APPENDIX II.

On Matrices*.

405. A set of n quantities

$$(x_1, \ldots, x_n)$$

is often denoted by a single letter x, which is then called a *row letter*, or a column letter. By the sum (or difference) of two such rows, of the same number of elements, is then meant the row whose elements are the sums (or differences) of the corresponding elements of the constituent rows. If m be a single quantity, the row letter mx denotes the row whose elements are $mx_1, \ldots, mx_n$. If x, y be rows, each of n quantities, the symbol xy denotes the quantity $x_1y_1 + \ldots\ldots + x_ny_n$.

406. The set of n equations denoted by

$$x_i = a_{i,1}\xi_1 + \ldots\ldots + a_{i,p}\xi_p, \qquad (i = 1, \ldots\ldots, n)$$

where n may be greater or less than p, can be represented in the form $x = a\xi$, where a denotes a rectangular block of np quantities, consisting of n rows each of p quantities, the r-th quantity of the i-th row being $a_{i,r}$. Such a block of quantities is called a *matrix*; we call $a_{i,r}$ the (i, r)th element of the matrix. The sum (or difference) of two matrices, of the same number of rows and columns, is the matrix formed by adding (or subtracting) the corresponding elements of the component matrices. Two matrices are equal only when all their elements are equal; a matrix vanishes only when all its elements are zero. If $\xi_1, \ldots, \xi_p$ be expressible by m quantities $X_1, \ldots, X_m$ by the equations

$$\xi_r = b_{r,1}X_1 + \ldots\ldots + b_{r,m}X_m, \qquad (r = 1, 2, \ldots\ldots, p),$$

so that $\xi = bX$, where b is a matrix of p rows and m columns, then we have

$$x_i = c_{i,1}X_1 + \ldots\ldots + c_{i,m}X_m, \qquad (i = 1, \ldots\ldots, n),$$

or $x = cX$, where

$$c_{i,s} = a_{i,1}b_{1,s} + \ldots\ldots + a_{i,p}b_{p,s}, \qquad \begin{pmatrix} i = 1, \ldots\ldots, n \\ s = 1, \ldots\ldots, m \end{pmatrix},$$

* The literature of the theory of matrices, or, under a slightly different aspect, the theory of bilinear forms, is very wide. The following references may be given: Cayley, *Phil. Trans.* 1858, or *Collected Works*, vol. II. (1889), p. 475; Cayley, *Crelle*, L. (1855); Hermite, *Crelle*, XLVII. (1854); Christoffel, *Crelle*, LXIII. (1864) and LXVIII. (1868); Kronecker, *Crelle*, LXVIII. (1868) or *Gesam. Werke*, Bd. I. (1895), p. 143; Schläfli, *Crelle*, LXV. (1866); Hermite, *Crelle*, LXXVIII. (1874); Rosanes, *Crelle*, LXXX. (1875); Bachmann, *Crelle*, LXXVI. (1873); Kronecker, *Berl. Monatsber.*, 1874; Stickelberger, *Crelle*, LXXXVI. (1879); Frobenius, *Crelle*, LXXXIV. (1878), LXXXVI. (1879), LXXXVIII. (1880); H. J. S. Smith, *Phil. Trans.*, CLI. (1861), also, *Proc. Lond. Math. Soc.*, 1873, pp. 236, 241; Laguerre, *J. d. l'éc. Poly.*, t. XXV., cah. XLII. (1867), p. 215; Stickelberger, *Progr. poly. Schule, Zürich*, 1877; Weierstrass, *Berl. Monats.* 1858, 1868; Brioschi, *Liouville*, XIX. (1854); Jordan, *Compt. Rendus*, 1871, p. 787, and *Liouville*, 1874, p. 35; Darboux, *Liouville*, 1874, p. 347.

$c_{i,s}$ being the (i, s)th element of a matrix of n rows and m columns; it arises from the equations $x=a\xi$, $\xi=bX$, whereof the result may be written $x=abX$; hence we may formulate the rule: *A matrix* a *may be multiplied into another matrix* b *provided the number of columns of* a *be the same as the number of rows of* b; *the* (i, s)*th element of the resulting matrix is the result of multiplying*, in accordance with the rule given above, *the* i-*th row of* a *by the* s-*th column of* b. Thus, for multiplication, matrices are not generally commutative, but, as is easy to see, they are associative.

The matrix whose (i, s)th element is $c_{s,i}$, where $c_{s,i}$ is the (s, i)th element of any matrix c of n rows and m columns, is called the transposed matrix of c, and may be denoted by $\bar{c}$; it has m rows and n columns, and, briefly, is obtained by interchanging the rows and columns of c. The matrix which is the transposed of a product of matrices is obtained by taking the factor matrices in the reverse order, each transposed; for example, if a, b, c be matrices,

$$\overline{abc}=\bar{c}\bar{b}\bar{a}.$$

407. The matrices which most commonly occur are square matrices, having an equal number of rows and columns. With such a matrix is associated a determinant, whose elements are the elements of the matrix. When the determinant of a matrix, a, of p rows and columns, does not vanish, the p linear equations expressed by $x=a\xi$ enable us to represent the quantities $\xi_1, \dots, \xi_p$ in terms of $x_1, \dots, x_p$; the result is written $\xi=a^{-1}x$, and a^{-1} is called the inverse matrix of a; the (i, r)th element of a^{-1} is the minor of $a_{r,i}$ in the determinant of the matrix a, divided by this determinant itself. The inverse of a product of square matrices is obtained by taking the inverses of the factor matrices in reverse order; for example, if a, b, c be square matrices, of the same number of rows and columns, for each of which the determinant is not zero, we have

$$(abc)^{-1}=c^{-1}b^{-1}a^{-1}.$$

The inverse of the transposed of a matrix is the transposed of its inverse; thus

$$(\bar{a})^{-1}=(\overline{a^{-1}}).$$

The determinant of a matrix a being represented by $|a|$, we clearly have $|ab|=|a|\,|b|$.

408. Finally, the following results are of frequent application in this volume: (i) If a be a matrix of n rows and p columns, and ξ a row of p quantities, the symbol $a\xi$ denotes a row of n quantities; if η be a row of n quantities, the product of these two rows, or $(a\xi)(\eta)$, is denoted by $a\xi\eta$. When $n=p$ this must be distinguished from the matrix which would be denoted by $a\,.\,\xi\eta$—this latter never occurs. We have then

$$a\xi\eta=\sum_{i=1}^{n}\sum_{r=1}^{p} a_{i,r}\,\xi_r\,\eta_i,$$

and this is called a bilinear form; we also clearly have the noticeable equation

$$a\xi\eta=\bar{a}\eta\xi\,;$$

(ii) if b be a matrix of n rows and q columns, the product of the two rows $a\xi$, $b\eta$, wherein η is now a row of q quantities, is given by either $(\bar{b}a)\,\xi\eta$ or $(\bar{a}b)\,\eta\xi$, so that we have

$$a\xi\,.\,b\eta=\bar{b}a\xi\eta=\bar{a}b\eta\xi.$$

The result of multiplying any square matrix, of p rows and columns, by the matrix E, of p rows and columns, wherein all the elements are zero except the diagonal elements, which are each unity, is to leave the multiplied matrix unaltered. For this reason the matrix E is often denoted simply by 1, and called the matrix unity of p rows and columns.

409. *Ex.* i. If a bilinear form axy, wherein x, y are rows of p quantities, and a is a square matrix of p rows and columns, be transformed into itself by the linear substitution $x=R\xi$, $y=S\eta$, where R, S are matrices of p rows and columns, then $aR\xi\,.\,S\eta=a\xi\eta$; hence

$$\bar{S}aR=a.$$

Ex. ii. If h be an arbitrary matrix of p rows and columns, such that the determinants of the matrices $a\pm h$ do not vanish, and the determinant of the matrix a do not vanish, prove that

$$(a+h)\,a^{-1}\,(a-h)=a-ha^{-1}\,h=(a-h)\,a^{-1}\,(a+h)\,;$$

hence shew that if

$$R=a^{-1}\,(a-h)\,(a+h)^{-1}\,a, \quad \bar{S}=a\,(a-h)^{-1}\,(a+h)\,a^{-1},$$

the substitutions $x=R\xi$, $y=S\eta$ transform axy into $a\xi\eta$.

For a substitution in which $R=S$ see Cayley, *Collected Works*, vol. II. p. 505. Cf. also Taber, *Amer. Journ.*, vol. XVI. (1894) and *Proc. Lond. Math. Soc.*, vol. XXVI. (1895).

Ex. iii. The matrices, of two rows and columns,

$$E=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \quad J=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},$$

give $E^2=E$, $J^2=-E$; and the determinant of the matrix

$$xE+yJ=\begin{pmatrix}x, & -y\\ y, & x\end{pmatrix}$$

vanishes, for real values of x, y, only when $x=0$, $y=0$.

Ex. iv. The matrices, of four rows and columns,

$$e=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}, \quad j_1=\begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&-1\\0&0&1&0\end{pmatrix}, \quad j_2=\begin{pmatrix}0&0&1&0\\0&0&0&1\\-1&0&0&0\\0&-1&0&0\end{pmatrix}, \quad j_3=\begin{pmatrix}0&0&0&1\\0&0&-1&0\\0&1&0&0\\-1&0&0&0\end{pmatrix},$$

give $j_1^2=j_2^2=j_3^2=-e$, $j_2j_3=-j_3j_2=j_1$, $j_3j_1=-j_1j_3=j_2$, $j_1j_2=-j_2j_1=j_3$, $j_1j_2j_3=-e$.

Hence these matrices obey the laws of the fundamental unities of the quaternion analysis. Further the determinant of the matrix

$$ex+j_1x_1+j_2x_2+j_3x_3=\begin{vmatrix}x & x_1 & x_2 & x_3\\ -x_1 & x & -x_3 & x_2\\ -x_2 & x_3 & x & -x_1\\ -x_3 & -x_2 & x_1 & x\end{vmatrix}$$

which is equal to $(x^2+x_1^2+x_2^2+x_3^2)^2$, vanishes, for real values of x, x_1, x_2, x_3, only when each of x, x_1, x_2, x_3 is zero. (Frobenius, *Crelle*, LXXXIV. (1878), p. 62.)

410. In the course of this volume we are often concerned with matrices of $2p$ rows and $2p$ columns. Such a matrix may be represented in the form

$$\mu=\begin{pmatrix}a & b\\ c & d\end{pmatrix},$$

wherein a, b, c, d are square matrices with p rows and columns; if μ' be another such matrix given by

$$\mu'=\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}$$

the (i, r)th element of the product $\mu'\mu$, when i and r are both less than $p+1$ is

$$a'_{i,1}\, a_{1,r} + \ldots\ldots + a'_{i,p}\, a_{p,r} + b'_{i,1}\, c_{1,r} + \ldots\ldots + b'_{i,p}\, c_{p,r},$$

and this is the sum of the (i, r)th elements of the matrices $a'a$, $b'c$; similarly when i and r are not both less than $p+1$; hence we may write

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a'a+b'c, & a'b+b'd \\ c'a+d'c, & c'b+d'd \end{pmatrix},$$

the law of formation for the product matrix being the same as if $a, b, c, d, a', b', c', d'$ were single quantities.

Ex. Denoting the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ respectively by 1 and j, the matrices of Ex. iv. can be denoted by

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad j_1 = \begin{pmatrix} -j & 0 \\ 0 & j \end{pmatrix}, \quad j_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad j_3 = \begin{pmatrix} 0 & -j \\ -j & 0 \end{pmatrix}.$$

411. We proceed now to prove the proposition* assumed in § 333, Chap. XVIII. Retaining the definitions of the matrices A_k, B, C, D there given, and denoting A_k^{-1}, B^{-1}, C^{-1}, D^{-1} respectively by a_k, b, c, d, we find

$$a_k = A_k, \text{ so that } A_k{}^2 = 1,$$

and

$$b = \begin{pmatrix} 0 & & & & 1 & & & \\ & 1 & & & & 0 & & \\ & & 1 & & & & 0 & \\ & & & 1 & & & & 0 \\ -1 & & & & 0 & & & \\ & 0 & & & & 1 & & \\ & & 0 & & & & 1 & \\ & & & 0 & & & & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & & & & 1 & & & \\ & 1 & & & & 0 & & \\ & & 1 & & & & 0 & \\ & & & 1 & & & & 0 \\ 0 & & & & 1 & & & \\ & 0 & & & & 1 & & \\ & & 0 & & & & 1 & \\ & & & 0 & & & & 1 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & & & & 0 & 1 & & \\ & 1 & & & 1 & 0 & & \\ & & 1 & & & & 0 & \\ & & & 1 & & & & 0 \\ 0 & & & & 1 & & & \\ & 0 & & & & 1 & & \\ & & 0 & & & & 1 & \\ & & & 0 & & & & 1 \end{pmatrix}$$

so that b, c, d differ respectively from B, C, D only in the change of the sign of the elements which are not in the diagonal. It is easy moreover to verify such facts as the following

$$B^4 = 1, \quad (BC)^3 = 1, \quad DA_2 = A_2 D, \quad A_k B A_k B = B A_k B A_k, \quad B^2 D B^2 A_2 = A_2 B^2 D B^2,$$

which are equivalent respectively with

$$b^4 = 1, \ (cb)^3 = 1, \ a_2 d = d a_2, \ b a_k b a_k = a_k b a_k b, \ a_2 b^2 d b^2 = b^2 d b^2 a_2;$$

but such results are immediately obvious from the interpretations of the matrices a_k, b, c, d which are now to be given.

Let Δ denote any matrix of $2p$ rows and columns, and let the four products

$$\Delta a_k, \quad \Delta b, \quad \Delta c, \quad \Delta d$$

* For a shorter proof of an equivalent result the reader may consult C. Jordan, *Traité des Substitutions* (Paris, 1870), p. 174. The theorem was first given by Kronecker, "Ueber bilineare Formen," *Monatsber. Berl. Akad.* 1866, *Crelle*, LXVIII. or in *Werke* (Leipzig, 1895), Bd. I. p. 160; the proof here given follows the lines there indicated.

be formed; the resulting matrices will differ from Δ in respects which are specified in the following statements:

(i) a_k interchanges the first and k-th columns (of Δ), and, at the same time, the $(p+1)$th and $(p+k)$th columns $(1<k<p+1)$. For the sake of uniformity we introduce also $a_1, =1$.

(ii) b interchanges the first and $(p+1)$th columns, at the same time changing the signs of the elements of the new first column.

(iii) c adds the first column to the $(p+1)$th.

(iv) d adds the first and second columns respectively to the $(p+2)$th and the $(p+1)$th.

Hence we have these results: if the matrices denoted by the following symbols be placed at the right side of any matrix Δ, of $2p$ rows and columns, so that the matrix Δ acts upon them, the results mentioned will accrue:—

$l_k=a_kb^2a_k$, changes the signs of the k-th and $(p+k)$th columns (of Δ),

$t_k=a_kb\,a_k$, interchanges the k-th and $(p+k)$th columns (of Δ), giving the new k-th column an opposite sign to that it had before its change of place,

$t'_k=a_kb^3a_k$, interchanges the k-th and $(p+k)$th columns, giving the new $(p+k)$th column a changed sign.

$m_k=a_kb^2cb^2a_k$, adds the k-th column to the $(p+k)$th.

$m'_k=a_kb^3cbcb^3a_k=a_kb^2c^{-1}b^2a_k$, subtracts the k-th column from the $(p+k)$th.

$n_k=a_kb^2cbca_k=a_kbc^{-1}b^3a_k$, adds the $(p+k)$th column to the k-th.

$n'_k=a_kb^3cba_k$, subtracts the $(p+k)$th column from the k-th.

$g_{r,s}=a_ra_2a_sa_2b^3dba_2a_sa_2a_r$, subtracts the s-th column from the r-th, and, at the same time, adds the $(p+r)$th column to the $(p+s)$th.

$g'_{r,s}=a_ra_2a_sa_2bdb^3a_2a_sa_2a_r$, adds the s-th column to the r-th, and, at the same time, subtracts the $(p+r)$th from the $(p+s)$th column.

$f_{r,s}=t_sg_{r,s}t'_s$, adds the $(p+r)$th and $(p+s)$th columns respectively to the s-th and r-th columns.

$f'_{r,s}=t_sg'_{r,s}t'_s$, subtracts the $(p+r)$th and $(p+s)$th columns respectively from the s-th and r-th columns.

To this list we add the matrix a_k, whose effect has been described, and the matrix b^2, which changes the sign both of the first and of the $(p+1)$th columns; then it is to be shewn that a product, P, of positive integral powers of these matrices, can be chosen such that, if Δ be any Abelian matrix of integers, given by

$$\Delta=\begin{pmatrix}\alpha & \beta\\ \alpha' & \beta'\end{pmatrix},\ \text{where } \alpha\bar\beta=\beta\bar\alpha,\ \alpha'\bar\beta'=\beta'\bar\alpha',\ \alpha\bar\beta'-\beta\bar\alpha'=1,$$

the product ΔP is the matrix unity—of which every element is zero except those in the diagonal, each of which is 1. Hence it will follow that $\mu=P^{-1}$; namely that every such Abelian matrix can be written as a product of positive integral powers of the matrices A_k, B, C, D. Up to a certain point of the proof we shall suppose the matrix Δ to be that for a transformation of any order, r.

In the matrices a_k, a_r, a_s, each of k, r, s is to be $<p+1$; and in general each of k, r, s is >1; but for the sake of uniformity it is convenient, as already stated, to introduce a matrix $a_1=1$; then each of k, r, s may have any positive value less than $p+1$.

412. Of the matrix Δ we consider first the first row, and of this row we begin with the p-th and $2p$-th elements, $a_{1,p}$, $\beta_{1,p}$; if the numerically greater of these elements be not a positive integer, use the matrix l_p to make it positive*—form, that is, the product Δl_p. Then, let γ be the greater, and δ the less of these two elements; if δ is positive, use the matrix m'_p or the matrix n'_p, as many times as possible, to subtract from γ the greatest possible multiple† of δ (i.e. if ν be the matrix upon which we are operating, $=\Delta$ or $=\Delta l_p$, form one of the products $\nu(m'_p)^r$, $\nu(n'_p)^s$); if δ is negative, use m_p or n_p to add to γ the greatest possible multiple of δ; so that, in either case, the remainder, γ', from γ, is numerically less than δ and positive. Now, by the matrix l_p, take the element δ to be positive‡; then again, by application of m_p or n_p or m'_p or n'_p replace δ by a positive quantity numerically less than γ'. Let this process alternately acting on the remainder from γ and δ, be continued until either γ or δ is replaced by zero. Then use the matrix t_p or t'_p to put this zero element at the $2p$-th place of the first row of the matrix, Δ', which, after all these changes, replaces Δ.

Let a similar process of alternate reduction and transposition be applied to Δ', until the $(1, 2p-1)$th element of the resulting matrix is zero. And so on. Eventually we arrive, in continuing the operation, at a matrix instead of Δ, in which there is a zero in each of the places formerly occupied by $\beta_{1,1}, \ldots\ldots, \beta_{1,p}$.

Now apply the processes given by b^2, l_p, $g_{1,p}$, $g_{p,1}$, and eventually a_p, if necessary, to reduce the $(1, p)$th element to zero. Then the processes b^2, l_{p-1}, $g_{1,p-1}$, $g_{p-1,1}$, a_{p-1}, as far as necessary, to reduce the $(1, p-1)$th element to zero; and so on, till the places, which in the original matrix were occupied by $a_{1,2}, \ldots, a_{1,p}$, are all filled by zeros.

Consider now the second row of the modified matrix. Beginning with the $(2, p)$th and $(2, 2p)$th elements, use the specified processes to replace the latter by a zero. Next replace, similarly, the $(2, 2p-1)$th element by a zero; and so on, finally replacing the $(2, p+2)$th element by a zero. The necessary processes will not affect the fact that all the elements in the first row, except the $(1, 1)$th element, are zero. Next reduce the elements occupying the $(2, p)$th, ..., $(2, 3)$th places to zero.

Proceeding thus we eventually have (i) the $(r, s+p)$th element zero, for every $r<p$ and every $s<p$, in which $s \geqq r$, (ii) the (r, s)th element zero, for every $r<p$ and every $s<p$, in which $s>r$. In other words the matrix has a form which may be represented, taking $p=4$, by the matrix ρ,

$$\rho = \left(\begin{array}{cccccccc} a_{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 & \beta_{21} & 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} & 0 & \beta_{31} & \beta_{32} & 0 & 0 \\ a_{41} & a_{42} & a_{43} & a_{44} & \beta_{41} & \beta_{42} & \beta_{43} & 0 \\ a'_{11} & a'_{12} & a'_{13} & a'_{14} & \beta'_{11} & \beta'_{12} & \beta'_{13} & \beta'_{14} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a'_{41} & a'_{42} & a'_{43} & a'_{44} & \beta'_{41} & \beta'_{42} & \beta'_{43} & \beta'_{44} \end{array}\right);$$

since now the original matrix is an Abelian matrix, and each of the matrices a_k, b, c, d is an Abelian matrix, it follows (Chap. XVIII., § 324) that $a\bar{\beta}=\beta\bar{a}$; if the original matrix be

* The changes of sign of the other elements of the same column which enter therewith do not concern us.

† The simultaneous subtractions, effected by the matrix m'_p, of the other elements of the column, do not concern us. Similar remarks apply to following cases.

‡ It is not absolutely necessary to use the matrix l_p in this or in the former case; but it conduces to clearness.

for greater generality supposed primarily to be associated with a transformation of order r, the value $r=1$ being introduced later, the determinant of the matrix is $\pm r^p$ (§ 324, Ex. i.) and is not zero; hence comparing in turn the 1st, 2nd, ..., rows of the matrices $a\bar{\beta}$ and $\beta\bar{a}$ we deduce that in the matrix ρ the elements $\beta_{21}, \beta_{31}, \beta_{32}, \ldots$ of the matrix β which are on the left side of the diagonal are also zero; thus, in ρ, every element of the matrix β is zero. Apply now to the matrix ρ the relation

$$a\bar{\beta}' - \beta\bar{a}' = r,$$

which in this case reduces to $a\bar{\beta}' = r$. Then it is immediately found that the elements of the matrix β' which are on the left side of the diagonal are also zero—and also that

$$a_{11}\beta'_{11} = \ldots\ldots = a_{pp}\beta'_{pp} = r.$$

The resulting form of the matrix ρ may then be shortly represented by

$\sigma =$ 

If now to the matrix σ we apply the processes given by the matrices $g_{1,2}$ or $g'_{1,2}$ and l_2, we may suppose a_{21} numerically less than a_{22}, and a_{22} positive; if then we apply the processes given by the matrices $g_{1,3}$ or $g'_{1,3}$ and l_3, and the processes given by the matrices $g_{2,3}$ or $g'_{2,3}$ and l_3, we may suppose a_{31}, a_{32} numerically less than a_{33}, and may suppose a_{33} to be positive. Proceeding thus we may eventually suppose all the elements of any row of the matrix a which are to the left of its diagonal to be less than the diagonal elements of that row—and may suppose that all the elements of the diagonal of the matrix a are positive; this involves that the diagonal elements of β' are positive, and in particular when r is a prime number involves that these elements are each 1 or r.

Further we may reduce the elements of the matrix a' which are in the diagonal of a', and those which are to the left of this diagonal, by means of the diagonal elements of the matrix β'. We begin with the elements of the last row of a'; by means of the processes given by the matrices n_p or n'_p we may suppose a'_{pp} to be numerically less than β'_{pp}; by means of the processes given by the matrices $f_{p,p-1}$ or $f'_{p,p-1}$ we may suppose $a'_{p,p-1}$ to be numerically less than $\beta'_{p,p}$; in general by means of the processes given by $f_{p,s}$ or $f'_{p,s}$ we may suppose $a'_{p,s}$ to be numerically less than $\beta'_{p,p}$. Similarly by the processes given by n_{p-1} or n'_{p-1} we may suppose $a'_{p-1,p-1}$ numerically less than $\beta'_{p-1,p-1}$, and by the processes $f_{p-1,s}$ or $f'_{p-1,s}$, where $s<p-1$, we may suppose $a'_{p-1,s}$ numerically less than $\beta'_{p-1,p-1}$. The general result is that in every row of the matrix a' we may suppose the diagonal element, and the elements to the left of the diagonal, to be all numerically less than the diagonal element of the same row of the matrix β'.

413. If then we take the case when $r=1$ we have the result that it is possible to form a product Ω of the $p+2$ matrices a_k, b, c, d, such that the product $\Delta\Omega$ has a form which may be represented, taking $p=3$, by

$$\Delta\Omega = \left(\begin{array}{cccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & a'_{12} & a'_{13} & 1 & \beta'_{12} & \beta'_{13} \\ 0 & 0 & a'_{23} & 0 & 1 & \beta'_{23} \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right),$$

wherein all the elements of each of the matrices a and β' to the left of the diagonals are zero, and all the elements of the matrix a' both in the diagonal, and to the left of the diagonal, are zero. Applying then the condition $a\bar{\beta}'=1$, we find that the elements of the matrix β' to the right of its diagonal are also zero, so that $\beta'=a=1$. Then finally, applying the condition $a'\bar{\beta}'=\beta'\bar{a}'$, equivalent to $a'=\bar{a}'$, we have $a'=0$. Thus the reduced matrix is the matrix unity of $2p$ rows and columns, *and* Δ, $=\Omega^{-1}$, *is expressed as a product of positive integral powers of the* $p+2$ *matrices* A_k, B, C, D, as desired. Since the determinant of each of the matrices A_k, B, C, D is $+1$, the determinant of the linear matrix Δ is also $+1$.

414. In the particular case $p=1$ the only matrices of the $p+2$ matrices A_k, B, C, D which are not nugatory are the two matrices B and C; we denote these here by U and V and put further

$$u=U^{-1}=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\quad v=V^{-1}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\quad v_1=uvu^3vu^3,\quad w=uvu^3,\quad w_1=u^2vu^3vu^2;$$

then we immediately verify the facts denoted by the following table

	u	u^2	u^3	v	v_1	w	w_1
(ξ, η)	$(-\eta, \xi)$	$(-\xi, -\eta)$	$(\eta, -\xi)$	$(\xi, \eta+\xi)$	$(\xi, \eta-\xi)$	$(\xi-\eta, \eta)$	$(\xi+\eta, \eta)$

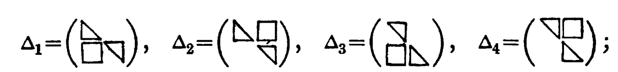
of which, for example, the first entry means that if $\Delta=\begin{pmatrix} a & \beta \\ a' & \beta' \end{pmatrix}$ be any matrix of 2 rows and columns, and we form the product Δu, then the columns ξ, η of the matrix Δ are interchanged, and at the same time the sign of the new first column is changed; we have in fact

$$\begin{pmatrix} a & \beta \\ a' & \beta' \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}=\begin{pmatrix} -\beta & a \\ -\beta' & a' \end{pmatrix};$$

hence it is immediately shewn, as in the more general case, that every matrix $\Delta=\begin{pmatrix} a & \beta \\ a' & \beta' \end{pmatrix}$, for which the integers a, β, a', β' satisfy the relation $a\beta'-a'\beta=1$, can be expressed as a product of positive integral powers of the two matrices

$$U=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\quad V=\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

415. Combining the final result for the decomposition of a linear Abelian matrix with the results obtained for any Abelian matrix of order r we arrive at the following statement, whereof the parts other than the one which has been formally proved may be deduced from that one, or established independently: let $\Delta=\begin{pmatrix} a & \beta \\ a' & \beta' \end{pmatrix}$ be any Abelian matrix of order r; then it is possible to find a linear matrix Ω expressible as a product of positive integral powers of the $(p+2)$ matrices A_k, B, C, D, which will enable us to write $\Delta=\Delta_i\Omega$, where Δ_i is an Abelian matrix of order r having any one, arbitrarily chosen, of the four forms representable by



and it is also possible to choose the linear matrix Ω to put Δ into the form $\Delta=\Omega\Delta_i$, where Δ_i is also any one, arbitrarily chosen, of these same four forms. It follows that the determinant of the matrix Δ is $+r^p$. In virtue of the equations $a_{ii}\beta'_{ii}=r\,(i=1, \ldots, p)$, which hold for any one of the matrices Δ_1, Δ_2, Δ_3, Δ_4, and the inequalities which may also be supposed to hold among the other elements, as exemplified, § 412, for the case of Δ_1, it is easy to find the number of different existing reduced matrices of any one of these forms. For instance when $p=2$, the number when r is a prime number is $1+r+r^2+r^3$; for $p=3$, and r

a prime number, it is $1+r+r^2+2r^3+r^4+r^5+r^6$; for details the reader may consult Hermite, *Compt. Rendus*, t. XL. (1855), p. 253, Wiltheiss, *Crelle*, XCVI. (1884), pp. 21, 22, and the book of Krause, *Die Transformation der Hyperelliptischen Functionen* (Leipzig, 1886), which deal with the case $p=2$; for the case $p=3$, see Weber, *Annali di Mat.* Ser. 2ª, t. IX. (1878), p. 139, where also the reduction to the form $\Delta=\Omega\begin{pmatrix} r & 0 \\ 0 & 1\end{pmatrix}\Omega'$, in which Ω, Ω' are linear matrices, is considered. Cf. also Gauss, *Disq. Arith.*, § 213; Eisenstein, *Crelle*, XXVIII. (1844), p. 327; Hermite, *Crelle*, XL., p. 264, XLI. (1851), p. 192; Smith, *Phil. Trans.* CLI. (1861), *Arts.* 13, 14.

416. Considering (cf. § 372) any reduction, of the form

$$\begin{pmatrix} a & \beta \\ a' & \beta'\end{pmatrix}=\begin{pmatrix} \rho & \sigma \\ \rho' & \sigma'\end{pmatrix}\begin{pmatrix} A & B \\ 0 & B'\end{pmatrix}, \text{ or say } \Delta=\Omega\Delta_0,$$

where $\begin{pmatrix} \rho & \sigma \\ \rho' & \sigma'\end{pmatrix}$ is a linear matrix, we prove that however this reduction be effected, (i) the determinant of the matrix B' is the same, save for sign, (ii) if μ be a row of p positive integers each less than r (including zero), the rows determined by the condition, $\frac{1}{r}B'\mu=$integral, are the same. For any other reduction of this kind, say $\Delta=\Omega'\Delta'_0$, must be such that

$$\Omega'=\begin{pmatrix} \rho & \sigma \\ \rho' & \sigma'\end{pmatrix}\begin{pmatrix} \overline{q}' & -q \\ -p' & p\end{pmatrix},\quad \Delta'_0=\begin{pmatrix} p & q \\ p' & q'\end{pmatrix}\begin{pmatrix} A & B \\ 0 & B'\end{pmatrix},$$

where $\begin{pmatrix} p & q \\ p' & q'\end{pmatrix}$ is a linear matrix; the condition that the matrix a' of the matrix Δ'_0 should vanish, namely $p'A=0$, requires (since $|A||B'|=r^p$ and therefore $|A|$, the determinant of A, is not zero) that $p'=0$; thus the reduction $\Delta=\Omega'\Delta'_0$ can be written

$$\begin{pmatrix} a & \beta \\ a' & \beta'\end{pmatrix}=\begin{pmatrix} \rho\overline{q}', & -\rho\overline{q}+\sigma p \\ \rho'\overline{q}', & -\rho'\overline{q}+\sigma'p\end{pmatrix}\cdot\begin{pmatrix} pA, & pB+qB' \\ 0, & q'B'\end{pmatrix}.$$

Now $p\overline{q}'=1$; therefore $|q'|=\pm 1$; thus $|q'B'|=\pm|B'|$, which proves the first result. Also, if μ be a row of integers such that $\frac{1}{r}B'\mu$ is a row of integers, $=m$ say, then $\frac{1}{r}q'B'\mu$, $=q'm$, is also a row of integers; while if $\frac{1}{r}q'B'\mu$ be a row of integers, $=n$ say, then $\frac{1}{r}\overline{p}q'B'\mu$, which is equal to $\frac{1}{r}B'\mu$, is equal to $\overline{p}n$, and is also a row of integers; since $q'B'$ is the matrix which, for the reduction $\Delta=\Omega'\Delta'_0$, occupies the same place as that occupied, for the reduction $\Delta=\Omega\Delta_0$, by the matrix B', the second result is also proved.

417. Considering any rectangular matrix whose constituents are integers, if all the determinants of $(l+1)$ rows and columns formed from this matrix are zero, but not all determinants of l rows and columns, the matrix is said to be of rank l. The following theorem is often of use, and is referred to § 397, Chap. XXII.; *In order that a system of simultaneous not-homogeneous linear equations, with integer coefficients, should be capable of being satisfied by integer values of the variables, it is necessary and sufficient that the rank l of, and the greatest common divisor of all determinants of order l which can be formed from, the matrix of the coefficients of the variables in these equations, should be unaltered when to this matrix is added the column formed by the constant terms in these equations.* For the proof the reader may be referred to H. J. S. Smith, *Phil. Trans.* CLI. (1861), *Art.* 11, and to Frobenius, *Crelle*, LXXXVI. (1879), pp. 171—2.

418. Consider a matrix of $n+1$ columns and $n+1$ or more rows, whose constituents are integers, of which the general row is denoted by

$$a_i\, b_i \ldots\ldots k_i,\, l_i,\, e_i\,;$$

let Δ be the greatest common divisor of the determinants formed from this matrix with $n+1$ rows and columns; let Δ' be the greatest common divisor of the determinants formed from this matrix with n rows and columns; then, since every determinant of the $(n+1)$th order may be written as a linear aggregate of determinants of the n-th order, the quotient Δ/Δ' is integral, $=M$, say. Then *the* $n+1$ *or more simultaneous linear congruences*

$$U_i = a_i x + b_i y + \ldots\ldots + k_i z + l_i t + e_i u \equiv 0 \pmod{M}$$

have just Δ *incongruent sets of solutions, and have a solution whose constituents have unity as their highest common divisor.* Frobenius, *Crelle*, LXXXVI. (1879), p. 193.

Also, *if in the m linear forms* ($m <=$ or $> n+1$)

$$U_i = a_i x + b_i y + \ldots\ldots + k_i z + l_i t + e_i u, \qquad (i=1, \ldots, m),$$

the greatest common divisor of the $m(n+1)$ *coefficients be unity, it is possible to determine integer values of* $x, y, \ldots, t, u$, *such that the m forms have unity as their greatest common divisor;* in particular, when $n=1$, *if the* $2m$ *numbers* a_i, b_i *have unity as their greatest common divisor, and the* $\frac{1}{2}m(m-1)$ *determinants* $a_i b_j - a_j b_i$ *be not all zero, it is possible to find an integer x so that the m forms* $a_i x + b_i$ *have unity as their greatest common divisor.* Frobenius, *loc. cit.*, p. 156.

419. The theorem of § 418 includes the theorem of § 357, p. 589; it also includes the simple result stated § 383, p. 637, note. It also justifies the assumption made in § 397, that the periods Ω, Ω' may be taken so that the simultaneous equations $ax' - a'x = 1$, $bx' - b'x = 0$ can be solved in integers in such a way that the $2p$ elements $rx - b$, $rx' - b'$ have unity as their greatest common divisor; assuming that r is not zero so that the $p(2p-1)$ determinants $a_i b_j - a_j b_i$, $a_i b_j' - a_j' b_i$, $a_i' b_j' - a_j' b_i'$ are not all zero, and that Ω' has been taken so that the $2p$ integers $a_1, \ldots, a_p, a_1', \ldots, a_p'$ have no common divisor other than unity, the necessary and sufficient condition for the solution of the equations $ax' - a'x = 1$, $bx' - b'x = 0$ is (§ 417) that the greatest common divisor, say M, of the $p(2p-1)$ binary determinants spoken of should divide each of the $2p$ integers $b_1, \ldots, b_p'$; if this condition is not already satisfied we may proceed as follows: find two coprime integers (§ 418) which satisfy the $2p$ congruences

$$\lambda b_i' + \mu a_i' \equiv 0, \quad \lambda b_i + \mu a_i \equiv 0 \pmod{M}, \qquad (i=1, \ldots, p),$$

and thence two integers ρ, σ such that $\lambda\sigma - \mu\rho = 1$; put $\Omega_1' = \lambda\Omega' + \mu\Omega$, $\Omega_1 = \rho\Omega' + \sigma\Omega$, $B_i = b_i\lambda + a_i\mu$, $A_i = b_i\rho + a_i\sigma$, $B_i' = b_i'\lambda + a_i'\mu$, $A_i' = b_i'\rho + a_i'\sigma$; then

$$b_i\Omega - a_i\Omega' = B_i\Omega_1 - A_i\Omega_1', \quad b_i'\Omega - a_i'\Omega' = B_i'\Omega_1 - A_i'\Omega_1',$$

and the greatest common divisor of the $p(2p-1)$ binary determinants $A_i B_j - A_j B_i$, $A_i B_j' - A_j' B_i$, $A_i' B_j' - A_j' B_i'$, which is equal to M, divides the $2p$ integers $B_1, \ldots, B_p'$; thus M is the greatest common divisor of these $2p$ integers; next put $\Omega_2 = M\Omega_1$, $\Omega_2' = \Omega_1'$, $\mathrm{b}_i = B_i/M$, $\mathrm{b}_i' = B_i'/M$, $\mathrm{a}_i = A_i$, $\mathrm{a}_i' = A_i'$; then the greatest common divisor of the $p(2p-1)$ binary determinants $\mathrm{a}_i\mathrm{b}_j - \mathrm{a}_j\mathrm{b}_i$, etc., is unity, and this is also the greatest common divisor of the $2p$ integers $\mathrm{b}_1, \ldots, \mathrm{b}_p'$. Now let (x, x') be any solution of the equations $\mathrm{a}x' - \mathrm{a}'x = 1$, $\mathrm{b}x' - \mathrm{b}'x = 0$, so that $(rx - \mathrm{b}, rx' - \mathrm{b}')$ is a solution of the equations $\mathrm{a}\xi' - \mathrm{a}'\xi = 0$, $\mathrm{b}\xi' - \mathrm{b}'\xi = 0$; let (ξ, ξ') be an independent solution of these latter equations (Smith, *Phil. Trans.*, CLI. (1861), *Art.* 4) so that the $p(2p-1)$ binary determinants $x_i\xi_j - x_j\xi_i$, etc., are not all zero, so chosen that the $2p$ elements ξ_i, ξ_i' have unity as their highest common divisor; then if h be any integer, the $2p$ elements $x_i + \mathrm{h}\xi_i$, $x_i' + \mathrm{h}\xi_i'$ form a solution of the equations $\mathrm{a}x' - \mathrm{a}'x = 1$, $\mathrm{b}x' - \mathrm{b}'x = 0$; let h be chosen so that the $2p$ elements $rx_i - \mathrm{b}_i + \mathrm{h}r\xi_i$, $rx_i' - \mathrm{b}_i' + \mathrm{h}r\xi_i'$ have no common factor greater than unity (§ 418). Putting $X = x + \mathrm{h}\xi$, *X'=x'+hÇi* the first column of the matrix in § 39*7 will consist of the elements of (a, a'), the (p + l)th column will consist of the elements of (b, b'), the second column will consist of the elements of *rX-* , *rX'— h';* and since these latter have unity as their greatest common factor, it is possible to construct the (p + 2)th and all other columns of this matrix (§ 420).

420. A theorem is assumed in § 396, which has an interest of its own—*If of an Abelian matrix of order r there be given the constituents of the first r columns, and also the constituents of the (p + l)th, ,.., (p+r)th columns (r<p), it is always possible to determine the remaining 2(p — r) columns.* For a general enunciation the reader may refer to Frobenius, *Creile,* LXXXIX. (1880), p. 40. We explain the method here by a particular case; suppose that of an Abelian matrix of order r, for ^? = 3, there be given the first and (p-hl)th columns ; denote the matrix by

(*a x t* I *b*) ;
I *a' of f* J ' I

the elements of the given columns will satisfy the relation *ab' — db—r;* it is required to determine in order the second, the fifth, the third and the sixth columns ; the relations arising from the equations

âa'-â'a = 0, *ßß?-ß'ß=0,* *äß-ä'ß=r*

so far as they affect these columns respectively, are as follows : ^

ax'-a'x—Qii . *ay'-a'y^O^* *af-a't=0* *au'-a^fu—0*
bxf-b'x^o] W ' *by'-b'y=0V* (ii), *M-b't=o* ... 6w'-6%=0
xy'-x'y=r) *xtf-x't=o* 'ul" *xu'-a/u^OY* (iv);
yt'-y't=0) *yu'-tfu^oi*
tu' -tu = r)

now let *(x, xf)* be a solution of equations (i) in which the *2p* constituents have no common factor other than unity ; determine 2 rows of *p* elements £, f' such that *xg —af(=l,* and denote *ag - a'g* by *A* and *b% - b'£* by ; then it is immediately verified that the values

y=r$-(Ab-Ba), *tf=r%-(AV-Ba!*

satisfy equations (ii) ; next let (£, *t')* be a solution of equations (iii) in which the *2p* constituents have no common factor other than unity ; determine 2 rows of *p* elements, v, i/, such that *tv —tfv= l,* and denote *av—a'v, bv' — b'v, xv—x^fv> yv—y'v* respectively by *A, By X, Y;* then it is immediately verified that the values

u=rv-(Ab-Ba)-(Xy- Yx), u'=rv'- (Ab'- Ba') - (Xy^1 - Yx)*

satisfy the equations (iv).