, $\mu_1 = mn_1$, as required.

Lemma 2. If φ is an element of R(H,C), where H is a self-conjugate subgroup of G, then $\varphi \equiv 0 \ (\lambda_G \lambda_H)$ if and only if $\varphi \equiv 0 \ (\lambda_H^2)$.

If $\varphi \equiv 0 \ (\lambda_H^2)$ then obviously $\varphi \equiv 0 \ (\lambda_G \lambda_H)$. Suppose conversely, that

$$(1) \qquad \varphi = \sum_{r,s} \psi_{rs} (g_r - 1)(h_s - 1), \quad g_r \text{ in } G, \ h_s \text{ in } H.$$

Let $\bar{g}_0, \bar{g}_1, \bar{g}_2, \ldots$ be a set of right hand residue class representatives module H, where $\bar{g}_0 = 1$. Then we may set

$$(2) \qquad \sum_r \psi_{rs} (g_r - 1) = \sum_t \bar{g}_t \theta_{ts}, \quad \theta_{ts} \text{ in } R(H, C).$$

Substituting in (1), and comparing the coefficients of $\bar{g}_0, \bar{g}_1, \ldots$ on the right and left, we have

$$\varphi = \sum_s \theta_{0s}(h_s - 1),$$
$$0 = \sum_s \theta_{ts}(h_s - 1), \quad t \neq 0;$$

so that

$$(3) \qquad \varphi = \sum_{s,t} \theta_{ts}(h_s - 1).$$

Now $\sum_t \theta_{ts} \equiv \sum_t \bar{g}_t \theta_{ts} \mod \lambda_G$,

$\equiv 0 \mod \lambda_G$ by (2).

But $\sum_t \theta_{ts}$ is in R(H,C), so that this entails $\sum_t \theta_{ts} \equiv 0 \mod \lambda_H$. By (3), then we have $\varphi \equiv 0 (\lambda_H^2)$ as required.

It should be noticed that multiplication of the ideals λ_H is not in general commutative and we cannot deduce from Lemma 2 that if $\varphi \equiv 0$ modulo $(\lambda_G\lambda_H, \lambda_H\lambda_G)$ then $\varphi \equiv 0 (\lambda_H^2)$. For, by lemma 1, we have that if G is Abelian, an element g of G is congruent to 1 modulo λ_G^2 only if it is equal to 1, (for it is easy to see that $x_1^{a_1} x_2^{a_2} \dots x_r^{a_r} \equiv 1 + a_1(x_1 - 1) + \dots + a_r(x_r - 1), (\lambda_G^2)$). Thus in general $g \equiv 1 \mod \lambda_G^2$ if g is an element of the derived group G'. By Lemma 2 then, $g \equiv 1 \mod \lambda_G\lambda_H$ only if g is in H'. But any element $ghg^{-1}h^{-1}$ of the commutator group (G,H) = F of G and H is congruent to 1 modulo $(\lambda_G\lambda_H, \lambda_H\lambda_G)$. We have, in fact,

$$ghg^{-1}h^{-1} - 1 = gh[(g^{-1}-1)(h^{-1}-1) - (h^{-1}-1)(g^{-1}-1)].$$

Conversely, if $g \equiv 1 \mod (\lambda_G\lambda_H, \lambda_H\lambda_G)$ then

g is in F = (G,H). For H/F is in the centrum of G/F, and therefore $\lambda_{G/F}\lambda_{H/F} = \lambda_{H/F}\lambda_{G/F}$ in R(G/F, C); so that g F ≡ 1 module $\lambda_{G/F}\lambda_{H/F}$, and therefore g is in F. Summing up:-

Corollary to Lemmas 1 and 2. Let G be a group, H a self conjugate subgroup of G. Then if g is an element of G

(i) $g \equiv 1 \mod \lambda_G^2$ if and only if g is in G';

(ii) $g \equiv 1 \mod \lambda_G \lambda_H$ if and only if g is in H';

(iii) $g \equiv 1 \mod (\lambda_G \lambda_H, \lambda_H \lambda_G)$ if and only if g is in (G,H).

Now let us prove our main theorem.

Theorem 14. Let G be a group whose second derived group consists of the identity alone, and the c-th group of whose upper central series is the whole group G. Then a group of normalised units of finite order in R(G,C) is isomorphic to a subgroup of G.

By Theorem 11, a group of normalised units of finite order in R(G,C) is finite; it therefore suffices to prove theorem 14 in case the quotient field of C is a finite extension of the rational field.

Let E be a unit of finite order in R(G,C). The image of E in the natural homomorphism of R(G,C) on R(G/G',C) is a trivial unit in the latter group ring, since G/G' is Abelian. If furthermore E is normalised, then this image is an element of G/G'. Let g_1 be any element of this

residue class module G'. We have then

$$E = g_1 + \sum_{i=1}^{r} \varphi_i (h_i - 1) ;$$

where $h_1, \ldots, h_r$, of orders $n_1, \ldots, n_r$, are a basis of the Abelian group G'. If the sum of the coefficients of the elements in φ_i is ρ_i then $\varphi_i \equiv \rho_i \mod \lambda_G$, and therefore

$$(5) \qquad E \equiv g_1 + \sum_{i=1}^{r} \rho_i (h_i - 1) \mod \lambda_G \lambda_{G'}.$$

Let us for the sake of clarity first suppose that we are dealing with the ring of rational integers as coefficient ring C, and treat the general case afterwards. Then from equation (5) we have,

$$E \equiv g_1 + \sum_{i=1}^{r} \rho_i (h_i - 1) \mod \lambda_G \lambda_{G'}$$

$$\equiv g_1 + \sum_{i=1}^{r} (1 + h_i + \cdots + h_i^{\rho_i - 1})(h_i - 1) \mod \lambda_G \lambda_{G'},$$

$$\equiv g_1 + \sum_{i} g_i h_1^{\rho_1} \cdots h_{i-1}^{\rho_{i-1}} (h_i^{\rho_i} - 1) \mod \lambda_G \lambda_{G'},$$

$$\equiv g_1 h_1^{\rho_1} \cdots h_r^{\rho_r} \mod \lambda_G \lambda_{G'}.$$

That is to say, every normalised unit E of finite order in R(G,C) satisfies a congruence

$$(6) \qquad E \equiv g \mod \lambda_G \lambda_{G'}$$

This congruence determines g uniquely. For by the corollary to Lemmas 1 and 2, $g \equiv g' \mod \lambda_G \lambda_{G'}$ implies that gg'^{-1} is in the derived group of G', - that is to say, is the identity.

Moreover, if we have also $E_1 \equiv g_1 \mod \lambda_G \lambda_{G'}$, then $EE_1 \equiv g g_1 \mod \lambda_G \lambda_{G'}$, so that the correspondence $E \to g$ provides a homomorphism of any group of normalised units of finite order on a subgroup of G. To show that it is an isomorphism, we must show that if

$$E \equiv 1 \mod \lambda_G \lambda_{G'}, \tag{7}$$

and E is a unit of finite order, then E = 1. By hypothesis G has the upper central series $Z_0 = 1, Z_1, \ldots, Z_c = G$. We proceed by induction on c; as if c = 1, G' consists of the identity alone, $\lambda_{G'}$ is the ideal (0), and the assertion is therefore trivial. Assume then that the assertion is true of the factor group G/Z_1. Let $\bar{E}$ be the unit of $R(G/Z_1, C)$ corresponding to E. Then (7) implies

$$\bar{E} \equiv 1 \mod \lambda_{G/Z_1} \lambda_{(G/Z_1)'}$$

and so by hypothesis $\bar{E} = 1$, or $E \equiv 1 \mod \lambda_{Z_1}$. It follows that the sum of the coefficients of elements of Z_1 in E is 1, so that not all of these coefficients are zero. Since Z is the centrum of G, it follows from Theorem 10 that E is trivial, say E = z. But we have already shown that (6) determines g uniquely, and therefore by (7), z = 1. Thus Theorem 14 is true if C is the ring of rational integers.

If C is not the ring of rational integers we cannot of course pass as above from equation (5) to equation (6).

However, we can choose a basis $w_0 = 1, w_1, \ldots, w_s$ of C, - that is, a set of integers $w_0, \ldots w_s$ such that every integer in C can be written uniquely in the form $a_0 w_1 + a_1 w_1 + \cdots + a_s w_s$ where $a_0, \ldots a_s$ are rational integers[1]. Let, in particular, ρ_i in (5) be equal to $\sum_{\nu=0}^{s} \rho_{\alpha i} w_\alpha$. Then by a similar process to that which led to (6), we can shew that there exists an element g in G such that

$$(6a) \qquad E \equiv g + \sum_{\alpha=1}^{s} \sum_{i=1}^{r} \rho_{\alpha i}\, \omega_\alpha (L_i - 1) \mod \lambda_G \lambda_{G'}$$

where $\rho_{\alpha i}$, $\alpha = 1, \ldots, s$, $i = 1, \ldots, r$, are rational integers. This congruence is equivalent to the assertion that if

$$(8) \qquad E = E_0 + E_1 w_1 + \cdots + E_s w_s,$$

where E_α, $\alpha = 0, \ldots, s$, are in $R(G, C_0)$, C_0 the ring of rational integers, then

$$(9) \qquad E_0 \equiv g \mod \lambda_G \lambda_{G'}, \quad E_\alpha \equiv 0 \mod \lambda_{G'}, \ \alpha \neq 0.$$

Now (8) determines the components $E_0, E_1, \ldots, E_s$ uniquely, since $1, w_1, \ldots, w_s$, form a basis for C. It therefore follows as before by the corollary to Lemmas 1 and 2, that (9) determines g uniquely. Moreover, if F is also a normalised unit of finite order, and

$$F = F_0 + F_1 w + \cdots + F_s w_s,$$

---

(1) Hilbert, op.cit., p.180.

where $F_0 \equiv g_1 \mod \lambda_G \lambda_{G'}, \quad F_\alpha \equiv 0 \mod \lambda_G, \alpha \neq 0.$

then we have $EF = (EF)_0 + (EF)_1 w_1 + \cdots + (EF)_s w_s$ where

$$(EF)_0 = E_0 F_0 + \sum_{\alpha,\beta=1}^{s} k_{\alpha\beta} E_\alpha F_\beta, \qquad k_{\alpha\beta} \text{ rational integers,}$$

$$\equiv g g_1 \mod \lambda_G \lambda_{G'}.$$

Thus the correspondence $E \to g$, where g is determined by (8) and (9), is a homomorphism of any group of normalised units of finite order of R(G,C) on a subgroup of G. We must finally show that it is an isomorphism by proving that if E is a normalised unit of finite order such that (8) holds and $E_0 \equiv 1 \mod \lambda_G \lambda_{G'}$, then $E = 1$. We prove this by induction precisely as in the case where the coefficient ring was the ring of rational integers. The only point at which there are fresh complications is in proving the special case $C = 1$. Then however, G is Abelian and E is therefore trivial, and being normalised, is an element z of G. Therefore $E = E_0$, and since $\lambda_{G'}$ is the ideal (0), $E_0 = 1$.

This completes the proof of Theorem 14.

Now let H be any group of units of finite order in R(G,C). Let y be an element of H, and y_0 the normalised unit such that $y = w\, y_0$, w in C. Then $y \to y_0$ is a homomorphism of H on to a group of normalised units. If we suppose that the elements of H are linearly independent, then in particular H contains no roots of unity, and therefore this homomorphism is an isomorphism. Thus by Theorem 14

H is isomorphic to a subgroup of G. Applying this to the special case in which the elements of H are a basis for R(G,C) and therefore H has the same order as G, we obtain:-

1st Corollary to Theorem 14. If G satisfies the conditions laid down in Theorem 1 , then R(G,C) is not isomorphic to another group ring R(H,C) unless G is isomorphic to H.

Furthermore, by the corollary to Theorem 1 , we have that if H is of the same order as G, and R(H,C) has a group of normalised units isomorphic to G, then the elements of this group are a basis for R(H,C). Thus we have that R(H,C) is isomorphic in R(G,C) and therefore G to H. We may thus state a limited converse to Theorem 1 :-

2nd Corollary to Theorem 14. If G satisfies the conditions laid down in Theorem 1 , and H is of the same order as G, but not isomorphic to G, then R(H,C) does not contain a group of normalised units isomorphic to G.

6. An Example

In this section we consider the detailed application of the theorems of the last three sections to a particular group ring. We take one of the simplest groups not of prime power order, namely the group G generated by two elements a, b, subject to the relations:-

$$a^p = b^{p-1} = 1 ; \quad b^{-1} a b = a^r ;$$

where p is an odd prime, and r a primitive number module p, - that is to say, $r^i \equiv 1 \bmod p$ if and only if i is a multiple of p-1.

The order of G is p(p-1), for every element can be written uniquely in the form $a^\rho b^x$, $\rho = 0,\ldots,p-1$; $x = 0,\ldots p-2$. Moreover the number of classes of conjugate elements is p; for the elements $a^\rho b^x$, $a^\sigma b^y$ are conjugate if $x = y \neq 0$, or if $x = y = 0$, $\rho \neq 0$, $\sigma \neq 0$. That is to say, the elements in any residue class with respect to $\{a\}$ except $\{a\}$ itself form a class, while the elements of $\{a\}$ fall into two classes, one consisting of the identity alone, the other of all other elements in $\{a\}$. There are therefore p absolutely irreducible representations of G. Of these, p-1 are of degree 1, namely

$$(1) \qquad a \to 1 ; \quad b \to w_0^\varkappa ; \quad \varkappa = 0, 1, \ldots, p-2 ;$$

where w_0 is any primitive (p-1)-th root of unity. The remaining representation is therefore of degree p-1, since

$(p-1)^2 + (p-1)\cdot 1^2 = p(p-1)$, the order of G. It can be obtained by first representing G as a permutation group on the residue classes $\{b\}a^\rho$ with respect to $\{b\}$, according to the scheme:-

(2) g is represented by: $\{b\}a^\rho \to \{b\}a^\rho g$.

This permutation group is doubly transitive, and as a linear representation of G is therefore the sum of the identical representation and just one other irreducible representation,[1] - the representation of degree p-1 we desire. By this construction, the representation can be written rationally.

From this enumeration of the representations of G, the decomposition of $A = R(G,k)$ into simple components follows from Theorem 1. We shall, however, prefer to unite the components corresponding to representations of degree 1, into a single component. Or, what comes to the same thing, we shall treat the representations (1) as a single representation

(3) $a \to 1, \quad b \to \bar{b}$;

on to the group ring $R(G^*,k)$, where G^* is the cyclic group $\{\bar{b}\}$ of order p-1. The remaining simple component is a total matric algebra of index p-1 over k. We shall in fact have

$$A = A_1 + A_2; \quad A_1 = A\cdot\frac{1+a+\cdots+a^{p-1}}{p}, \quad A_2 = A\cdot\frac{p-1-a-\cdots-a^{p-1}}{p}.$$

Here A_1 is isomorphic to the group ring $R(G^*,k)$ and A_2 to the total matrix algebra of index p-1.

---

(1) Speiser, op.cit., ch.8, § 39.

An element of R(G,k) is, of course, determined uniquely by its components in A_1 and A_2. Let us seek to determine what conditions these components must satisfy if the element is to lie in R(G,C). Firstly it is clear from (3) that the first component must be an element in $R(G^*,C)$ and that conversely given any element in $R(G^*,C)$, it is the first component of an element in R(G,C). The condition imposed on the second components will clearly depend on the basis chosen for the total matric algebra A_2. We proceed therefore to show how that basis may most conveniently be chosen. Since A_2 is isomorphic to the algebra of matrices representing elements of R(G,k) in the irreducible representation of G of degree p-1, this is the same as choosing the most convenient form for that representation.

Observe firstly that by equation (4) of section 3, - with, in this case, $n = p(p-1)$ and $n_\rho = p-1$, - an element in R(G,k) with first component zero, and second component a matrix whose elements are integers divisible by p is in R(G,C), provided only that our representation has been chosen so that the matrices representing elements of G have integral elements. That is to say, what we have to consider is the form the representation takes module p. Now over the Galois field of order p, the group algebra of G ceases to be semi-simple. We have in fact $(a-1)^p \equiv a^p - 1 = 0 \mod p$; and since,

if g is any element in G, $g(a-1) = (a^s-1)g = (a-1).(a^{s-1}+\dots+a+1)g$, the ideal (a-1) is nilpotent. As a matter of fact it forms the radical of the group algebra, and therefore the quotient algebra with respect to the radical is isomorphic to the group algebra of a cyclic group of order $p-1$. It is, in particular, commutative, and any representation of G in the Galois field is therefore equivalent to a representation by matrices whose elements above the main diagonal are zero[1].

Let us proceed to verify all this explicitly. From the derivation of the representation from the representation as a permutation group on the residue classes $\{b\}a^\rho$, we obtain the following form, where we have set $\{b\}a^\alpha = x_\alpha$, and, to remove the identical representation, $x_0 = -x_1-x_2-\dots-x_{p-1}$:-

(4)
a is represented by: $x'_\alpha = x_{\alpha+1}$, $\alpha = 1, 2, \dots, p-2$;
$x'_{p-1} = -x_1 - x_2 - \dots - x_{p-1}$;

b is represented by: $x'_\alpha = x_{\tau\alpha}$, $\alpha = 1, 2, \dots, p-1$;

where $\overline{\tau\alpha} \equiv \tau\alpha \bmod p$, and $\overline{\tau\alpha} = 1,2,\dots$ or $p-1$. We may verify by evaluating the characters that the representation is indeed irreducible, for we have generally

$a^\rho b^\gamma$ is represented by: $x'_\alpha = x_{\frac{\tau\gamma(\rho+\alpha)}{}}$;

---

(1) Cf. B.L. van der Waerden, Moderne Algebra, vol. II, ch. XVII, § 121.

where x_0, if it occurs on the right hand side, is replaced by $-x_1 - x_2 - \ldots - x_{p-1}$. Consider the element

$$\sum_{\gamma=0}^{p-2} \left(a^{\tau^\gamma j - i} - a^{\tau^\gamma j}\right) b^{-\gamma}, \qquad (i, j = 1, \ldots, p-1),$$

of $R(G,C)$. Its first component, by (3), is zero. Its second component is the matrix of the transformation

$$x'_\alpha = \sum_{\gamma=0}^{p-2} \left(x_{\overline{\tau^{-\gamma}(\alpha+\tau^\gamma j - i)}} - x_{\overline{\tau^{-\gamma}(\alpha+\tau^\gamma j)}}\right)$$

$$= \sum_{k=1}^{p-1} \left(x_{\overline{k(\alpha-i)+j}} - x_{\overline{k\alpha+j}}\right).$$

Now if $\alpha \neq i$, then as k varies from 1 to $p-1$, then $k.\alpha$ and $k(\alpha-i)$ equally vary over all the non-zero residue classes mod p, and therefore $x'_\alpha = 0$. On the other hand

$$x'_i = \sum_{k=1}^{p-1} \left(x_j - x_{\overline{ki+j}}\right)$$

$$= p\,x_j - \sum_{\alpha=0}^{p-1} x_\alpha$$

which is equal to $p\,x_j$, when we have set $x_0 = -x_1 - x_2 \ldots - x_{p-1}$ on the right hand side. The matrix in question is therefore $p\,E_{ij}$, and, as we asserted above, an element of $R(G,k)$ whose first component is zero and whose second component is $p\,A_\cdot$, (A an integral matrix) is therefore in $R(G,C)$.

We now replace the basis $x_1, \ldots, x_{p-1}$ of the vector space by a new basis

$$(5) \qquad y_\alpha = \sum_{\beta=1}^{p-1} \binom{p-\beta}{\alpha} x_\beta, \qquad \alpha = 1, \ldots, p-1;$$

where $\binom{x}{\alpha}$ as usual represents the polynomial $\frac{x(x-1)\cdots(x-\alpha+1)}{1.2.\cdots.\alpha}$.

Since $\binom{p-\beta}{\alpha} = 0$ if $\beta > p-\alpha$, and $\binom{p-\beta}{\alpha} = 1$ if $\beta = p-\alpha$, (5) is a change of basis having an integral unimodular matrix. We wish to determine the form taken by the representation (4) with respect to this new basis. Firstly, a is represented by

$$y'_\alpha = \sum_{\beta=1}^{p-1} \binom{p-\beta}{\alpha} x'_\alpha$$

$$= \sum_{\beta=1}^{p-2} \binom{p-\beta}{\alpha} x_{\beta+1} - \binom{1}{\alpha}(x_1 + \cdots + x_{p-1})$$

$$= \sum_{\beta=1}^{p-1} \binom{p-\beta+1}{\alpha} x_\beta - \binom{p}{\alpha} x_1 - \binom{1}{\alpha}(x_1 + \cdots + x_{p-1}).$$

Now we have identically in x, $\binom{x}{\alpha} = \binom{x-1}{\alpha} + \binom{x-1}{\alpha-1}$ whence

$$y'_\alpha = \sum_{\beta=1}^{p-1} \binom{p-\beta}{\alpha} x_\beta + \sum_{\beta=1}^{p-1} \binom{p-\beta}{\alpha-1} x_\beta - \binom{p}{\alpha} x_1 - \binom{1}{\alpha}(x_1 + x_1 + \cdots + x_{p-1}).$$

Now $\binom{p}{\alpha} \equiv 0 \bmod p$; and if $\alpha > 1$, $\binom{1}{\alpha} = 0$; whereas if $\alpha = 1$, $\binom{p-\beta}{\alpha-1} = \binom{1}{\alpha} = 1$; thus:

(6a) a is represented by:

$$y'_1 \equiv y_1 \bmod p;$$

$$y'_\alpha \equiv y_\alpha + y_{\alpha-1} \bmod p, \quad \alpha = 2, \ldots, p-1.$$

As for the element b, this is represented by:-

$$y'_\alpha = \sum_{\beta=1}^{p-1} \binom{p-\beta}{\alpha} x'_\beta = \sum_{\beta=1}^{p-1} \binom{p-\beta}{\alpha} x_{\tau\beta};$$

whence $y'_\alpha \equiv \sum_{\beta=1}^{p-1} \binom{p-\tau^*\beta}{\alpha} x_\beta \pmod{p}$; where $\tau^*\tau \equiv 1 \pmod{p}$.

Now $\binom{p-\tau^*\beta}{\alpha}$ is a polynomial in β of degree α in β, and taking integral values for integral values of β. It is therefore equal to an expression of the form

$$f_0 + f_1\binom{p-\beta}{1} + f_2\binom{p-\beta}{2} + \cdots + f_\alpha\binom{p-\beta}{\alpha},$$

where, since $\binom{p-\tau^*\beta}{\alpha}$ is divisible for p if $\beta = p$, f_0 is divisible by p. Also, comparing the coefficient of the leading term, $f_\alpha = \tau^{*\alpha}$. Thus

(6b) b is represented by $y'_\alpha \equiv f_1 y_1 + f_2 y_2 + \cdots + f_{\alpha-1} y_{\alpha-1} + \tau^{*\alpha} f_\alpha \pmod{p}$.

In short, the basis of the algebra A_2 of second components can be so chosen that, modulo p, the second components of a and b take the forms

$$\begin{Vmatrix} 1 & 0 & & \\ 1 & 1 & \ddots & 0 \\ & \ddots & \ddots & 1 \\ 0 & & 1 & 1 \end{Vmatrix} \quad \text{and} \quad \begin{Vmatrix} \tau^* & 0 & & \\ * & \tau^{*2} & \ddots & 0 \\ & \ddots & \ddots & 0 \\ * & & * & \tau^{*p-1} \end{Vmatrix} \quad \text{respectively.}$$

It now follows readily that if the matrix X is the second component of an element in R(G,C) its elements above the main diagonal are zero modulo p. If, moreover the first component of the same element of R(G,C) is zero, then the element is of the form (a-1)x, x in R(G,C), and therefore the elements of X in the main diagonal are zero modulo p. Conversely, if an element of R(G,k) has first component zero

and second component a matrix with integer elements, those in and above the main diagonal being zero modulo p, then it is in R(G,C). We have already proved this if all the elements of the second component are zero modulo p; it suffices therefore to show that we can construct an element of R(G,C) having first component zero, and second component of the form above, the residue classes modulo p of the elements below the main diagonal being preassigned arbitrarily. But the elements $1, b, \ldots, b^{p-2}$ have second components whose main diagonals are, in some order $(s, s^2, \ldots, s^{p-1})$ for $s = 1, 2, \ldots, p-1$, modulo p. These are linearly independent modulo p, and therefore we can find an element of R(G,C) the elements of the main diagonal of whose second component fall into arbitrarily preassigned residue classed modulo p. By multiplication by $(a-1)^i$, $i = 1, \ldots, p-2$ we obtain elements of R(G,C) whose first component is zero, and whose second component has in its main diagonal and its first (i-1) subdiagonals, elements congruent to zero modulo p, but in the i-th subdiagonal elements of arbitrary residue classes modulo p. Our required construction is now obvious. To sum up:-

The group algebra R(G,k) is the direct sum of A_1, isomorphic to the group algebra $R(G_1^*, k)$ of a cyclic group $\{G^*\}$ or order p-1, and A_2, a total matric algebra of index $p-1$ over k. An element of R(G,k) is in R(G,C) if and only if

its component in A_1 is $\varphi(b^*)$ in $R(G^*, C)$, and its component in A_2 is a matrix with integer elements, those above the main diagonal being congruent to zero, those in it to $\varphi(r^*)$, $\varphi(r^{*2})$, ..., $\varphi(r^{*p-1})$ respectively modulo p; provided that the basis of A_2 is conveniently chosen.

What then can be said of the units in R(G,C) ? The first component of such a unit is, of course, a unit in $R(G^*, C)$, the second a unimodular matrix. We have then obviously:-

The group U of units in R(G,C) has a self-conjugate subgroup U_0 consisting of all units whose component in A_1 is 1. U_0 is isomorphic to the group of all matrices with determinant unity and elements in C, those above the main diagonal being congruent to zero and those in it to unity modulo p. The factor group U/U_0 is isomorphic to the unit group of $R(G^*, C)$.

What, in particular, can be said about a normalised unit of finite order ? The first component of such a unit is a normalised unit of finite order in $R(G^*, C)$ - that is, since G^* is Abelian, an element of G^*. Consider first a unit whose first component is 1. Its second component takes, modulo p, the form $\left\| \begin{matrix} 1 & & 0 \\ \mu & 1 & \\ & \ddots & \\ * & \cdots & 1 \end{matrix} \right\|$, for some value of μ. Its characteristic function is therefore of the form:-

$$(x-1)^{p-1} + \lambda_1 p (x-1)^{p-2} + \cdots + \lambda_{p-2} p (x-1) + (\mu + \lambda_{p-1} p) \cdot p .$$

A characteristic root w is therefore a root of unity satisfying the congruence $(w-1)^{p-1} \equiv 0 \mod p$, and as we showed in the proof of Theorem 13 in Section 5, w is therefore a p-th root of unity. If we add the hypothesis that $\mu \equiv 0 \mod p$, we obtain

$$(w-1)^{p-1} \equiv 0 \mod (p^2, p(w-1)),$$

this is clearly false if w is a primitive p-th root of unity. It follows that w = 1; and as this is true of all the characteristic roots of our matrix, which by hypothesis has finite order, the unit we are dealing with must be unity.

Next, let u be a unit whose first component is b^{*e} where $ef = p-1, f>1$. Its second component has the form $\left\| \begin{matrix} r^{*e} & & 0 \\ \mu & r^{*2e} & \\ & & \ddots \\ * & & r^{*(f-1)e} \end{matrix} \right\|$ modulo p, for some value of μ. Raising u to the power f, we obtain a unit whose first component is 1. Its second component, it may be verified, has a first principal minor $\left\| \begin{matrix} 1 & 0 \\ \varphi_f & \mu \end{matrix} \right\|$ modulo p, where $\varphi_f = r^{*e(f-1)}\left(1 + r_1^{*e} + \dots + r_{f-1}^{*e(f-1)}\right)$. Now $r^{*e} \not\equiv 1 \mod p$; but $r^{*ef} \equiv 1 \mod p$; therefore $\varphi_f \equiv 0 \mod p$. It follows from the previous paragraph that so that u is of order f.

Now, let U be a group of normalised units of finite order in R(G,C), U_0 its subgroup of elements with first component 1. By Theorem 12, the order of U_0 is not greater than $p^{(p-1)}$, and since all its elements have order p, U_0, if it does not consist of the identity alone, is a cyclic group

of order p. Let the group of first components of elements of U be generated by b^{*e}, where $ef = p-1$, as above. Let a_1 generate U_0, and let b_1 be an element of U having first component b^{*e}. We have seen already that

$$a_1^p = b_1^f = 1.$$

But if the second components of a_1, b_1, have respectively first principal minors of the forms $\left\| \begin{matrix} 1 & 0 \\ \mu & 1 \end{matrix} \right\|$, $\left\| \begin{matrix} \tau^{*e} & 0 \\ \lambda & \tau_1^{*2e} \end{matrix} \right\|$, modulo p, then $b_1^{-1} a_1 b_1$ has correspondingly $\left\| \begin{matrix} \tau^e & 0 \\ \lambda\tau^{3e} & \tau^{2e} \end{matrix} \right\|$ $\left\| \begin{matrix} 1 & 0 \\ \mu & 1 \end{matrix} \right\|$ $\left\| \begin{matrix} \tau_1^{*e} & 0 \\ \lambda & \tau_1^{*2e} \end{matrix} \right\|$, which is equal to $\left\| \begin{matrix} 1 & 0 \\ \tau^e\mu & 1 \end{matrix} \right\|$; it follows that

$$b_1^{-1} a_1 b_1 = a_1 \tau^e.$$

Thus U is isomorphic to the subgroup $\{a, b^e\}$ of G, under the correspondence $a_1 \to a$, $b_1 \to b^e$.

It may further be noted that if G′ is the subgroup $\{a, b^{e'}\}$ of G, and U is a group of units of finite order in R(G′,C) then the first components of elements of U must certainly be elements of the group $\{b^{*e'}\}$. Thus the group $\{b^{*e}\}$ is a subgroup of $\{b^{*e'}\}$, and the subgroup of G isomorphic to U is likewise a subgroup of G′. That is to say, we have shown that if G′ is any group generated by two elements a, c subject to the relations:-

$$a^p = c^e = 1, \quad c^{-1} a c = a^s;$$

where s is of order f precisely modulo p, and $ef = p-1$; then a group of normalised units of finite order in R(G′,C) is isomorphic to a subgroup of G′.

The most important cases are the two extremes, G′ = G, and the dihedral group of order $2p$.

7. Group Rings of Groups without Elements of Finite Order

In this final section we shall prove that for a certain class of groups G without elements of finite order, whatever be the coefficient ring K, provided only that it has no zero divisors, the ring R(G,K) has no zero divisors and only trivial units. The groups for which this is true include free groups and free Abelian groups; and generally, if it is true for any two groups it is true also for their face product and for their direct product. A theorem of this kind is clearly quite different in character from those that we have proved concerning the group rings of finite groups, chiefly in that it is independent of the coefficient ring, whereas the theorems of the previous sections depend essentially on the fact that the coefficients are taken from rings of algebraic integers. Naturally, the methods used to prove the theorems are also of a different kind.

We make first two definitions. Let X, Y be any two sets of elements of the group G. Then a pair x, y of elements in X, Y respectively will be said to have the isolated product xy, with respect to X, Y, if the product $x'y'$ of an element x' in X by an element y' in Y is equal to xy only if $x' = x$ and $y' = y$. Similarly two subsets X_0, Y_0, of X, Y respectively will be said to have the isolated product set X_0Y_0 if the product $x'_r y'$ of an element x' in X by an element y' in

Y is equal to the product xy of an element x in X_0 by an element y in Y_0 only if x' is in X_0 and y' is in Y_0.

Then the following lemma is almost obvious.

Lemma. If in any two non-vacuous finite subsets X, Y of G, we can find a pair x, y of elements having an isolated product, then R(G,K) has no zero divisors. If furthermore whenever X or Y has more than one element, we can choose two such pairs, then R(G,K) has only trivial units.

Here, and throughout this section K stands for a ring without zero divisors.

Let P, Q be any two elements of R(G,K), and let X, Y stand for the sets of elements having non-zero coefficients in P, Q, respectively. If the pair x, y in X, Y respectively have an isolated product xy with respect to X, Y, then the coefficient of xy in the product of P,Q is precisely the product of the coefficients of x in P and y in Q, and is therefore not zero. Thus if there is in any pair of finite subsets, X, Y a pair x,y having an isolated product then if $P \neq 0$, $Q \neq 0$, we cannot have $PQ = 0$. If furthermore either P or Q is not of the form λg then either X or Y has more than one element, and the second half of the lemma follows.

Whether or not the hypothesis of the second half of the lemma follows from the hypothesis of the first half, I do not know. Certainly it does not follow from internal considerations on any two given sets X, Y, for if we take the sets $X_0 = (1, g, g^4)$, $Y_0 = (1, g^2, g^3)$, in the cyclic group $\{g\}$ of order 5, then the condition of the first half holds for all subsets of X_0 and Y_0, but the condition of the second half does not hold for the sets X_0, Y_0 themselves. For the whole group, of course, neither condition holds.

The hypothesis of the second half of the lemma is equivalent to the following condition, which for convenience of reference we label as Condition I.

Condition I. If X, Y are non-vacuous finite sets of elements of the group G, of which at least one contains more than one element, then we can find two pairs of non-vacuous subsets, X_1, Y_1, and X_2, Y_2, such that (i) X_i and Y_i have the isolated product set X_iY_i, (i = 1, 2) (ii) either X_1 and X_2 or Y_1 and Y_2 have no elements in common.

If Condition I holds, we can find in any non-vacuous finite sets X, Y, of elements of G, of which at least one has two or more elements, two pairs of elements having an isolated product. This is obvious if either X or Y contains just one element. We prove it therefore by induction on

the sum of the numbers of elements in X and in Y. By the hypothesis of the induction, then, we can find a pair of elements x_i, y_i in X_i, Y_i having a product $x_i y_i$ isolated with respect to X_i, Y_i. The product is however then isolated with respect to X, Y, since we cannot have $x_i\, y_i = x\, y$, (x in X, y in Y) unless x is in X_i, y in Y_i. Moreover we cannot have $x_1 = x_2$ and $y_i = y_2$, as then both X_1 and X_2, and Y_1 and Y_2 would have elements in common. By the Lemma therefore:-

Theorem 15. If G satisfies Condition I, R(G,K) has no zero divisors and only trivial units.

In attempting to prove that condition I holds for a particular group it is useful to realise that if the condition holds for the particular sets X, Y, it holds for any other pair of the form $g_1\, X\, g_2$, $g_2^{-1}\, Y\, g_3$, since obviously the subsets X_1, Y_1, of X, Y have an isolated product set if and only if the same is true of the subsets $g_1\, X_1\, g_2$, $g_2^{-1}\, Y$, g_3 of $g_1\, X\, g_2$, $g_2^{-1}\, Y$, g_3. Thus we may always, if it is convenient, suppose that the sets X, Y both contain the identity elements. Again, if G has a subgroup F which satisfies condition I, then the condition holds for any two sets X, Y, of G, of which at least one contains only elements of F. For suppose X only contains elements of F. If the elements of Y are in the same left residue class with respect

to F, - which we may take to be F itself, then the condition holds by assumption. If on the other hand at least two left residue classes F g_1 and F g_2 contain elements of Y, we may take $X_1 = X_2 = X$, Y_1 consists of all elements of Y in F g_1, Y_2 consists of all elements of Y in F g_2, and the condition holds.

Condition I is, however, very difficult to ~~that~~ treat in any particular case, and it is convenient to deal with a condition that probably holds for a more restricted class of groups, but is easier to apply. The function $\gamma(g)$ of elements in G whose values are rational integers is called an indexing of G if there exists an element of g such that $\gamma(g) = 1$, and for all g_1, g_2, in G, $\gamma(g_1 g_2) = \gamma(g_1) + \gamma(g_2)$. That is to say, γ is a homomorphism of G on the additive group of rational integers. A group G is said to be indicable if there exists a function γ indexing it. Then our condition is:-

Condition II. Every subgroup, other than the identity ~~alone~~ alone, generated by a finite set of elements of G is indicable.

Theorem 16. If G satisfies condition II, R(G,K) has no zero divisors, and only trivial units.

We shall shew that Condition II implies Condition I. To that end, let X, Y be finite sets of elements of G, of which at least one contains more than one element. We may without loss of generality suppose that both X and Y contain the element 1. Let H be subgroup generated by the elements of X and Y. H does not consist of the identity alone, and therefore there exists an indexing γ of H. Let m_1, m_2 be respectively the greatest and least values of m such that there exist elements x in X having $\gamma(x) = m$. Let X_i (i = 1 or 2) be the subset of X consisting of those elements x for which $\gamma(x) = m_i$. Define similary for Y the numbers n_1, n_2 and the subsets Y_1, Y_2. Then clearly the pair X_i, Y_i of subsets of X and Y have an isolated product set, for $\gamma(xy)$, (x in X, y in Y), is equal to $m_i + n_i$ only if x is in X_i and y in Y_i. Moreover we cannot have $X_1 = X_2$ and $Y_1 = Y_2$, for that would mean $m_1 = m_2$ and $n_1 = n_2$, and since both X and Y contain 1, the common value would in each case be zero. This, however, would imply $\gamma(g) = 0$ for all elements of H, contrary to the definition of an indexing.

Plainly, a free group, or a free Abelian group, is indicable. Moreover, a subgroup of a free group (or of a free Abelian group) not consisting of the identity alone is itself a free group (or a free Abelian group).[1] These groups

(1) Schreier, Abhandlung aus dem Mathematische Seminar der Hamburgischen Universitat, V, 161-183, (1927).

therefore satisfy the Condition II. So also does any Abelian group without elements of finite order, since a subgroup generated by a finite number of elements of such a group is a free Abelian group.

We next show that if two groups G and H satisfy condition I, (or condition II) then so do their direct product G x H and their free product G o H.

Theorem 17. If a group G has a self-conjugate subgroup H such that both H and the factor group G/H satisfy condition I, (or condition II), then G satisfies condition I, (or condition II).

(i) Consider first condition I. Let X, Y be non-vacuous finite sets of elements of G, of which at least one has more than one element. If all the elements of X lies in the same residue class modulo H, and the same is true of Y, then since condition I holds for H, we can find subsets X_1, X_2, Y_1, Y_2, having the desired properties. Otherwise, consider the sets $\bar{X}$, $\bar{Y}$ of elements in G/H formed by replacing every element z in X, Y, respectively by its residue class z H. There are finite non-vacuous sets of elements of G/H, of which at least one contains more than one element. Since Condition I holds for G/H, we can determine subsets $\bar{X}_1$, $\bar{X}_2$ $\bar{Y}_1$, $\bar{Y}_2$ of $\bar{X}_2$, $\bar{Y}$ according to the requirements of that condition. Let X_i be the set of all elements x in X such that xH is in

$\bar{X}_i$, and define Y_i correspondingly. Then X_1, X_2, Y_1, Y_2 satisfy the requirements of Condition I. For if x, y are in X_i, Y_i respectively, but x', y' are not, then x y and x'y' cannot be in the same residue class mod H, and a fortiori cannot be equal. So also, if, say, $\bar{X}_1$ and $\bar{X}_2$ have no common elements, neither have X_1 and X_2.

(ii) Now consider condition II. Let F be a subgroup of G generated by a finite number of elements. If it is in H, it is indicable, since condition II holds for H. Otherwise, the set of residue classes f H of elements in F is a subgroup of G/H not consisting of the identity alone and generated by a finite number of elements. It therefore has an indexing, say $\bar{\gamma}$. Then $\gamma(f) = \bar{\gamma}(f\,H)$ is an indexing of F.

Theorem 18. If two groups G, H, satisfy condition I or II, so does their direct product, G x H.

For G x H contains a subgroup self-conjugate subgroup isomorphic to G whose factor group is isomorphic to H.

Theorem 19. If two groups G, H, satisfy condition I or II, so does their free product G o H.

An element of G o H can be written in the form $e = g_1 h_1 \cdots g_r h_r$, $(g_i \in G,\ h_i \in H,\ i = 1, \cdots r)$. Then the correspondence $e \to [g_1 \cdots g_r,\ h_1 \cdots h_r]$ is a homomorphism of G o H on G x H.

The theorem therefore follows from Theorem 17 and ~~1~~, when we have shown that the kernel of this homomorphism is a free group. This kernel consists of all elements $g_1h_1\, g_2h_2 \cdots g_rh_r$ for which $g_1 g_2 \cdots g_r = h_1 h_2 \cdots h_r = 1$ Its intersection with any subgroup conjugate to either G or H consists of the identity alone, and it follows from a theorem of ~~Kursch~~ Kurosh on subgroups of free products that it is therefore a free group[1]. However, we may show without appealing to that theorem that U is generated freely by the commutators $(g,h) = ghg^{-1}h^{-1}$, $(g \in G,\ h \in H,\ g \neq 1,\ h \neq 1)$. For we may show by induction on r that

$$g_1h_1\, g_2h_2 \cdots g_rh_r = \prod_{i=1}^{r-1} (g_1 \cdots g_i,\ h_1 \cdots h_i)(g_1 \cdots g_{i+1},\ h_1 \cdots h_i)^{-1}\, g_1 \cdots g_r\, h_1 \cdots h_r,$$

so that the commutators do indeed generate the kernel. We may furthermore show by induction on r that if

$$\delta = (g_1, h_1)^{e_1} (g_2, h_2)^{e_2} \cdots (g_r, h_r)^{e_r}, \quad g_i \in G,\ h_i \in H,\ g_i \neq 1,\ h_i \neq 1,\ e_i = \pm 1,$$

and for no value of i is $g_i = g_{i+1}$, $h_i = h_{i+1}$ and $e_i + e_{i+1} = 0$ then

$$\delta = x_1 x_2 \cdots x_s, \qquad x_i \text{ in } G \text{ or } H,\ x_i \neq 1, \text{ and } x_i \text{ and } x_{i+1}$$

not in the same group G or H; where, if $e_r = 1$, $x_{s-1} = g_r^{-1}$ and $x_s = h_r^{-1}$ and if $e_r = -1$, $x_{s-1} = h_r^{-1}$, $x_s = g_r^{-1}$. Thus $\delta \neq 1$, and there are no non-identical relations between the generators (g, h).

---

(1) Mathematische Annalen, 109, 647-660, (1934).

We next consider some examples of groups satisfying condition II.

First, let G be generated by $a_1,\dots,a_n$, subject to relations

(1) $\quad a_s^{\lambda_s} = W_s(a_1,\dots,a_{s-1}), \quad s = r+1,\dots,n, \quad W_s \neq 1$.

G is derived from the free group $\{a_1,\dots,a_r\}$ by a finite number of applications of the process of replacing a given group by a free product with united subgroups of itself and a free cyclic group[1]. Obviously there exists an indexing of G in which $\gamma(a_1) \neq 0$. We shall make the further restrictive assumption that an indexing γ exists in which $\gamma(a_s) = 0$, $s = 1,\dots,n$. We may suppose further that $\gamma(a_1) = 1$; for otherwise we can replace G by the free product G' of G and a free cyclic group $\{a_0\}$, and extend γ to G' by setting $\gamma(a_0) = 1$. Then if G' satisfies condition II, so certainly does G, which is a subgroup of G'.

Now, to show that G satisfies condition II, it suffices, by Theorem 17, to show that the subgroup G_0 sent into zero by the indexing γ is a free group. This subgroup, however, is generated by the quantities $A_{s\rho} = a_1^{\rho} a_s a_1^{-\rho-c_s}$, $\rho = 0, \pm 1, \pm 2, \dots$ ad inf. $s = 2,\dots,n$, where $c_s = \gamma(a_s)$. For let $g = a_{i_1}^{e_1} a_{i_2}^{e_2} \dots a_{i_k}^{e_k}$, and set $\rho_0 = 0$, $\rho_\alpha = \gamma(a_{i_1}^{e_1} \dots a_{i_\alpha}^{e_\alpha})$, $\alpha = 1,\dots,k$. We have

---

(1) For the definition and properties, used frequently in this section, of free products with united subgroups, see Schreier, loc.cit., 164-168.

(2) $g = a_{i_1}^{e_1} \dots a_{i_k} = \prod_{\alpha=1}^{k} a_1^{\rho_{\alpha-1}} a_{i_\alpha}^{e_\alpha} a_1^{-\rho_\alpha} \cdot a_1^{\rho_k} = \prod_{\alpha=1}^{k} B_\alpha \cdot \phi_1^{\rho_k}$, say.

Now if $i_\alpha = 1$ then $B_\alpha = 1$; if $i_\alpha \neq 1$, $e_\alpha = 1$, then $B_\alpha = A_{i_\alpha \rho_{\alpha-1}}$; if $i_\alpha \neq 1$, $e_\alpha = -1$, then $B_\alpha = A^{-1}_{i_\alpha \rho_\alpha}$. Moreover if g is in G_0, $\rho_k = 0$. Thus (2) provides a translation for expressions in $a_1, \dots, a_n$ that represents elements in G_0, into expressions in $A_{s\rho}$. Thus $A_{s\rho}$ generate G_0.[1] What, we must next ask, are the relations between them. Two expressions in $a_1, \dots, a_n$ represent the same element in G if and only if they can be transformed into one another by a series of transformations of the following forms:-

(i) insertion or removal of terms of the form $a_i^e a_i^{-e}$;

(ii) replacement of the right hand side of one of equations (1) by the left hand side.

On translation into terms of the generators $A_{s\rho}$, by means of (2) these processes become:-

(i) insertion or removal of terms of the form $A_{s\rho}^e A_{s\rho}^{-e}$;

(ii) replacement of the right hand side of one of the following equations by its left hand side:-

(3) $A_{s\rho} A_{s\rho+c_s} \dots A_{s\,\rho+(\delta_s-1)c_s} = W_{\rho s}(A_{2\sigma}, \dots A_{s-1,\sigma})$.

---

(1) Cf. Schreier, loc.cit.

where, of course, $W_{\rho s}$ depend on the W_s of equations (1). Thus equations (3) are defining relations for G_0. However, equations (3) are simply definitions, in terms of the generators

(4) $A_{s\rho}$, $s = 2, \cdots, n$; $\rho = 0, \pm 1, \pm 2, \cdots$ ad. inf. if $s = 2, \cdots, r$; $\rho = 0, 1, \cdots, \lambda_s c_s - 1$, if $s = r+1, \cdots, n$;

of the remaining generators $A_{s\rho}$, $s = r+1, \cdots, n$, $\rho < 0$ or $\rho > \lambda_s c_s - 1$. Thus G_0 is generated freely by the generators (4). G therefore satisfies condition II as required.

The simplest case of a group of the above type is that generated by x, y subject to $x^m = y^n$. If m is prime to n, this is the group of a torus knot. If we take another class of knots, - those formed by the process of doubling a simple circuit - their groups are generated by generators a, b, subject to the relation

$$a^{2n+1} = b\, a^n\, b^{-2} a^n\, b .$$

This group G is not, of course, of the above form. However, it has an indexing $\gamma(a) = 0$, $\gamma(b) = 1$ and the subgroup such that $\gamma(g) = 0$ can be shown by the same process as was used above to be generated by $a_i = b^i a b^{-1}$, $i = 0, \pm 1, \pm 2, \cdots$ ad inf., subject to

(5) $a_i^{2n+1} = a_{i+1}^n\, a_{i-1}^n$, $i = 0, \pm 1, \pm 2, \cdots$ ad inf..

We wish to shew that this group G_0 satisfies condition II. Now a subgroup of G_0 generated by a finite number of elements is a contained in a subgroup G_{rs}, generated by $a_r, a_{r+1}, \cdots, a_s$,

and it suffices to show that G_{rs} for all r,s satisfies condition II. Now a system of defining relations for G_{rs} is given by (5) for $i = r + 1,\ldots,s-1$. For let $R(a_r,\ldots,a_s)$ be any relation between $a_r,\ldots,a_s$. It is a consequence of relations (5); for $i = r' + 1,\ldots,s' - 1$, say, since it must be a consequence of a finite number of them. Thus $R(a_r,\ldots,a_s)$ is true in the group $G^*_{r's'}$ generated by $a_{r'}, a_{r'+1}, \ldots a_{s'}$, subject to

$$(6) \qquad a_i^{2n+1} = a_{i+1}^{n} \cdot a_{i-1}^{n}, \qquad i = r'+1,\ldots,s'-1.$$

This group, however, can be obtained from G^*_{rs}, - generated by $a_r,\ldots,a_s$ subject to (6) for $i = r + 1,\ldots,s - 1$, - by a repetition of the process of forming a free product with united subgroups of it and a free cyclic group. It therefore contains G^*_{rs} as a subgroup, and $R(a_r,\ldots,a_s)$ must be a consequence of (6) for $i = r + 1,\ldots,s - 1$, and therefore $R(a_r,\ldots,a_1)$ a consequence of (5) for $i = r + 1,\ldots,s - 1$, as required. G_{rs} is therefore of the form previously considered, when we write (5) in the form

$$a_{i+1}^{n} = a_i^{2n+1} a_{i-1}^{-n};$$

and it remains only to show that there exists an indexing of G_{rs}, in which none of $\gamma(a_r), \ldots, \gamma(a_s)$ are zero. However, defining $\gamma(a_r)$ and $\gamma(a_{r+1})$ arbitrarily, $\gamma(a_{r+2}),\ldots,\gamma(a_s)$ are determined successively by (5); and we have

$$n\left(\gamma(a_{i+1}) - \gamma(a_i)\right) = \gamma(a_i) + n\left(\gamma(a_i) - \gamma(a_{i+1})\right).$$

Thus if we take $\gamma(a_{r+1}) > \gamma(a_r) > 0$ we have $\gamma(a_i) > \gamma(a_{i-1})$ for all i, and therefore $\gamma(a_i) > 0$.

Thus, finally G satisfies condition II.

As a third example, consider the group G generated by $a_1, a_2, \ldots$ ad inf., subject to

$$(7) \qquad a_{i-1} = a_i a_{i+1} a_i^{-1} a_{i-1}^{-1}, \quad i = 2, 3, \ldots \text{ ad inf.}$$

This group is interesting as an example of a group which satisfies condition II, though it is obviously its own derived group. We have, in fact, that any subgroup of G generated by a finite number of elements is a free group. For such a subgroup is contained in a sub-group $\{a_r, a_{r+1}\}$ for some value of r, and it therefore suffices to show that this group is free. Let $R(a_r, a_{r+1})$ be a relation between a_r and a_{r+1}, holding as a consequence of equations (7) for $i = 2, \ldots, r'$, $(r' > r)$. Then $R(\alpha_r, \alpha_{r+1})$ holds in the free group generated by $\alpha_{r'}, \alpha_{r'+1}$ when $\alpha_{r'-1}, \alpha_{r'-2}, \ldots$ are defined successively by

$$\alpha_{i-1} = \alpha_i \alpha_{i+1} \alpha_i^{-1} \alpha_{i+1}^{-1}.$$

However $\{\alpha_{r'-1}, \alpha_{r'}\} = \{\alpha_{r'} \alpha_{r'+1} \alpha_{r'}^{-1} \alpha_{r'+1}, \alpha_{r'}\}$ is clearly a free group, and so by induction on s is $\{\alpha_{r'-s}, \alpha_{r'-s+1}\}$ and in particular $\{\alpha_r, \alpha_{r+1}\}$. Thus $R(\alpha_r, \alpha_{r+1})$ and also $R(a_r, a_{r+1})$ is a trivial relation, as was required to be proved.

If we desired to imbed this group G in a group having a finite generator and relation system, we may take generators

a, b, and relation

$$b = (aba^{-1}a^{2}ba^{-2}) = ababa^{-1}b^{-1}ab^{-1}a^{-2}.$$

This group has an indexing $\gamma(a) = 1$, $\gamma(b) = 0$; the subgroup of elements g such that $\gamma(g) = 0$ is isomorphic to the group G above, being generated by $a_i = a^i b a^{-i}$, subject to (7). Thus the group satisfies condition II, though all its derived groups after the first are equal.

It is obvious that neither condition I nor condition II can hold in a group having elements of finite order. It is a plausible hypothesis, however, that if a group has no elements of finite order then its group ring is without zero divisors and has only trivial units. It is therefore natural to enquire whether such a group can fail to satisfy either of conditions I and II. The answer in the case of condition II is certainly yes. It suffices to construct a group without elements of finite order, and generated by a finite number of elements, which is its own derived group. Let G be generated by x, y, subject to $x^3 = y^2$; H by ξ, η subject to $\xi^3 = \eta^2$. Let G_0 be the subgroup of G generated by $y\,x^{-1}$, and $(y\,x^{-1})^6\,x^{-3}$. Since x^3 is in the centrum of G, G_0 is a free Abelian group on its two generators. Define similarly the subgroup H_0 of H generated by $\eta\,\xi^{-1}$ and $(\eta\,\xi^{-1})^6\,\xi^{-3}$ and let F be the free product of G and H, with identification of the subgroups G_0 and H_0 according to the scheme:

$\eta \xi^{-1} = (\eta x^{-1})^6 x^{-3}$; $\eta x^{-1} = (\eta \xi^{-1})^6 \xi^{-3}$.

F has a finite generator system, and is without elements of finite order, since G and H are. But F^1, the derived group of F, is equal to F. For any element in G is congruent modulo G', and therefore modulo F', to a power of yx^{-1}. However $\eta x^{-1} = (\eta \xi^{-1})^6 \xi^{-3}$ which can be written $(\eta \xi^{-1})^6 \eta^{-6} \xi^6$ and is therefore in F'. Similarly, every element of H is in F', and so F' = F.

The question concerning condition I is more difficult. That condition is very unwieldy in application, and I have not been able to determine, for any group without elements of finite order in which condition II does not hold, whether it holds or not.