THE UNITS OF GROUP-RINGS

By GRAHAM HIGMAN.

[Received and read 16 February, 1939.]

1. *Introduction.*

Let G be any group, and K any ring. The formal sums

$$r_1 e_1 + r_2 e_2 + \ldots + r_n e_n, \quad r_i \in K, \quad e_i \in G \quad (i = 1, 2, \ldots, n), \tag{1.1}$$

when addition and multiplication are defined in the obvious way, form a ring, the group-ring of G over K, which will be denoted by $R(G, K)$. Henceforward, we suppose that K has the modulus 1, and we denote the identity in G by e_0. Then $R(G, K)$ has the modulus $1 . e_0$. Since no confusion can arise thereby, the element $1 . e$ in $R(G, K)$ will be written as e, and whenever it is convenient, the elements e_0 in G and re_0 in $R(G, K)$ as 1 and r respectively. The symbol e, with or without subscripts, will always denote an element in G.

If the elements E_1, E_2 in $R(G, K)$ satisfy $E_1 E_2 = 1$, E_1 will be said to be a left unit, and E_2 a right unit in $R(G, K)$. If η is a left (or right) unit in K, then ηe is a left (or right) unit in $R(G, K)$. Such a unit will be described as trivial. The units in $R(G, K)$ form a group if and only if every right unit is also a left unit. This is so, for instance, if both G and K are Abelian. It is also true if G is a finite group, and K is any ring of complex numbers, for then the regular representation† of G can be extended to give an isomorphism of $R(G, K)$ in the ring of ordinary matrices.

The first object of this paper is to study units in $R(G, C)$, where C is the ring of rational integers. In § 2 we take G to be a finite Abelian group,

† A. Speiser, *Theorie der Gruppen von endlicher Ordnung* (2 ed., Berlin, 1927), 172. J. H. M. Wedderburn, *Lectures on matrices* (New York, 1934), 149.

and consider the more general coefficient ring C', where C' is the integer ring of a finite algebraic extension k' of the rational field k. We first investigate the algebra $R(G, k')$, and determine the structure of its integer ring, and of the unit group of that integer ring. We then show that a unit of finite order in $R(G, C')$ is trivial, and that the ranks of the unit groups of $R(G, C')$ and of the integer ring of $R(G, k')$ are equal. This suffices to prove, for the particular case of the rational ring C, that $R(G, C)$ has non-trivial units unless either the orders of all the elements of G divide four, or they all divide six, in which case $R(G, C)$ has only trivial units. In § 3 we consider groups all of whose elements have finite order, and show that, if G is such a group, and $R(G, C)$ has only trivial units, then either G is Abelian, or it is the direct product of a quaternion group and an Abelian group, all of whose elements other than the identity have order two. In § 4 we show that $R(G, C)$ has only trivial units if G belongs to a class of infinite discrete groups that includes free groups and free Abelian groups.

Section 5 is concerned with a condition on G which can be expressed as follows: Consider the following transformations on a matrix $||a_{ij}||$, $i, j = 1, \ldots, n$, whose elements are in $R(G, C)$:

(1.2)

(a) Multiplying a row on the left, or a column on the right by $\pm e$; that is, replacing the row $(a_{i1}, \ldots, a_{in})$ by $(\pm ea_{i1}, \ldots, \pm ea_{in})$, or the column $(a_{1i}, \ldots, a_{ni})$ by $(\pm a_{1i}e, \ldots, \pm a_{ni}e)$, $e \in G$;

(b) Adding to one row (column) of $||a_{ij}||$ a left (right) multiple of another row (column) by an element in $R(G, C)$; that is, replacing the row $(a_{i1}, \ldots, a_{in})$ by $(a_{i1}+ra_{j1}, \ldots, a_{in}+ra_{jn})$, or the column $(a_{1i}, \ldots, a_{ni})$ by $(a_{1i}+a_{1j}r, \ldots, a_{ni}+a_{nj}r)$, $i \neq j$, $r \in K$;

(c) Bordering $||a_{ij}||$ with a row and a column of zeros meeting in a 1; that is, putting $a_{in+1} = a_{n+1i} = 0$, $i = 1, \ldots, n$, $a_{n+1n+1} = 1$; or the inverse of this.

Then the condition on G is that if $||a_{ij}||$ has a left inverse $||a^*_{ij}||$, so that

$$\sum_{r=1}^{n} a^*_{ir} a_{rj} = \delta_{ij} \quad (i, j = 1, \ldots, n), \tag{1.3}$$

then $||a_{ij}||$ is transformable into the one-rowed matrix $||1||$ by a sequence of transformations (1.2).

The converse, that if a matrix $||a_{ij}||$ has a left inverse, so has any matrix derivable from it by transformations (1.2), is, of course, always true

If G is Abelian and $R(G, C)$ has a non-trivial unit E, the condition is not satisfied. For the determinant $|a_{ij}|$ can then be defined as in elementary algebra, and is altered under transformations (1.2) only by a factor $\pm e$. The one-rowed matrix $\|E\|$ with determinant E cannot, therefore, be transformed into $\|1\|$ though it has the left inverse $\|E^{-1}\|$. On the other hand we show in § 5 that the condition is satisfied for certain groups other than that consisting of the identity alone.

These results are applicable to the topology of a polyhedron P if we take G to be its fundamental group. For K. Reidemeister† has shown that the invariants of certain "incidence matrices" under transformations (1.2) are invariants‡ of P. Also J. H. C. Whitehead§ could only prove a certain topological theorem for a polyhedron whose fundamental group satisfies the above matrix condition.

I should like to thank Mr. Whitehead for many helpful suggestions and much good advice that he has given me, both in the investigation of these problems and in the writing of this paper.

2. *Finite Abelian groups.*

In this section we determine the structure of the unit group of $R(G, C')$, where G is a finite Abelian group, and C' is the integer ring of a finite algebraic extension k' of the rational field k. To that end we consider $R(G, k')$, which is a commutative algebra over k'. It is known‖ that $R(G, k')$ is semi-simple, and therefore is the direct sum of simple algebras over k', each of which, being commutative, is isomorphic to an algebraic extension¶ of k'. Moreover there exists†† an extension $k'(\zeta)$ of k', such that in the corresponding reduction of $R\big(G, k'(\zeta)\big)$ each simple algebra over $k'(\zeta)$ is isomorphic to $k'(\zeta)$. That is, if g is the order of G, there exist elements $\eta_0, \eta_1, \ldots, \eta_{g-1}$ in $R\big(G, k'(\zeta)\big)$ such that

$$(2.1) \qquad (a) \quad \eta_i\eta_j = 0, \quad i \neq j, \quad i, j = 0, 1, \ldots, g-1;$$

$$(b) \quad \eta_i^2 = \eta_i, \quad i = 0, 1, \ldots, g-1.$$

† "Homotopiegruppen von Komplexen", *Abhandlung aus dem Mathematischen Seminar der Hamburgischen Universität*, 10 (1934), 211–215.

‡ Reidemeister proved they are combinatorial invariants, and Whitehead, *Quart. J. of Math.* (Oxford Series), 10 (1939), 81–83, has since proved they are topological invariants of P.

§ *Proc. London Math. Soc.* (2), 45 (1939), 243–327.

‖ Wedderburn, *loc. cit.*, 168.

¶ Wedderburn, *loc. cit.*, 159 [Theorem 5 (iii)].

†† Wedderburn, *loc. cit.*, 168.

The first step is the explicit determination of these elements. We then carry out explicitly the reduction of $R(G, k')$ to a sum of fields. This enables us immediately to ascertain the structure of the unit group of the integer ring of $R(G, k')$. Finally we prove the two results concerning the unit group of $R(G, C')$, namely that its elements of finite order are all trivial, and that its rank is the same as that of the unit group of the integer ring of $R(G, k')$.

If h is the maximum order of any element in G, ζ can in fact be taken to be a primitive h-th root of unity. For since G is Abelian there are precisely† g irreducible mutually inequivalent representations of G, and each is of order 1. Denote them by $\Gamma^0, \Gamma^1, \ldots, \Gamma^{g-1}$, and the elements of G by $e_0, e_1, \ldots, e_{g-1}$. We can regard Γ^i as a homomorphism of G in a multiplicative group of complex numbers, and write

$$\Gamma^i(e_j) = \chi_j^{\,i} \quad (i, j = 0, 1, \ldots, g-1). \tag{2.2}$$

Since the order of any element in G divides h, $\chi_j^{\,i}$ is an h-th root of unity and therefore a number in $k'(\zeta)$. We have‡, if $\bar{\chi}_j^{\,i}$ denotes the reciprocal of $\chi_j^{\,i}$,

$$\begin{cases} (a) \quad \sum_{r=0}^{g-1} \chi_r^{\,i} \bar{\chi}_r^{\,j} = \delta_{ij} g \quad (i, j = 0, 1, \ldots, g-1), \\ (b) \quad \sum_{r=0}^{g-1} \chi_i^{\,r} \bar{\chi}_j^{\,r} = \delta_{ij} g \quad (i, j = 0, 1, \ldots, g-1). \end{cases} \tag{2.3}$$

Define elements $\eta_0, \eta_1, \ldots, \eta_{g-1}$ in $R\big(G, k'(\zeta)\big)$ by

$$\eta_i = \frac{1}{g} \sum_{r=0}^{g-1} \chi_r^{\,i} e_r \quad (i = 0, 1, \ldots, g-1). \tag{2.4}$$

Given s, e_r can be written uniquely in the form $e_t e_s$, and then $\chi_r^{\,i} = \chi_t^{\,i} \chi_s^{\,i}$; so that we have

$$\eta_i = \frac{1}{g} \sum_{t=0}^{g-1} \chi_t^{\,i} \chi_s^{\,i} e_t e_s = \chi_s^{\,i} \eta_i e_s,$$

or

$$\eta_i e_s = \bar{\chi}_s^{\,i} \eta_i \quad (i, s = 0, 1, \ldots, g-1). \tag{2.5}$$

Multiplying by $\chi_s^{\,j}$ and summing over $s = 0, 1, \ldots, g-1$, we obtain (2.1) in virtue of (2.3a).

---

† Speiser, *loc. cit.*, compare Theorem 136, p. 159, with Theorem 154, p. 176.

‡ Speiser, *loc. cit.*, 171, 173. The developments of this section as far as the proof of equations (2.1) are the Abelian case of the first part of paragraph 58 of Speiser's book.

The linear independence of $\eta_0, \eta_1, \ldots, \eta_{g-1}$ follows from equations (2.1) and since their number is equal to the rank of $R\big(G, k'(\zeta)\big)$ they form a basis for that ring. That is,

$$E = \sum_{r=0}^{g-1} a_r e_r = \sum_{r=0}^{g-1} b_r \eta_r, \tag{2.6}$$

where E is any element in $R\ G, k'(\zeta)\big)$; and, by equations (2.1), (2.5) and (2.4),

$$\begin{cases} (a) \quad b_i = \sum_{r=0}^{g-1} a_r \bar{\chi}_r{}^i & (i = 0, 1, \ldots, g-1), \\ (b) \quad a_i = \frac{1}{g} \sum_{r=0}^{g-1} b_r \chi_i{}^r & (i = 0, 1, \ldots, g-1). \end{cases} \tag{2.7}$$

In particular, since e_0 is the identity and therefore $\chi_0{}^i = 1, i = 0, 1, \ldots, g-1$, or directly from equations (2.1),

$$e_0 = \eta_0 + \eta_1 + \ldots + \eta_{g-1}. \tag{2.8}$$

If σ is any transformation in the Galois group of $k'(\zeta)$ relative to k', the correspondence $e_j \to \sigma\big(\Gamma^i(e_j)\big) = \sigma(\chi_j{}^i)$ is a homomorphism, and therefore is one of the representations $\Gamma^0, \Gamma^1, \ldots, \Gamma^{g-1}$. We denote it by $\Gamma^{\sigma(i)}$ and say that $\Gamma^{\sigma(i)}$ is conjugate to Γ^i. We denote by ξ_i a root of unity whose order is the least common multiple of the orders of $\chi_0{}^i, \chi_1{}^i, \ldots, \chi_{g-1}^i$, so that $k'(\xi_i)$ is the least extension of k' in which the representation Γ^i exists. Clearly ξ_i is an h-th root of unity. But, since h is the maximum order of any element in G, we can write G as the direct product† of a cyclic group $\{e\}$ of order h, and another group G'. If Γ^i is the representation $e \to \zeta$, $e' \to 1$, $e' \in G'$, or any of its conjugates, then plainly ξ_i is a primitive h-th root of unity. We have thus established the last part of Theorem 1:

THEOREM 1. *Let $\Gamma^0, \Gamma^1, \ldots, \Gamma^{p-1}$ be a complete set of irreducible, mutually inequivalent, and, relative to k', non-conjugate representations of a finite Abelian group G. Then the ring $R(G, k')$ is the direct sum of the fields $R_0, R_1, \ldots, R_{p-1}$, where R_α is isomorphic to $k'(\xi_\alpha)$, defined as above, $\alpha = 0, 1, \ldots, p-1$. The numbers $\xi_0, \xi_1, \ldots, \xi_{p-1}$ are h-th roots of unity, of which at least one is primitive.*

It remains to prove the first part of the Theorem.

† This is an immediate consequence of the theorem concerning the expression of a finite Abelian group as the direct product of cyclic groups of prime-power order. See *e.g.*, Speiser, *loc. cit.*, Theorem 48, p. 62.

Let U_α be the subgroup of the Galois group consisting of those transformations σ for which $\sigma(\alpha) = \alpha$. Then σ is in U_α if and only if

$$\sigma(\chi_i^\alpha) = \chi_i^\alpha \quad (i = 0, 1, \ldots, g-1);$$

that is, if, and only if, σ leaves invariant every number in $k'(\xi_\alpha)$. Therefore, by the fundamental theorem of the Galois theory†, a number is left invariant by every transformation in U_α, if and only if it is in $k'(\xi_\alpha)$.

By (2.7a) a necessary condition for E, given by (2.6), to be in $R(G, k')$ is that

$$\sigma(b_i) = b_{\sigma(i)} \quad (i = 0, 1, \ldots, g-1), \tag{2.9}$$

holds for every transformation σ in the Galois group. By (2.7b) this condition is also sufficient. If equations (2.9) hold, b_α is in $k'(\xi_\alpha)$ $(\alpha = 0, 1, \ldots, p-1)$. Conversely, given b_α in $k'(\xi_\alpha)$ $(\alpha = 0, 1, \ldots, p-1)$, equations (2.9) can be solved uniquely for b_i $(i = 0, 1, \ldots, g-1)$. For, by hypothesis, to each number i of the set $0, 1, \ldots, g-1$ we can assign a transformation τ_i in the Galois group such that $\tau_i(i) = \alpha$ is one of the numbers $0, 1, \ldots, p-1$. Then $b_i = \tau_i^{-1}(b_\alpha)$, so that a solution, if it exists, is unique. On the other hand, if $\sigma(i) = j$, we have $\tau_j(j) = \beta$, where β is one of the numbers $0, 1, \ldots, p-1$, and therefore $\tau_j \sigma \tau_i^{-1}(\alpha) = \beta$. Hence we must have $\alpha = \beta$, and $\tau_j \sigma \tau_i^{-1}$ is in U_α. Since b_α is in $k'(\xi_\alpha)$, $\tau_j \sigma \tau_i^{-1}(b_\alpha) = b_\alpha$ *i.e.* $\sigma \tau_i^{-1}(b_\alpha) = \tau_j^{-1}(b_\alpha)$. Defining b_i as $\tau_i^{-1}(b_\alpha)$, therefore, we have a solution of equations (2.9). There is thus a $1-1$ correspondence between elements in $R(G, k')$ and sequences $(b_0, b_1, \ldots, b_{p-1})$, b_α in $k'(\xi_\alpha)$ $(\alpha = 0, 1, \ldots, p-1)$. If we denote E, given by (2.6) and satisfying (2.9), by $(b_0, b_1, \ldots, b_{p-1})$, we have, by (2.1),

$$\begin{cases} (a) \quad (b_0, b_1, \ldots, b_{p-1}) + (c_0, c_1, \ldots, c_{p-1}) = (b_0 + c_0, b_1 + c_1, \ldots, b_{p-1} + c_{p-1}), \\ (b) \quad (b_0, b_1, \ldots, b_{p-1})\,(c_0, c_1, \ldots, c_{p-1}) = (b_0 c_0, b_1 c_1, \ldots, b_{p-1} c_{p-1}). \end{cases} \tag{2.10}$$

If, therefore, R_α consists of those sequences for which $b_\beta = 0$, $\beta \neq \alpha$, the theorem is true.

The element E in $R(G, k')$ is said to be integral if it satisfies an equation of the form

$$E^r + a_{r-1} E^{r-1} + \ldots + a_1 E = 0, \text{ with } a_1, \ldots, a_{r-1} \text{ rational integers.}$$

The integral elements in $R(G, k')$ form a ring, the integer ring of $R(G, k')$, and the integral element E is a unit of this ring if there exists another integral element E' such that $EE' = 1$. By (2.10), the element

† B. L. van der Waerden, *Moderne Algebra*, 1 (2 ed., Berlin, 1937), 163.

E, given by (2.6), is integral in $R(G, k')$ if, and only if, b_α is integral in $k'(\xi_\alpha)$ $(\alpha = 0, 1, \ldots, p-1)$; and it is a unit in this integer ring if, and only if, b_α is a unit in $k'(\xi_\alpha)$. Hence we have

THEOREM 2. *The unit group of the integer ring of $R(G, k')$ is the direct product of groups isomorphic to the unit groups of $k'(\xi_0)$, $k'(\xi_1)$, ..., $k'(\xi_{p-1})$.*

If E, given by (2.6), is in $R(G, C')$, by (2.7a) it is in the integer ring of $R(G, k')$. The unit group of $R(G, C')$ is therefore a subgroup of the unit group of this integer ring.

THEOREM 3. *A unit of finite order in $R(G, C')$ is trivial.*

Let E, given by (2.6), be a unit of order m. Then

$$b_i^m = 1 \quad (i = 0, 1, \ldots, g-1)$$

and therefore b_i and each of its conjugates has absolute value 1. The same is true of χ_j^i. Since E is a unit, we can choose i so that a_i is not zero. Now

$$|a_i| = \left| \frac{1}{g} \sum_{r=0}^{g-1} b_r \chi_i^r \right| \leqslant \frac{1}{g} \sum_{r=0}^{g-1} |b_r \chi_i^r| = 1,$$

and the same is true for each conjugate of a_i. But the product of these conjugates is the norm of a_i, a rational non-zero integer. Hence equality holds above, and

$$b_0 \chi_i^0 = b_1 \chi_i^1 = \ldots = b_{g-1} \chi_i^{g-1} = a_i, \quad b_j = a_i \bar{\chi}_i^j \quad (j = 0, 1, \ldots, g-1).$$

By (2.7b) and (2.3b), $a_j = 0$, if $j \neq i$, so that the unit E is trivial.

This disposes of the finite part of the unit group. We have next

THEOREM 4. *There exists an integer n such that the n-th power of any unit in the integer ring of $R(G, k')$ is in $R(G, C')$.*

Let n be the number of residue classes mod g in $k'(\zeta)$ that are prime to g, and let E, given by (2.6), be a unit in the integer ring of $R(G, k')$. Then

$$b_i \quad (i = 0, 1, \ldots, g-1)$$

is a unit in $k'(\zeta)$ and is therefore prime to g. By Fermat's theorem for ideals†,

$$b_i^n \equiv 1 \mod g,$$

i.e.

$$b_i^n - 1 = c_i g \quad [c_i \text{ an integer in } k'(\zeta)].$$

† D. Hilbert, *Gesammelte Abhandlungen*, 1 (Berlin, 1932), 82.

By (2.8) therefore,

$$E^n = e_0 + \sum_{i=0}^{g-1} (b_i^n - 1)\eta_i = e_0 + \sum_{i=0}^{g-1} c_i \cdot g\eta_i.$$

By (2.4) the coefficients in $g\eta_i$ are algebraic integers. So, therefore, are those in E^n, which is therefore an element in $R(G, C')$.

THEOREM 5. *The unit groups of $R(G, C')$ and of the integer ring of $R(G, k')$ have the same rank.*

Since E^{-n} is the n-th power of E^{-1}, it also is in $R(G, C')$, so that E^n is a unit in $R(G, C')$. Moreover the n-th powers of an independent set of units are themselves independent, so that the rank of the unit group of $R(G, C')$ cannot be less than the rank of the unit group of the integer ring of $R(G, k')$. But the former group is a subgroup of the latter, and cannot therefore have a greater rank, whence the theorem follows.

Applying these results to $R(G, C)$ we obtain

THEOREM 6. *If G is a finite Abelian group, $R(G, C)$ has non-trivial units unless G is the direct product of*

(i) *l cyclic groups of order two, $l \geqslant 0$,*

and (ii) *either* (*a*) *m cyclic groups of order three, $m \geqslant 0$ or* (*b*) *n cyclic groups of order four, $n \geqslant 0$,*

in which cases $R(G, C)$ has only trivial units.

The "direct product of 0 groups ..." is, of course, to be interpreted conventionally as the group consisting of the identity alone.

By Theorem 3, a unit of finite order in $R(G, C)$ is trivial. Conversely, since C contains no units of infinite order, a trivial unit in $R(G, C)$ is of finite order. Hence $R(G, C)$ has only trivial units if, and only if, the rank of its unit group is zero. By Theorem 5, Theorem 2, and the last sentence of Theorem 1, the rank of the unit group of $R(G, C)$ is zero if, and only if, the rank of the unit group of $k(\zeta)$ is zero, that is to say†, if, and only if, $h = 2$, 3, 4, or 6. Finally the groups mentioned in the enunciation are just those‡ for which $h = 2$, 3, 4, or 6.

3. *Groups all of whose elements have finite order.*

THEOREM 7. *Let G^* be the direct product of a group G and a cyclic group of order two. If all the units in $R(G, C)$ are trivial, so are all the units in $R(G^*, C)$.*

† Hilbert, *loc. cit.*, 102 (Theorem 47).

‡ This is an immediate consequence of the theorem concerning the expression of a finite Abelian group as the direct product of cyclic groups of prime-power order. See, *e.g.*, Speiser, *loc. cit.*, Theorem 48, p. 62.

Let the cyclic group of order two be generated by f. An element in $R(G^*, C)$ can be written uniquely in the form $\alpha+\beta f$, where α, β are in $R(G, C)$. If

$$(\alpha+\beta f)(\gamma+\delta f) \equiv \alpha\gamma+\beta\delta+(\alpha\delta+\beta\gamma)f = 1,$$

then
$$\alpha\gamma+\beta\delta = 1, \quad \alpha\delta+\beta\gamma = 0.$$

Hence
$$(\alpha+\beta)(\gamma+\delta) = 1, \quad (\alpha-\beta)(\gamma-\delta) = 1.$$

Because $R(G, C)$ has only trivial units, we must have $\alpha+\beta = \pm e_1$, $\alpha-\beta = \pm e_2$. Hence $\alpha = \frac{1}{2}(\pm e_1 \pm e_2)$. But α is in $R(G, C)$, so that we must have $e_1 = e_2$, so that $\alpha+\beta = \pm(\alpha-\beta)$. If $\alpha+\beta = \alpha-\beta = \pm e_1$, we have $\alpha = \pm e_1$, $\beta = 0$, and so $\alpha+\beta f = \pm e_1$. If $\alpha+\beta = -(\alpha-\beta) = \pm e_1$, we have similarly, $\alpha+\beta f = \pm e_1 f$. In all cases $\alpha+\beta f$ is a trivial unit, and the theorem is therefore proved.

THEOREM 8. *Let G be a quaternion group. Then all the units in $R(G, C)$ are trivial.*

Let the group G be generated by x, y, z, subject to

$$x^2 = y^2 = z^2 = xyz = P,$$

say, and let $A = a_0+a_1x+a_2y+a_3z+b_0P+b_1xP+b_2yP+b_3zP$ be a unit in $R(G, C)$. The correspondence $x \to i$, $y \to j$, $z \to k$, $P \to -1$ is a homomorphism of $R(G, C)$ on the ring of quaternions with integer coefficients. In this ring the only units† are ± 1, $\pm i$, $\pm j$, $\pm k$. Hence A is carried into one of these quantities. That is, for some index i ($i = 0$, 1, 2, or 3).

$$(3.1) \qquad a_i-b_i = \pm 1, \quad a_j-b_j = 0 \quad (j \neq i, j = 0, 1, 2, 3).$$

Let G' be a direct product of two cyclic groups of order two, and let its elements be $1, x', y', z'$. The correspondence $x \to x'$, $y \to y'$, $z \to z'$, $P \to 1$ is a homomorphism of $R(G, C)$ on $R(G', C)$. In this ring, by Theorem 6, or by Theorem 7, the only units are ± 1, $\pm x'$, $\pm y'$, $\pm z'$. Hence A is carried into one of these quantities. That is, for some index i' ($i' = 0$, 1, 2, or 3),

$$(3.2) \qquad a_{i'}+b_{i'} = \pm 1, \quad a_j+b_j = 0 \quad (j \neq i', j = 0, 1, 2, 3).$$

† The norm $a^2+b^2+c^2+d^2$ of the unit $a+bi+cj+dk$ must be equal to 1.

Since a_i, b_i are integral, we have, on comparing (3.1) and (3.2), $i = i'$. Hence either

$$a_i = \pm 1, \quad b_i = 0, \quad a_j = b_j = 0 \quad (j \neq i),$$

or

$$a_i = 0, \quad b_i = \pm 1, \quad a_j = b_j = 0 \quad (j \neq i).$$

In either case the unit A is trivial.

THEOREM 9. *Let G be a group such that all the units in $R(G, C)$ are trivial. Then, if P, Q are in $R(G, C)$, $PQ = 0$ implies $QP = 0$.*

Suppose on the contrary that $PQ = 0$, $QP \neq 0$. Then $(QP)^2 = 0$, so that

$$(1-3QP)(1+3QP) = 1.$$

Since $QP \neq 0$, $1-3QP$ cannot be of the form $\pm e$, and is therefore a non-trivial unit.

THEOREM 10. *Let G be a group such that all the units in $R(G, C)$ are trivial. Then every cyclic sub-group of G of finite order is self-conjugate.*

Let e_1 generate a sub-group of order n, and let e_2 be any element in G. Let

$$P = e_2(1-e_1), \quad Q = 1+e_1+e_1^2+\ldots+e_1^{n-1}.$$

Then $PQ = 0$, so that, by Theorem 9, $QP = 0$. That is

$$e_2+e_1e_2+\ldots+e_1^{n-1}e_2 = e_2e_1+e_1e_2e_1+\ldots+e_1^{n-1}e_2e_1.$$

For some r, therefore,

$$e_2e_1 = e_1^r e_2, \quad i.e. \quad e_2e_1e_2^{-1} = e_1^r.$$

That is to say, the subgroup $e_2\{e_1\}e_2^{-1}$ coincides with $\{e_1\}$ and $\{e_1\}$ is self-conjugate.

THEOREM 11. *If all the elements of a group G have finite order, $R(G, C)$ has non-trivial units unless G is either*

(i) *an Abelian group the orders of whose elements all divide four;*

or (ii) *an Abelian group the orders of whose elements all divide six;*

or (iii) *the direct product of a quaternion group and an Abelian group the orders of whose elements all divide two.*

In these cases $R(G, C)$ has only trivial units.

Let G be a group whose elements all have finite order such that $R(G, C)$ has only trivial units. By Theorem 6, the orders of the elements of G can only be 2, 3, 4, or 6. If G is Abelian it must therefore be of type

(i) or (ii). If G is not Abelian, by Theorem 10, every cyclic subgroup of G is self-conjugate, and G is therefore Hamiltonian. It is known† that a finite Hamiltonian group is the direct product of a group of type (iii) and an Abelian group all of whose elements have odd order; and this theorem can easily be extended to cover groups all of whose elements have finite order‡. If, however, the second factor in this product were not the identity alone, G would contain an element of order $4p$, where p is an odd prime, which is impossible. Hence G is of type (iii).

Conversely, let G be a group of type (i), (ii), or (iii), and let E be a unit in $R(G, C)$, where

$$E = \lambda_1 e_1 + \ldots + \lambda_r e_r.$$

Then $e_1, \ldots, e_r$ generate a finite subgroup G' of G. G' is itself of one of the three given types, and E is a unit in $R(G', C)$. But all the units in $R(G', C)$ are trivial, by Theorem 6 if G' is Abelian, and by Theorems 7 and 8 if G' is not Abelian. Hence E is a trivial unit, and $R(G, C)$ has only trivial units.

4. *Infinite discrete groups.*

A group H is said to be indexed if we are given a homomorphism γ of H in the additive group of rational integers, such that $\gamma(H)$ does not consist of zero alone. In general, a group can be indexed in more than one way. If e is an element in H, $\gamma(e)$ will be called the degree of e (relative to γ). If K is any ring, an element in $R(H, K)$ which can be put in the form

$$P = m_1 e_{i_1} + m_2 e_{i_2} + \ldots + m_r e_{i_r},$$

† H. Hilton, *Finite groups* (Oxford, 1908), 178.

‡ Hilton's proof (*loc. cit.*) requires the following alterations:

(i) The theorem at the top of page 177 is replaced by:

There are no Hamiltonian groups the orders of all of whose elements are powers of p, if p is a prime greater than 2. If $p = 2$, a Hamiltonian group all of whose elements have orders a power of p is the direct product of a quaternion group, and a group all of whose elements other than the identity have order 2.

The proof is unchanged.

(ii) To show that a Hamiltonian group is the direct product of groups all the elements in any one of which have orders which are powers of the same prime, we need two observations. First, the commutator of two elements in a Hamiltonian group is a power of each of them. Elements having relatively prime orders therefore commute. Secondly, if two elements in a Hamiltonian group have orders p^α and p^β, the subgroup that they generate is isomorphic to a factor group of the group given by $X^{p^\alpha} = 1$, $Y^{p^\beta} = 1$, $XYX^{-1} = Y^r$, for some value of r, and the order of this group is $p^{\alpha+\beta}$. The elements of a Hamiltonian group having a power of p as order therefore form a group.

where $e_{i_1}, e_{i_2}, \ldots, e_{i_r}$ are all of degree α, will be called homogeneous of degree α. Any element P in $R(H, K)$ can be written in the form

$$P = P_{\alpha_1} + P_{\alpha_2} + \ldots + P_{\alpha_p}, \tag{4.1}$$

P_{α_i} homogeneous of degree α_i, $\alpha_1 < \alpha_2 < \ldots < \alpha_p$. Plainly, if $P = 0$, then, in any such expansion, $P_{\alpha_i} = 0$, $i = 1, \ldots, p$. If similarly

$$Q = Q_{\beta_1} + Q_{\beta_2} + \ldots + Q_{\beta_q}, \tag{4.2}$$

Q_{β_i} homogeneous of degree β_i, $\beta_1 < \beta_2 < \ldots < \beta_q$, then we have

$$PQ = P_{\alpha_1} Q_{\beta_1} + \ldots + P_{\alpha_p} Q_{\beta_q}, \tag{4.3}$$

where the unwritten terms have degrees exceeding the degree $\alpha_1 + \beta_1$ of $P_{\alpha_1} Q_{\beta_1}$ but less than the degree $\alpha_p + \beta_q$ of $P_{\alpha_p} Q_{\beta_q}$.

A group G is said to be indicable throughout if every subgroup of G not consisting of the identity alone can be indexed. Any free group can obviously be indexed, and any subgroup of a free group is either a free group or the identity alone†, so that any free group is indicable throughout. Similarly any free Abelian group is indicable throughout. In an Appendix to this paper we show that, if two groups are indicable throughout, so are their free product and their direct product.

THEOREM 12. *If G is indicable throughout and K has no zero-divisors, $R(G, K)$ has no zero-divisors.*

In other words we must show that, if

$$P = m_1 e_{i_1} + m_2 e_{i_2} + \ldots + m_r e_{i_r}, \quad Q = n_1 e_{j_1} + n_2 e_{j_2} + \ldots + n_s e_{j_s} \tag{4.4}$$

($r \geqslant 1$. $s \geqslant 1$; $m_{i_\lambda} \neq 0$, $n_{j_\lambda} \neq 0$; $e_{i_\lambda} \neq e_{i_\mu}$, $e_{j_\lambda} \neq e_{j_\mu}$, if $\lambda \neq \mu$) are elements of $R(H, K)$, then $P \cdot Q \neq 0$. Plainly it is sufficient to prove this assertion in the case $e_{i_1} = e_{j_1} = 1$. The proof is by induction on $r+s$. If $r = s = 1$ the assertion is true because K has no zero-divisors.

Suppose then that it is true for $r+s < n$ $(n > 2)$ and suppose that $r+s = n$. Then $e_{i_1}, \ldots, e_{i_r}, e_{j_1}, \ldots, e_{j_s}$ generate a subgroup H of G not consisting of the identity alone. H can therefore be indexed, and we can suppose P, Q, to be given by (4.1), (4.2), with none of $P_{\alpha_1}, P_{\alpha_p}, Q_{\beta_1}, Q_{\beta_q}$ zero. P and Q cannot both be homogeneous of degree zero, or we should have $\gamma(H) = 0$. But e_{i_1}, e_{j_1} are both of degree zero. Hence either $p > 1$ or $q > 1$. In either

† O. Schreier, "Die Untergruppen der freien Gruppen", *Abhandlungen aus dem Mathematischen Seminar des Hamburgischen Universität*, 5 (1927), 161–183.

case we have, $P_{\alpha_1} Q_{\beta_1} \neq 0$ by the hypothesis of the induction. By (4.3), therefore, $PQ \neq 0$.

THEOREM 13. *If G is indicable throughout and K has no zero-divisors, all the units of $R(G, K)$ are trivial.*

This is a corollary of the assertion: If P, Q are given by (4.4) with $r+s > 2$, then

$$PQ = p_1 e_{\kappa_1} + p_2 e_{\kappa_2} + \ldots + p_t e_{\kappa_t}$$

($p_\lambda \neq 0$, $e_{\kappa_\lambda} \neq e_{\kappa_\mu}$ if $\lambda \neq \mu$), and $t \geqslant 2$. As before, it is sufficient to prove the assertion when $e_{i_1} = e_{j_1} = 1$. Let H have the same meaning as in the proof of Theorem 12. Since $r+s > 2$, H does not consist of the identity alone. It can therefore be indexed and we can suppose P, Q to be given by (4.1), (4.2) with none of P_{α_1}, P_{α_p}, Q_{β_1}, Q_{β_q} zero. As in the proof of Theorem 12 we have either $p > 1$ or $q > 1$, and therefore $\alpha_1+\beta_1 \neq \alpha_p+\beta_q$. But, by Theorem 12, $P_{\alpha_1} Q_{\beta_1} \neq 0$, $P_{\alpha_p} Q_{\beta_q} \neq 0$. These, as we have seen, have different degrees, so that by (4.3) our assertion is true.

5. *Matrices.*

Let G be a group satisfying the following condition:

Given $a_1, a_2, \ldots, a_n$ in $R(G, C)$ such that the equation

$$\lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_n a_n = 1 \tag{5.1}$$

can be solved for $\lambda_1, \lambda_2, \ldots, \lambda_n$ in $R(G, C)$, then we can transform $a_1, a_2, \ldots, a_n$ into $1, 0, \ldots, 0$ by a sequence of transformations of the following types:

(5.2) (*a*) replacing a_i by $a_i + r a_j$ ($j \neq i$), r being an element in $R(G, C)$;

(*b*) replacing a_i by $\pm e a_i$, e being an element in G.

Then G satisfies the matrix condition of § 1. For we may take $a_1, a_2, \ldots, a_n$ to be the last column of any matrix with a left inverse whose elements are in $R(G, C)$. By (1.3), equation (5.1) can then be solved. We can therefore reduce the last column of the matrix to the form $0, 0, \ldots, 0, 1$, by a manipulation of rows according to transformations (1.2). Hence the order of the matrix can be reduced, and by repeating the process we eventually arrive at the matrix $\|1\|$.

THEOREM 14. *The above condition is satisfied by the cyclic groups of orders two, three, and four, and by the direct product of two cyclic groups of order two.*

We shall prove the theorem for the cyclic group of order four. The other cases are similar.

Let G be generated by e, with $e^4 = 1$, and let $a_1, a_2, \ldots, a_n$ be elements in $R(G, C)$ such that (5.1) can be solved. The correspondence $e \to i$ is a homomorphism of $R(G, C)$ on the ring of Gaussian integers. In this ring there is an algorithm†; any sequence $\rho_1, \rho_2, \ldots, \rho_n$ can be reduced to the form $\sigma, 0, \ldots, 0$ by a sequence of transformations of the following types:

(5.3) (*a*) replacing $\rho_j + r\rho_k$ $(j \neq k)$, r being a Gaussian integer;

(*b*) replacing ρ_j by $-\rho_i$ or by $\pm i\rho_j$.

Let $\rho_1, \ldots, \rho_n$ be the images of $a_1, \ldots, a_n$ in the homomorphism. Any transformation (5.3) on $\rho_1, \ldots, \rho_n$ can be induced by an appropriate transformation (5.2) on $a_1, \ldots, a_n$. This sequence can therefore be transformed by means of transformations (5.2) into a sequence of the form:

$$a_1' = a_1' + \beta_1' e + \gamma_1' e^2 + \delta_1' e^3, \quad a_2' = (a_2' + \beta_2' e)(1+e^2),$$

$$\ldots, \quad a_n' = (a_n' + \beta_n' e)(1+e^2).$$

Using in a similar way the homomorphism $e \to -1$ of $R(G, C)$ on the ring of integers, we transform this sequence in turn into one of the form:

$$a_1'' = a_1'' + \beta_1'' e + \gamma_1'' e^2 + \delta_1'' e^3, \quad a_2'' = (a_2'' + \beta_2'' e)(1+e^2),$$

$$a_3'' = a_3''(1+e)(1+e^2), \quad \ldots, \quad a_n'' = a_n'(1+e)(1+e^2);$$

and this can itself be transformed into a sequence of the form:

$$(5.4) \quad a_1''' = a_1''' + \beta_1''' e + \gamma_1''' e^2 + \delta_1''' e^3, \quad a_2''' = (a_2''' + \beta_2''' e)(1+e^2),$$

$$a_3''' = a_3'''(1+e)(1+e^2), \quad a_4''' = \ldots a_n''' = 0.$$

Now let us call a transformation (5.2*a*), or the resultant of a sequence of such transformations, admissible if, when it is applied to (5.4), the result is of the same form:

$$(5.5) \quad a_1^{(\mathrm{iv})} = a_1^{(\mathrm{iv})} + \beta_1^{(\mathrm{iv})} e + \gamma_1^{(\mathrm{iv})} e^2 + \delta_1^{(\mathrm{iv})} e^3, \quad a_2^{(\mathrm{iv})} = (a_2^{(\mathrm{iv})} + \beta_2^{(\mathrm{iv})} e)(1+e^2),$$

$$a_3^{(\mathrm{iv})} = a_3^{(\mathrm{iv})}(1+e)(1+e^2), \quad a_4^{(\mathrm{iv})} = \ldots = a_n^{(\mathrm{iv})} = 0.$$

† van der Waerden, *loc. cit.*, '62.

Consider now the functions

$$\phi_1 = \alpha_1''' + \beta_1''' + \gamma_1''' + \delta_1''', \quad \phi_2 = \alpha_2''' + \beta_2''', \quad \phi_3 = \alpha_3'''.$$

An admissible transformation (5.2a) alters at most one of them. Hence an admissible sequence of transformations such that, when the transformations of the sequence are applied successively to (5.4), at each stage one of $|\phi_1|$, $|\phi_2|$, $|\phi_3|$ is reduced, must be of finite length. Suppose now that (5.5) represents the result of applying such a sequence of maximal length to (5.4). Then no admissible transformation applied to (5.5) reduces the absolute value of any of the corresponding functions

$$\phi_1 = \alpha_1^{(\mathrm{iv})} + \beta_1^{(\mathrm{iv})} + \gamma_1^{(\mathrm{iv})} + \delta_1^{(\mathrm{iv})}, \quad \phi_2 = \alpha_2^{(\mathrm{iv})} + \beta_2^{(\mathrm{iv})}, \quad \phi_3 = \alpha_3^{(\mathrm{iv})}.$$

But the transformation $a_3^{(\mathrm{iv})} \to a_3^{(\mathrm{iv})} + m(1+e^2)(1+e)\,a_1^{(\mathrm{iv})}$ leaves $a_1^{(\mathrm{iv})}$ and $a_2^{(\mathrm{iv})}$ unaltered, and carries $a_3^{(\mathrm{iv})}$ into $(a_3^{(\mathrm{iv})} + 4m\phi_1)(1+e)(1+e^2)$. It is therefore an admissible transformation, and changes ϕ_3 into $\phi_3 + 4m\phi_1$. Hence, for all integral values of m, we have $|\phi_3 + 4m\phi_1| \geqslant |\phi_3|$. Therefore either $\phi_1 = 0$ or $2|\phi_3| \leqslant |\phi_1|$. Similarly, either $\phi_3 = 0$ or $|\phi_1| \leqslant 2|\phi_3|$. That is to say, either $\phi_1 = 0$, $\phi_3 = 0$ or $|\phi_1| = 2|\phi_3|$. But the equation in $a_i^{(\mathrm{iv})}$ corresponding to (5.1) is soluble for λ_i in $R(G, C)$. Hence, putting $e = 1$, we have, for some integral values of μ_1, μ_2, μ_3,

$$\mu_1\phi_1 + 2\mu_2\phi_2 + 4\mu_3\phi_3 = 1.$$

Hence $\phi_1 \neq 0$, $|\phi_1| \neq 2|\phi_3|$. Therefore $\phi_3 = 0$. Similarly, $\phi_2 = 0$, so that

$$a_1^{(\mathrm{iv})} = \alpha_1^{(\mathrm{iv})} + \beta_1^{(\mathrm{iv})}e + \gamma_1^{(\mathrm{iv})}e^2 + \delta_1^{(\mathrm{iv})}e^3,$$

$$a_2^{(\mathrm{iv})} = \alpha_2^{(\mathrm{iv})}(1-e)(1+e^2), \quad a_3^{(\mathrm{iv})} = \ldots = a_n^{(\mathrm{iv})} = 0.$$

Treating similarly the functions $\psi_1 = \alpha_1^{(\mathrm{iv})} - \beta_1^{(\mathrm{iv})} + \gamma_1^{(\mathrm{iv})} - \delta_1^{(\mathrm{iv})}$, $\psi_2 = \alpha_2^{(\mathrm{iv})}$, we can reduce this to the form $a^{(\mathrm{v})}$, 0, ..., 0. The theorem now follows, since all the units in $R(G, C)$ are trivial.

THEOREM 15. *The matrix condition of* § 1 *holds for the free cyclic group.*

Let $\|a_{ij}\|$ be a matrix whose elements are in $R(G, C)$, where G is the free cyclic group generated by x. Obviously we can transform $\|a_{ij}\|$ by means of transformations (1.2) so that it contains only positive powers of x. Moreover we can transform it so that it contains no power of x higher than the first. For let x^n, $n > 1$, be the highest power of x in $\|a_{ij}\|$, and

let $a_{ij} = p_{ij}x^n + q_{ij}$, where q_{ij} contains no power higher than the $(n-1)$-th, and p_{ij} is an integer. Then we have

$$\|p_{ij}x^n+q_{ij}\| \to \left\| \begin{array}{c|c} p_{ij}x^n+q_{ij} & 0 \\ \hline 0 & \delta_{ij} \end{array} \right\| \to \left\| \begin{array}{c|c} p_{ij}x^n+q_{ij} & \delta_{ij}x \\ \hline 0 & \delta_{ij} \end{array} \right\|$$

$$\to \left\| \begin{array}{c|c} q_{ij} & \delta_{ij}x \\ \hline -p_{ij}x^{n-1} & \delta_{ij} \end{array} \right\|,$$

and the assertion follows by induction on n.

Suppose, therefore, that $a_{ij} = b_{ij} + c_{ij}x$, where b_{ij} and c_{ij} are integers. Since the ordinary elementary transformations on integer matrices† are a particular case of transformations (1.2), we may suppose either that $\|b_{ij}\|$ or that $\|c_{ij}\|$ has diagonal form. But if $\|a_{ij}\|$ has an inverse, the determinant $|a_{ij}|$ has the value $\pm x^p$, so that at least one of $|b_{ij}|$, $|c_{ij}|$ is zero. If $|b_{ij}|$ is zero suppose that $\|b_{ij}\|$ is reduced to diagonal form; otherwise suppose that $\|c_{ij}\|$ is reduced to diagonal form. Then some column of $\|a_{ij}\|$, which we may take to be the last, consists either entirely of integers or entirely of integer multiples of x. In the latter case multiply it by x^{-1}. By a further manipulation of rows, this column can be made to take the form

$$(0, 0, \ldots, 0, \lambda),$$

where, since $\|a_{ij}\|$ has an inverse, $\lambda = \pm 1$. Hence the order of the matrix can be reduced without destroying its linearity. By an induction on order the theorem follows.

Appendix.

The purpose of this appendix is to show that, if two groups are indicable throughout, so are their direct product and their free product.

LEMMA. *If a self-conjugate subgroup H of a group G and the corresponding factor group G/H are both indicable throughout, then G is indicable throughout.*

Let K be a subgroup of G not consisting of the identity alone. If K is contained in H, it can be indexed, since H is indicable throughout. If,

† See, for instance, those given by M. Bôcher, *Introduction to higher algebra* (New York, 1907), 268, ex. 2. The interchange of two rows, or columns, can be brought about thus: $(a, b) \to (a, a+b) \to (-b, a+b) \to (-b, a) \to (b, a)$, so that this type of transformation is superfluous.

however, K is not contained in H, let D be the intersection of K and H. Then D is a self-conjugate subgroup of K, and the factor group K/D is isomorphic to a subgroup of G/H not consisting of the identity alone†. It can, therefore, be indexed. We can, therefore, index K by giving each of its elements the degree of the element of K/D containing it.

THEOREM 1. *If two groups are indicable throughout, their direct product is indicable throughout.*

For the direct product $G \times H$ of two groups G and H, contains a self-conjugate subgroup isomorphic to G, whose factor group is isomorphic to H.

THEOREM 2. *If two groups are indicable throughout, their free product is indicable throughout.*

An element in the free product $G \circ H$ of two groups G and H can be written in the form

$$\gamma = g_1 h_1 g_2 h_2 \dots g_r h_r \quad (r \geqslant 1,\ g_i \epsilon G,\ h_i \epsilon H,\ i = 1, 2, \dots, r). \tag{1}$$

Consider the self-conjugate subgroup U consisting of those elements for which

$$g_1 g_2 \dots g_r = 1; \quad h_1 h_2 \dots h_r = 1. \tag{2}$$

The factor group $(G \circ H)/U$ is isomorphic to the direct product $G \times H$ of G and H. Theorem 2 therefore follows from the lemma when we have proved the following theorem.

THEOREM 3. *The subgroup U of the free product $G \circ H$ of two groups G and H, defined as above, is a free group freely generated by the commutators $(g, h) = ghg^{-1}h^{-1}$, where g, h cover independently all elements other than the identity in G, H respectively.*

We have, identically, as can easily be shown by induction on r,

$$g_1 h_1 g_2 h_2 \dots g_r h_r$$
$$= \left\{ \prod_{i=1}^{r-1} (g_1 g_2 \dots g_i,\ h_1 h_2 \dots h_i)(g_1 g_2 \dots g_{i+1},\ h_1 h_2 \dots h_i)^{-1} \right\} g_1 g_2 \dots g_r h_1 h_2 \dots h_r.$$

Omitting on the right any commutators in which either term is 1, and the factor $g_1 g_2 \dots g_r h_1 h_2 \dots h_r$, we obtain an expression for γ, given by (1) and

† Speiser, *loc. cit.*, 36 (Theorem 25). Speiser's proof in no way depends on the fact that he is dealing with finite groups.

satisfying (2), in terms of the commutators (g, h), $g \in G$, $h \in H$, $g \neq 1$, $h \neq 1$. These commutators do therefore generate U.

To prove that U is the free group in these generators, we must show that if the expression

$$\delta = (a_1, b_1)^{\eta_1} (a_2, b_2)^{\eta_2} \dots (a_q, b_q)^{\eta_q} \tag{3}$$

$$(a_i \in G,\ b_i \in H,\ a_i \neq 1,\ b_i \neq 1,\ \eta_i = \pm 1,\ i = 1, 2, \dots, q)$$

is equal to 1, then for some value of i

$$a_i = a_{i+1},\quad b_i = b_{i+1},\quad \eta_i + \eta_{i+1} = 0. \tag{4}$$

Now if an element δ of $G \circ H$ can be written as $x_1 x_2 \dots x_p$ $(p \geqslant 1)$, where x_i is an element of G or H, $x_i \neq 1$, and no two consecutive elements x_i, x_{i+1} are in the same group G or H, then $\delta \neq 1$. It is sufficient therefore to show that if δ is given by (3) with (4) false for $i = 1, \dots, q-1$, then δ can be put in this form with $x_1 = a_1$, $x_2 = b_1$, or $x_1 = b_1$, $x_2 = a_1$, according as $\eta_1 = 1$ or $\eta_1 = -1$. This is certainly true for $q = 1$, and will be proved by induction on q. Since the rôles of G and H are identical there is no loss of generality in supposing that $\eta_1 = 1$. The element $(a_2, b_2)^{\eta_2} (a_3, b_3)^{\eta_3} \dots (a_q, b_q)^{\eta_q}$, by the hypothesis of the induction, can be written in the form $a_2 b_2 X$ or in the form $b_2 a_2 X$ according as $\eta_2 = 1$ or $\eta_2 = -1$. In the former case, $\delta = a_1 b_1 a_1^{-1} b_1^{-1} a_2 b_2 X$. In the latter, if $b_1 \neq b_2$, $\delta = a_1 b_1 a_1^{-1} b_1^{-1} b_2 a_2 X$, and if $b_1 = b_2$, $\delta = a_1 b_1 a_1^{-1} a_2 X$. We cannot also have $a_1 = a_2$, since (4) is false for $i = 1$. In all cases δ is reduced to the desired form.

Balliol College,
Oxford.