February 13th, 1873.

Dr. HIRST, F.R.S., President, in the Chair.

Prof. R. Stawell Ball and Dr. J. Hopkinson were elected Members; and Prof. A. G. Greenhill, of Cooper's Hill College, was proposed for election.

The following papers were read:—

Prof. H. J. S. Smith "On the Higher Singularities of Plane Curves," and "On Systems of Linear Congruences."

Mr. J. Macleod "On the Application of the Hodograph to the Solution of Problems on Projectiles."

The President, Mr. Roberts, and Mr. Cotterill, made remarks on the communications.

The following presents were received:—

"Annual of the Royal School of Naval Architecture," No. 3, Jan. 1873: from Mr. C. W. Merrifield, F.R.S.

"Bulletin des Sciences Mathématiques," table des matières, Vol. iii., and No. 1, Vol. iv., Jan. 1873.

"Crelle," 75 Band, 3^{er} Heft.

"Monatsbericht," Sept. and Oct. 1872.

"Journal of the London Institution," No. 18, Jan. 27, 1873.

ARITHMETICAL NOTES.*

By HENRY J. STEPHEN SMITH, Savilian Professor of Geometry in the University of Oxford.

I.—*On the Arithmetical Invariants of a Rectangular Matrix, of which the Constituents are Integral Numbers.*

1. Let $\|a_{\nu}\|$ represent a rectangular matrix of the type $n \times (n+m)$, and let ∇ , be the greatest common divisor of the $\frac{\prod_{\mu}}{\prod s \cdot \prod (n-s)}$
 $\times \frac{\prod (n+m)}{\prod s \cdot \prod (n+m-s)}$ minor determinants of order s which appertain to

* Being three Papers read at the January and February (1873) Meetings of the Society.

it; so that, in particular, ∇_n is the greatest common divisor of the $\frac{\Pi(m+n)}{\Pi n \cdot \Pi m}$ determinants of the matrix; the numbers $\nabla_n, \nabla_{n-1}, \dots \nabla_1$ are the *arithmetical invariants* of the matrix. We suppose that the matrix is aszygetic; i. e., that the $\frac{\Pi(m+n)}{\Pi n \cdot \Pi m}$ determinants are not all equal to zero. We then have the theorem (Memoir, p. 318 *sqq.**) :

Theorem (a). "The quotient $\frac{\nabla_s}{\nabla_{s-1}}$ is the greatest common divisor of the quotients obtained by dividing each minor determinant of order s by the greatest common divisor of its own first minors."

Let p be a prime dividing ∇_i , and let I_i be the exponent of the highest power of p which divides ∇_i ; any minor of order i which is divisible by p^{I_i} may be said to be divisible *in excess* by p^i . Using this abbreviated mode of expression, we may enunciate the two following corollaries :

Corollary (b). "Any minor determinant, which is not divisible in excess by p , contains at least one first minor which is not divisible in excess by p ."

Corollary (c). "Any minor determinant, which is not divisible in excess by p^i , contains at least one first minor which is not divisible in excess by p^i ."

Or, which is the same thing,

"If all the first minors of a given minor are divisible in excess by p^i , the given minor is itself divisible in excess by p^i ."

Of these corollaries, the first is a particular case of the second; and the second is only a re-statement, in other words, of the theorem (a).

2. It is the object of this note to establish a theorem, which may be regarded as reciprocal to the theorem (a).

Theorem (A). "The fraction $\frac{\nabla_{s-1}}{\nabla_s}$ is the greatest common divisor of the fractions obtained by dividing each minor of order $s-1$ by the greatest common divisor of its first majors; or, which is the same thing, the integral number $\frac{\nabla_s}{\nabla_{s-1}}$ is the least common denominator of these fractions."

Any square matrix which contains a given square matrix is here called, for brevity, a *major* of that matrix; if the given square matrix be of order $s-1$, its *first majors* are the square matrices of order s which contain it.

* The references in this and the two following notes are to a Memoir "On Systems of Linear Indeterminate Equations and Congruences" (Phil. Trans., vol. cli., pp. 293—326).

The theorem (A) admits of two corollaries, corresponding to the corollaries (b) and (c):

Corollary (B). "Any minor determinant, which is not divisible in excess by p , is contained in at least one first major which is not divisible in excess by p ."

Corollary (C). "Any minor determinant, which is not divisible in excess by p^* , is contained in at least one first major which is not divisible in excess by p^* ."

Or, which is the same thing,

"If all the first majors of a given minor are divisible in excess by p^* , the given minor is itself divisible in excess by p^* ."

3. To prove the theorem (A), we consider, in the first place, a square matrix $\|a_{ij}\|$ of the type $n \times n$, so that $\nabla_n = \Sigma \pm a_{11} a_{22} \dots a_{nn}$; and we represent the minor determinant $\frac{d \nabla_n}{d a_{ij}}$ by Δ_{ij} , so that the reciprocal matrix is $\|\Delta_{ij}\|$. The determinant of this matrix is ∇_n^{n-1} , and the greatest common divisor of its minor determinants of order i is $\nabla_n^{i-1} \times \nabla_{n-i}$.

Let $M = \frac{\Pi n}{\Pi(s-1) \cdot \Pi(n-s+1)}$, $N = n-s+1$; let k_μ [$\mu = 1, 2, 3, \dots M^2$] represent any one of the M^2 minors of order $s-1$ which appertain to the matrix $\|a_{ij}\|$; let $k_{\mu,\nu}$ [$\nu = 1, 2, 3, \dots N^2$] represent any one of the first majors of k_μ ; let d_μ be the greatest common divisor of these N^2 numbers; lastly, let K_μ and $K_{\mu,\nu}$ represent the minors which, in the reciprocal matrix $\|\Delta_{ij}\|$, are reciprocal to the minors k_μ and $k_{\mu,\nu}$ in the matrix $\|a_{ij}\|$; so that, for example, if $k_\mu = \Sigma \pm a_{11} a_{22} \dots a_{s-1, s-1}$, $K_\mu = \Sigma \pm A_{s, s} A_{s+1, s+1} \dots A_{n, n}$; and if $k_{\mu,\nu} = \Sigma \pm a_{11} a_{22} \dots a_{s, s}$, $K_{\mu,\nu} = \Sigma \pm A_{s+1, s+1} \dots A_{n, n}$. Thus the N^2 first minors of K_μ are precisely the determinants $K_{\mu,\nu}$; we also have the equations $K_\mu = \nabla_n^{n-s} \times k_\mu$, $K_{\mu,\nu} = \nabla_n^{n-s-1} \times k_{\mu,\nu}$; so that, applying the theorem (a) to the matrix $\|\Delta_{ij}\|$, we find that the greatest common divisor of the M^2 integral numbers, $[\nabla_n^{n-s} \times k_\mu] \div [\nabla_n^{n-s-1} \times d_\mu] = \nabla_n \times \frac{k_\mu}{d_\mu}$, is the quotient $[\nabla_n^{n-s} \times \nabla_{s-1}] \div [\nabla_n^{n-s+1} \times \nabla_s] = \nabla_n \times \frac{\nabla_{s-1}}{\nabla_s}$; that is to say, the greatest common divisor of the M^2 fractions $\frac{k_\mu}{d_\mu}$ is the fraction $\frac{\nabla_{s-1}}{\nabla_s}$, in accordance with the theorem (A). The corollaries (B) and (C) may be immediately verified by observing that, if either of them were supposed untrue for any given minor k_μ , the corresponding fraction $\frac{k_\mu}{d_\mu}$ would acquire a denominator which could not be a sub-multiple of $\frac{\nabla_s}{\nabla_{s-1}}$.

4. To extend the demonstration to the case of an oblong matrix of the type $n \times (m+n)$, we retain the preceding notations, so far as they are applicable; and we put $M_1 = \frac{\Pi(n+m)}{\Pi(s-1) \cdot \Pi(n+m-s+1)}$, $N_1 = n+m-s+1$; so that the values of μ and ν are now $[1, 2, \dots M \times M_1]$ and $[1, 2, \dots N \times N_1]$ respectively. Let Q be a common multiple of the $M \times M_1$ numbers d_μ , and let us complete the given rectangular matrix into a square one by adding rows of constituents each of which is divisible by Q . In the resulting square matrix, any given minor k_μ (appertaining to the given rectangular matrix) will have N_1^2 first majors; but it is evident that the greatest common divisor of these N_1^2 first majors will be the same as that of the $N \times N_1$ first majors which appertain to the given rectangular matrix. Hence the $M \times M_1$ fractions $\frac{k_\mu}{d_\mu}$, obtained by dividing each minor of order $s-1$ in the given matrix by the greatest common divisor of its first majors, occurs among the M_1^2 fractions similarly derived from the completed square matrix; also the numbers ∇_s and ∇_{s-1} are evidently the same for both matrices. Applying, therefore, the theorem (A) to the square matrix, we see that $\frac{\nabla_{s-1}}{\nabla_s}$ is a common divisor of the $M \times M_1$ fractions $\frac{k_\mu}{d_\mu}$; that it is the greatest common divisor of these fractions, may be proved by considering a minor determinant of order s in the given matrix, which is not divisible in excess by p ; this minor determinant contains [by the corollary (b)] a first minor which is itself not divisible in excess by p ; if k_μ be this first minor, the denominator of the corresponding fraction $\frac{k_\mu}{d_\mu}$ necessarily contains the prime p raised to the power $I_s - I_{s-1}$.

It will be observed that, whether we consider a rectangular or a square matrix, the corollary (C) is an immediate consequence from the theorem (A); but the theorem (A) does not follow conversely from the corollary (C). For the absence of factors prime to $\frac{\nabla_s}{\nabla_{s-1}}$ from the least common denominator of the fractions $\frac{k_\mu}{d_\mu}$ is asserted in the theorem, but is not asserted in the corollary.

5. Every common divisor of the first minors of a given minor is evidently a common divisor of the first majors of that minor; and, if the matrix be square, a consideration of the reciprocal matrix shows that, conversely, every common divisor, prime to the determinant of the matrix, of the first majors of any given minor, divides the first minors of that minor. We thus obtain the self-reciprocal theorem:

Theorem (dD). "In any square matrix, the greatest common divisor of the first minors of any given minor is identical with the greatest common divisor of its first majors, so far as factors prime to the determinant of the matrix are concerned."

This theorem is not universally true in the case of oblong matrices, at least if we suppose that, in its enunciation, the words "determinant of the matrix" are replaced by the words "greatest common divisor of the determinants of the matrix." If, for example, $\|a\|$ is a square matrix of order $n-1$, and $\|b\|$ is a matrix of the type $n \times (n+m)$, of which the determinants are relatively prime, the symbol $\left\| \begin{smallmatrix} 0 & b \\ a & \end{smallmatrix} \right\|$ may serve to represent a matrix of the type $n \times (2n+m-1)$, in which the first $n-1$ constituents of the uppermost row are zeros. In this matrix the greatest common divisor of the first majors of $|a|$ is evidently $|a|$ itself; and this greatest common divisor is prime to the greatest common divisor of the determinants of the matrix, because these determinants are relatively prime; but unless $\|a\|$ is an unit matrix, its determinant cannot be equal to the greatest common divisor of its own first minors.

6. It may be added, that the properties to which this note refers admit of being stated in a generalized form. Thus, we may replace the enunciations of the theorems (a), (A), and (dD) by the following:

Theorem (a'). "The quotient $\frac{\nabla_s}{\nabla_{s-i}}$ is the greatest common divisor of the quotients obtained by dividing each minor determinant of order s by the greatest common divisor of its own first minors of order $s-i$."

Theorem (A'). "The fraction $\frac{\nabla_{s-i}}{\nabla_s}$ is the greatest common divisor of the fractions obtained by dividing each minor of order $s-i$ by the greatest common divisor of its own majors of order s ."

Theorem (dD'). "In any square matrix, the greatest common divisor of the minors of order $s-i$ appertaining to a given minor of order s is identical with the greatest common divisor of the majors of order $s+i$ appertaining to the given minor, so far as factors prime to the determinant of the matrix are concerned."

A very slight modification of the proof of the theorem (a), (Mém. pp. 318—320.) supplies a proof of the theorem (a'), and from it the theorems (A') and (dD') may be inferred by means of the methods employed in this note to establish the theorems (A) and (dD).

II.—On Systems of Linear Congruences.

1. Let

$$(1) \dots A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n}x_n \equiv A_{i,n+1} \pmod{M},$$

$$i = 1, 2, 3, \dots n,$$

represent a system of n linear congruences; let

$$D_n, D_{n-1}, \dots, D_1,$$

$$\nabla_n, \nabla_{n-1}, \dots, \nabla_1,$$

respectively denote the arithmetical invariants of the augmented and unaugmented matrices of the system; *i. e.*, of the matrices

$$(2) \dots \dots \dots \|A_{ij}\| \quad \begin{matrix} i = 1, 2, \dots n, \\ j = 1, 2, \dots n+1, \end{matrix}$$

and

$$(3) \dots \dots \dots \|A_{ij}\| \quad \begin{matrix} i = 1, 2, \dots n, \\ j = 1, 2, \dots n; \end{matrix}$$

let d_i and δ_i be the greatest common divisors of M with $\frac{D_i}{D_{i-1}}$, and of M with $\frac{\nabla_i}{\nabla_{i-1}}$ respectively; lastly, let $d = d_1 \times d_2 \times \dots d_n$, $\delta = \delta_1 \times \delta_2 \times \dots \delta_n$.

We then have the two theorems (Memoir, p. 320):

"The necessary and sufficient condition for the resolvibility of the system (1) is $d = \delta$."

"When this condition is satisfied, the number of its incongruous solutions is $d = \delta$."

There are similar theorems (Memoir, p. 323) relating to defective and redundant systems of congruences. Some observations which may serve in certain cases to facilitate the applications of the theory are contained in the present note.

2. Consider separately the powers of the different prime numbers dividing the modulus M . Let p be one of these primes; and let μ, α_i, α be the exponents of the highest powers of p which divide M, D_i, ∇_i respectively.

Then, because $\frac{D_{i+1}}{D_i} \div \frac{D_i}{D_{i-1}}, \frac{\nabla_{i+1}}{\nabla_i} \div \frac{\nabla_i}{\nabla_{i-1}}, \nabla_i \div D_i$, and

$\frac{\nabla_i}{\nabla_{i-1}} \div \frac{D_i}{D_{i-1}}$, are all integral (Memoir, pp. 317—320), we have the inequalities

$$(4) \dots \alpha_n - \alpha_{n-1} \geq \alpha_{n-1} - \alpha_{n-2} \geq \dots \geq \alpha_1 - \alpha_0;$$

$$(5) \dots \alpha_n - \alpha_{n-1} \geq \alpha_{n-1} - \alpha_{n-2} \geq \dots \geq \alpha_1 - \alpha_0;$$

$$(6) \dots \alpha_i \geq \alpha_i;$$

$$(7) \dots \alpha_i - \alpha_{i-1} \geq \alpha_i - \alpha_{i-1}.$$

Let $a_\sigma - a_{\sigma-1}$ be the first term in the series (4) which is less than μ ; so that, if $a_n - a_{n-1} < \mu$, we have $\sigma = n$, and in every other case

$$(8) \dots\dots\dots a_{\sigma+1} - a_\sigma \geq \mu > a_\sigma - a_{\sigma-1}.$$

We may then replace the two theorems of the Memoir by the two following:

"The necessary and sufficient condition for the resolvability of the congruences (1), considered with regard to the modulus p^n , is

$$(9) \dots\dots\dots a_\sigma = a_\sigma."$$

"When this condition is satisfied, the number of incongruous solutions is $p^{a_\sigma + (n-\sigma)\mu}$."

For the condition of resolvability is (Memoir, p. 321) that the greatest common divisor of the numbers

$$(10) \dots\dots\dots p^a, p^{a_{n-1}+\mu}, p^{a_{n-2}+2\mu}, \dots\dots p^{n\mu},$$

should be the same as the greatest common divisor of the numbers

$$(11) \dots\dots\dots p^{a_n}, p^{a_{n-1}+\mu}, p^{a_{n-2}+2\mu}, \dots\dots p^{n\mu}.$$

The greatest common divisor of the numbers (10) is $p^{a_\sigma + (n-\sigma)\mu}$; for it follows from the inequalities (8) and (4) that, in the series (10), the exponent $a_\sigma + (n-\sigma)\mu$ is less than any exponent which follows it, and not greater than any which precedes it. Again, if $a_\sigma = a_\sigma$, $p^{a_\sigma + (n-\sigma)\mu}$ is also the greatest common divisor of the numbers (11); for it is equal to one of them, and it certainly divides all of them, because it divides all the numbers (10), each of which, by virtue of the inequalities (6), divides one of the numbers (11). But if $a_\sigma > a_\sigma$, the greatest common divisor of the numbers (11) is a power of p having an exponent higher than $a_\sigma + (n-\sigma)\mu$. For the inequality $a_\sigma > a_\sigma$, combined with the inequality (7), implies the successive inequalities $a_{\sigma+1} > a_{\sigma+1}$, $a_{\sigma+2} > a_{\sigma+2}$, ... $a_n > a_n$; so that every exponent in the series (11), which precedes $a_\sigma + (n-\sigma)\mu$, surpasses the corresponding exponent in (10), and therefore certainly surpasses $a_\sigma + (n-\sigma)\mu$. And again, the exponents following $a_\sigma + (n-\sigma)\mu$ in the series (11) also surpass $a_\sigma + (n-\sigma)\mu$, for these exponents are not less than the corresponding exponents in (10), each of which is greater than $a_\sigma + (n-\sigma)\mu$. Thus the condition for the equality of the two greatest common divisors, i. e., for the resolvability of the congruences (1), is $a_\sigma = a_\sigma$. And, by transforming the proposed system (Memoir, p. 322) into an equivalent system of the type

$$(12) \dots\dots\dots \frac{\nabla_{n-\sigma+1}}{\nabla_{n-\sigma}} b_\sigma \equiv c_\sigma \pmod{p^n},$$

it is immediately ascertained that, when this condition is satisfied, the number of incongruous solutions is equal to $p^{a_\sigma + (n-\sigma)\mu}$, i. e., to the common value of the two greatest common divisors.

3. The criterion of resolvability just established differs in form only from that given in the Memoir; and the coincidence of the two may be shown by observing that the equation $a_s = a_s$, combined with the inequalities (7), implies the equations $a_{s-1} = a_{s-1}$, $a_{s-2} = a_{s-2}$, ... $a_1 = a_1$. As here stated, the criterion of resolvability, and the expression for the number of solutions, depend only on the numbers σ , ∇_s , D_s , and do not involve explicitly the consideration of the two complete series of invariants. When μ surpasses $a_n - a_{n-1}$, the condition of resolvability is $a_n = a_n$, and the number of solutions is p^{a_n} . In this case we only need to determine the invariants ∇_n and D_n , or rather the exponents of the highest powers of p dividing those numbers. But when $\mu \leq a_n - a_{n-1}$, it is necessary to calculate successively the invariants D_n , D_{n-1} , D_{n-2} , ... in order to ascertain the index σ for which the inequalities (8) are satisfied. It will be observed, however, that since every minor of order s , which is not divisible in excess by p , contains a minor of order $s-1$ which is itself not divisible in excess by p , it is always possible to restrict the examination of the minors of order $s-1$ (which is required in order to obtain the value of D_{s-1}) to those which are contained in a single minor of order s .

We may also notice that if, in the series of differences

$$a_n - a_n, a_{n-1} - a_{n-1}, \dots, a_1 - a_1,$$

$a_s - a_s$ is the first which is equal to zero, $p^{a_{s+1} - a_s}$ is the highest power of p for which the proposed congruences are resolvable.

4. In the case of a redundant or defective system, as well as in the case of a system such as (1), which is neither defective nor redundant, it will be found that the equation of condition $d = \delta$ may be replaced by the equation $a_s = a_s$. And in all these cases alike, whenever the system admits of any solution at all, the number of incongruous solutions is $p^{a_s + (n-s)\mu}$, n denoting the number of the indeterminates.

5. In the case of a redundant system, the condition $d = \delta$, or $a_s = a_s$, although necessary, is not sufficient (Memoir, p. 324). The complete condition of resolvability in this case is that the greatest common divisor of the numbers

$$(13) \dots p^{a_{n+1}}, p^{a_n + \mu}, p^{a_{n-1} + 2\mu}, \dots, p^{(n+1)\mu},$$

should be the same as the greatest common divisor of the numbers

$$(14) \dots p^{a_n + \mu}, p^{a_{n-1} + 2\mu}, \dots, p^{(n+1)\mu}.$$

And the identity of these two greatest common divisors implies not only (as in art. 2) the equation $a_s = a_s$, but also the inequality

$$(15) \dots \mu \leq a_{n+1} - a_n;$$

since, if this condition be not satisfied, a_{n+1} will be less than any of the exponents following it in the series (13), and therefore less than any exponent in the series (14).

The two conditions expressed by the equation $a_n = a_n$, and the inequality (15), are sufficient as well as necessary. But it is remarkable that the exponent μ not only satisfies the inequality (15), but also the inequality

$$(16) \dots\dots\dots \mu \leq a_{n+1} - a_n,$$

which is, in general, closer than (15), because $a_n \geq a_n$. To prove this, consider, in the given redundant system, any set of $n+1$ congruences such that the determinant of their augmented matrix is not divisible in excess by p ; and multiply these $n+1$ congruences, taken in order, by the determinants of their unaugmented matrix. The sum of the products is the determinant of the augmented matrix; we infer that this determinant is divisible by $p^{a_n + \mu}$, i. e. that $a_{n+1} \geq a_n + \mu$.

Since (as has been said) the two conditions of resolvibility, taken together, are sufficient, they must involve the inequality (16). To deduce it from them, we may employ the following lemma:

$$\text{" Let } \begin{matrix} \| Q_i \| & i = 1, 2, \dots n, \\ & j = 1, 2, \dots n+m, \end{matrix}$$

represent any square or oblong matrix of integral numbers, and let $\| q \|$ be a partial matrix consisting of any s of the n horizontal rows of $\| Q \|$; also let $Q_n, Q_{n-1}, \dots; q_n, q_{n-1}, \dots$ be the arithmetical invariants of $\| Q \|$ and $\| q \|$ respectively; then, if r is any number not surpassing s , $\frac{Q_n}{Q_{n-r}}$ is divisible by $\frac{q_n}{q_{n-r}}$."

To establish this lemma, let us suppose that $\| q \|$ consists of the last s rows of $\| Q \|$, and let us replace $\| Q \|$ by a compound matrix of the form $\| Q' \| \times \| Q'' \|$, in which $\| Q'' \|$ is a prime matrix of the same type as $\| Q \|$, and $\| Q' \|$ is a square matrix of the form

$$\left\| \begin{matrix} h_1, & k_{1,2}, & k_{1,3}, & \dots & k_{1,n} \\ 0, & h_2, & k_{2,3}, & \dots & k_{2,n} \\ 0, & 0, & h_3, & \dots & k_{3,n} \\ \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & 0, & \dots & h_n \end{matrix} \right\|$$

Then the greatest common divisor of any horizontal row of minors in $\| Q \|$ is the same as the greatest common divisor of the corresponding row of minors in $\| Q' \|$ (Memoir, p. 311); it is sufficient, therefore, to verify the lemma in the case of this last matrix. In it we have

$$\begin{aligned} h_1 \times h_2 \times \dots \times h_n &= Q_n, \\ h_{n-s+1} \times h_{n-s+2} \times \dots \times h_n &= q_n; \end{aligned}$$

and if we multiply $h_1 \times h_2 \times \dots \times h_{n-s} = \frac{Q_n}{q_s}$ by any minor of order $s-r$ contained in the last s rows of $\|Q'\|$, we obtain a product which is either a minor of $\|Q'\|$ of the order $n-r$, or else is equal to zero; this product is therefore in every case divisible by Q_{n-r} ; i. e., $\frac{Q_n}{q_s} \times q_{s-r}$ is divisible by Q_{n-r} , or $\frac{Q_n}{Q_{n-r}}$ is divisible by $\frac{q_s}{q_{s-r}}$.

To apply this lemma to the case which we are considering here, we change n into $n+1$, and we put $s=n$, $r=n-s$. Attending only to the powers of p , we thus find

$$a_{n+1} - a_n \geq a_{s+1} - a_s.$$

But $a_s = a_n$, and $a_{s+1} - a_s \geq \mu$; therefore $a_{n+1} - a_n \geq \mu$.

6. When the determinants of the augmented or unaugmented matrix of a proposed system of congruences vanish, we may add multiples of the modulus to the constituents of these matrices, so as to obtain determinants which do not vanish. We proceed, however, to show that this preliminary operation is unnecessary, and that the preceding theory is immediately applicable, notwithstanding the evanescence of the determinants.

If, in any matrix of which the arithmetical invariants are $\nabla_n, \nabla_{n-1}, \dots, \nabla_1$, the minor determinants of order $s+1$ are all equal to zero, we must attribute the same value to the invariant ∇_{s+1} ; and *vice versa*, if $\nabla_{s+1} = 0$, the minor determinants of order $s+1$ must themselves be all equal to zero. Let $\nabla_{s+1} = 0$, $\nabla_s > 0$, so that $\nabla_{s+r} = 0$ ($r = 1, 2, \dots, n-s$), $\nabla_{s-r} > 0$ ($r = 0, 1, 2, \dots, s-1$). The quotients $\frac{\nabla_s}{\nabla_{s-1}}, \frac{\nabla_{s-1}}{\nabla_{s-2}}, \dots, \frac{\nabla_1}{\nabla_0}$ are determinate positive integers, and the quotient $\frac{\nabla_{s+1}}{\nabla_s}$ is zero; but the

quotients $\frac{\nabla_{s+2}}{\nabla_{s+1}}, \dots, \frac{\nabla_n}{\nabla_{n-1}}$, assume the indeterminate form $\frac{0}{0}$. To these quotients we attribute the value zero: this may be regarded as an arbitrary definition of the value of these indeterminate numbers; it is, however, suggested by the observation that if the constituents of the matrix, instead of being integral numbers, were rational and integral functions of an indeterminate quantity, every factor of ∇_s would also be a factor of ∇_{s+1} , and would be contained in ∇_{s+1} oftener than in ∇_s ; i. e., $\frac{\nabla_{s+1}}{\nabla_s}$ would vanish with ∇_s .

7. Let us first suppose that the proposed system of congruences,

$$(17) \dots A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n+m}x_{n+m} \equiv A_{n,m+1} \pmod{p^r},$$

$$i = 1, 2, 3, \dots, n, \quad m \geq 0,$$

is not redundant; and let the invariants $\nabla_n, \nabla_{n-1}, \dots$ of its unaugmented matrix vanish as far as ∇_{s+1} inclusively, but let ∇_s not vanish. The integers,

$$\begin{aligned} a_n, & a_{n-1}, \dots a_{s+1}, \\ a_n - a_{n-1}, & \dots a_{s+1} - a_s, \\ a_n, & a_{n-1}, \dots a_{s+2}, \\ a_n - a_{n-1}, & \dots a_{s+2} - a_{s+1}, \end{aligned}$$

may then be regarded as greater than any assigned number; and if, in the inequalities (8), which determine the index σ , we adopt this interpretation of these symbols, the criterion of resolvability, and the expression for the number of solutions, will continue applicable to the system (17) without any modification whatever. For the criterion of resolvability this is evident, because the demonstration of art. 2 subsists unchanged. To prove the same thing for the formula which expresses the number of solutions, we employ the following lemma:

"The matrix $\|A_{i,j}\|$ $\begin{matrix} i = 1, 2, \dots n, \\ j = 1, 2, \dots n+m, \end{matrix}$

(in which ∇_{s+1} vanishes, but ∇_s does not vanish,) satisfies an equation of the form

$$(A) \dots \dots \dots \|\beta\| \times \|A_{i,j}\| \times \|\gamma\| = \begin{vmatrix} q_{ij}, & 0 \\ 0, & 0 \end{vmatrix},$$

in which $\|\beta\|$ is an unit matrix of the type $n \times n$, $\|\gamma\|$ an unit matrix of the type $(n+m) \times (n+m)$, $\begin{vmatrix} q_{ij}, & 0 \\ 0, & 0 \end{vmatrix}$ a matrix of the type $n \times (n+m)$, which has all its constituents equal to zero, except those composing the partial matrix $\|q_{ij}\|$; this partial matrix being of the type $s \times s$, and having for its arithmetical invariants $\nabla_s, \nabla_{s-1}, \dots \nabla_0$."

Consider the system,

$$(18) \dots \dots A_{i,1}x_1 + A_{i,2}x_2 + \dots + A_{i,n+m}x_{n+m} = 0, \\ i = 1, 2, 3, \dots n,$$

which is equivalent to s independent equations; and take for $\|\gamma\|$ any unit matrix of the type $(n+m) \times (n+m)$, in which the last $n+m-s$ columns are the $n+m-s$ rows of a fundamental set of solutions of the system (18). The compound matrix $\|A\| \times \|\gamma\|$ will be of the form $\|c_{ij}, 0\|$, where $\|c_{ij}\|$ is a partial matrix of the type $n \times s$, and $\|0\|$ is a partial matrix, composed entirely of zeros, of the type $n \times (n+m-s)$; so that $\|c_{ij}, 0\|$ is of the same type as $\|A\|$. Again, consider the system

$$(19) \dots \dots c_{1,j}x_1 + c_{2,j}x_2 + \dots + c_{n,j}x_n = 0, \\ j = 1, 2, 3, \dots s,$$

of which the equations are independent; and take for $\|\beta\|$ any unit matrix of the type $n \times n$, in which the $n-s$ lowest rows are the $n-s$

rows of a fundamental set of solutions of the system (19). The compound matrix $\|\beta\| \times \|A\| \times \|\gamma\|$ is then of the form $\begin{vmatrix} q_v, 0 \\ 0, 0 \end{vmatrix}$.

If therefore, in the system (17), we transform the indeterminates by the substitution

$$(x_1, x_2, \dots x_{n+m}) = \|\gamma\| \times (y_1, y_2, \dots y_{n+m}),$$

and at the same time replace the congruences themselves by others linearly derived from them by multiplication with the constituents of the rows of $\|\beta\|$, we obtain an equivalent system of the form

$$(20) \dots q_{1,j} y_1 + q_{2,j} y_2 + \dots q_{s,j} y_s \equiv h_j \pmod{p^r}, \\ j = 1, 2, \dots s,$$

in which the indeterminates $y_{s+1}, \dots y_{n+m}$ do not appear explicitly. By the theorem of art. 2, the number of solutions of (20) is $p^{a_s + (s-s)r}$ and to each of these solutions there correspond $p^{(n+m-s)r}$ solutions of (17), because each of the indeterminates $y_{s+1}, \dots y_{n+m}$ may have any one of p^r values. Thus the number of solutions of (17) is $p^{a_s + (n+m-s)r}$.

8. Next, let the proposed system of congruences be redundant; and, as before, let ∇_{s+1} vanish, but not ∇_s . In this case also the demonstration relating to the criteria of resolubility subsists unchanged; to determine the number of solutions, we select from the proposed system a partial system of s equations such that the determinants of its unaugmented matrix are not divisible in excess by p . Every solution of this partial system satisfies the remaining congruences of the proposed system; i. e., the number of solutions of the proposed system is $p^{a_s + (n-s)r}$, if n be the number of indeterminates.

9. It is worth while to observe that, in the equation (A), we may attribute to the partial matrix $\|q_v\|$ the simple form $\begin{vmatrix} \nabla_s & \nabla_{s-1} & \dots & \nabla_1 \\ \nabla_{s-1} & \nabla_{s-2} & \dots & \nabla_0 \end{vmatrix}$. For if $\|u\|$ and $\|v\|$ are reducing units of $\|q_v\|$, so that

$$\|u\| \times \|q_v\| \times \|v\| = \begin{vmatrix} \nabla_s & \nabla_{s-1} & \dots & \nabla_1 \\ \nabla_{s-1} & \nabla_{s-2} & \dots & \nabla_0 \end{vmatrix},$$

we may replace $\|u\|$ and $\|v\|$, which are both of the type $s \times s$, by unit matrices of the types $n \times n$ and $(n+m) \times (n+m)$ respectively; and may then compound these substituted units with the unit matrices $\|\beta\|$ and $\|\gamma\|$. The unit matrices thus substituted for $\|u\|$ and $\|v\|$ contain $\|u\|$ and $\|v\|$ as partial matrices; their forms are sufficiently indicated by the symbols $\begin{vmatrix} u & \\ 0 & I \end{vmatrix}$, $\begin{vmatrix} v & \\ 0 & J \end{vmatrix}$; where I and J are matrices of the types $n \times (n-s)$ and $(n+m-s) \times (n+m)$ respectively, and are subject to no restriction other than that implied by the equations

$$\begin{vmatrix} u & \\ 0 & I \end{vmatrix} = 1, \quad \begin{vmatrix} v & \\ 0 & J \end{vmatrix} = 1.$$

Another transformation of a matrix, in which the first $n-s$ invariants vanish, is sometimes useful; viz., we may write

$$\|A\| = \|\omega\| \times \left\| 0, 0, \dots 0, \frac{\nabla_s}{\nabla_{s-1}}, \frac{\nabla_{s-1}}{\nabla_{s-2}}, \dots \frac{\nabla_1}{\nabla_0} \right\| \times \|Q\|,$$

where $\|\omega\|$ is an unit matrix of the type $n \times n$, and $\|Q\|$ is a matrix of the same type as $\|A\|$, of which the s lowest rows form a prime matrix, while the others are arbitrary. The proof of this transformation presents no difficulty, and may be omitted here.

10. When the absolute terms in a linear system of congruences are all congruous to zero, the criteria of resolvability are always satisfied, as they ought to be, because the system is satisfied by attributing to the indeterminates values congruous to zero, and therefore certainly admits of one solution at least. In this case, however, it is usually of importance to determine, not the whole number of solutions, but the number of solutions prime to the modulus (*i. e.*, the number of solutions in which one at least of the indeterminates is prime to the modulus). Reducing the proposed congruences to an equivalent system of the form (12), which can always be done by the transformations indicated in the Memoir (p. 322), and in art. 7 of the present note, we find that if N is the whole number of solutions, $N \div p^{n-s}$ is the number of solutions in which every indeterminate has a value divisible by p , so that $N \left(1 - \frac{1}{p^{n-s}}\right)$ is the number of solutions prime to the modulus. And, in general, if k_i is the number of terms in the series (5) which satisfy the inequality $\alpha_{s+1} - \alpha_s \geq \mu - i$, so that, in particular, $k_0 = n - s$, the number of solutions in which every indeterminate has a value divisible by p^i will be found to be $N \div p^{k_0 + k_1 + \dots + k_{i-1}}$.

11. The transformation of a given square matrix indicated by the equation

$$(21) \dots \dots \|A_j\| = \|\alpha\| \times \left\| \frac{\nabla_n}{\nabla_{n-1}}, \frac{\nabla_{n-1}}{\nabla_{n-2}}, \frac{\nabla_{n-2}}{\nabla_{n-3}}, \dots \frac{\nabla_1}{\nabla_0} \right\| \times \|\beta\|$$

forms the basis of many of the demonstrations in this and the preceding note. It has been already pointed out (Memoir, p. 314) that this equation always admits of an infinite number of solutions: this observation may be verified as follows. If $\|u_{ij}\|$ is any unit matrix of which the constituents are defined by the equations

$$u_{i,j} = \lambda_{i,j}, \quad j < i,$$

$$u_{i,j} = \lambda_{i,j} \frac{\nabla_{n-i+1}}{\nabla_{n-i}} \div \frac{\nabla_{n-j+1}}{\nabla_{n-j}}, \quad j \geq i,$$

the matrix $\|v_{ij}\|$, of which the constituents are defined by the equations

$$v_{ij} = \lambda_{ij}, \quad j \geq 1,$$

$$v_{ij} = \lambda_{ij} \frac{\nabla_{n-i+1}}{\nabla_{n-j}} \div \frac{\nabla_{n-i+1}}{\nabla_{n-i}}, \quad j \leq i,$$

will also be an unit matrix; and, if $\|\alpha\|$, $\|\beta\|$ be two given unit matrices satisfying the equation (21), that equation will also be satisfied by the unit matrices comprehended in the formulæ

$$\|\alpha\| \times \|u\|, \quad \|v\|^{-1} \times \|\beta\|,$$

and by them only.

III.—On an Arithmetical Demonstration of a Theorem in the Integral Calculus.

1. Let
$$a_{i1}y_1 + a_{i2}y_2 + \dots + a_{in}y_n = b_i \quad \left. \begin{matrix} i = 1, 2, 3, \dots n \end{matrix} \right\} \dots\dots\dots (A)$$

represent a system of linear equations, in which the numbers a_{ij} and b_i are integral, the determinant $\nabla = |a_{ij}|$ being different from zero and positive. If, considering the numbers b_i with regard to the modulus ∇ , we attribute to them in succession the " ∇ " systems of values of which they are susceptible with regard to that modulus, we have the arithmetical theorem (Memoir, p. 325):

(i.) "The system (A) is resolvable in integral numbers y for precisely ∇^{-1} of the " ∇ " systems b ."

2. Let Σ represent a complex, or multiplicity, of order n , of which the indeterminates $y_1, y_2, \dots y_n$ are independent. Any system of values assigned to the indeterminates is called a point of Σ ; and if the values are integral, the point is an integer point. Let

$$\left. \begin{matrix} [x_{i1}, x_{i2}, x_{i3}, \dots x_{in}] \\ i = 1, 2, 3, \dots n, \end{matrix} \right\}$$

represent n given integer points of Σ ; we shall suppose these n points to be asyzygetic, so that the determinant $\nabla = |x_{ij}|$ is different from zero, and may be assumed to be positive. We then obtain the theorem:

(ii.) "The number of integer points $[X_1, X_2, \dots X_n]$ which satisfy the inequalities

$$0 < X_1 \frac{d\nabla}{dx_{i1}} + X_2 \frac{d\nabla}{dx_{i2}} + \dots + X_n \frac{d\nabla}{dx_{in}} \leq \nabla,$$

$$i = 1, 2, 3, \dots n,$$

is precisely ∇ ."

For, by the theorem (i.), the equations

$$\left. \begin{aligned} X_1 \frac{d\nabla}{dx_{i_1}} + X_2 \frac{d\nabla}{dx_{i_2}} + \dots + X_n \frac{d\nabla}{dx_{i_n}} = B_i \end{aligned} \right\} \dots\dots\dots (B),$$

$$i = 1, 2, 3, \dots n$$

of which the determinant is ∇^{n-1} , and in which each of the numbers B_i is supposed to receive in succession every value from 1 to ∇^{n-1} inclusive, are resolvable in integral numbers X for $\nabla^{(n-1)}$ of these $\nabla^{(n-1)}$ systems of values. But the solution of the equations (B) is given by the system

$$\nabla X_j = B_1 x_{1j} + B_2 x_{2j} + \dots + B_n x_{nj},$$

$$j = 1, 2, 3, \dots n.$$

If therefore the equations (B) are resolvable in integral numbers for any particular system of values of the numbers B_i , considered with regard to the modulus ∇ , they are resolvable for the $\nabla^{(n-2)}$ systems of values congruous to that particular system for the modulus ∇ , but incongruous to one another for the modulus ∇^{n-1} . Hence, if k be the number of systems of values, taken with regard to the modulus ∇ , for which the equations (B) are resolvable in integral numbers, we have $k \times \nabla^{(n-2)} = \nabla^{(n-1)}$, or $k = \nabla$; a result which establishes the theorem (ii.).

3. Another proof of the same theorem may be obtained as follows: The number of systems of values for which the equations (B) are resolvable in integral numbers is equal to the number of solutions of the congruences

$$B_1 x_{1j} + B_2 x_{2j} + \dots + B_n x_{nj} \equiv 0, \pmod{\nabla},$$

$$j = 1, 2, 3, \dots n,$$

in which $B_1, B_2, \dots B_n$ are the indeterminates. And the number of solutions of this system of congruences is ∇ . (Memoir, p. 320, or arts. 1—3 of the preceding note.)

4. Let

$$[y_{i_1}, y_{i_2}, \dots y_{i_n}]$$

$$i = 1, 2, 3, \dots n,$$

represent any n aszygetic points of Σ ; and let λ_j be a positive common measure of the n quantities $y_{1,j}, y_{2,j}, \dots y_{n,j}$, so that we have n^2 equations of the form $y_{ij} = x_{ij} \times \lambda_j$, in which the numbers x_{ij} are integral, and $|x_{ij}| = \nabla$ is different from zero and positive.

Let $D = |y_{ij}| = \nabla \times \prod_{j=1}^{j=n} \lambda_j$; the number of points of Σ , which are of the type $[X_1 \lambda_1, X_2 \lambda_2, \dots X_n \lambda_n]$, $X_1, X_2, \dots$ denoting integral numbers, and which satisfy the inequalities

$$0 < (X_1 \lambda_1) \frac{dD}{dy_{i_1}} + (X_2 \lambda_2) \frac{dD}{dy_{i_2}} + \dots + (X_n \lambda_n) \frac{dD}{dy_{i_n}} \leq D \dots\dots\dots (C),$$

is, by the theorem (ii.), equal to $D \div \Pi\lambda = \nabla$; that is to say, the product $\Pi\lambda$, taken as many times as there are points $(X_1\lambda_1, X_2\lambda_2, \dots X_n\lambda_n)$ satisfying the conditions (C), is equal to D . Let $\lambda_1, \lambda_2, \dots \lambda_n$ be infinitesimal, and let U represent the integral $\int \dots \int dY_1 dY_2 \dots dY_n$, extended to all values of $Y_1, Y_2, \dots Y_n$ which satisfy the inequalities

$$0 < Y_1 \frac{dD}{dy_{i1}} + Y_2 \frac{dD}{dy_{i2}} + \dots + Y_n \frac{dD}{dy_{in}} \leq D \Bigg\};$$

$$i = 1, 2, 3, \dots n$$

we have, by the definition of a definite integral, $U = D$.

5. This well-known result (which may be described as a generalization of the expression for the volume of a parallelepiped in space referred to three rectangular axes) may of course be otherwise obtained by employing the formula for the transformation of a multiple integral; viz., if we put

$$u_i = Y_1 \frac{dD}{dy_{i1}} + Y_2 \frac{dD}{dy_{i2}} + \dots + Y_n \frac{dD}{dy_{in}},$$

$$i = 1, 2, 3, \dots n,$$

the limits of u_i are 0 and D , and the functional determinant is D^{n-1} ;

hence $\int_0^D \dots \int_0^D \int_0^D du_1 du_2 \dots du_n = D^{n-1} \times U$, or $D = U$.

But as we have obtained the value of the definite integral U by a direct process, we may employ the result to demonstrate the formula for the transformation of a multiple integral; and this it may be worth while to do, because some of the demonstrations which have been given of that formula are not free from obscurity.

6. For convenience of expression, we may regard the indeterminates $X_1, X_2, X_3, \dots X_n$ as rectangular coordinates of a homogeneous and isotropic space of n dimensions. On this supposition we may define the volume unit of Σ to be that portion of Σ which is comprised between the limits

$$0 \leq X_i \leq 1,$$

$$i = 1, 2, 3, \dots n;$$

so that $dX_1 dX_2 \dots dX_n$ represents an element of Σ having the form (in n dimensions) of a rectangular parallelepiped. In any multiple integral

$\int V d\Sigma$, of order n , we must regard the integration as extending over a certain "integral space," or portion of Σ ; this integral space is to be resolved into infinitesimal elements, which may be of any form whatever, but which must exhaust the whole of it; each element is to be multiplied by the function V of its coordinates; and the definite in-

tegral is the sum obtained by adding the results. When the indeterminates are transformed by the equations

$$\left. \begin{aligned} X_i &= \phi_i(x_1, x_2, x_3, \dots, x_n) \\ i &= 1, 2, 3, \dots, n \end{aligned} \right\} \dots\dots\dots (D),$$

we have to consider a new space σ , in which the new indeterminates $x_1, x_2, \dots, x_n$ may be regarded as rectangular coordinates; to each element of the first space corresponds an element of the second space, and *vice versa*; the equations (D), whether by their own nature or by restrictions imposed on their interpretation, being supposed to establish a "one-to-one" correspondence between the two integral spaces. The problem of the transformation of a multiple integral then reduces itself to the determination of the ratio of corresponding elementary spaces $d\Sigma$ and $d\sigma$. By the nature of infinitesimal magnitudes, this ratio is independent of the particular form assigned to either element (the form of one of course determines the form of the other). Let us take for the element $d\sigma$ the parallelepiped (in n dimensions) of which one vertex is at the point $[x_1, x_2, \dots, x_n]$, and of which the adjacent n vertices are

$$\begin{aligned} x_1 + \delta_1 x_1, \quad x_2 + \delta_1 x_2, \quad \dots, \quad x_n + \delta_1 x_n, \\ i = 1, 2, 3, \dots, n, \end{aligned}$$

the quantities $\delta_i x_j$ being infinitesimal and asyzygetic; so that, by the theorem of art. 4, the volume of the parallelepiped (which is an infinitesimal of order n) is $|\delta_i x_j|$. If

$$\begin{aligned} \delta_i X_j &= \left(\frac{dX_j}{dx_1} \right) \delta_i x_1 + \left(\frac{dX_j}{dx_2} \right) \delta_i x_2 + \dots + \left(\frac{dX_j}{dx_n} \right) \delta_i x_n, \\ i &= 1, 2, \dots, n, \quad j = 1, 2, 3, \dots, n, \end{aligned}$$

the element $d\Sigma$, corresponding to the element $d\sigma = |\delta_i x_j|$, is evidently $|\delta_i X_j|$. But $|\delta_i X_j| \div |\delta_i x_j| = \left| \frac{dX_i}{dx_j} \right|$; i. e., the ratio of corresponding spaces is the functional determinant; a conclusion which establishes the theorem of transformation.

7. If we decompose the spaces Σ and σ into elementary parallelepipeds of the type $dX_1 dX_2 \dots dX_n, dx_1 dx_2 \dots dx_n$, we may write the equation

$$\int U dS = \int U \times \left| \frac{dX_i}{dx_j} \right| \times d\sigma$$

in the form

$$\int \dots \int U dX_1 dX_2 \dots dX_n = \int \dots \int U \times \left| \frac{dX_i}{dx_j} \right| \times dx_1 dx_2 \dots dx_n.$$

In this equation $dX_1 dX_2 \dots dX_n$ and $dx_1 dx_2 \dots dx_n$ are not corresponding elements; but the substitution of elements which do not

correspond for elements which do correspond is admissible, because the value of a definite integral is not altered by substituting one mode of decomposition into elements for another. It may be added that the symbol $\int U d\Sigma$, which involves no hypothesis as to the form of the element $d\Sigma$, supplies the most general and abstract expression of the definite integral; while the symbol $\int \dots \iint U dX_1 dX_2 \dots dX_n$, which indicates a particular mode of decomposition into elements, suggests at the same time a particular method of obtaining its value by successive integration.

8. It will be seen that, when a definite order is established among the indeterminates (X) and (x), the ratio of corresponding elements in the two spaces is determined in sign as well as in magnitude; but that if two indeterminates in either set be interchanged, the sign of this ratio is also changed. The Jacobian loci $\left| \frac{dX_i}{dx_j} \right| = 0$ and $\left| \frac{dX_i}{dx_j} \right| = \infty$ (which for our present purpose we take together) may be regarded, in general, as dividing the space Σ into two regions A and B, in the first of which $\left| \frac{dX_i}{dx_j} \right|$ is positive, and in the second negative. Similarly, σ is divided by the corresponding loci $\left| \frac{dx_i}{dX_i} \right| = \left| \frac{dX_i}{dx_j} \right|^{-1} = \infty, = 0$, into two regions a and b respectively corresponding to A and B, in such a manner that corresponding elements have the same sign in the regions A, a , and opposite signs in the regions B, b . But in using the formula for the transformation of a multiple integral, it is in general convenient to give to the functional determinant its absolute value, thus considering the elements of both spaces as positive throughout. And when the space over which the integration extends is traversed or bounded by the Jacobian loci, it is always necessary to examine the circumstances which present themselves at those loci.

Investigation of the Disturbance produced by a Spherical Obstacle on the Waves of Sound. By the Hon. J. W. STRUTT, M.A.

[Read November 14th, 1872.]

Introduction.

When a train of plane waves otherwise unimpeded impinge on a space occupied by matter, whose mechanical properties differ from those