A REMARK ON SIEGEL'S THEOREM ON ALGEBRAIC CURVES

K. Mahler

The main case of *Siegel's* theorem on algebraic curves* may be stated as follows:

Theorem 1. *Let*

$$\mathfrak{C}: f(x, y) = 0$$

be an irreducible algebraic curve of genus $g \geqslant 1$, $f(x, y)$ being a polynomial with algebraic coefficients. Let K be an algebraic field of finite degree over the rational field; let $\mathfrak{o}$ be the ring of integers in K; and let j be a positive rational integer. Then there are at most finitely many points (x, y) on $\mathfrak{C}$ for which $jx \varepsilon \mathfrak{o}$ and $y \varepsilon K$.

In this paper, we shall generalize Theorem 1 and prove a result in which neither the coefficients of $f(x, y)$ nor the coordinates x, y need be algebraic numbers.

1. Denote by J the ring of all rational integers, and by R, G and C the field of all rational numbers, the Gaussian field, and the field of all complex numbers, respectively. Further denote by X and Y a finite J-module and a finite R-module in C, respectively. In other words, X is the set of all sums

$$x = u_1 \xi_1 + u_2 \xi_2 + \ldots + u_m \xi_m \qquad (u_1, u_2, \ldots, u_m \varepsilon J),$$

where $\xi_1, \xi_2, \ldots, \xi_m$ are finitely many fixed complex numbers that are linearly independent over R. Similarly Y is the set of all sums

$$y = v_1 \eta_1 + v_2 \eta_2 + \ldots + v_n \eta_n \qquad (v_1, v_2, \ldots, v_n \varepsilon R),$$

where again $\eta_1, \eta_2, \ldots, \eta_n$ are certain fixed numbers in C that are linearly independent over R.

We denote by $Z = X \times Y$ the product space of X and Y consisting of all points (x, y), where $x \varepsilon X$ and $y \varepsilon Y$. For shortness, we call Z a *JR-lattice*.

The generalization of Siegel's theorem takes the following form†:

Theorem 2. *Let*

$$\mathfrak{C}: f(x, y) = 0$$

---

* C. L. Siegel, *Abh. Preuss. Akad. Wiss.* (1929), No. 1.

† An analogous theorem holds in which the coefficients of $f(x, y)$ and the elements of the two moduli X and Y are p-adic numbers or, more generally, $\mathfrak{p}$-adic numbers.

[Mathematika 2 (1955), 116–127]

be an irreducible algebraic curve of genus $g \geqslant 1$, $f(x, y)$ *being a polynomial with arbitrary real or complex coefficients; let further* Z *be an arbitrary real or complex* JR*-lattice. Then at most finitely many points of* Z *lie on* $\mathfrak{C}$.

That this theorem implies Theorem 1 is obvious because, by classical theorems on algebraic fields, $j^{-1}\mathfrak{o}$ is a finite J-module and K a finite R-module in C. Conversely, Theorem 2 will be proved by reducing the assertion to one covered by Theorem 1.

2. The proof of Theorem 2 will be based on the following:

LEMMA 1. *Let* Γ: $F(x, y) = 0$, *where* $F(x, y) \in C[x, y]$ *is of degree* $d \geqslant 3$, *be an irreducible algebraic curve of genus* $g \geqslant 1$. *A positive number* δ *exists, with the following property:*

If $G(x, y) \in C[x, y]$ *is of the same degree* d, *and if the absolute values of all coefficients of* $G(x, y) - F(x, y)$ *are less than* δ, *then the curve* Δ : $G(x, y) = 0$ *is likewise irreducible and at least of genus* 1.

To prove this lemma, we first note the nearly trivial fact that every limit curve of a set of reducible curves, all of the same degree, is itself reducible. In the non-trivial case of irreducible curves, the lemma is contained in the following theorem of B. Segre*:

" *If* Θ *is an infinite set of irreducible algebraic curves in* r*-dimensional projective space, all of order* d *and genus* g, *then the genus of no irreducible limiting curve of* Θ *is greater than* g."

3. We now begin the proof of Theorem 2. This proof is indirect.
Let $\mathfrak{C}$: $f(x, y) = 0$ and Z be defined as in the theorem. We shall assume from now on that the assertion is false, so that the intersection of curve and lattice:

$$W = \mathfrak{C} \cap Z$$

contains infinitely many distinct points

$$(x, y) = (u_1 \xi_1 + u_2 \xi_2 + \ldots + u_m \xi_m,\ v_1 \eta_1 + v_2 \eta_2 + \ldots + v_n \eta_n).$$

This hypothesis will finally lead to a contradiction.

Denote by $$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_l$$

all the coefficients of $f(x, y)$, arranged in a fixed, but arbitrary, order. The $l+m+n$ complex numbers

$$\alpha_1, \alpha_2, \ldots, \alpha_l, \xi_1, \xi_2, \ldots, \xi_m, \eta_1, \eta_2, \ldots, \eta_n$$

---

* *Proc. London Math. Soc.* (2), 47 (1942), 351–403, in particular p. 363.

generate a certain smallest extension field

$$\mathrm{P} = R(\alpha_1, \alpha_2, \ldots, \alpha_l, \xi_1, \xi_2, \ldots, \xi_m, \eta_1, \eta_2, \ldots, \eta_n)$$

of R.

We may immediately exclude the case that P is a finite algebraic extension of R. For then a positive rational integer j exists such that

$$j\xi_1, j\xi_2, \ldots, j\xi_m$$

are elements of the ring $\mathfrak{o}$ of all algebraic integers in $K = \mathrm{P}$. It follows that there are infinitely many distinct points (x, y) on $\mathfrak{C}$ for which $jx \in \mathfrak{o}$ and $y \in K$, contrary to Theorem 1.

4. The extension field P is thus transcendental over R. As it is obtained from R by adjoining *finitely* many complex numbers, P may be obtained as an extension of the form

$$\mathrm{P} = R(\sigma_1, \sigma_2, \ldots, \sigma_p, \tau).$$

Here

$$\sigma_1, \sigma_2, \ldots, \sigma_p,$$

where $p \geqslant 1$, are complex numbers which are algebraically independent over R, while τ is a complex number which is algebraic, say of degree q, over the purely transcendental extension

$$\mathrm{P}_0 = R(\sigma_1, \sigma_2, \ldots, \sigma_p)$$

of R.

The number τ may still be chosen in many distinct ways. There is no loss of generality in assuming that τ is integral over the polynomial ring

$$I = R[\sigma_1, \sigma_2, \ldots, \sigma_p],$$

hence that τ satisfies an irreducible algebraic equation

$$Q(\sigma_1, \sigma_2, \ldots, \sigma_p; \tau) \equiv \tau^q + \sum_{\kappa=1}^{q} Q_\kappa(\sigma_1, \sigma_2, \ldots, \sigma_p)\tau^{q-\kappa} = 0$$

with coefficients

$$Q_\kappa(\sigma_1, \sigma_2, \ldots, \sigma_p) \qquad (\kappa = 1, 2, \ldots, q)$$

in I. The polynomial $Q(\sigma_1, \sigma_2, \ldots, \sigma_p; \tau)$ then belongs to $I[\tau]$.

5. In terms of the numbers $\sigma_1, \sigma_2, \ldots, \sigma_p, \tau$, the coefficients of $f(x, y)$ and the generators of X and Y can be written as rational functions

$$\alpha_\lambda = \frac{A_\lambda(\sigma_1, \sigma_2, \ldots, \sigma_p, \tau)}{A(\sigma_1, \sigma_2, \ldots, \sigma_p)} \qquad (\lambda = 1, 2, \ldots, l),$$

$$\xi_\mu = \frac{X_\mu(\sigma_1, \sigma_2, \ldots, \sigma_p, \tau)}{X(\sigma_1, \sigma_2, \ldots, \sigma_p)} \qquad (\mu = 1, 2, \ldots, m),$$

$$\eta_\nu = \frac{Y_\nu(\sigma_1, \sigma_2, \ldots, \sigma_p, \tau)}{Y(\sigma_1, \sigma_2, \ldots, \sigma_p)} \qquad (\nu = 1, 2, \ldots, n).$$

Here

$$A_\lambda(\sigma_1, \sigma_2, \ldots, \sigma_p, \tau), \quad X_\mu(\sigma_1, \sigma_2, \ldots, \sigma_p, \tau), \quad Y_\nu(\sigma_1, \sigma_2, \ldots, \sigma_p, \tau)$$

are polynomials in $I[\tau]$, while the denominators

$$A(\sigma_1, \sigma_2, \ldots, \sigma_p), \quad X(\sigma_1, \sigma_2, \ldots, \sigma_p), \quad Y(\sigma_1, \sigma_2, \ldots, \sigma_p)$$

belong to I. These denominators are distinct from zero, both as formal polynomials and as complex numbers.

On substituting the expressions A_λ/A for the coefficients α_λ, $f(x, y)$ assumes the form

$$f(x, y) = \frac{\Phi(x, y \mid \sigma_1, \sigma_2, \ldots, \sigma_p, \tau)}{\phi(\sigma_1, \sigma_2, \ldots, \sigma_p)},$$

where Φ lies in the polynomial ring

$$I[x, y, \tau] = R[x, y, \sigma_1, \sigma_2, \ldots, \sigma_p, \tau],$$

while ϕ belongs to I and is distinct from zero, again both as a formal polynomial and as a complex number.

We may then replace $f(x, y)$ by $\phi f(x, y)$ without changing the curve $\mathfrak{C}$. Hence there is no loss of generality in assuming that $\phi = 1$ and that therefore

$$f(x, y) = \Phi(x, y \mid \sigma_1, \sigma_2, \ldots, \sigma_p, \tau)$$

is a polynomial, with coefficients in R, not only in the variables x and y, but also in the complex numbers $\sigma_1, \sigma_2, \ldots, \sigma_p, \tau$.

6. Now let

$$(x, y) = (u_1 \xi_1 + u_2 \xi_2 + \ldots + u_m \xi_m, \; v_1 \eta_1 + v_2 \eta_2 + \ldots + v_n \eta_n)$$

be an arbitrary point of Z. Then, in terms of $\sigma_1, \sigma_2, \ldots, \sigma_p, \tau$,

$$x = \frac{\sum_{\mu=1}^{m} u_\mu X_\mu(\sigma_1, \sigma_2, \ldots, \sigma_p, \tau)}{X(\sigma_1, \sigma_2, \ldots, \sigma_p)} \quad \text{and} \quad y = \frac{\sum_{\nu=1}^{n} v_\nu Y_\nu(\sigma_1, \sigma_2, \ldots, \sigma_p, \tau)}{Y(\sigma_1, \sigma_2, \ldots, \sigma_p)}.$$

On substituting these expressions for x and y in

$$f(x, y) = \Phi(x, y \mid \sigma_1, \sigma_2, \ldots, \sigma_p, \tau),$$

$f(x, y)$ becomes a quotient

$$f(x, y) = \frac{\Psi(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n \mid \sigma_1, \sigma_2, \ldots, \sigma_p, \tau)}{X(\sigma_1, \sigma_2, \ldots, \sigma_p)^d \, Y(\sigma_1, \sigma_2, \ldots, \sigma_p)^d}.$$

Here the numerator Ψ belongs to the polynomial ring

$$R[u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n, \sigma_1, \sigma_2, \ldots, \sigma_p, \tau],$$

and d denotes the degree of $f(x, y)$ in x and y. By the construction,

$$X(\sigma_1, \sigma_2, \ldots, \sigma_p) \neq 0, \quad Y(\sigma_1, \sigma_2, \ldots, \sigma_p) \neq 0,$$

so that the quotient is well defined.

By hypothesis, $W = \mathfrak{C} \cap Z$ has infinitely many distinct elements (x, y). Each such point is characterized by the $m+n$ parameters

$$u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n,$$

of which the first m are rational integers and the last n are rational numbers. For shortness, denote this set of $m+n$ parameters by (u_μ, v_ν) and write Ω for the set of all systems (u_μ, v_ν) that correspond to elements of W. To each element (u_μ, v_ν) of Ω there corresponds an equation

$$\Psi(u_\mu, v_\nu \,|\, \sigma_1, \sigma_2, \ldots, \sigma_p, \tau) \equiv \Psi(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n \,|\, \sigma_1, \sigma_2, \ldots, \sigma_p, \tau) = 0$$

connecting the numbers $\sigma_1, \sigma_2, \ldots, \sigma_p, \tau$. The left-hand side of this equation is an element of $I[\tau]$ because the parameters u_μ and v_ν are rational numbers. This left-hand side is therefore divisible by the irreducible polynomial $Q(\sigma_1, \sigma_2, \ldots, \sigma_p; \tau)$.

7. We now replace the p independent complex numbers

$$\sigma_1, \sigma_2, \ldots, \sigma_p,$$

and the complex number τ connected with them by the equation

$$Q(\sigma_1, \sigma_2, \ldots, \sigma_p; \tau) = 0,$$

by p independent complex variables

$$s_1, s_2, \ldots, s_p$$

and a dependent complex variable t for which

$$Q(s_1, s_2, \ldots, s_p; t) = 0.$$

The change from $\sigma_1, \sigma_2, \ldots, \sigma_p, \tau$ to $s_1, s_2, \ldots, s_p, t$ maps the field $\mathrm{P} = R(\sigma_1, \sigma_2, \ldots, \sigma_p, \tau)$ isomorphically onto a new field

$$\mathrm{P}^* = R(s_1, s_2, \ldots, s_p, t)$$

and preserves all rational relations. Thus $f(x, y)$ is mapped on a new polynomial

$$f^*(x, y) = \Phi(x, y \,|\, s_1, s_2, \ldots, s_p, t)$$

with the coefficients

$$\alpha_\lambda^* = \frac{A_\lambda(s_1, s_2, \ldots, s_p, t)}{A(s_1, s_2, \ldots, s_p)} \qquad (\lambda = 1, 2, \ldots, l).$$

Simultaneously, $\mathfrak{C}$ is mapped on the new curve

$$\mathfrak{C}^*: f^*(x, y) = 0.$$

Next, the generators ξ_μ of X and η_ν of Y are changed into the generators

$$\xi_\mu^* = \frac{X_\mu(s_1, s_2, \ldots, s_p, t)}{X(s_1, s_2, \ldots, s_p)} \qquad (\mu = 1, 2, \ldots, m)$$

of a new J-module, X^* say, and the generators

$$\eta_\nu^* = \frac{Y_\nu(s_1, s_2, \ldots, s_p, t)}{Y(s_1, s_2, \ldots, s_p)} \qquad (\nu = 1, 2, \ldots, n)$$

of a new R-module, Y^* say. Both sets of m generators ξ_μ^* and of n generators η_ν^* are linearly independent over R as functions of $s_1, s_2, \ldots, s_p, t$, because they are so for the special values

$$s_1 = \sigma_1, \quad s_2 = \sigma_2, \quad \ldots, \quad s_p = \sigma_p, \quad t = \tau.$$

Define Z^* as the JR-lattice $X^* \times Y^*$. Then to every point

$$(x, y) = (u_1 \xi_1 + u_2 \xi_2 + \ldots + u_m \xi_m, \; v_1 \eta_1 + v_2 \eta_2 + \ldots + v_n \eta_n)$$

of Z there corresponds the point

$$(x^*, y^*) = (u_1 \xi_1^* + u_2 \xi_2^* + \ldots + u_m \xi_m^*, \; v_1 \eta_1^* + v_2 \eta_2^* + \ldots + v_n \eta_n^*)$$

of Z^*. In particular, the points (x^*, y^*) belonging to systems (u_μ, v_ν) in Ω form the set $W^* = \mathfrak{C}^* \cap Z^*$ of all points of Z^* that lie on $\mathfrak{C}^*$. It is clear that, for $(u_\mu, v_\nu) \in \Omega$, the equation

$$\Psi(u_\mu, v_\nu \,|\, s_1, s_2, \ldots, s_p, t) = 0$$

is satisfied since the polynomial Ψ is divisible by Q.

8. Denote by C^p the p-dimensional space formed by all points

$$\mathbf{s} = (s_1, s_2, \ldots, s_p), \quad \mathbf{s}' = (s_1', s_2', \ldots, s_p'), \quad \boldsymbol{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_p), \text{ etc.,}$$

with complex coordinates. We consider C^p as a linear vector space over C, and we make it a metric space by defining the distance between any two points $\mathbf{s}$ and $\mathbf{s}'$ by the formula

$$\rho(\mathbf{s}, \mathbf{s}') = +\{|s_1 - s_1'|^2 + |s_2 - s_2'|^2 + \ldots + |s_p - s_p'|^2\}^{1/2}.$$

With respect to this metric, terms like neighbourhood, closed and open sets, closure, etc., can be defined as usual.

By definition, t is a root of the algebraic equation

$$Q(s_1, s_2, \ldots, s_p, t) \equiv t^q + \sum_{\kappa=1}^{q} Q_\kappa(s_1, s_2, \ldots, s_p)\, t^{q-\kappa} = 0.$$

This equation is irreducible in $R[s_1, s_2, \ldots, s_p, t]$, but may become reducible in $C[s_1, s_2, \ldots, s_p, t]$. In any case, its discriminant

$$D(\mathbf{s}) = D(s_1, s_2, \ldots, s_p),$$

say, with respect to t is not zero identically in $\mathbf{s}$ and lies in the polynomial ring $R[s_1, s_2, \ldots, s_p]$. Since $\sigma_1, \sigma_2, \ldots, \sigma_p$ are algebraically independent over R, we necessarily have

$$D(\boldsymbol{\sigma}) \neq 0.$$

Hence a neighbourhood U_0 of $\boldsymbol{\sigma}$ exists such that

$$D(\mathbf{s}) \neq 0 \quad \text{if} \quad \mathbf{s} \varepsilon U_0.$$

In this neighbourhood, the equation $Q = 0$ has then q distinct roots

$$t = t_1, \ t_2, \ \ldots, \ t_q$$

which form the branches of one or more algebraic functions of $\mathbf{s}$. We denote by $t^0(\mathbf{s})$ that root for which

$$t^0(\boldsymbol{\sigma}) = \tau.$$

Then, for $\mathbf{s} \varepsilon U_0$, $t^0(\mathbf{s})$ is a continuous branch of an algebraic function of $\mathbf{s}$, as follows immediately from the form of the equation $Q = 0$ for $t^0(\mathbf{s})$.

Since further

$$A(\sigma_1, \sigma_2, \ldots, \sigma_p) \neq 0, \quad X(\sigma_1, \sigma_2, \ldots, \sigma_p) \neq 0, \quad Y(\sigma_1, \sigma_2, \ldots, \sigma_p) \neq 0,$$

there exists a neighbourhood U_1 of $\boldsymbol{\sigma}$ contained in U_0 such that

$$A(s_1, s_2, \ldots, s_p) \neq 0, \quad X(s_1, s_2, \ldots, s_p) \neq 0, \quad Y(s_1, s_2, \ldots, s_p) \neq 0 \quad \text{if} \quad \mathbf{s} \varepsilon U_1.$$

In this neighbourhood, the expressions

$$A_\lambda\left(s_1, s_2, \ldots, s_p, t^0(\mathbf{s})\right), \quad X_\mu\left(s_1, s_2, \ldots, s_p, t^0(\mathbf{s})\right), \quad Y_\nu\left(s_1, s_2, \ldots, s_p, t^0(\mathbf{s})\right)$$

are continuous branches of algebraic functions of $\mathbf{s}$, and so the same is true for the quotients

$$\alpha_\lambda{}^0(\mathbf{s}) = \frac{A_\lambda\left(s_1, \ldots, s_p, t^0(\mathbf{s})\right)}{A(s_1, \ldots, s_p)},$$

$$\xi_\mu{}^0(\mathbf{s}) = \frac{X_\mu\left(s_1, \ldots, s_p, t^0(s)\right)}{X(s_1, \ldots, s_p)},$$

$$\eta_\nu{}^0(\mathbf{s}) = \frac{Y_\nu\left((s_1, \ldots, s_p, t^0(s)\right)}{Y(s_1, \ldots, s_p)}.$$

Finally

$$f^0(x, y \mid \mathbf{s}) = \Phi\left(x, y \mid s_1, s_2, \ldots, s_p, t^0(\mathbf{s})\right),$$

for fixed x and y, is likewise a continuous branch of an algebraic function of $\mathbf{s}$ if $\mathbf{s} \varepsilon U_1$.

The moduli X^* and Y^* become now moduli $X^0(\mathbf{s})$ and $Y^0(\mathbf{s})$ with the generators $\xi_\mu{}^0(\mathbf{s})$ and $\eta_\nu{}^0(\mathbf{s})$, respectively. For variable $\mathbf{s}$, these generators are still linearly independent over R.

Denote by $\mathfrak{C}^0(\mathbf{s})$ the curve

$$\mathfrak{C}^0(\mathbf{s}) : f^0(x, y \mid \mathbf{s}) = 0,$$

by $Z^0(\mathbf{s})$ the JR-lattice $X^0(\mathbf{s}) \times Y^0(\mathbf{s})$, and by $W^0(\mathbf{s}) = \mathfrak{C}^0(\mathbf{s}) \cap Z^0(\mathbf{s})$ the intersection of $\mathfrak{C}^0(\mathbf{s})$ and $Z^0(\mathbf{s})$. Then $W^0(\mathbf{s})$ consists of the points $\left(x^0(\mathbf{s}), y^0(\mathbf{s})\right)$ where

$$x^0(\mathbf{s}) = \sum_{\mu=1}^{m} u_\mu \xi_\mu{}^0(\mathbf{s}), \quad y^0(\mathbf{s}) = \sum_{\nu=1}^{n} v_\nu \eta_\nu{}^0(\mathbf{s}),$$

and where (u_μ, v_ν) run over the elements of Ω. Corresponding to each such point $\left(x^0(\mathbf{s}), y^0(\mathbf{s})\right)$ the equation

$$\Psi\left(u_\mu, v_\nu \mid s_1, s_2, \ldots, s_p, t^0(\mathbf{s})\right) = 0$$

holds identically for $\mathbf{s} \varepsilon U_1$.

9. By hypothesis, the original curve $\mathfrak{C} : f(x, y) = 0$ is irreducible and at least of genus 1. Therefore, by Lemma 1, the same is true for all curves $\mathfrak{C}' : f'(x, y) = 0$ where f' is of the same degree as f and is such that the absolute values of all coefficients of $f' - f$ are smaller than a certain positive number δ.

We apply this result to the two curves

$$\mathfrak{C} : f(x, y) = 0 \quad \text{and} \quad \mathfrak{C}^0(\mathbf{s}) : f^0(x, y \mid \mathbf{s}) = 0.$$

From the construction,

$$\mathfrak{C}^0(\boldsymbol{\sigma}) = \mathfrak{C},$$

and the coefficients $\alpha_\lambda{}^0(\mathbf{s})$ of $\mathfrak{C}^0(\mathbf{s})$ are continuous functions of $\mathbf{s}$ in the neighbourhood U_1 of $\boldsymbol{\sigma}$. It follows then that a neighbourhood U of $\boldsymbol{\sigma}$, contained in U_1, exists such that, for $\mathbf{s} \varepsilon U$, $\mathfrak{C}^0(\mathbf{s})$ is of the same degree as $\mathfrak{C}$, while at the same time the absolute values of all coefficients of $f^0(x, y \mid \mathbf{s}) - f(x, y)$ are less than δ. Hence, for $\mathbf{s} \varepsilon U$, $\mathfrak{C}^0(\mathbf{s})$ is still irreducible and at least of genus 1.

10. As we found earlier, the generators $\xi_\mu{}^0(\mathbf{s})$ of $X^0(\mathbf{s})$ and similarly the generators $\eta_\nu{}^0(\mathbf{s})$ of $Y^0(\mathbf{s})$ are linearly independent over R as long as $\mathbf{s}$ is a variable point. On the other hand, there may be special points $\mathbf{s} \varepsilon U$

for which the generators of $X^0(\mathbf{s})$ or those of $Y^0(\mathbf{s})$ cease to be linearly independent.

Let us consider the points $\mathbf{s}$ in U for which, say, the linear relation

$$u_1 \xi_1{}^0(\mathbf{s})+u_2 \xi_2{}^0(\mathbf{s})+\ldots+u_m \xi_m{}^0(\mathbf{s})=0 \tag{1}$$

holds; here $u_1, u_2, \ldots, u_m$ are given rational numbers not all zero. This equation is equivalent to

$$\sum_{\mu=1}^{m} u_\mu X_\mu\left(s_1, s_2, \ldots, s_p, t^0(\mathbf{s})\right)=0,$$

and it does not hold identically in $\mathbf{s}$. Hence t can be eliminated from the two equations

$$\sum_{\mu=1}^{m} u_\mu X_\mu(s_1, s_2, \ldots, s_p, t)=0, \quad Q(s_1, s_2, \ldots, s_p;\ t)=0.$$

The resultant,

$$H(u_\mu \mid \mathbf{s}) \equiv H(u_1, u_2, \ldots, u_m \mid s_1, s_2, \ldots, s_p)$$

say, is a polynomial in $R[u_1, u_2, \ldots, u_m, s_1, s_2, \ldots, s_p]$ and does not vanish identically in $\mathbf{s}$. It can be written explicitly in the form

$$H(u_\mu \mid \mathbf{s})=\sum_{j_1=0}^{g_1} \sum_{j_2=0}^{g_2} \ldots \sum_{j_p=0}^{g_p} h_{j_1 j_2 \ldots j_p}(u_1, u_2, \ldots, u_m)\, s_1^{j_1} s_2^{j_2} \ldots s_p^{j_p},$$

where the coefficients

$$h_{j_\pi}(u_\mu)=h_{j_1 j_2 \ldots j_p}(u_1, u_2, \ldots, u_m)$$

are elements of $R[u_1, u_2, \ldots, u_m]$. These coefficients do not all vanish and are rational numbers. It is of importance that *the degrees* $g_1, g_2, \ldots, g_p$ *are independent of the special choice of the* u_μ.

Evidently the relation (1) can hold for a point $\mathbf{s}$ only if $\mathbf{s}$ satisfies the condition

$$H(u_\mu \mid \mathbf{s})=0.$$

In exactly the same way we can treat linear relations

$$v_1 \eta_1{}^0(\mathbf{s})+v_2 \eta_2{}^0(\mathbf{s})+\ldots+v_n \eta_n{}^0(\mathbf{s})=0$$

between the generators $\eta_\nu{}^0(\mathbf{s})$ of $Y^0(\mathbf{s})$, and we then obtain an analogous condition

$$K(v_\nu \mid \mathbf{s})=0,$$

where

$$K(v_\nu \mid \mathbf{s})=\sum_{j_1=0}^{g_1'} \sum_{j_2=0}^{g_2'} \ldots \sum_{j_p=0}^{g_p'} k_{j_1 j_2 \ldots j_p}(v_1, v_2, \ldots, v_n)\, s_1^{j_1} s_2^{j_2} \ldots s_p^{j_p}$$

is an element of $R[v_1, v_2, \ldots, v_n, s_1, s_2, \ldots, s_p]$. Again, for rational $v_1, v_2, \ldots, v_n$ not all zero, the polynomials

$$k_{j_\pi}(v_\nu) = k_{j_1 j_2 \ldots j_p}(v_1, v_2, \ldots, v_n)$$

do not all vanish and have rational values.

11. Denote now by K_1 any finite algebraic extension field of the Gaussian field G of degree

$$[K_1 : G] > \max(g_1, g_1'),$$

by K_2 any finite algebraic extension field of K_1 of degree

$$[K_2 : K_1] > \max(g_2, g_2'),$$

etc., and finally by K_p any finite algebraic extension field of K_{p-1} of degree

$$[K_p : K_{p-1}] > \max(g_p, g_p').$$

This choice implies that if θ is a primitive element of one of the fields $K_1, K_2, \ldots, K_p$, and if $\gamma \neq 0$ belongs to G, then $\gamma\theta$ is still a primitive element of the same field. *Hence the primitive elements of each of these p fields are everywhere dense in the complex field C.*

Let $\mathbf{s} = (s_1, s_2, \ldots, s_p)$ be an arbitrary point in U for which s_1 is primitive in K_1, s_2 is primitive in K_2, etc., and finally s_p is primitive in K_p. We can easily show that then *both the generators $\xi_\mu{}^0(\mathbf{s})$ of $X^0(\mathbf{s})$ and the generators $\eta_\nu(\mathbf{s})$ of $Y^0(\mathbf{s})$ are linearly independent over R.*

It suffices to consider the generators of $X^0(\mathbf{s})$, as the other module $Y^0(\mathbf{s})$ can be treated analogously.

If a relation

$$u_1 \xi_1{}^0(\mathbf{s}) + u_2 \xi_2{}^0(\mathbf{s}) + \ldots + u_m \xi_m{}^0(\mathbf{s}) = 0$$

with rational $u_1, u_2, \ldots, u_m$ not all zero holds, then $\mathbf{s}$ satisfies the equation

$$H(u_\mu \mid \mathbf{s}) \equiv \sum_{j_1=0}^{g_1} \sum_{j_2=0}^{g_2} \ldots \sum_{j_p=0}^{g_p} h_{j_1 j_2 \ldots j_p}(u_1, u_2, \ldots, u_m) s_1^{j_1} s_2^{j_2} \ldots s_p^{j_p} = 0.$$

However, the coefficients $h_{j_\pi}(u_\mu)$ are rational numbers and do not all vanish. Since s_1 is a primitive element of K_1, and since

$$[K_1 : R] \geqslant [K_1 : G] > g_1,$$

at least one of the sums

$$\sum_{j_1=0}^{g_1} h_{j_1 j_2 \ldots j_p}(u_1, u_2, \ldots, u_m) s_1^{j_1}, \quad \text{where} \quad 0 \leqslant j_2 \leqslant g_2, \ldots, 0 \leqslant j_p \leqslant g_p,$$

must be different from zero, and all these sums are elements of K_1. Next, since s_2 is a primitive element of K_2, and since

$$[K_2 : K_1] > g_2,$$

at least one of the sums

$$\sum_{j_1=0}^{g_1} \sum_{j_2=0}^{g_2} h_{j_1 j_2 \dots j_p}(u_1, u_2, \dots, u_m) s_1^{j_1} s_2^{j_2}, \text{ where } 0 \leqslant j_3 \leqslant g_3, \dots, 0 \leqslant j_p \leqslant g_p,$$

does not vanish, and all these sums have values in K_2. The argument can be continued. Finally, s_p is a primitive element in K_p and

$$[K_p : K_{p-1}] > g_p,$$

whence
$$H(u_\mu \mid \mathbf{s}) \neq 0.$$

The assumed linear relation leads therefore to a contradiction.

12. The proof of Theorem 2 may now be completed as follows. The neighbourhood U of σ contains infinitely many points $\mathbf{s}$ with coordinates that are primitive elements of $K_1, K_2, \dots, K_p$, respectively; for, as we found, the primitive elements of these fields are dense in C. Select one such point $\mathbf{s} = \boldsymbol{\theta} = (\theta_1, \theta_2, \dots, \theta_p)$ in U. Since the coordinates of $\boldsymbol{\theta}$ are algebraic numbers, $t^0(\boldsymbol{\theta})$ is likewise an algebraic number.

It follows now, from what has already been proved, that the curve $\mathfrak{C}^0(\boldsymbol{\theta})$ is defined by an equation

$$f^0(x, y \mid \boldsymbol{\theta}) \equiv \Phi\left(x, y \mid \theta_1, \theta_2, \dots, \theta_p, t^0(\boldsymbol{\theta})\right) = 0$$

with algebraic coefficients, and that it is irreducible and at least of genus 1. We can further show that there are *infinitely many* distinct points of the JR-lattice $Z^0(\boldsymbol{\theta}) = X^0(\boldsymbol{\theta}) \times Y^0(\boldsymbol{\theta})$ on $\mathfrak{C}^0(\boldsymbol{\theta})$.

For we know that all points

$$\left(x^0(\boldsymbol{\theta}),\ y^0(\boldsymbol{\theta})\right)$$

$$= \left(u_1 \xi_1{}^0(\boldsymbol{\theta}) + u_2 \xi_2{}^0(\boldsymbol{\theta}) + \dots + u_m \xi_m{}^0(\boldsymbol{\theta}),\ v_1 \eta_1{}^0(\boldsymbol{\theta}) + v_2 \eta_2{}^0(\boldsymbol{\theta}) + \dots + v_n \eta_n{}^0(\boldsymbol{\theta})\right)$$

of $Z^0(\boldsymbol{\theta})$ for which (u_μ, v_ν) belongs to the infinite set Ω, lie on the curve. It suffices therefore to prove that there correspond *distinct* points (x, y) of the JR-lattice to different sets (u_μ, v_ν). But this is true because the generators $\xi_\mu{}^0(\boldsymbol{\theta})$ of $X^0(\boldsymbol{\theta})$ and the generators $\eta_\nu{}^0(\boldsymbol{\theta})$ of $Y^0(\boldsymbol{\theta})$ are linearly independent over R by the proof given in the last section.

Denote by K the finite algebraic extension field of R generated by the $m+n$ numbers

$$\xi_1{}^0(\boldsymbol{\theta}),\ \xi_2{}^0(\boldsymbol{\theta}),\ \dots,\ \xi_m{}^0(\boldsymbol{\theta}),\ \eta_1{}^0(\boldsymbol{\theta}),\ \eta_2{}^0(\boldsymbol{\theta}),\ \dots,\ \eta_n{}^0(\boldsymbol{\theta}),$$

by $\mathfrak{o}$ the ring of all algebraic integers in K, and by j a positive integer such that the m products

$$j\xi_1{}^0(\boldsymbol{\theta}),\ j\xi_2{}^0(\boldsymbol{\theta}),\ \dots,\ j\xi_m{}^0(\boldsymbol{\theta})$$

belong to $\mathfrak{o}$. The points $\left(x^0(\boldsymbol{\theta}), y^0(\boldsymbol{\theta})\right)$ of $Z^0(\boldsymbol{\theta})$ satisfy the conditions

$$jx_0(\boldsymbol{\theta}) \varepsilon \mathfrak{o}, \quad y^0(\boldsymbol{\theta}) \varepsilon K$$

of Theorem 1 and, by the construction, there are infinitely many such points on $\mathfrak{C}^0(\theta)$.

As this is a contradiction to Theorem 1, the set Ω cannot be infinite. This means that the original curve $\mathfrak{C}$ cannot contain infinitely many points of the JR-lattice Z, hence that Theorem 2 is true. This completes the proof*.

Note added December, 1955. I conclude this paper by stating a conjecture which I have not as yet succeeded in proving and which may be of some interest.

Let R and C be again the rational and complex fields, and let Ω denote an arbitrary subfield of C. Let $\mathfrak{C}$: $f(x, y) = 0$ be an irreducible algebraic curve of genus $g \geqslant 1$, where $f(x, y)$ is a polynomial in $\Omega[x, y]$. Denote by G any system of g points (x_j, y_j), $1 \leqslant j \leqslant g$, on $\mathfrak{C}$ which is *rational over* Ω (*i.e.* the rational symmetric functions of the coordinates of these g points lie in Ω). By means of the integrals of the first kind on $\mathfrak{C}$, the addition of systems G can be defined [see A. Weil, *Acta Math.* 52 (1928), 20 *et seq*.], and these systems then form an Abelian group Γ, say. Weil, in his paper, proved that Γ has finitely many generators if Ω is any simple algebraic extension of R. I conjecture, more generally, that Γ has still only finitely many generators when Ω is obtained from R by adjoining finitely many *algebraic or transcendental* elements of C.

Department of Mathematics,
University of Manchester,
Manchester, 13.

(*Received 26th March,* 1955.)

* I wish to express my thanks to D. G. Northcott for reading my manuscript and noticing an error in my original proof of Lemma 1, and to B. Segre for giving the reference to his paper of 1942 which allowed me to correct this error.

Printed by C. F. Hodgson & Son, Ltd., Pakenham Street, London, W.C.1.