On totally reducible binary forms: II.

C Hooley

Hardy-Ramanujan Journal
Vol.25 (2002) 22-49

On totally reducible binary forms : II

C. Hooley, FRS.

1. **Introduction**. This paper is the sequel to the first one of the above title ([13], to which we refer as I for brevity), in which we stated we would fulfil the promise made in our paper [3] to resolve the following two problems for binary forms f of degree $l \geq 3$ that are totally reducible as a product of l essentially distinct linear factors with integral coefficients:

(i) to find an asymptotic formula for the number $\Upsilon(n) = \Upsilon_l(n)$ of positive integers that are expressible by f and do not exceed n, each such integer being counted just once regardless of multiplicity of representations;

(ii) to find an upper bound for the number $\nu(n) = \nu_l(n)$ of such integers that are represented in essentially more than one way, where it is to be understood that different representations of a number are to be regarded as essentially distinct when they are not associated through a rational automorphic of the form.

Having settled in I the second question by proving that

$$\nu(n) = O\left(n^{\frac{2}{l}-\eta_l+\epsilon}\right) \tag{1}$$

where

$$\eta_l = \begin{cases} 1/l^2, \text{ if } \ l = 3, \\ (l-2)/l^2(l-1), \text{ if } \ l > 3, \end{cases} \tag{2}$$

and having then deduced that it is usual for a number represented by f to have essentially just one representation, we now ultimately proceed to the first and shall obtain the asymptotic formula

$$\Upsilon(n) = C(f)n^{\frac{2}{l}} + O\left(n^{\frac{2}{l}-\eta_l+\epsilon}\right) \qquad (C(f) > 0)$$

by a procedure that allows us if desired to calculate the value of the constant $C(f)$ in any individual case.

Owing to the concept of the *essential difference* between representations by f, a prerequisite to our work is an understanding of the automorphics of totally reducible binary forms and we therefore, in the apparent absence of previous investigations, devote a large part of the paper to the elucidation of the structure of such automorphics; thus we extend to the category of totally reducible binary forms a study that has long been regarded being of importance in the arithmetical theory of forms. Revealed as being not deficient in interesting properties, the automorphic system is systematically examined to a point beyond that needed for our final goal, the main milestones in the work being Theorems 1 and 2, to which the reader is referred for details.

With this knowledge of the automorphics we proceed to the asymptotic formula for $\Upsilon(n)$ by means of (1) and formulae for sums containing the function $r(m)$ that counts the total number of representations of an integer m by f. Yet we should mention that, had we been content with a weaker result in the required direction, we could have easily derived the lower bound

$$\Upsilon(n) > C_1(f)n^{\frac{2}{l}} \qquad\qquad (C_1(f) > 0, \quad n > n_0)$$

from (1) and merely the single formula

$$\sum_{0<m\leq n} r(m) \sim \ B_1(f)n^{\frac{2}{l}}$$

as soon as we had early on discovered that the number of automorphics of f is absolutely bounded, thus bettering the final argument in I that shewed that it was exceptional for a number represented by f to have more than essentially one representation.

Having indicated how the programme proposed in I will be completed, we find it timely to mention Heath-Brown's very recent paper [1] on rational points on surfaces in projective space that has profound consequences for the theory of binary forms. In particular, generalizing the work of ourselves and others on all binary cubic forms, some quartic forms, sums of two powers, and products of linear forms ([1] itself and [2] are good references for these results, it not being deemed appropriate to quote a full list of citations in view of the nature of our present work), he has settled question (ii) above for all binary forms with integral coefficients of degree three or more - irreducible or reducible over the rationals -, although we must add that in the case under review in our present paper his demonstration is much more taxing for the reader than the one given in I. Yet, while he opined that it might be possible to obtain an asymptotic formula for $\Upsilon(n)$ in the general case, he avoided further discussion of the matter, no doubt because of the other aspects of the subject requiring his attention. It therefore seems appropriate that we should append some brief comments on the automorphics and $\Upsilon(n)$ in

the natural case most distant from ours in which f is irreducible, especially as some of what we have to say enlarges on some comments made in [1] on the former topic.

2. **Preliminaries and the group structure.** In I, being totally reducible over the rationals with no repeated factors, the binary form $f = f(x, y)$ degree $l \geq 3$ was expressed as a product

$$\prod_{1 \leq i \leq l} (h_i x + k_i y) = \prod_{1 \leq i \leq l} L_i(x, y) \tag{3}$$

of linear factors with integer coefficients and therefore had discriminant

$$D = D(f) = \prod_{1 \leq i < j \leq l} (h_i k_j - h_j k_i)^2 > 0.$$

But, since the search for automorphics would be hindered without the use of matrices, it is now desirable to modify the above notation by letting

$$\mathbf{h}_i = (h_i, k_i) \text{and } \mathbf{x} = (x, y) \tag{4}$$

be row and column vectors, respectively, and then rewriting (3) as

$$f(\mathbf{x}) = \prod_{1 \leq i \leq l} \mathbf{h}_i \mathbf{x} = \prod_{1 \leq i \leq l} L_i(\mathbf{x}); \tag{5}$$

here x and y are usually indeterminates but towards the conclusion may be the coordinates of lattice points in the plane. In parallel, having formed the counterpart of (4) with capital letters throughout, we then denote any non-zero 2 x 2 matrix (usually with rational elements) by a bold capital letter other than $\mathbf{H}$ and $\mathbf{X}$ but write the zero matrix as 0. Thus, in particular, the invariant property of the discriminant may be stated as

$$D(F) = M^{l^2 - l} D(f) \tag{6}$$

when $f(\mathbf{x})$ is transformed into $F(\mathbf{X})$ by a substitution $\mathbf{x} = \mathbf{B}\mathbf{X}$ of modulus $M = |\mathbf{B}|$. Lastly we should confirm that by an *automorphic* of f we mean here a rational substitution $\mathbf{x} = \mathbf{A}\mathbf{X}$ with the property that

$$f(\mathbf{x}) = f(\mathbf{X}), \tag{7}$$

although in practice it will often be convenient to let the term refer to the matrix $\mathbf{A}$ rather than the substitution it defines.

The first property of an automorphic $\mathbf{A}$ stems from (6) because it implies that

$$|\mathbf{A}| = \pm \mathbf{I}. \tag{8}$$

Therefore, as is clear from (7), to every automorphic there corresponds an inverse automorphic, and we confirm that the set of all automorphics of f forms a group with identity $\mathbf{I}$ when the operation of multiplication corresponds to the compounding of substitutions (or of multiplication of the representing matrices). Also, since

$$f(\mathbf{x}) = \prod_{1\le i\le l} \mathbf{h}_i\mathbf{x} = \prod_{1\le i\le l} \mathbf{h}_i\mathbf{A}\mathbf{X} = \prod_{1\le i\le l} \mathbf{h}_i\mathbf{X},$$

the uniqueness of the factorization of $f(\mathbf{X})$ implies that the effect of an automorphic transformation is to reorder its factors and affect them with numerical multipliers. Let us then first dismiss what turns out to be the trifling case where at least three of the factors are changed into multiples of themselves. In this instance, since there are three non-proportional vectors $\mathbf{h}_i$ for which $\mathbf{h}_i\mathbf{A}$ is a multiple of $\mathbf{h}_i$, the matrix $\mathbf{A}$ is scalar and is therefore $\mathbf{I}$ or -$\mathbf{I}$ by (8), the latter case occurring when and only when l is even. Any automorphic other than these is then regarded as being *non-trivial*.

This deduction furnishes us with the opportunity to say that the case $l = 2$ has been omitted not only because our application demands that $l > 2$ but also because the structure of the automorphics in the quadratic case is atypical in the general situation. The latter feature is discerned from the formation of the two systems of automorphics defined by

$$\mathbf{h}_1\mathbf{x} = \lambda\mathbf{h}_1\mathbf{X},\ \mathbf{h}_2\mathbf{x} = \lambda^{-1}\mathbf{h}_2\mathbf{X}$$

and

$$\mathbf{h}_1\mathbf{x} = \mu\mathbf{h}_2\mathbf{X},\ \mathbf{h}_2\mathbf{x} = \mu^{-1}\mathbf{h}_1\mathbf{X},$$

each of which contain infinitely many members in contrast to what we shall find later when $l \ge 3$.

If there be a non-trivial automorphic $\mathbf{A}$, then there is at least one factor in $f(\mathbf{x})$ that it changes into a numerical multiple of a different one. Hence, by temporarily reordering the subscripts, we can construct a sequence of equations

$$\mathbf{h}_1\mathbf{A} = \lambda_1\mathbf{h}_2,\ \mathbf{h}_2\mathbf{A} = \lambda_2\mathbf{h}_3, ..., \text{etc.}, \qquad (\mathbf{h}_2 \ne \mathbf{h}_1) \tag{9}$$

that ends when the last $\mathbf{h}_i$ on the right has already occurred and is then easily seen to be $\mathbf{h}_1$. Thus, letting $r > 1$ denote the number of equations in (9), we deduce that

$$\mathbf{h}_1\mathbf{A}^r = \lambda_1\lambda_2 \ldots. \lambda_r\mathbf{h}_1 \text{ and } \mathbf{h}_2\mathbf{A}^r = \lambda_1\lambda_2 \ldots.. \lambda_r\mathbf{h}_2,$$

whence

$$\begin{bmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \end{bmatrix} \mathbf{A}^r = \lambda_1\lambda_2....\lambda_r \begin{bmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \end{bmatrix}$$

so that $\mathbf{A}^r = \lambda_1\lambda_2...\lambda_r\mathbf{I}$ and then $\mathbf{A}^r = \pm\ \mathbf{I}$ by (8). But, being of order 2 x 2 and not being scalar, $\mathbf{A}$ has a minimum polynomial of degree two that must divide either $\lambda^r - 1$ or $\lambda^r + 1$. It must therefore take one of the four forms

$$\text{(i) } \lambda^2 - \lambda + 1, \quad \text{(ii) } \lambda^2 + \lambda + 1, \quad \text{(iii) } \lambda^2 + 1, \quad \text{(iv) } \lambda^2 - 1 \tag{10}$$

that answer to (non-trivial) automorphics $\mathbf{A}$ satisfying the equations

$$\text{(i)}' \ \mathbf{A}^3 = -\ \mathrm{I}, \quad \text{(ii)}' \ \mathbf{A}^3 = \ \mathbf{I}, \quad \text{(iii)} \ \mathbf{A}^2 = -\ \mathbf{I}, \quad \text{(iv)} \ \mathbf{A}^2 = \mathbf{I}.$$

Some preliminary comments on what has so far been inferred can helpfully preface the systematic examination of the structure of automorphic systems. In case (i) the matrix $-\mathbf{I}$ is an automorphic and l is even with the consequence that $-\mathbf{A}$ is of type (ii) and a treatment of (ii) comprehends that of (i). Also, in case (ii) no factor in f is left projectively unaltered by $\mathbf{A}$ because the characteristic roots of $\mathbf{A}$ are the non-real cube roots ω and ω^2 of unity; hence all the factors of f constitute disjoint sets of triplets, the effect of $\mathbf{A}$ and $\mathbf{A}^2$ being to permute cyclically the elements in each triplet. Thus case (ii) can only occur when l is a multiple of three. Similarly case (iii) can only happen when l is even because the characteristic roots of $\mathbf{A}$ would be $\pm\ i$; here, of course, $-\mathbf{I}$ is an automorphic. Yet, in case (iv), l may be odd because it will be seen there might be one factor at most in f that the automorphic transforms into a proportional one even though earlier we worked with the weaker datum that there were not more than two such factors.

Having isolated the types of automorphic that can present themselves in association with a given form, we need a suitable way to describe them in order to analyze how their totality is formed. Accordingly, borrowing a nomenclature due to Mathews in his work on binary cubic forms [5], we designate rational 2 x 2 matrices (whether automorphics or not)whose minimum equations are of type (i) or (ii) as *sub-triplicate* and those whose minimum equations are of type (iii) or (iv) as *sub-duplicate*; furthermore, the symbols $\mathbf{T}$, $\mathbf{D}$, $\mathbf{E}$ (with or without subscript) are to denote, respectively, automorphics belonging to categories (i) or (ii), (iii), (iv). We shall then, for the time being, ignore the form f underlying the previous analysis and shall merely consider how an assembly of such matrices $\mathbf{T}$, $\mathbf{D}$, $\mathbf{E}$ can form a group G in combination, where appropriate, with $-\mathbf{I}$.

Our quest is most easily conducted by using the theory of the rational similarity of matrices. To do this, we first observe that, if $\mathbf{P}$ be a rational non-singular matrix, then the replacement of each element $\mathbf{G}$ in the group by the similar matrix

$$\mathbf{P}\ \mathbf{G}\ \mathbf{P}^{-1} \tag{11}$$

gives rise to an isomorphic group G' in which sub-duplicate and sub-triplicate matrices are derived from elements of the same type. Next, whatever be the group to which they belong, matrices of type $\mathbf{T}$, $\mathbf{D}$, and $\mathbf{E}$ are all non-derogatory in that their characteristic and minimum polynomials are the same, wherefore one verifies from (10) that, for appropriate rational numbers a', b', c' in each instance satisfying the relevant condition stated below, we have

$$\mathbf{D} = \begin{bmatrix} a' & b' \\ c' & -a' \end{bmatrix} \qquad (a'^2 + b'c' = 1),$$

$$\mathbf{E} = \begin{bmatrix} a' & b' \\ c' & -a' \end{bmatrix} \qquad (a'^2 + b'c' = -1),$$

and

$$\mathbf{T} = \begin{bmatrix} a' & b' \\ c' & \pm 1 - a' \end{bmatrix} \qquad (a'^2 \pm a' + b'c' + 1 = 0). \tag{12}$$

With these representations together with a special canonical form to suit each occasion, we are empowered to pursue the investigation by working in whatever isomorphic reflection G' of the group suits us.

We first examine the situation

$$\text{A} \quad - \quad \textit{the assembly contains a sub} - \textit{duplicate of type } \mathbf{D},$$

which, being non-derogatory, may be assumed to be

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

by (10) and the theory of rational similarity (see, for example, MacDuffee [4]). Let us now suppose that, apart from the inverse $\mathbf{D}^{-1} = -\mathbf{D}$, there were another sub-duplicate

$$\mathbf{Q} = \begin{bmatrix} a' & b' \\ c' & -a' \end{bmatrix}$$

within so that

$$\mathbf{DQ} = \begin{bmatrix} c' & a' \\ a' & b' \end{bmatrix}$$

would be either sub-duplicate or sub-triplicate. In the former case, $b' = c'$, $|\mathbf{Q}| = |\mathbf{DQ}| = -a'^2 - b'^2$ is negative and thus -1, and we may write

$$\mathbf{Q} = \mathbf{E}_1 = \frac{1}{c} \begin{bmatrix} a & b \\ b & -a \end{bmatrix} \tag{13}$$

and

$$\mathbf{DQ} = \mathbf{E}_2 = \frac{1}{c}\begin{bmatrix} -b & a \\ a & b \end{bmatrix} \tag{14}$$

where a, b, c are (relatively prime) Pythagorean integers satisfying $a^2 + b^2 = c^2$. Alternatively, if $\mathbf{DQ}$ were sub-triplicate, then $|\mathbf{Q}| = |\mathbf{DQ}| = 1$ and $b' - c' = \pm 1$ by (12) with the implication that $1 = -a'^2 - b'c' = -a'^2 - b'^2 \pm b' \leq \frac{1}{4}$, which inequality is impossible. Consequently, save for $-\mathbf{D}$, any sub-duplicates in the system other than $\mathbf{D}$ are of type $\mathbf{E}$.

Next, if there were within the system a sub-triplicate

$$\mathbf{T} = \begin{bmatrix} a' & b' \\ c' & \pm 1 - a' \end{bmatrix}$$

with determinant $a'(\pm 1 - a') - b'c' = 1$, we could form the product

$$\mathbf{DT} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a' & b' \\ c' & \pm 1 - a' \end{bmatrix} = \begin{bmatrix} -c' & \mp 1 + a' \\ a' & b' \end{bmatrix},$$

which would be sub-triplicate because it cannot be a sub-duplicate with positive determinant. Hence $b' - c' = \pm 1$ and we would infer with some choice of signs that

$$a'^2 \pm a' + 1 + b'^2 \pm b' + 1,$$

the impossibility of which on account of the inequality $u^2 \pm u + 1 \geq \frac{3}{4}$ demonstrates that there are no sub-triplicates in the system.

Finally, there can only be essentially two sub-duplicates of type $\mathbf{E}$, since if $\mathbf{E} \neq \pm\ \mathbf{E_1}$ then, not being $\pm\ \mathbf{I}$ or a sub-triplicate, the matrix $\mathbf{EE_1}$ with determinant 1 is $\pm\ \mathbf{D}$. Hence $\mathbf{E} = \mp\ \mathbf{DE_1} = \mp\ \mathbf{E_2}$ and we substantiate the assertion.

To summarize the situation when A obtains, we see that either the only members of the group are $\pm\ \mathbf{I}, \pm\ \mathbf{D}$ or there are the exactly four additional members $\pm\mathbf{E_1}, \pm\ \mathbf{E_2}$ given by (13) and (14), this still being the position when we revert to the original group. For future reference, we append part of the group table when all eight elements are present;

$$\mathbf{DE_1} = \mathbf{E_2}, \mathbf{ED_1} = -\mathbf{E_2}, \mathbf{E_2E_1} = \mathbf{D}, \mathbf{E_1E_2} = -\mathbf{D}, \mathbf{DE_2} = -\mathbf{E_1}, \mathbf{E_2D} = \mathbf{E_1}. \tag{15}$$

Having finished with case A, we go on to the situation

B – *the congregation contains no sub-duplicate of type* $\mathbf{D}$ *but does contain one of type* $\mathbf{E} = \mathbf{E}_1$, *say,*

which is non-derogatory and for present purposes can therefore be taken to be the companion matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

by an appropriate choice of $\mathbf{P}$ in (11).

If there should be another constituent unequal to $\pm\mathbf{E}_1$, then it certainly includes a sub-duplicate

$$\mathbf{E}_2 = \begin{bmatrix} a_1 & b_1 \\ c_1 & -a_1 \end{bmatrix} \neq \pm\mathbf{E}_1$$

because, having determinant -1, the product of $\mathbf{E}_1$ and a sub-triplicate is a sub-duplicate essentially distinct from $\mathbf{E}_1$. In this situation the matrix

$$\mathbf{E}_2\mathbf{E}_1 = \begin{bmatrix} a_1 & -b_1 \\ c_1 & a_1 \end{bmatrix} \qquad (a_1^2 + b_1c_1 = 1)$$

of determinant 1 is sub-triplicate and has constituents satisfying the conditions $2a_1 = \pm 1$ and $b_1c_1 = \frac{3}{4}$, where the minus sign must be taken when - $\mathbf{I}$ is not included and where it is permitted in the opposite case because $\mathbf{E}_2$ can then be changed into $-\mathbf{E}_2$. Also, if

$$\mathbf{E}_3 = \begin{bmatrix} -\frac{1}{2} & b_2 \\ c_2 & \frac{1}{2} \end{bmatrix} \qquad (b_2c_2 = \frac{3}{4})$$

enjoy the same status as $\mathbf{E}_2$ but be unequal to $\pm\,\mathbf{E}_2$, then

$$\mathbf{E}_2\mathbf{E}_3 = \begin{bmatrix} \frac{1}{4} + b_1c_2 & \frac{1}{2}b_1 - \frac{1}{2}b_2 \\ -\frac{1}{2}c_1 + \frac{1}{2}c_2 & \frac{1}{4} + b_2c_1 \end{bmatrix}$$

is not $\pm\,\mathbf{I}$ and is therefore sub-triplicate, whence $\frac{1}{2} + b_1c_2 + b_2c_1 = \pm 1$ and thus $b_1c_2 + b_2c_1 = \frac{1}{2}$ or $-\frac{3}{2}$. Consequently, as $b_1 = 3/(4c_1)$ and $b_2 = 3/(4c_2)$, the ratio $u = c_2/c_1$ satisfies the condition

$$u + \frac{1}{u} = \frac{2}{3} \quad \text{or} \quad -2,$$

that is, either $(u+1)^2$ or $u^2 - \frac{2}{3}u + 1 = 0$, the latter being impossible for real u. This means that $\mathbf{E}_2$ determines $\mathbf{E}_3$ and vice versa because $b_2 = -b_1, c_2 = -c_1$, and we thus infer that, other than $\mathbf{E}_1$, there are only two essentially different sub-duplicates, which may be expressed as

$$\mathbf{E}_2 = \begin{bmatrix} -\frac{1}{2} & b \\ c & \frac{1}{2} \end{bmatrix},\ \mathbf{E}_3 = \begin{bmatrix} -\frac{1}{2} & -b \\ -c & \frac{1}{2} \end{bmatrix} \qquad (bc = \frac{3}{4}) \tag{16}$$

before we revert to the original group. To these we adjoin the sub-triplicates

$$\mathbf{T} = \mathbf{E}_2\mathbf{E}_3 = \begin{bmatrix} \frac{1}{2} & b \\ -c & -\frac{1}{2} \end{bmatrix} \text{ and } \mathbf{T}^2 = \begin{bmatrix} -\frac{1}{2} & -b \\ c & -\frac{1}{2} \end{bmatrix} = \mathbf{E}_3\mathbf{E}_2 = \mathbf{E}_2\mathbf{E}_1 \tag{17}$$

together with $-\mathbf{T}$ and $-\mathbf{T}^2$ when $-\mathbf{I}$ belongs to the set. There are no other sub-triplicates; indeed, if $\mathbf{T}_1$ were sub-triplicate, then $\mathbf{E}_2\mathbf{T}_1$ of negative determinant would be $\pm\mathbf{E}_1$ or $\pm\mathbf{E}_3$, whence $\mathbf{T}_1 = \pm\mathbf{E}_2\mathbf{E}_1$ or $\pm\mathbf{E}_1\mathbf{E}_3$ and thus $\mathbf{T}_1$ would be $\pm\mathbf{T}^2$ or $\pm\mathbf{T}$. Consequently, if we agree for simplicity that $-\mathbf{I}$ is not to be in the system, then the group table contains the entries

$$\mathbf{E}_1\mathbf{E}_2 = \mathbf{E}_2\mathbf{E}_3 = \mathbf{E}_3\mathbf{E}_1 = \mathbf{T}; \quad \mathbf{E}_2\mathbf{E}_1 = \mathbf{E}_3\mathbf{E}_2 = \mathbf{E}_1\mathbf{E}_3 = \mathbf{T}^2 \tag{18}$$

when the system contains more than the solitary element $\mathbf{E}_1$.

The final case is

$$\mathrm{C} - \textit{the only non} - \textit{trivial elements are sub} - \textit{triplicate},$$

one of which $\mathbf{T}$ may for present purposes be assumed by (10) to be in the canonical form

$$\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \tag{19}$$

and another of which will be its square

$$\mathbf{T}^2 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}. \tag{20}$$

If there were another essentially different sub-triplicate $\mathbf{T}_1$, which may be assumed to be

$$\begin{bmatrix} a & b \\ c & -1-a \end{bmatrix}$$

by a previous comment, then

$$\mathbf{T}_1\mathbf{T} = \begin{bmatrix} -b & a-b \\ 1+a & c+a+1 \end{bmatrix} \text{ and } \mathbf{T}_1\mathbf{T}^2 = \begin{bmatrix} b-a & -a \\ -c-1-a & -c \end{bmatrix}$$

are both sub-triplicate and so

$$a-b+c = 0 \text{ or } -2 \quad \text{and} \quad a-b+c = \pm 1.$$

This being impossible, the only non-trivial elements in the aggregate are $\mathbf{T}, \mathbf{T}^2$ and possibly $-\mathbf{T}$ and $-\mathbf{T}^2$.

However, in case C, we should remark that we can always adjoin three essentially distinct sub-duplicates to produce a full system of type B. This is confirmed by taking them in the present context to be

$$\mathbf{E}_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \mathbf{E}_2 = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, \mathbf{E}_3 = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}, \tag{21}$$

a choice of matrices that we shall have occasion to refer to later. Yet it does not follow that the existence of sub-triplicate automorphics for a form implies that there are necessarily sub-duplicate ones also. Nor is it true that a set of sub-triplicates has a unique adjoining set of sub-duplicates - a failure that will be a source of some extra difficulty in due course.

We have identified all structures that might be possessed by complete sets of automorphics of completely reducible binary forms of degree exceeding two. Although our conclusions can be interpreted geometrically because automorphic transformations permute the asymptotes of the curve $f = n$, it is not easy to substitute a geometrical argument for the more algebraic approach here adopted, particularly as this would not only tell against out powers of description but would also not furnish the numerical information we shall need. We should also stress that we have not yet shewn that actual forms answer to each of the patterns that have been established. But, before we attend to this matter in the next section, we should affirm that, if $f(\mathbf{x})$ have the automorphic $\mathbf{A}$ and $F(\mathbf{X})$ be the metamorphic of f under the non-singular substitution $\mathbf{X} = \mathbf{P}\mathbf{x}$, then $\mathbf{P}\mathbf{A}\mathbf{P}^{-1}$ is an automorphic of $F(\mathbf{X})$; here

$$F(\mathbf{X}) = \prod_{0<i\leq l} \mathbf{H}_i\mathbf{X},$$

where $\mathbf{X}$ and $\mathbf{H}_i$ are contragradient quantities because $\mathbf{h}_i = \mathbf{H}_i\mathbf{P}$. Thus, if G in the sixth paragraph in this section consist of the automorphics of f, then its isomorphic echo G' formed through (11) according to the dictates of cases A, B, or C is formed in like manner from F, the coefficients of which are rational but not necessarily integral. Save in one instance, however, this is a principle we shall avoid, since we prefer to work with the original set of automorphics owned by a given form. Thus the symbols $\mathbf{D}$, $\mathbf{E}$, and $\mathbf{T}$ will not usually denote the canonical and semi-canonical representations appearing in the earlier examination of A, B, and C.

3. **Forms with prescribed sets of automorphics - cases B and C.** In summary our main conclusion will be that generically (we do not delay to give an exact meaning to this term) a totally reducible form of degree $l \geq 4$ has only trivial automorphics but that, to whatever automorphic pattern in A, B, or C be postulated, there correspond forms of any degree $l \geq 4$ that is not trivially incompatible with the proposed layout (e.g. l must be a multiple of 3 if C be intended. The case $l = 3$, with which we start, is, however, exceptional and will be important in our discussion of larger values of l.

When $f(\mathbf{x})$ is a cubic, let us write it as

$$\mathbf{h}_1\mathbf{x}.\mathbf{h}_2\mathbf{x}.\mathbf{h}_3\mathbf{x} = L_1(\mathbf{x})L_2(\mathbf{x})L_3(\mathbf{x})$$

as in (5) and let the signed minors in

$$\begin{bmatrix} h_1 & h_2 & h_3 \\ k_1 & k_2 & k_3 \end{bmatrix}$$

taken in the obvious order be H_1, H_2, H_3, all of which are non-zero by the non-vanishing of the discriminant. Then, in view of the identity

$$H_1L_1(\mathbf{x}) + H_2L_2(\mathbf{x}) + H_3L_3(\mathbf{x}) = 0, \tag{22}$$

the six substitutions (of determinant $H_1H_2H_3$)

$$X = -H_iL_i(\mathbf{x}), \quad Y = -H_jL_j(\mathbf{x}) \quad (i \neq j; 1 \leq i, j \leq 3)$$

all transform $H_1H_2H_3f(\mathbf{x})$ into the form

$$XY(X + Y). \tag{23}$$

Since compounding one such substitution with the inverse of one of them creates an automorphic of f, there are six automorphics in all, as may be also inferred by treating (23) directly. Furthermore, it is easily verified that we are presented with a complete system of type B, especially if we note that the automorphics of (23) include $\mathbf{T}$ and the matrices (21) in the analysis of C. Thus every cubic admits a full complement of automorphics, a property that we shall shortly see is not enjoyed by arbitrary forms of higher degree.

The automorphic set of a given cubic is unique and therefore determined by $\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3$. But, to obtain the explicit expressions for the sub-triplicates $\mathbf{T}, \mathbf{T}^2$ we prefer, we substitute in (22) the equations

$$\mathbf{h}_2 = \lambda\mathbf{h}_1\mathbf{T}, \quad \mathbf{h}_3 = \mu\mathbf{h}_2\mathbf{T}^2, \quad \mathbf{h}_3 = (\mu/\lambda)\mathbf{h}_2\mathbf{T}$$

related to (9) to obtain

$$\mathbf{h}_1(H_1\mathbf{I} + \lambda H_2\mathbf{T} + \mu H_3\mathbf{T}^2) = 0$$

so that $H_1\mathbf{I} + \lambda H_2\mathbf{T} + \mu H_3\mathbf{T}^2$ is singular. Then, since the minimum polynomial $1 + u + u^2$ of $\mathbf{T}$ is irreducible over the rationals, we deduce that $\lambda = H_1/H_2$ and $\mu = H_1/H_3$, which yield

$$H_2\mathbf{h}_2 = H\mathbf{h}_1\mathbf{T}, \qquad H_3\mathbf{h}_3 = H_2\mathbf{h}_2\mathbf{T}$$

and hence the desired evaluation of $\mathbf{T}$ as the matrix

$$\begin{bmatrix} H_1\mathbf{h}_1 \\ H_2\mathbf{h}_2 \end{bmatrix}^{-1} \begin{bmatrix} H_2\mathbf{h}_2 \\ H_3\mathbf{h}_3 \end{bmatrix} = \frac{1}{H_1H_2H_3} \begin{bmatrix} H_2^2h_2k_2 - H_1H_3k_1h_3 & H_2^2k_2^2 - H_1H_3k_1k_3 \\ -H_2^2h_2^2 + H_1H_3h_1h_3 & -H_2^2h_2k_2 + H_1H_3h_1k_3 \end{bmatrix}, \tag{24}$$

no entry being an identically zero rational function. A similar expression is available for the other sub-triplicate $\mathbf{T}^2$ whose action is to take the factors $\mathbf{h}_1\mathbf{x},\ \mathbf{h}_2\mathbf{x},\ \mathbf{h}_3\mathbf{x}$ into multiples of $\mathbf{h}_3\mathbf{x},\ \mathbf{h}_1\mathbf{x},\ \mathbf{h}_2\mathbf{x}$, respectively; it is of course derived from $\mathbf{T}^{-1}$, which equals

$$\frac{1}{H_1H_2H_3}\begin{bmatrix} -H_2^2h_2k_2+H_1H_3h_1k_3 & -H_2^2k_2^2+H_1H_3k_1k_3 \\ H_2^2h_2^2-H_1H_3h_1h_3 & H_2^2h_2k_2-H_1H_3k_1h_3 \end{bmatrix}. \tag{25}$$

Conversely, apart from scalar multipliers, cubic forms sharing the same set of automorphics are identical. Supposing that $f(\mathbf{x})$ to have given sub-duplicates $\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3$ (and hence given sub-triplicates via (18)), then by a suitable ordering of the subscripts we have

$$\mathbf{h}_1\mathbf{E}_1 = \lambda_1\mathbf{h}_1,\ \mathbf{h}_2\mathbf{E}_1 = \lambda_2\mathbf{h}_3,\ \mathbf{h}_3\mathbf{E}_1 = \lambda_3\mathbf{h}_2,$$

where $\lambda_2\lambda_3 = 1$ because $\mathbf{E}_1^2 = \mathbf{I}$. Hence, as $\mathbf{E}_1$ is an automorphic, $\lambda_1 = 1$ and $\mathbf{h}_1$ is the unique (to within a scalar multiple) characteristic vector of $\mathbf{E}_1$ (taken on the left) corresponding to the characteristic root 1 (the other root is - 1). Similarly $\mathbf{h}_2,\ \mathbf{h}_3$ are, respectively, characteristic vectors of $\mathbf{E}_2,\ \mathbf{E}_3$ associated with the value 1 of the characteristic roots, and the proposition follows.

The above method is the basis for shewing there is actually a (unique) cubic form admitting a given full set of proposed automorphics of type B. This is constructed by taking integral characteristic vectors $\mathbf{h}_1,\ \mathbf{h}_2,\ \mathbf{h}_3$ of $\mathbf{E}_1,\ \mathbf{E}_2,\ \mathbf{E}_3$ corresponding to the characteristic roots of value 1. These are non-proportional and $f(\mathbf{x}) = \mathbf{h}_1\mathbf{x}.\mathbf{h}_2\mathbf{x}.\mathbf{h}_3\mathbf{x}$ has distinct factors, since if for example $\mathbf{h}_1\mathbf{E}_1 = \mathbf{h}_1$ and $\mathbf{h}_1\mathbf{E}_2 = \mathbf{h}_1$ then by (18) we would have $\mathbf{h}_1\mathbf{T} = \mathbf{h}_1\mathbf{E}_1\mathbf{E}_2 = \mathbf{h}_1\mathbf{E}_2 = \mathbf{h}_1$, which would imply that $\mathbf{T}$ had a real characteristic root. Also, as $\mathbf{h}_2\mathbf{E}_1 = (\mathbf{h}_2\mathbf{E}_2)\mathbf{E}_1 = (\mathbf{h}_2\mathbf{E}_1)\mathbf{E}_3$, $\mathbf{h}_2\mathbf{E}_1$ is a characteristic vector of $\mathbf{E}_3$ associated with the characteristic root 1 and is therefore $\lambda\mathbf{h}_3$. Hence $\mathbf{h_3E_3} = \lambda^{-1}\mathbf{h_2}$ and $f(\mathbf{E}_1\mathbf{x}) = f(\mathbf{x})$, the matrices $\mathbf{E}_2,\ \mathbf{E}_3$ being similarly automorphics as are then $\mathbf{T}$ and $\mathbf{T}^2$.

Still involving ourselves with cases B and C, we proceed to the more general case where l is thrice an integer m, say. Let us take *arbitrary* integral vectors $\mathbf{h_1^{(i)}} = \mathbf{h^{(i)}}$ for $1 \le i \le m$ and, with any given sub-triplicate matrix $\mathbf{T}$ and suitable scalars λ_i, μ_i, form the integral vectors $\mathbf{h}_2^{(i)} = \lambda_i\mathbf{h}_1^{(i)}\mathbf{T}$ and $\mathbf{h}_3^{(i)} = \mu_i\mathbf{h}_1^{(i)}\mathbf{T}^2$, where clearly no two vectors $\mathbf{h}_j^{(i)}$ with different markings are proportional. Then, since the metamorphic of the form

$$f^{(i)}(\mathbf{x}) = \mathbf{h}_1^{(i)}\mathbf{x}.\mathbf{h}_2^{(i)}\mathbf{x}.\mathbf{h}_3^{(i)}\mathbf{x}$$

under the rational substitution $\mathbf{x} = \mathbf{TX}$ is

$$\mathbf{h}_1^{(i)}\mathbf{TX}.\mathbf{h}_2^{(i)}\mathbf{TX}\ .\ \mathbf{h}_3^{(i)}\mathbf{TX} \quad = \quad \lambda_i^{-1}\mathbf{h}_2^{(i)}\mathbf{X}.\lambda_i\mu_i^{-1}\mathbf{h}_3^{(i)}\mathbf{X}.\mu_i\mathbf{h}_1\mathbf{X} = f^{(i)}(\mathbf{X}),$$

we see that $\mathbf{T}$ and $\mathbf{T}^2$ are automorphics of $f^{(i)}(\mathbf{x})$ and then of the form

$$f_m(\mathbf{x}) = \prod_{1\le i\le m} f^{(i)}(\mathbf{x}) \tag{26}$$

having distinct linear factors. Thus there are forms of arbitrary degree $3m$ that admit subtriplicate automorphics. Conversely, from the comments in §2, one deduces that the factors of any form admitting an automorphic system $\mathbf{T}, \mathbf{T}^2$ may so ordered that the form is cast into the shape (26). In this event, because in particular $\mathbf{T}$ is an automorphic of $f^{(1)}(\mathbf{x})$ and $f^{(2)}(\mathbf{x})$ when $m > 1$, (24) and (25) imply a non-trivial polynomial relationship between the coefficients of the factors in $f^{(1)}(x)$ and $f^{(2)}(x)$. Thus, generically, factorizable forms of degree greater than three have no automorphic system of type C.

We must next treat matters when the full panoply of case B is in place so that automorphics of type $\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3$ appear in addition to $\mathbf{T}$ and $\mathbf{T}^2$. We take the forms $f^{(i)}(\mathbf{x})$ as before and construct integral forms of the type

$$g^{(i)}(\mathbf{x}) = \rho_i f^{(i)}(\mathbf{E}_1\mathbf{x}), \tag{27}$$

observing that $\mathbf{E}_1$ in the definition may be replaced by $\mathbf{E}_2$ or $\mathbf{E}_3$ because, for example,

$$f^{(i)}(\mathbf{E}_1\mathbf{x}) = f^{(i)}(\mathbf{T}^2\mathbf{E}_1 x) = f^{(i)}(\mathbf{E}_2 x)$$

by (18). Then

$$g^{(i)}(\mathbf{Tx}) = \rho_\mathbf{i}\mathbf{f^{(i)}}(\mathbf{E_1 Tx}) = \rho_\mathbf{i}\mathbf{f^{(i)}}(\mathbf{E_2 x}) = \mathbf{g^{(i)}}(\mathbf{x})$$

and $\mathbf{T}$and $\mathbf{T}^2$ are automorphics of

$$\gamma^{(i)}(\mathbf{x}) = f^{(i)}(\mathbf{x})g^{(i)}(\mathbf{x}),$$

as are $\mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3$ in virtue of the relations

$$g^{(i)}(\mathbf{E}_j\mathbf{x}) = \rho_i f^{(i)}(\mathbf{x}) \text{ and } f^{(i)}(\mathbf{E}_j\mathbf{x}) = \rho_i^{-1} f^{(i)}(\mathbf{x}).$$

Thus there are forms

$$\gamma_m(\mathbf{x}) = \prod_{1\le i\le m} \gamma^{(i)}(\mathbf{x}) \tag{28}$$

of arbitrary degree $6m$ with given automorphics $\mathbf{T}, \mathbf{T}^2, \mathbf{E}_1, \mathbf{E}_2, \mathbf{E}_3$; these naturally also admit the automorphic $\mathbf{I}$. As for forms of a degree that is an odd multiple $2r+1$ of three, all we need to do is take $\gamma_r(\mathbf{x})$ as in (28) and multiply it by the unique cubic having the assigned automorphics. Conversely, by augmenting previous reasoning, we do not find it difficult to shew that all forms admitting a full system under B are of the type already produced; these we have seen to be non-generic when $l > 3$.

To continue our analysis of case B we must dispose of the situation where it is given that $f(\mathbf{x})$ has an automorphic of type $\mathbf{E}$ but should note that case A will also arise as soon as we consider how other automorphics can be adjoined. Here to each linear factor $\mathbf{h}_i\mathbf{x}$ there corresponds a factor $\mathbf{h}_j = \lambda\mathbf{h}_i\mathbf{E}$. If $\mathbf{h}_i$ and $\mathbf{h}_j$ be unequal, then $\mathbf{h}_i = \lambda^{-1}\mathbf{h}_j\mathbf{E}$ and $\mathbf{E}$ is an automorphic of the divisor $\mathbf{h}_i\mathbf{x}.\mathbf{h}_j\mathbf{x}$ of $f(\mathbf{x})$. If, however, $i = j$, then $\lambda = \pm 1$, the negative sign in which must be disallowed because it could only occur at most once and the form cannot be permitted to change sign. We thus obtain forms with an even number of factors, unless one factor correspond to the characteristic vector of $\mathbf{E}$ related to the characteristic root 1. This conclusion being subsumed for $l = 3$ under earlier decisions about cubic forms, the circumstances currently delineated are nevertheless not generic for forms of higher degree. But we postpone the proof till later in order to avail ourselves of a method developed to treat case A, to which we shall go on after settling two final aspects of cases B and C.

The first is that forms admitting any automorphic $\mathbf{E}$ do not generically have other non-trivial automorphics in a system of type B. This is clear when l is not divisible by three so let us, for sake of illustration, consider the case $l = 6$ by utilizing the final principle enunciated in §2. We are thus presented with a form (or multiple thereof) constructed from general vector coefficients $\mathbf{h}_1,\ \mathbf{h}_2,\ \mathbf{h}_3$ and their transforms $\mathbf{h}_1\mathbf{E}, \mathbf{h}_2\mathbf{E}, \mathbf{h}_3\mathbf{E}$, where

$$\mathbf{E} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

is the canonical form in the examination of case B and where therefore the last three vectors are obtained by the first by reversing the signs of $k_1,\ k_2,\ k_3$. By previous arguments, if the form possess sub-triplicate automorphics, then expression (24) in $\mathbf{h}_1,\ \mathbf{h}_2,\ \mathbf{h}_3$ must equal either (24) or (25) in terms of the transformed vectors. Hence, since $H_1,\ H_2,\ H_3$ change sign as a result of applying $\mathbf{E}$, we compare either the leading elements in (24) in the two circumstances or compare the second elements in the first rows of (24) and (25) that answer to each situation. In the first trial it is easily ascertained that the elements are unequal because $\mathbf{h}_1,\ \mathbf{h}_2,\ \mathbf{h}_3$ are generic, whereas in the second the elements are equal but opposite in sign. Hence, in general, the form admits only the non-trivial automorphic $\mathbf{E}$.

The other fact we wish to establish is that generically a form admitting a system of automorphics $\mathbf{T}, \mathbf{T}^2$ does not possess a maximal system in category B. This is not as easy as it seems because, as already stated, for given $\mathbf{T}$ a set $\mathbf{E}_1,\ \mathbf{E}_2,\ \mathbf{E}_3$ to augment the group structure of matrices is not unique. To demonstrate this proposition it is plain by previous arguments that it suffices to consider the case $l = 6$ and $f(\mathbf{x})$ is of type (26) with $m = 2$. Then, if $\mathbf{E} = \mathbf{E}_1$, say, be also an automorphic, then by the construction in (27) and the group

table (18) we have, for example,

$$\mathbf{h}_1^{(2)} = \rho \mathbf{h}_1^{(1)} \mathbf{E}_1 \quad = \quad \rho \mathbf{h}_1^{(1)} \mathbf{T} \mathbf{E}_2$$

and

$$\mathbf{h}_1^{(2)} \mathbf{T} = \rho \mathbf{h}_1^{(1)} \mathbf{E}_1 \mathbf{T} \quad = \quad \rho \mathbf{h}_1^{(1)} \mathbf{E}_2,$$

whence

$$\begin{bmatrix} \mathbf{h}_1^{(2)} \\ \mathbf{h}_1^{(2)} \mathbf{T} \end{bmatrix} \quad = \quad \rho \begin{bmatrix} \mathbf{h}_1^{(1)} \mathbf{T} \\ \mathbf{h}_1^{(1)} \end{bmatrix} \mathbf{E}_2$$

with the implication that

$$\begin{vmatrix} \mathbf{h}_1^{(2)} \\ \mathbf{h}_1^{(2)} \mathbf{T} \end{vmatrix} \quad = \quad \rho^2 \begin{vmatrix} \mathbf{h}_1^{(1)} \\ \mathbf{h}_1^{(1)} \mathbf{T} \end{vmatrix} \tag{29}$$

since $|\mathbf{E}_2| = -1$. Let us now write $\mathbf{h}_1^{(1)} = \left(h^{(1)}, k^{(1)}\right), \mathbf{h}^{(2)} = \left(h^{(2)}, k^{(2)}\right)$, and

$$\mathbf{T} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix},$$

where $\alpha + \delta = 1$ and $\alpha\delta - \beta\gamma = 1$. Then, since (29) becomes

$$\begin{vmatrix} h^{(2)} & k^{(2)} \\ \alpha h^{(2)} + \gamma k^{(2)} & \beta h^{(2)} + \delta k^{(2)} \end{vmatrix} \quad = \quad \rho^2 \begin{vmatrix} h^{(1)} & k^{(1)} \\ \alpha h^{(1)} + \gamma k^{(1)} & \beta h^{(1)} + \delta k^{(1)} \end{vmatrix},$$

we deduce that

$$\beta h^{(2)2} + (\delta - \alpha) h^{(2)} k^{(2)} - \gamma k^{(2)2} \quad = \quad \rho^2 (\beta h^{(1)2} + (\delta - \alpha) h^{(1)} k^{(1)} - \gamma k^{(1)2}, \tag{30}$$

the quadratic form here having determinant

$$(\delta - \alpha)^2 + 4\beta\gamma = (\delta + \alpha)^2 - 4(\alpha\delta - \beta\gamma) = -3$$

and therefore being positive definite on multiplication of (30) by -1 if necessary.

From the construction of $f(\mathbf{x})$ we may assume that $\mathbf{h}_1^{(1)}$ and $\mathbf{h}_2^{(2)}$ are generic with both $h^{(1)}, k^{(1)}$ and $h^{(2)}, k^{(2)}$ relatively prime. On the other hand, clearing the quadratic form of denominators to lead to a properly primitive form ψ, we would have

$$\psi(h^{(2)}, k^{(2)}) = \rho^2 \psi(h^{(1)}, k^{(1)}),$$

which would yield an impossibility if we fixed $h^{(1)}$, $k^{(1)}$ and chose $h^{(2)}$, $k^{(2)}$ so that $\psi(h^{(2)}, k^{(2)})$ was a large prime number (or, more easily, a large square-free number). Our assertion is therefore substantiated.

4. **Forms with prescribed sets of automorphics - case A.** We switch our attention to forms having systems of automorphics of type A. If $\mathbf{hx}$ divide a form $f(\mathbf{x})$ possessing the automorphic $\mathbf{D}$, then so do $\lambda\mathbf{hDx}$ and

$$\psi_{\mathbf{h}}(\mathbf{x}) = \mathbf{hx}.\lambda\mathbf{hDx}$$

for a suitable scalar λ because $\mathbf{D}$ has purely imaginary characteristic roots. Since $\psi(\mathbf{Dx}) = -\psi(\mathbf{x})$, the form is therefore a product of an even number of such quadratics and l is a multiple of four. Conversely, by reasoning similar to that used in the previous Section, one sees that one can construct forms of arbitrary degree $4m$ having a given matrix $\mathbf{D}$ as an automorphic.

Suppose now that $f(\mathbf{x})$ also admits automorphics $\mathbf{E}_1$ and $\mathbf{E}_2$ of the sort considered under the classification of Category A. Then the argument in paragraph 8 of §3 demonstrates that, for every factor $\mathbf{hx}$ of f, there is a distinct one of the form $\lambda_i\mathbf{hE}_i\mathbf{x}$ because f has even degree. Like reasoning shewing that $\lambda\mathbf{hDx}$ is non-proportional to $\lambda_1\mathbf{hE}_1\mathbf{x}$ and $\lambda_2\mathbf{hE}_2\mathbf{x}$, we deduce that f is a product of quartics of the type

$$\psi^*_{\mathbf{h}}(\mathbf{x}) = \mathbf{hx}.\lambda\mathbf{hDx}.\lambda_1\mathbf{hE}_1\mathbf{x}.\lambda_2\mathbf{hE}_2\mathbf{x} \tag{31}$$

Also, multiplying the matrices

$$\mathbf{I}, \mathbf{D}, \mathbf{E}_1, \mathbf{E}_2$$

by $\mathbf{D}, \mathbf{E}_1, \mathbf{E}_2$ in turn, we obtain the rows

$$\mathbf{D}, -\mathbf{I}, -\mathbf{E}_2, \mathbf{E}_1$$
$$\mathbf{E}_1, \mathbf{E}_2, \mathbf{I}, \mathbf{D}$$
$$\mathbf{E}_2, -\mathbf{E}_1, -\mathbf{D}, \mathbf{I}$$

with the conclusion that $\psi^*_{\mathbf{h}}(\mathbf{x})$ itself possesses a full set of automorphics of type A. Thus there is no limitation on the number of quartics $\psi^*_{\mathbf{h}}(\mathbf{x})$ of which f is composed, while it is illuminating to confirm that $\psi^*_{\mathbf{h}}(\mathbf{x})$ itself is a multiple of the product $\psi_{\mathbf{h}}(\mathbf{x})\psi_{\mathbf{E}_2\mathbf{h}}(\mathbf{x})$ in accord with our earlier finding. Conversely, given any proposed full system of the type A, we can clearly find forms of arbitrary degree $4m$ admitting it by simply choosing vectors $\mathbf{h}$ in (31) that are not characteristic vectors of $\mathbf{E}_1$ or $\mathbf{E}_2$.

To investigate the degree of generality possessed by the various classes of forms pertaining to Category A it is desirable to express quartic factorizable forms in a canonical manner. Letting

$$f(\mathbf{x}) = \mathbf{h}_1\mathbf{x}.\mathbf{h}_2\mathbf{x}.\mathbf{h}_3\mathbf{x}.\mathbf{h}_4\mathbf{x} = \phi(\mathbf{x})\mathbf{h}_4\mathbf{x}, \text{ say,} \tag{32}$$

we find a rational linear substitution $\mathbf{x} = \mathbf{P}\mathbf{X}$ as earlier to throw a suitable numerical multiple of the cubic $\phi(\mathbf{x})$ into $XY(X+Y)$ so that $F(\mathbf{X}) = f(\mathbf{x})$ has the configuration

$$XY(X+Y)(aX+bY), \tag{33}$$

where it may be assumed that $(a,b) = 1$. This is not unique because $\phi(\mathbf{x})$ can be cast into $F(\mathbf{X})$ in six ways, while $\phi(\mathbf{x})$ can be chosen in four ways. However, the constancy of the anharmonic ratio of quantities transformed under an homography implies that, if $XY(X+Y)(cX+dY)$ be another metamorphic of (32) under our procedure, then certainly the anharmonic ratio c/d of $0, \infty; -d/c, -1$ is equal to one of

$$a/b, b/a; 1-a/b, 1-b/a; b/(b-a), a/(a-b); \tag{34}$$

indeed, whatever final factor $ax+by$ in (33) present itself, the set in (34) remains invariant save for order. There are thus actually at most six canonical forms pertaining to a given quartic, any one of which determines the others. Furthermore, it is plain from (34) that generically none of the final factors in the canonical forms of $f(\mathbf{x})$ is of the type $\pm(u^2X - v^2Y)$ for coprime integers u, v.

Let us suppose that the quartic form admits an automorphic of type $\mathbf{D}$. Then, for one of the forms (32) corresponding to f, there will be an automorphic $\mathbf{D}_1$ that has the effect of interchanging X and Y and also $X+Y$ and $aX+bY$. Having positive determinant, it thus induces a linear substitution

$$X = \lambda\eta, \quad Y = -\lambda^{-1}\xi, \tag{35}$$

which transforms $(X+Y)(aX+bY)$ into the product

$$\left(-\lambda^{-1}\xi + \lambda\eta\right)\left(-b\lambda^{-1}\xi + a\lambda\eta\right)$$

that must equal $-(\xi+\eta)(a\xi+b\eta)$. Hence $\lambda^2 = -b/a$ and we deduce that

$$a = \pm u^2, \quad b = \mp v^2, \quad (u,v) = 1;$$

furthermore, we confirm in this event that (35) is actually an automorphic of the type $\mathbf{D}$ when $\lambda = \pm\sqrt{(-b/a)}$. Consequently, generically, quartic factorizable forms do not admit automorphics of the sort $\mathbf{D}$ and, a fortiori, neither do forms of general degree $4m$.

We must next consider in what circumstances does a form f admitting an automorphic $\mathbf{D}$ also possess an automorphic $\mathbf{E} = \mathbf{E}_1$, say, and hence also $\mathbf{E}_2$ and $\mathbf{E}_3$. Taking quartics first and using the canonical form

$$XY(X+Y)(u^2X - v^2Y),$$

we must look for a substitution of modulus -1 that, for example, transforms X and $X+Y$ into multiples of $\xi+\eta$ and ξ. We find that

$$X = \lambda^{-1}(\xi+\eta) \text{ and } X+Y = \lambda\xi$$

so that

$$Y = (\lambda - \lambda^{-1})\xi - \lambda^{-1}\eta$$

must be a multiple of $u^2\xi - v^2\eta$. Hence $\lambda^2 - 1 = u^2/v^2$ and we require that u^2+v^2 be a perfect square. Thus, generically, forms of degree $4m$ admitting an automorphic of type **D** do not possess a full system of automorphics belonging to Category A.

Two other matters need to be addressed in this Section. The first concerns the assertion made in §3 that generically a form of degree four or more does not own an automorphic of type **E**. It again being enough to take the case where f is a quartic with such an automorphic, let (33) be that canonical form of f which is such that the derived automorphic $\mathbf{E}_1$ has the effect of interchanging X and Y and also $X+Y$ and $aX+bY$. Then, if we imitate the analysis from ((35) above but suppress the minus sign in this equation, we easily find now that $a = \pm u^2, b = \pm v^2$, and $ax+by = \pm(u^2x+v^2y)$, therefore substantiating our claim. Moreover, if f also admit an automorphic **D**, then a slight modification of previous thinking produces the further condition that $u^2 - v^2$ be a perfect square w^2. Consequently, a form admitting an automorphic **E** does not generically possess a full system of automorphics of type A any more than, as shewn earlier, it can possess a full system of type B.

We have completed our deliberations on prescribed sets of automorphics and therefore encapsulate our main conclusions in

THEOREM 1. *Apart from the trivial system containing* **I** *and also* -**I** *when the degree is even, the automorphic systems of totally reducible forms of degree* $l \geq 3$ *are limited to partial or complete structures delineated in* A, B, *and* C *above.*

Every cubic form admits a full system of type B; *conversely, to each system, there answers a unique (to within numerical multiples) cubic possessing it.*

Corresponding to any proposed automorphic system, either trivial or of types A, B, *or* C *(incomplete or full), there exist forms of any degree* $l > 3$ *that is not inconsistent with the type of system (e.g., if the form be to admit* **T**, *then* l *must be a multiple of* 3*). Therefore, generically, a form of degree exceeding three appertaining to an automorphic system will not*

appertain to a wider system; in particular, a general form of degree exceeding three only admits trivial automorphics.

5. **Integral and associated points.** We draw nearer to our final goal by introducing the concept of association between lattice points $\mathbf{x}$ in order to provide a path from the total number $r(n)$ of representations of an integer n by f to the number $r_1(n)$ of such representations that are essentially different. Supposing that f be given, we shall say in the notation $\mathbf{x}\sim\mathbf{x}'$ that the lattice points $\mathbf{x}$, $\mathbf{x}'$ are *associated* (relative to f) if there be an automorphic $\mathbf{A}$ of f with the property that $\mathbf{x}' = \mathbf{A}\mathbf{x}$. Since association constitutes an equivalence relation, the integral points in the plane are distributed into disjoint sets, each of which contains all points, finite in number, that are associated with any one of its members. We should then note that it can happen that a point $\mathbf{x}$ is associated with itself not only through the trivial automorphic but also through another one $\mathbf{A}$, in which case $\mathbf{x} = \mathbf{A}\mathbf{x}$ so that $\mathbf{A}$ is of the type $\mathbf{E}$ and $\mathbf{x}$ lies on a finite number of radii vectores emanating from the origin.

However, from our intended application of our earlier work, we also need a different and somewhat less shallow relationship between points and automorphics. Let us suppose that f has at least two essentially different non-trivial automorphics $\mathbf{A}$ and $\mathbf{B}$. In this case, it is not obvious that, if $\mathbf{x}$ be an integral point for which both $\mathbf{A}\mathbf{x}$ and $\mathbf{B}\mathbf{x}$ are integral, then so is $\mathbf{A}\mathbf{B}\mathbf{x}$, or, in other words, that the automorphics turning a given integral point $\mathbf{x}$ into another one form a sub-group $G(\mathbf{x})$ of G. Yet this, as we shall shew, is actually true and greatly simplifies our later analysis of sets of points associated through more than a single automorphic.

To found this principle we shall usually, but not invariably, work not with the group G of automorphics of f but with an isomorphic group G', which is chosen by deciding whether G belong to A, B or C and then identifying the group of matrices used in §2 to discuss the case at issue. If now $\mathbf{A}_1$ in G' be derived from $\mathbf{A}$ in G by the transformation (11) that is appropriate for the circumstances, we have $\mathbf{A}= \mathbf{P}^{-1}\mathbf{A}_1\,\mathbf{P}$ and then

$$\mathbf{P}\mathbf{A} = \mathbf{A}_1\mathbf{P}, \qquad \mathbf{P}(\mathbf{A}\mathbf{x}) = \mathbf{A}_1(\mathbf{P}\mathbf{x}),$$

where we may clearly assume that

$$\mathbf{P} = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

has coprime integral elements and $\triangle = |\alpha\delta - \beta\gamma| > 0$. To profit from this, let a point (or vector) $\mathbf{u} = (u, v)$ with integral elements be termed *special* if it be of the form $\mathbf{P}\mathbf{x}$ for integral

$\mathbf{x}$, the two conditions that it be so being evidently

$$\delta u - \beta v \equiv 0, \text{mod } \triangle, \qquad (36)_{\text{A}}$$

$$\gamma u - \alpha v \equiv 0, \text{mod } \triangle. \qquad (36)_{\text{B}}$$

Therefore the relation of association (relative to f) translates into a relation between special points $\mathbf{u}, \mathbf{u}'$ of the type $\mathbf{u}' = \mathbf{A}_1\mathbf{u}$, and what we wish to establish is tantamount to shewing that $\mathbf{A}_1\mathbf{B}_1\mathbf{u}$ is special when $\mathbf{u}$, $\mathbf{A}_1\mathbf{u}$, $\mathbf{B}_1\mathbf{u}$ are. But, in practice, when working in G' we adopt the custom in §2 of not distinguishing notationally between its elements and the corresponding ones in G.

Since the square of a sub-duplicate is a trivial automorphic, it is clear that we can limit our investigations to cases where G or G' contains two essentially distinct non-trivial elements. The first such situation being where f appertains to a full system in Category A, we are provided with the matrices

$$\mathbf{D} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{E}_1 = \frac{1}{c}\begin{bmatrix} a & b \\ b & -a \end{bmatrix}, \quad \mathbf{E}_2 = \frac{1}{c}\begin{bmatrix} b & -a \\ -a & -b \end{bmatrix},$$

where $c^2 = a^2 + b^2$ and $\mathbf{E_1D} = -\mathbf{DE_1} = \mathbf{E_2}$. These matrices transform a special vector $\mathbf{u}$ into

$$(-v, u), \quad \frac{1}{c}(au + bv, bu - av), \quad \frac{1}{c}(bu - av, -au - bv),$$

where the conditions for any one of these to be special lie in the appropriate line of the equations

$$\beta u + \delta v \equiv 0, \quad \text{mod}\Delta, \qquad (37)_{\text{A}} \qquad \alpha\text{u} + \gamma\text{v} \equiv 0, \quad \text{mod } \Delta, \quad (37)_{\text{B}}$$

$$\delta(au + bv - \beta(bu - av) \equiv 0, \quad \text{mod c}\Delta, \quad (38)_{\text{A}} \quad \gamma(\text{au} + \text{bv}) - \alpha(\text{bu} - \text{av}), \quad \text{mod c}\Delta, \quad (38)_{\text{B}}$$

$$\delta(bu - av) + \beta(au + bv) \equiv 0, \quad \text{mod c}\Delta, \qquad (39)_{\text{A}} \quad \gamma(\text{bu} - \text{av}) + \alpha(\text{au} + \text{bv}), \quad \text{mod c}\Delta, \quad (39)_{\text{B}}$$

Let us now suppose, for instance, that both $\mathbf{Du}$ and $\mathbf{E}_1\mathbf{u}$ are special so that all the stipulations $(36)_{\text{A}}, (37)_{\text{A}}$, and $(38)_{\text{A}}$ are in place with the first implication that

$$(\beta^2 + \delta^2)(u^2 + v^2) = (\delta u - \beta v)^2 + (\beta u + \delta v)^2 \equiv 0, \text{mod } \triangle^2.$$

Hence, since

$$\begin{aligned} \{\delta(bu - av) + \beta(au + bv)\}^2 \quad &\equiv \quad \{\delta(au + bv) - \beta(bu - av)\}^2 \\ &+ \quad \{\delta(bu - av) + \beta(au + bv)\}^2, \text{mod } c^2\triangle^2, \end{aligned}$$

and the right-hand term in the congruence equals

$$\begin{aligned}(\beta^2+\delta^2)\{(au+bv)^2+(bu-av)^2\} &= (a^2+b^2)(\beta^2+\delta^2)(u^2+v^2)\\ &= c^2(\beta^2+\delta^2)(u^2+v^2),\end{aligned}$$

we infer that $(39)_{\mathrm{A}}$ holds; a similar argument involving the equations with subscript B being valid, it follows that $\mathbf{E}_2\mathbf{u}$ and thus $\mathbf{E}_1\mathbf{Du}$ and $\mathbf{DE}_1$ are special. All other cases that can occur can be handled analogously and we have established the proposed principle for case A.

There is no need to transfer to G' when treating case C. Here there are essentially just the two automorphics $\mathbf{T}$, $\mathbf{T}^2$ satisfying $\mathbf{T^2} = -\mathbf{T} - \mathbf{I}$, whence $\mathbf{T^2x}$ is integral when $\mathbf{Tx}$ and $\mathbf{x}$ are.

Reverting to G', we go over to a full system in Category B and wish first to demonstrate our assertion is true in respect of two essentially different automorphics of type $\mathbf{E}$, which evidently may be chosen to be

$$\mathbf{E}_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \mathbf{E}_2 = \begin{bmatrix} -\frac{1}{2} & b' \\ c' & \frac{1}{2} \end{bmatrix} = \frac{1}{2}\begin{bmatrix} -1 & 3b/c \\ c/b & -1 \end{bmatrix}$$

and which combine to form

$$\mathbf{T} = \mathbf{E}_1\mathbf{E}_2 = \begin{bmatrix} -\frac{1}{2} & b' \\ -c' & -\frac{1}{2} \end{bmatrix} \quad = \quad \frac{1}{2}\begin{bmatrix} -1 & 3b/c \\ -c/b & -1 \end{bmatrix},$$

where b, c are non-zero (coprime) integers. If we multiply the special vector $\mathbf{u}$ by these matrices in turn, we obtain

$$(u,-v), \quad \frac{1}{2bc}\left(\{bcu+3b^2v\},\{c^2u-bcv\}\right), \quad \frac{1}{2bc}\left(\{bcu+3b^2v\},-\{c^2u-bcv\}\right),$$

which obey the first parts marked by the subscript A of the criterion for *speciality* when, respectively,

$$\delta u + \beta v \equiv 0, \bmod \triangle, \tag{40}_{\mathrm{A}}$$

$$\delta(bcu+3b^2v) - \beta(c^2u-bcv) = bc(\delta u+\beta v) + 3b^2\delta v - c^2\beta u \equiv 0, \bmod 2bc\triangle, \tag{41}_{\mathrm{A}}$$

$$\delta(bu+3b^2v) + \beta(c^2u-bcv) = bc(\delta u-\beta v) + 3b^2\delta v + c^2\beta u \equiv 0, \bmod 2bc\triangle. \tag{42}_{\mathrm{A}}$$

In the present situation, therefore, we need to show that $(37)_{\mathrm{A}}, (40)_{\mathrm{A}}$ and $(41)_{\mathrm{A}}$ imply $(42)_{\mathrm{A}}$ in the two cases $\triangle$ odd and $\triangle$ even, of which the first is slightly easier because then $\delta u \equiv \beta v \equiv 0, \mod\triangle$, with the implication that $\delta u - \beta v$ and $\delta u + \beta v$ are congruent to each other, $\mathrm{mod}2\triangle$, and to either 0 or $\triangle, \mathrm{mod}2\triangle$. In the former event the left sidesof $(41)_{\mathrm{A}}$ and $(42)_{\mathrm{A}}$ are congruent, $\mathrm{mod}2bc\triangle$, to

$$\begin{aligned} L &= 3b^2\delta v - c^2\beta u \equiv 0, \mathrm{mod}2bc\triangle,\\ \text{and M} &= 3b^2\delta v + c^2\beta u,\end{aligned}$$

respectively, wherefore, since

$$M^2 - L^2 = 12b^2c^2\delta u\beta v \equiv 0, \mathrm{mod}4b^2c^2\triangle^2, \tag{43}$$

we conclude that $M \equiv 0, \mathrm{mod}2bc\triangle$, and that $(42)_\mathrm{A}$ holds. On the other hand, if $\triangle$ be the common residue of $\delta u - \beta v$ and $\delta u + \beta v, \mathrm{mod}2\triangle$, then $L \equiv bc\triangle, \mathrm{mod}2bc\triangle$, and we need to shew that $M \equiv bc\triangle, \mathrm{mod}2bc\triangle$. But by (43), $M^2 \equiv L^2 \equiv b^2c^2\triangle^2, \mathrm{mod}4b^2c^2\triangle^2$, which congruence implies our requirement. Since the case where $\triangle$ is even is similar, we complete the treatment of the A-equations and go to deal in like manner with the B-equations, reaching the initial conclusion that the integrality of $\mathbf{x}$, $\mathbf{E}_1\mathbf{x}$, $\mathbf{E}_2\mathbf{x}$ implies that of $\mathbf{Tx}$.

It is clear that a slight rearrangement in the argument shews that the integrality of $\mathbf{x}$, $\mathbf{E}_1\mathbf{x}$, and $\mathbf{Tx}$ leads to that of $\mathbf{E}_2\mathbf{x}$, while the conclusion reached for Category C means that $\mathbf{T}^2\mathbf{x}$ is integral when $\mathbf{x}$ and $\mathbf{Tx}$ are. The validity of the principle in all situations under Category B then follows because any sub-duplicate in the original system G can be assigned to the canonical form with which the analysis of this category in §2 is concerned (this may mean a change in the isomorphic G' that is used).

In summary, we state

THEOREM 2. *Let us consider the rational automorphics of an integral fully factorizable form of degree three or more. Then those rational automorphics that transform a (non-zero) integral point* $\mathbf{x}$ *into another integral point form a sub-group* $G(\mathbf{x})$ *of the group* G *of all automorphics. If* $G(\mathbf{x})$ *contain at least two essentially distinct non-trivial members that are not both related to* $\mathbf{T}$ *and* $\mathbf{T}^2$, *then* $G(\mathbf{x}) = G$.

The last part is clear from the group tables presented earlier.

In the second part of this Section we wish to shew how to determine the integral points $\mathbf{x}$ that admit a given automorphic $\mathbf{A}$ in the sense that $\mathbf{Ax}$ is also integral. As $\mathbf{A}$ can be expressed in the form

$$\frac{1}{\triangle}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

where $\triangle > 0, \pm\triangle = \alpha\delta - \beta\gamma$, and $(\alpha, \beta, \gamma, \delta) = 1$, the points in question correspond to the solutions of the congruence

$$\alpha x + \beta y \equiv 0, \mathrm{mod}\triangle, \quad \gamma x + \delta y \equiv 0, \mathrm{mod}\triangle, \tag{44}$$

and form a two dimensional lattice. If we require the area of a fundamental parallelogram so as to introduce a more specific aspect in future calculations, we use the theory of integral

matrices to find unimodular matrices **R, S** with integer elements that have the property that

$$\mathbf{RAS} = \frac{1}{\triangle}\begin{bmatrix} 1 & 0 \\ 0 & \triangle^2 \end{bmatrix} = \begin{bmatrix} 1/\triangle & 0 \\ 0 & \triangle \end{bmatrix}.$$

Hence, if for any integral point $\mathbf{x}$ we let $\mathbf{u} = (u,v)$ be the integral point $\mathbf{Sx}$, we deduce that $\mathbf{Ax}$ is integral when and only when $\mathbf{u} \equiv \mathbf{0}, \mathrm{mod}\triangle$, with the conclusion that the area is $\triangle$.

If an integral point $\mathbf{x}$ be also transformed into an integral point by another non-trivial automorphic (essentially distinct from $\mathbf{A}$) with the parameter $\square$ corresponding to $\triangle$ in (44), then we have just shewn it is transformable into an integral point by all automorphics. Being closed under vector addition, the set of all such points is also a lattice, which is non-empty and two dimensional because all vectors $\mathbf{x} \equiv 0, \mathrm{mod}[\triangle, \square]$, belong to it. To find the area of its fundamental parallelogram in any particular instance is easily achieved in principle by an extension of the earlier method; this procedure, however, we here avoid in the interests of brevity because the resulting valuations are cumbrous to state.

6. **The asymptotic formula for** $\Upsilon(n)$. All is in readiness for the derivation of the required formula for $\Upsilon(n)$. The first thing to be done is to establish an asymptotic formula, in relatively crude form, for the sum

$$\sum\nolimits_1 = \sum_{0<m\leq n} r(m),$$

or, what is the same, for the number of lattice points (x, y) satisfying the inequality $0 < f(x, y) \leq n$. To evaluate this, we note that the l asymptotes $h_i x + k_i y = 0$ of the curve $f(x, y) = n$ divide the plane into $2l$ semi-infinite triangles when they are appropriately arranged, the curve lying in alternate such triangles (see I, §2). Consider the contribution to $\sum_1$ from the lattice points in one of the appropriate triangles whose radial sides, or semi-infinite asymptotes, are given in polar coordinates by $\theta = \theta_1, \theta = \theta_2$, where $0 \leq \theta_1 < \theta_2 < 2\pi$; notice that when l is even the curve also lies in the opposite region produced by a rotation through the angle π. On setting $g(\theta) = f(\cos\theta, \sin\theta)$, we verify that within this region

$$A_1 \mathrm{min}(\theta_2 - \theta, \theta - \theta_1) < \mathrm{g}(\theta) < \mathrm{A}_2(\theta_2 - \theta), \mathrm{A}_2(\theta - \theta_1) \tag{45}$$

and then in the part R_n circumscribed by the curve $f = n$ the radial co-ordinate r is limited by the inequality

$$r^l g(\theta) \leq n.$$

Consequently the area of R_n equals

$$\frac{1}{2} n^{\frac{2}{l}} \int_{\theta_1}^{\theta_2} \frac{d\theta}{g^{\frac{2}{l}}(\theta)} = C_1 n^{\frac{2}{l}}, \tag{46}$$

since the integral is convergent by (45). The values of C_1 for the various apposite regions will normally differ, although any two that are related through an automorphic of the form will be the same; in particular, if $l = 3$, then all three values of C_1 are the same.

As for the lattice points themselves in R_n, the discussion in §3 of I, shews that they are all restricted by the condition

$$|x|, |y| < A_3 n^{\frac{1}{l-1}}. \tag{47}$$

Thus these points lie in a region within a perimeter $O\left(n^{\frac{1}{l-1}}\right)$ and an area which is that part of (46) related to values of r less than $2A_3 n^{\frac{1}{l-1}}$. Since the remaining part of (46) corresponds to values of θ, for which

$$g(\theta) < A_4 n / n^{\frac{l}{l-1}} = A_4 n^{-\frac{1}{l-1}}$$

and hence for which

$$\theta - \theta_1 \text{ or } \theta_2 - \theta < A_5 n^{-\frac{1}{l-1}}$$

by (47), its area does not exceed

$$A_6 n^{\frac{2}{l}} \int_0^{A_4 n^{-\frac{1}{l-1}}} \frac{dv}{v^{\frac{2}{l}}} = O\left(n^{\frac{2}{l} - (1 - \frac{2}{l}\frac{1}{l-1})}\right) = O\left(n^{\frac{1}{l-1}}\right).$$

Hence, combining the donations from all the relevant regions, we find that

$$\sum\nolimits_1 = C n^{\frac{2}{l}} + O\left(n^{\frac{1}{l-1}}\right). \tag{48}$$

Next, letting $r_1 m$ be as before the number of essentially different representations of m by f, that is, the number of non-associated sets of representations, we need to estimate the sum

$$\Upsilon_1(n) = \sum_{0<m\leq n} r_1(m).$$

To this end we generalize the sum $\sum_1$ and, for any non-trivial automorphic $\mathbf{A}$ of f, let

$$\sum\nolimits_{\mathbf{A}} = \sum_{0<f(\mathbf{x})\leq n}^{*} 1,$$

where the asterisk sign indicates that the vectors $\mathbf{x}$ are confined to those for which $\mathbf{Ax}$ is integral and where therefore $\sum_{\mathbf{T}} = \sum_{\mathbf{T}^2}$; similarly, should there be at least two essentially different non-trivial automorphics $\mathbf{B}$, $\mathbf{C}$ that are not both of the type $\mathbf{T}$, $\mathbf{T}^2$, we write

$$\sum\nolimits_{all} = \sum_{0<f(\mathbf{x})\leq n}^{\dagger} 1,$$

the obelisk sign indicating that the vectors $\mathbf{x}$ are confined to those for which $\mathbf{Ax}$ is integral for all automorphics $\mathbf{A}$ of f and hence, by Theorem 2, for merely $\mathbf{A} = \mathbf{B}$ and $\mathbf{A} = \mathbf{C}$. By the discussion at the end of §5 the evaluation of these sums is similar to that of $\sum_1$ save that the areas of fundamental parallelograms are changed from 1 to numbers $\triangle_{\mathbf{A}}$ and $\triangle_{all}$, the latter being calculated by using any relevant pair $\mathbf{B}$, $\mathbf{C}$. Consequently

$$\sum\nolimits_A = \frac{Cn^{\frac{2}{l}}}{\triangle_{\mathbf{A}}} + O\left(n^{\frac{1}{l-1}}\right) \text{and} \sum\nolimits_{\text{all}} = \frac{\text{Cn}^{\frac{2}{\text{l}}}}{\triangle_{\text{all}}} + \text{O}\left(\text{n}^{\frac{1}{\text{l}-1}}\right). \tag{49}$$

We are now enabled to illustrate the process of finding a formula for $\Upsilon_1(n)$ by considering cases that are of the easiest and hardest varieties.

First, if f have no non-trivial automorphic, then

$$\begin{aligned} \Upsilon_1(n) &= \sum_{0<m\leq n} r(m) = \sum\nolimits_1 = Cn^{\frac{2}{l}} + O\left(n^{\frac{1}{l-1}}\right) \\ \text{or } \Upsilon_1(\text{n}) &= \frac{1}{2}\sum_{0<m\leq n} r(m) = \frac{1}{2}Cn^{\frac{2}{l}} + O\left(n^{\frac{1}{l-1}}\right) \end{aligned}$$

according as l is odd or even, since in the latter instance - $\mathbf{I}$ is a trivial automorphic.

At the other extreme, let us take a form f of odd degree l that admits all the automorphics $\mathbf{E}_1$, $\mathbf{E}_2$, $\mathbf{E}_3$, $\mathbf{T}$, $\mathbf{T}^2$ in a system of Category B. Then we note that in counting a point $\mathbf{x}$ the sum $\sum_{\mathbf{E}}$ also counts the associate $\mathbf{Ex}$ because $\mathbf{E}(\mathbf{Ex}) = \mathbf{x}$; similarly in counting $\mathbf{x}_1$ the sum $\sum_{\mathbf{T}}$ also counts $\mathbf{Tx}_1$ and $\mathbf{T}^2\mathbf{x}_1$, because we have already shewn that $\mathbf{T}^2\mathbf{x}_1$ is integral when $\mathbf{Tx}_1$ is; lastly in counting $\mathbf{x}_2$ the sum $\sum_{all}$ also counts all the associates of $\mathbf{x}_2$. Also $\mathbf{x}_1$, $\mathbf{Tx}_1$, $\mathbf{T}^2\mathbf{x}_1$ are always distinct, as are $\mathbf{x}$ and $\mathbf{Ex}$ save when $\mathbf{x}$ lies on one radius vector through the origin. With these observations in mind and by combinatorial ideas, whose genesis we chose not to explain, we are guided to the expression

$$\Upsilon_2(n) = \sum\nolimits_1 - \frac{1}{2}\left(\sum\nolimits_{\mathbf{E}_1} + \sum\nolimits_{\mathbf{E}_2} + \sum\nolimits_{\mathbf{E}_3}\right) - \frac{2}{3}\sum\nolimits_{\mathbf{T}} + \frac{4}{3}\sum\nolimits_{all} \tag{50}$$

and to the consideration of the influence upon it of each representation by f of a number m not exceeding n.

We first account for the representations in those complete sets of associates containing no element that is left invariant under the action of a non-trivial automorphic. In this situation each set contains either (i) exactly one element or (ii) exactly two elements associated through an automorphic $\mathbf{E}$ or (iii) exactly three elements associated through $\mathbf{T}$ and $\mathbf{T}^2$ or (iv) exactly six elements associated through all five non-trivial automorphics. Then the contributions of the set to the terms in $\Upsilon_2(n)$ and then $\Upsilon_2(n)$ itself are as follows: case (i), 1 to $\sum_1$, 0 to

remaining sums, and 1 to $\Upsilon_2(n)$; case (ii), 2 to $\sum_1$ and one $\sum_{\mathbf{E}_i}$, 0 to remaining sums, and $2-1=1$ to $\Upsilon_2(n)$; case (iii), 3 to $\sum_1$ and $\sum_{\mathbf{T}}$, 0 to remaining sums, and $3-2=1$ to $\Upsilon_2(n)$; and case (iv), 6 to $\sum_1$, all $\sum_{\mathbf{E}_i}$, $\sum_{\mathbf{T}}$, $\sum_{all}$, and $6-9-4+8=1$ to $\Upsilon_2(n)$. Thus $\Upsilon_2(n)$ and $\Upsilon_1(n)$ can only disagree in regard to representations $\mathbf{x}$ for which $\mathbf{E}_i\mathbf{x}=\mathbf{x}$ and these, lying as they do on three radii vectores, have cardinality $O\left(n^{\frac{1}{l-1}}\right)$ by (47). Therefore

$$\Upsilon_1(n)=\Upsilon_2(n)+O\left(n^{\frac{1}{l-1}}\right),$$

from which, (48), and (49) we deduce that there is again an asymptotic formula of the type

$$\Upsilon_1(n)=D(f)n^{\frac{2}{l}}+O\left(n^{\frac{1}{l-1}}\right). \tag{51}$$

Moreover, since there are six automorphics,

$$\Upsilon_1(n)\geq\frac{1}{6}\sum\nolimits_1=\frac{1}{6}Cn^{\frac{2}{l}}+O\left(n^{\frac{1}{l-1}}\right)$$

so that $C(f)>0$. When l is even, the reasoning is similar except that the value of $C(f)$ will be one half of what it was before because of the presence of the automorphic -**I**.

Following analogous processes in all other cases we find that (51) is always true. Also, the difference between $\Upsilon_1(n)$ and $\Upsilon(n)$ is

$$\sum_{\substack{0<m\leq n\\ r_1(m)\geq 1}}\{r_1(m)-1\}=\sum_{\substack{0<m\leq n\\ r_1(m)>1}}r_1(m)=O\left(\sum_{\substack{0<m\leq n\\ r_1(m)>1}}d(m)\right)$$
$$=O\{n^{\epsilon}\nu(n)\}=O\left(n^{\frac{2}{l}-\eta_l+\epsilon}\right),$$

where $\nu(n)$ and η_l appear in (1) and (2). We thus obtain our main

THEOREM 3. *Let $\Upsilon(n)$ be the number of positive integers not exceeding n that are representable by a totally reducible binary form f of degree $l\geq 3$, where each such integer is counted once regardless of the number of ways it can be represented. Then, as $n\to\infty$, we have*

$$\Upsilon(n)=C(f)n^{\frac{2}{l}}+O\left(n^{\frac{2}{l}-\eta_l+\epsilon}\right), \tag{52}$$

where $C(f)>0$.

7. **Irreducible forms.** As promised in the Introduction, we briefly report on the extent to which our findings can be extended to cover irreducible forms of degree $l\geq 3$. First, since

the principles of §2 require little modification to suit the new context, it is still true that non-trivial automorphics must belong to one of the Categories A, B, and C. But, since the characteristic roots of the automorphic matrices are algebraic numbers of degree at most 2 and the linear factors in f involve algebraic numbers of degree l, no non-trivial automorphic can ever leave a factor of f essentially unchanged and therefore there is a greater limitation on the degrees of forms possessing certain types of automorphic systems. Conversely, we can still find irreducible forms answering to each pattern in Categories A, B, and C even though the methods of §§3 and 4 can no longer be used. To indicate how we must now proceed, it must suffice to consider the following illustrative example in bare outline.

Suppose that we require a form $f(x,y)$ to admit a rational automorphic of type $\mathbf{T}$ and therefore to have degree $l = 3m$. Then there would be a substitution $x = \alpha X + \beta Y$, $y = \gamma X + \delta Y$ under which the metamorphic $F(X,Y) = f(\alpha X + \beta Y, \gamma X + \delta Y)$ of f would admit the automorphics

$$\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \tag{53}$$

as in (19) and (20). If θ_1 be a zero of $\psi(u) = F(u,1)$, then so are

$$\theta_2 = -1 - \frac{1}{\theta_1}, \quad \theta_3 = -\frac{1}{\theta_1 + 1},$$

whence

$$\phi = \theta_1 - \frac{1}{\theta_1} - \frac{1}{\theta_1 + 1}$$

is invariant under the relative isomorphisms $\theta_1 \to \theta_2 \to \theta_3$ of $\mathrm{Q}(\theta_1)$. Consequently ϕ is of degree $m = \frac{1}{3}l$ over G and satisfies an irreducible equation

$$a_0 u^m + \ldots + a_m = 0$$

with integral coefficients, from which fact it follows that each zero of $\psi(u)$ is a zero of

$$\sum_{r=0}^{m} a_r \{u(u+1)\}^r (u^3 + u^2 - 2u - 1)^{m-r}$$

and that $F(X,Y)$ takes the shape of

$$\sum_{r=0}^{m} a_r \{XY(X+Y)\}^r (X^3 + X^2 Y - 2XY^2 - Y^3)^{m-r};$$

conversely it is easily verified that any such form has the automorphics (53). The case $r = 1$ is of special interest because a method is provided for constructing Abelian cubic forms.

In summation, irreducible forms are usually less well endowed with automorphics than are their fully reducible cousins despite all systems of types A, B, and C being possible in suitable circumstances. For example, the only cubics with non-trivial automorphics are now the Abelian ones, the determinants of which are minus thrice a perfect square, while quintics and septimics are devoid of all such ornament. Also the bound $l \cdot l!$ given by Heath-Brown for the number of automorphics can be reduced to 12.

Finally, the method of §6 can be directed at the new situation, although the treatment of $\sum_1$ and its generalizations entail an appeal to the Thue-Siegel-Roth theorem in the manner of our [2] or Heath-Brown's [1]. Using the latter author's important estimate for $\nu(n)$, we can then enunciate

THEOREM 4. *The asymptotic formula in Theorem* 3 *is valid for a suitable positive value of* η_l *when* f *is an irreducible binary form of degree* $l \geq 3$ *with integral coefficients.*

References

[1] D. R. Heath-Brown, Counting rational points on algebraic curves and surfaces, Annals of Mathematics, 155(2002), 553-595.

[2] C. Hooley, On binary cubic forms: II, J. Reine Angew. Math, 521(2000), 185-240.

[3] C. Hooley, On totally reducible binary forms: I, Proc. Indian Acad. Sci.(Math.Sci.), Vol III, No 3(2001), 249-262.

[4] C. C. MacDuffee, The theory of matrices, Chelsea (New York), 1946.

[5] G. B. Mathews, Messenger Math., 20(1891), 70-74.

Address

School of Mathematics,
University of Wales, Cardiff,
P.O. Box 926,
Cardiff,
CF24 4YH.