

Gordan's Theorem for Double Binary Forms.

By Professor H. W. TURNBULL.

(Received 18th November 1922. Read 9th February 1923).

§ 1. Gordan's Theorem, that the complete system of irreducible concomitants of a given form is *finite*, has been extended by Hilbert * to cover wide ranges of systems of variables. Gordan † and Study ‡ have dealt shortly with the problem for double binary forms, approaching the subject through the theory of binary types. The following pages give a proof after the manner of Gordan's proof for ordinary binary forms, which has the advantage of providing a practical method for constructing the complete system. As illustrations, the cases of the (1, 2), (2, 2), and (3, 3) forms are considered.

It is probable that the method would also solve the problem of double binary perpetuants. §

§ 2. In the *Proc. Roy. Soc. Edinburgh*, Vol. xliii., 1923, I have discussed double binary forms, introducing the nomenclature of Gordan, necessary in the following proof which deals with the system belonging to the double binary (n, n') form

$$f = a_2^n a_z^{n'} = b_2^n b_z^{n'} = \text{etc.}$$

If $z = x + iy$, $z' = x - iy$ and $n = n'$ then f answers to plane circular curves. There appears to be no way of proving this theorem by an induction involving only symmetrical forms (1, 1), (2, 2), ... (n, n) ; but the system (n, n') can be found if $n' \leq n$ and if all systems $(N, n' - i)$ are known where $i > 0$ and N is a finite number depending on n, n' .

Suppose that the knowledge of the (n, n') system requires a preliminary system copied from the complete system (λ, μ) , then

* *Math. Ann.*, Bd. 30 and 36. Cf. Maurer, "Ueber die Endlichkeit der Invarianten Systeme." *München. Sitzungsberichte der Math.* Bd. 29, 1899.

† Cf. *Math. Ann.*, Bd. 33, pp. 387-389; also *Sitz. bericht. der Phys.-med. Soc. Erlangen*, (1888), p. 35.

‡ *Ibid.*, p. 31.

Cf. Grace and Young, *Algebra of Invariants*, pp. 326-338.

the (n, n') system is said to *involve* the (λ, μ) system. It is first necessary to prove a lemma to show that the number of systems involved in (n, n') is finite, and that the systems can be arranged in a definite order. Let the system $(n-i, n'-j)$ be called of lower rank if one or both of i, j exceed zero.

§ 3. LEMMA I. — *If, for all values of n, n' such that $n \geq n', n \geq n_0, n' \geq n'_0$, the systems involved in (n, n') are either of lower rank or are included in the systems $(kn, n'-i), i=1, 2 \dots n'$, then (n_0, n'_0) involves a finite number of systems and they can be ordinally arranged, k being a finite positive integer.*

For let (α, β) denote any one of the systems here specified; then $\beta \leq n'_0$, whereas α may exceed n_0 , but certainly does not exceed $k n_0, n_0$ which is finite. Corresponding to values of β from 0 to n'_0 inclusive let the greatest values of α be $\alpha_0, \alpha_1, \dots \alpha_{n'_0}$. It follows that the systems involved in (n, n') which are not of lower rank are included in those whose rank is lower than that of $(\alpha_0, 0), (\alpha_1, 1), \dots (\alpha_{n'_0}, n'_0)$. But this last sequence also includes systems of lower rank than (n, n') since $\alpha_i \geq n, k > 0$. The sequence, therefore, defines the order required, namely the first α_0 binary forms in ascending order, followed by α_1 forms linear in z' in ascending order of z , followed by $(\alpha_2 - 1)$ forms of the second order in z' and of orders 2, 3, ... α_2 respectively in z ; and so on till $\alpha_{n'_0}$ is reached. It will be seen that $\alpha_{n'_0} = n_0$.

Since the systems (n, m) and (m, n) are of the same character, and one is known if the other is known, then there has been no loss of generality in the argument above by assuming $n \geq n'$.

This lemma is required at several stages in the following proof of Gordan's Theorem, the value of k being either 2 or 3. It will be found that, in particular, knowledge of the binary duodecimic must precede that of the $(3, 3)$ form.

§ 4. *Systems of forms derived by transvection from two given systems.*

The developments of the binary theory (*Cf. Algebra of Invariants, loc. cit.*) apply with a few modifications to the present case.

Thus if U, V are symbolic products $A_1^{\alpha_1} \dots A_m^{\alpha_m}$ and $B_1^{\beta_1} \dots B_n^{\beta_n}$ of forms belonging to two systems (A) and (B) , the set of terms of all possible transvectants

$$(U, V)^{\rho_1}$$

is called the system derived by transvection from (A) and (B) . Any such transvectant contains reducible terms if, when

$$U = U_1 U_2, V = V_1 V_2, \rho = \sigma + \tau, \rho_1 = \sigma_1 + \tau_1,$$

it is possible to construct $(U_1, V_1)^{\sigma\sigma_1}$ and $(U_2, V_2)^{\tau\tau_1}$; for example, σ must not exceed the order of z in U_1 . It follows that *the number of transvectants $(U, V)^{\rho_1}$ (derived from finite systems (A) and (B)) which do not contain reducible terms is finite.* The proof is that for binary forms with four Diophantine equations in place of two: let this be called Lemma II.

It is convenient to have a symbol to denote systems derived by transvection as above. Let

$$[(A), (B)]$$

denote such a system. Then the notation may be extended to more complex systems as

$$[[(A), (B)], (C)].$$

The two further lemmas of the binary theorem may be taken over with little modification. Let $(A) \equiv c$, or $(A) \equiv c \pmod{H}$ symbolise that the system (A) is finite and complete, or that the system (A) is finite and relatively complete for the modulus H . Then we may enunciate the two lemmas:

LEMMA III.—If $(A) \equiv c$ and $(B) \equiv c$, then $[(A), (B)] \equiv c$.

LEMMA IV.—If a finite system of forms (A) , all the members of which are covariants of the (n, n') form f , include f , and if $(A) \equiv c \pmod{H, K}$; if further $(B) \equiv c \pmod{G}$, where (B) includes one form B_1 whose only determinantal factors are H , then the relation

$$[(A), (B)] \equiv c \pmod{G, K}$$

is satisfied.

These may be proved as for binary forms if we add the following modifications: transvectants should be considered:—

- (i) In order of ascending total degree of UV in the coefficients of the forms involved in A, B .

- (ii) Those for which the degree of UV is the same are taken in ascending degree of U .
- (iii) Those for which these two degrees are the same are taken in ascending order of the total index $(\rho + \rho_1)$.

§ 5. *Method of proof of Gordan's Theorem.*

If we can successively build up systems of

$$f = a_z^n a_{z'}^{n'} = b_z^n b_{z'}^{n'} = \text{etc.}$$

complete for the moduli $(a'b')$, $(a'b')^2$, ... $(a'b')^n$ respectively, then at the last stage the system is absolutely complete. Let such relative systems be called A_1, A_2, \dots, A_n . Then any form derived by convolution of members of the system A_r is a rational integral function of these members or else contains a factor equivalent to $(a'b')^r$. It must be recollected that A_r involves any factor (ab) to any index up to n .

Let $H_r = (ab)^r (a'b')^s a_z^{n-r} a_{z'}^{n'-s} b_z^{n-r} b_{z'}^{n'-s}$

and let $h_r = (ab)^r (a'b')^s :$

with H_r, h_r for the notation when $r = 0$.

Then the construction of the systems A_1, A_2, \dots, A_n falls into three sections according to the order of H_r in z' , as s takes the values 1, 2, ... n' in succession.

First we consider $s < n'/2$, next $s = n'/2$, next $s > n'/2$.

§ 6. *Case I., $s < n'/2$.*

The system A_1 is the complete system of $f = a_z^n a_{z'}^{n'}$ regarded as a binary form of order n in z . For if C is a product of terms of this system then a convolution of C contains at least one factor $(a'b')$ or no factor $(a'b')$ in which case the term is by hypothesis a function of terms C . Symbolically,

$$\overline{C} \equiv F(C) \pmod{(a'b')},$$

therefore $C \equiv c \pmod{(ab)(a'b'), (a'b')^2}$.

Also C includes f and so satisfies the conditions for A_1 .

Now suppose that we know all the systems A_1, A_2, \dots to A_r . We must form the next system A_{r+1} . There are two sub-cases

according as $s = 2k - 1$ or $2k$. First if $s = 2k - 1$; then we have

$$\begin{aligned} A_s &= A_{2k-1} \equiv c \pmod{(\alpha' \beta')^{2k-1}} \\ &\equiv c \pmod{(\alpha' \beta')^{2k-1} (ab), (\alpha' \beta')^{2k}}. \end{aligned}$$

Now we can shew that if B_k is the auxiliary system consisting of the single form

$$K = H_{1, 2k-1} = (ab) (\alpha' \beta')^{2k-1} a_z^{n-1} b_z^{n-1} \alpha_z'^{n'-2k+1} b_z'^{n'-2k+1},$$

then B_k is complete for the modulus $(\alpha' \beta')^{2k}$. This follows if we can shew that all transvectants

$$(K, K)^{i_1}$$

are of grade $2k$ in $(\alpha' \beta')$. But if $i_1 \neq 0$ this last transvectant may be dealt with as a binary form in $\alpha' \beta' c' d'$ which is known to be of higher grade since $2k - 1 = s < \frac{n'}{2}$ (Cf. *Algebra of Invariants*, pp. 71-77). Also when $i_1 = 0$ each term of this transvectant is of type

$$(\alpha' \beta')^{2k-1} (c' d')^{2k-1} (ab) (cd) M.$$

But after bracketing α' in each of the $2k - 1$ brackets $(c' d')$, this type may be expressed as a sum of transvectants $N(\theta, \delta)^\mu$ where δ contains all the symbols d' and θ all $\alpha' \beta' c'$ and N all symbols belonging to z . In this, θ is of higher grade $2k$ (*loc cit.* § 70) since the bracket factors of $\theta = (\alpha' \beta')^{2k-1} (\alpha' c')^\lambda$ and $2k - 1 \geq \lambda > \frac{1}{2}(2k - 1)$.

Hence B_k satisfies the relation

$$B_k \equiv c \pmod{(\alpha' \beta')^{2k}},$$

whence, by Lemma IV,

$$[A_{2k-1}, B_k] \equiv c \pmod{(\alpha' \beta')^{2k}}$$

which determines A_{2k} , that is A_{s+1} , if s is odd.

Next if $s = 2k$ we must find the system A_{2k+1} from A_{2k} . We shall require an auxiliary system B_{2k} containing $(\alpha' \beta')^{2k}$ ($= h_{2k}$) such that

$$B_{2k} \equiv c \pmod{(\alpha' \beta')^{2k+1}}.$$

Suppose that the binary $(n, 0)$ system A_1 is

$$(\phi) = \phi_1, \phi_2, \dots, \phi_p,$$

each ϕ being a generalized transvectant of f . Since h_{2k} denotes $(\alpha' \beta')^{2k}$ the orders $(2n, 2n' - 2k)$ of H_{2k} are of higher rank than

$(n, 0)$ respectively. So we may copy a set of transvectants for H_{2k} ,

$$(\psi) = \psi_1, \psi_2, \dots, \psi_p,$$

on the model of the set (ϕ) of lower rank.

If $(\overline{H_{2k}}, \overline{H_{2k}}, \dots)$ denote a generalized transvectant of forms $\overline{H_{2k}}$, where at least one of $\overline{H_{2k}}$ is convolved from H_{2k} and the others are identical with H_{2k} , then any term t_r of ψ_r may be written

$$t_r = \psi_r + \Sigma(\overline{H_{2k}}, \overline{H_{2k}}, \dots).$$

But, for the convolved term, $\overline{H_{2k}} \equiv 0 \pmod{(a'b')^{2k+1}, (a'b')^{2k}(ab)}$; hence

$$t_r \equiv \psi_r \pmod{(a'b')^{2k+1}, (a'b')^{2k}(ab)}.$$

Again, since the system (ϕ) is absolutely complete, then any term convolved from a product of (ψ) must satisfy

$$\overline{\psi} \equiv F(\psi) \pmod{Q}$$

where Q denotes transvectants whose index for a' symbols exceeds zero, otherwise Q is within the range copied from the $(n, 0)$ form and therefore included in $F(\psi)$.

But, if $i > 0, 2k < \frac{n'}{2}$,

$$(a'b')^{2k}(b'c')^i(c'd')^{2k} \equiv 0 \pmod{(a'b')^{2k+1}} \quad (\text{loc. cit. §73}),$$

then hence if $r_2 > 0, (H_{2a', 2k}, H_{2a', 2k})^{r_1, r_2} \equiv 0 \pmod{(a'b')^{2k+1}}$.

This implies that Q is of grade $(a'b')^{2k+1}$. It follows that the system

$$(t)_1 = t_1, t_2, \dots, t_p,$$

includes H_{2k} and is complete for the moduli $(a'b')^{2k}(ab), (a'b')^{2k+1}$ whose total indices are odd. Hence

$$(t)_1 \equiv c \pmod{(a'b')^{2k}(ab)^2, (a'b')^{2k+1}}$$

so that

$$[A_{2k}, (t)_1] \equiv c \pmod{(a'b')^{2k}(ab)^2, (a'b')^{2k+1}}.$$

Proceeding in the same way we may rid ourselves of the first of these two moduli by forming a system $(t)_2$ for the $(2n-4, 2n'-4k')$ form

$$H_{2, 2k} = (a'b')^{2k}(ab)^2 Z,$$

Z representing necessary a, a' factors, on the model of

$$(\phi) = \phi_1, \phi_2, \dots, \phi_p,$$

§ 7. Case II., $s = \frac{n'}{2}$.

As in *Algebra of Invariants*, § 73, this case leads to a new modulus when s is even: the system derived from A_s by the preceding argument will be finite and complete for moduli

$$(a'b')^{s+1}, (b'c)^s (c'a')^s (a'b')^s.$$

Let this system be called C_s . To derive the system A_{s+1} from C_s we proceed as follows:—

Let
$$J = (b'c)^s (c'a')^s (a'b')^s a_2^n b_2^n c_2^n$$

$$j = (b'c)^s (c'a')^s (a'b')^s,$$

and suppose $(\Omega) = \Omega_1, \Omega_2, \dots, \Omega_s$

the complete system of the binary form J of orders $(3n, 0)$ which by Lemma I. is already known. As before let

$$(\tau)_0 = \tau_1, \tau_2, \dots, \tau_s$$

denote single terms chosen from (Ω) , each Ω being given as a generalized transvectant of J ; then

$$\tau_r \equiv \Omega_r + \Sigma (\overline{J}, \overline{J}, \dots).$$

Since (Ω) is absolutely complete, then

$$(\tau)_0 \equiv c \pmod{\overline{J}}$$

where

$$\overline{J} = j (bc)^p (ca)^q (ab)^r Z, \quad p+q+r > 0;$$

and since j is of weight $3s$ which is even, we may take $p+q+r > 1$ and so, by Jordan's Lemma, at least one of p, q, r may be taken as not less than 2. This Lemma states that if $x+y+z=0$, then any product of powers of x, y, z of order m can be expressed linearly in terms of such products as contain one exponent equal to or greater than $\frac{2m}{3}$. It applies here since

$$(bc)a_s + (ca)b_s + (ab)c_s = 0,$$

and it may be further applied to the case above where $p+q+r=m$ so as to express all moduli $(bc)^p (ca)^q (ab)^r$ in terms of a smaller set of the same type with $p \geq \frac{2m}{3}$. Let such a set, when each member

is multiplied by j , be written

$$(\dot{j})_m = j'_m, j''_m, \dots j_m^{(km)}.$$

We may therefore construct a sequence of systems $\Delta_0, \Delta_2 \dots \Delta_m$ by introducing systems $(\tau)'_m, (\tau)''_m, \dots$ each from binary forms belonging to j'_m, j''_m, \dots exactly as $(\tau)_0$ was constructed from j . Thus

$$\left. \begin{aligned} \Delta_0 &= [C_{2n}(\tau)_0] \equiv c \pmod{(a'b')^{k+1}, j_2}, \\ \Delta_2 &= [\Delta_0, (\tau)_2] \equiv c \pmod{(a'b')^{k+1}, (j)_4}; (j)_4 = j''_4, j''_4; \\ \Delta_4 &= [[\Delta_2, (\tau)_4], (\tau)_4''] \equiv c \pmod{(a'b')^{k+1}, (j)_6} \\ &\dots\dots\dots \\ \Delta_m &= [\dots [\Delta_{m-2}, (\tau)'_m] \dots (\tau)_m^{(km)}] \\ &\equiv c \pmod{(a'b')^{k+1}, (j)_{m+2}}, \quad m \leq \frac{3n}{2} - 2. \end{aligned} \right\}$$

Finally when $m = \frac{3n}{2} - 2$, $(j)_{m+2}$ consists of the single invariant*

$$I = [(bc)(ca)(ab)]^n [(b'c')(c'a')(a'b')]^n.$$

If I is added to the system Δ_m , the combination will be complete for the modulus $(a'b')^{k+1}$, which is what we require. Thus we have found a system A_{s+1} from A_s if either $s < \frac{n'}{2}$ or $s = \frac{n'}{2}$.

§ 8. Case III., $s > \frac{n'}{2}$.

Since $2n' - 2s < n'$ we know by Lemma I. the complete system $(\Omega)_{ks}$ of the $(2n - 2k, 2n' - 2s)$ form H_{ks} . Now the bracket factors of H_{ks} are

$$h(k, s) = (ab)^k (a'b')^s;$$

hence a form convolved from H_{ks} has bracket factors $h(p, q)$, where

$$p \geq k, \quad q \geq s, \quad p + q > k + s.$$

As before let one term from each of the transvectants $(\Omega)_{ks}$ be chosen and let $(\omega)_{ks}$ denote such chosen terms. Then, since Ω is absolutely complete,

$$(\omega)_{ks} \equiv c \pmod{h(p, q)} \equiv c \pmod{h(k, s+1), h(k+1, s)}.$$

* $I = 0$ unless $n, n', \frac{1}{2}(n+n')$ are all even.

§ 10. The $(2, 2)^*$ form $f = a_x^2 a_y'^2 = b_x^2 b_y'^2 = \text{etc.}$

The general method readily establishes the complete system of 18 forms. For the system A_1 consists of f and P_2 where

$$P_2 = (ab)^2 a_y'^2 b_y'^2$$

and $A_1 \equiv c \pmod{(ab)(a'b'), (a'b')^2}$.

Let $J = (ab)(a'b') a_x b_x a_y b_y'$ which is complete for the modulus $(a'b')^2$. Then $[A_1, J] \equiv c \pmod{(a'b')^2}$.

Since f, J are of the same orders we need only consider the terms $(f, J)^{\rho\rho_1}, (P_2, J)^{\rho\rho_1}, (P_2, J^2)^{\rho\rho_1}$, $\rho, \rho_1 = 0, 1, 2$.

$$\begin{aligned} \text{Since } J^2 &= Hf^2 - 2C_3 f + P_2 P_2' \\ &= 0 \pmod{f, (a'b')^2} \end{aligned}$$

the third of these transvectants may be rejected.

This gives the system

$$A_2 = f, P_2, J, P_3, \Delta,$$

where

$$A_2 \equiv c \pmod{(a'b')^2},$$

$$P_3 = (ab)^2 (a'c') c_x^2 a_y' b_y'^2 c_y',$$

$$\Delta = (bc)(ca)(ab)(b'c')(c'a')(a'b').$$

Now the modulus $(a'b')^2$ of the system A_2 belongs to the binary quartic

$$P_2' = (a'b')^2 a_x^2 b_x^2$$

whose complete system is known. We may take *single* terms to represent members of this system, for such single terms are complete for modulus M , where M is convolved from P_2' , that is

$$M = (a'b')^2 (ab) = 0 \text{ or else } M = (a'b')^2 (ab)^2 = H, \text{ an invariant.}$$

Let the single terms chosen be

$$P_2, Q_4 = (a'b')^2 (bc)^2 (c'd')^2 Z,$$

$$P_6 = (a'b')^2 (c'd')^2 (e'f')^2 (bc)^2 (de),$$

$$\Delta_4 = (ab)^2 (cd)^2 (a'd')^2 (b'c')^2,$$

and

$$J_6 = (a'b')^2 (c'd')^2 (e'f')^2 (bc)^2 (de)^2 (af)^2.$$

Then if to these we add H the whole set is absolutely complete.

Hence the complete system of f is the derived system of

$$(f, P_2, P_3, J, \Delta) \text{ and } (P_2', Q_4, P_6, \Delta_4, H, J_6).$$

The detailed investigation of these presents no serious difficulty. The indices of necessary transvectants never exceed 2 in value; J_6 is reducible; Δ , Δ_4 , H are invariants. The result is a set of 18 forms.

§ 11. The (3, 3) form $f = \alpha_x^2 \alpha_y^3$.

Using the same notation as far as bracket factors are concerned P'_2 is now a (6, 2) form $\alpha_x^6 \alpha_y'^2$. If A_1 is the system of P'_2 as a binary sextic it is complete mod $(\alpha' \beta')$, and therefore also complete mod $(\alpha' \beta') (\alpha \beta)$, $(\alpha' \beta')^2$.

If now $J_\alpha = (\alpha \beta) (\alpha' \beta') \alpha_x^2 \beta_x^6 \alpha_y' \beta_y'$, then $J_\alpha \equiv c \pmod{(\alpha' \beta')^2}$. Hence $[A_1, J_\alpha] \equiv c \pmod{(\alpha' \beta')^2}$.

Now $(\alpha' \beta')^2 \alpha_x^6 \beta_x^6$ is a binary form of order twelve. Single terms extracted from its complete system are complete mod $(\alpha \beta)^2 (\alpha' \beta')^2$. Transvecting these terms with $[A_1, J_\alpha]$ produces a system complete mod $(\alpha' \beta')^2 (\alpha \beta)^4$.

This last modulus belongs to a binary quartic whose complete system together with the invariant $(\alpha' \beta')^2 (\alpha \beta)^6$ gives, by transvection with the existing system, a complete system for P'_2 .

Now take $f = \alpha_x^2 \alpha_y^3$. From f as a binary cubic in x we construct $A_1 = f$, P_2 , t , Δ where $t = (P_2, f)^{10}$, $\Delta = (P_2, P_2)^{20}$.

If $J = (ab) (\alpha' b') \alpha_x^2 b_x^2 \alpha_x'^2 b_x'^2$, $[A_1, J] \equiv c \pmod{(\alpha' b')^2}$ (§ 6). But P'_2 the (6, 2) form gives a system B_2 of single terms complete mod $(\alpha' b')^3 (ab)$, $(\alpha' b')^2 (ab)^2$, of which the latter leads to a (2, 2) form whose system is complete in single terms mod $(\alpha' b')^3 (ab)^2$, i.e. mod $(\alpha' b')^3 (ab)^3$.

We can now deduce the system A_3 complete mod $(ab)^2 (ab)$, and from the system of this modulus, i.e. from the binary quartic $(\alpha' b')^3 (ab) \alpha_x^2 b_x^2$ we finally derive a complete system of f , if we include the invariant $(\alpha' b')^3 (ab)^3$.

I take this opportunity of thanking the Committee of the Carnegie Trust for their material aid in furthering the preparation and the publication of this investigation.