ON ALGEBRAIC RELATIONS BETWEEN TWO UNITS OF AN ALGEBRAIC FIELD

K. MAHLER.

(Manchester.)

In this paper, I determine all irreducible algebraic equations $F(x, y) = 0$ which admit infinitely many different solutions $x = \xi$, $y = \eta$ in units ξ, η of a finite algebraic field; here $F(x, y) \neq 0$ is a polynomial in x and y with algebraic coefficients irreducible over the complex field. The result takes the simple form that $F(x, y)$ must consist of exactly two terms.

For the proof, I more generally study equations $F(x, y) = 0$ with an infinity of solutions in integers x, y of a finite algebraic field for which y allows only a given finite set of prime ideal factors.

The investigation depends essentially on Siegel's theorem on the integral solutions of Diophantine equations (1). For the special case of the rational field, I published already a similar proof in an earlier paper, and I apply here the same ideas (2).

I. *A lemma on irreducible polynomials.*

[1] Let $\mathfrak{F}$ be the field of all complex numbers, $\mathfrak{F}(x)$ the field of all rational functions of x with coefficients in $\mathfrak{F}$, and $\mathfrak{F}(x, y]$ the ring of all polynomials in y with coefficients in $\mathfrak{F}(x)$. Such a polynomial is called normed if the highest occurring power of y has the coefficient 1.

Denote by

(1) $$f(x, y) = y^n + a_1(x)y^{n-1} + \ldots + a_n(x)$$

a normed element of $\mathfrak{F}[x, y]$ which is irreducible over $\mathfrak{F}(x)$ and is of exact degree $n \geqslant 1$ in y. This expression can be factorized in the form

$$f(x, y) = \prod_{h=1}^{n} (y - \varphi_h(x))$$

where

(3) $$\varphi_1(x), \varphi_2(x), \ldots \varphi_n(x)$$

are algebraic functions of x. We exclude the special case when

$$n = 1, \quad \varphi_1(x) = \text{constant};$$

then none of the functions (3) is a constant, as follows immediately from the irreducibility of $f(x, y)$.

[2] We assume from now on that there exist a number $\alpha \neq 0$ and a prime number $N \geqslant 2$ such that the new polynomial

$$f(x, \alpha y^N)$$

is reducible over $\mathfrak{F}(x)$. Then the simpler polynomial

$$f(x, y^N)$$

is likewise reducible and so can be written as a product

4) $$f(x, y^N) = g(x, y)\, h(x, y)$$

where $g(x, y)$ and $h(x, y)$ are elements of $\mathfrak{F}(x, y]$ of positive degree in y. Without loss of generality, let from now on $g(x, y)$ be normed and irreducible over $\mathfrak{F}(x)$.

[3] $f(x, y^N)$ remains unchanged if y is replaced by εy where ε is a primitive Nth root of unity. Hence $f(x, y^N)$ is divisible by all N polynomials.

(5) $$g(x, \varepsilon^k y) \quad (k = 0, 1, \ldots, N-1).$$

These polynomials are also irreducible over $\mathfrak{F}(x)$ since $g(x, y)$ is so.

[4] If $G(x, y)$ is any element of $\mathfrak{F}(x, y]$ of positive degree less than n in y, then $G(x, y^N)$ cannot divide $f(x, y^N)$. For then $G(x, y)$ evidently would divide $f(x, y)$, contrary to the irreducibility of $f(x, y)$.

---

(1) C. L. Siegel. — *Preuss. Akad. d. Wissensch., Phys.-Math. Kl.*, 1929, Nr. 1.

(2) K. Mahler, *Journ. of the Lond. Math. Soc. 13* (1938), p. 173-177.

[5] The last result implies that we cannot have

$$(6)\quad g(x,y)=g(x,\varepsilon y)=g(x,\varepsilon^2 y)=\ldots=g(x,\varepsilon^{N-1}y).$$

identically in y. For then

$$g(x,y)=\frac{1}{N}\sum_{k=0}^{N-1} g(x,\varepsilon^k y)$$

remains unchanged if y is replaced by εy, and so $g(x,y)$ is of the form

$$g(x,y)=G(x,y^N)$$

where $G(x,y)$ is an element of $\mathfrak{F}(x,y]$ of positive degree less than n in y. This is, however, impossible since $G(x,y^N)$ divides $f(x,y^N)$.

[6] We can further say that no two of the polynomials (5) have a common factor in $\mathfrak{F}(x,y]$ which is of positive degree in y.

For, by hypothesis, $f(x,y)=0$ has no solution y = constant; therefore the term $a_n(x)$ of $f(x,y)$ does not vanish identically in x. Since $g(x,y)$ divides $f(x,y^N)$, its constant term $g(x,o)$ is then likewise not identically zero.

Suppose now, say, that the two polynomials

$$g(x,\varepsilon^k y) \text{ and } g(x,\varepsilon^\varkappa y)$$
$$\text{where } 0\leqslant k<\varkappa\leqslant N-1.$$

have a common factor in $\mathfrak{F}(x,y]$ which is of positive degree in y. Since both polynomials are irreducible, they differ only by a factor $\varphi(x)\not\equiv 0$ in $\mathfrak{F}(x)$:

$$g(x,\varepsilon^k y)=\varphi(x)\,g(x,\varepsilon^\varkappa y).$$

On putting $y=0$, this identity shows that $\varphi(x)$ is identically 1, hence that

$$g(x,\varepsilon^k y)=g(x,\varepsilon^\varkappa y),$$

whence

$$(7)\quad g(x,y)=g(x,\varepsilon^{\varkappa-k}y)=g(x,\varepsilon^{2(\varkappa-k)}y)=\ldots$$
$$=g(x,\varepsilon^{(N-1)(\varkappa-k)}y).$$

Since N is a prime and $0\leqslant k<\varkappa\leqslant N-1$, $\varkappa-k$ is prime to N; the integers

$$o,\ \varkappa-k,\ 2(\varkappa-k),\ \ldots\ (N-1)(\varkappa-k)$$

form therefore a complete system of residues (mod N). This means that the identities (7) are the same as the dentites (6), except for the order; and the identities (6) have already been shown to be impossible.

[7] Since any two of the functions (5) are relatively prime, and since each of these functions divides $f(x,y^N)$, their product

$$(8)\quad \gamma(x,y)=\prod_{k=0}^{N-1} g(x,\varepsilon^k y)$$

likewise divides $f(x,y^N)$. Now $\gamma(x,y)$ remains unchanged if y is replaced by εy; therefore $\gamma(x,y)$ is of the form

$$\gamma(x,y)=G(x,y^N)$$

where $G(x,y)$ is an element of $\mathfrak{F}(x,y]$ of positive degree in y. By [4], this implies that

$$G(x,y)=\varphi(x)f(x,y)$$

where $\varphi(x)$ is an element of $\mathfrak{F}(x)$ which is not identically zero, and so by (8),

$$(9)\quad \prod_{k=0}^{N-1} g(x,\varepsilon^k y)=\varphi(x)f(x,y^N).$$

This equation shows that $g(x,y)$ is of exact degree n in y; as $g(x,y)$ is normed, it is then of the form

$$g(x,y)=y^n+b_1(x)y^{n-1}+\ldots+b_n(x),$$

where $b_1(x)$, $b_2(x)$, ..., $b_n(x)$ are elements of $\mathfrak{F}(x)$. Therefore

$$g(x,\varepsilon^k y)=\varepsilon^{kn}y^n+\ldots+b_n(x)$$

and

$$\prod_{k=0}^{N-1} g(x,\varepsilon^k y)=\varepsilon\sum_{k=0}^{N-1} kn\,y^{nN}+$$
$$\ldots+b_n(x)^N=y^{nN}+\ldots+b_n(x)^N,$$

while

$$\varphi(x)f(x,y^N)=\varphi(x)y^{nN}+\ldots+\varphi(x)a_n(x).$$

We see then that $\varphi(x)\equiv 1$; the relation between $f(x,y)$ and $g(x,y)$ takes thus the simple form

$$(10)\quad \prod_{k=0}^{N-1} g(x,\varepsilon^k y)=f(x,y^N).$$

[8] By (2), $f(x,y^N)$ can be factorized as follows :

$$(11)\quad f(x,y^N)=\prod_{h=1}^{n}\prod_{k=0}^{N-1}(y-\varepsilon^k\varphi_h(x)^{1/N}).$$

On comparing with (10), we find that

$$(12)\quad g(x,y)=\prod_{l=1}^{n}(y-\varepsilon^{k_l}\varphi_{h_l}(x)^{1/N}),$$

where

$$(h_1,k_1),(h_2,k_2),\ldots,(h_n,k_n)$$

are n different pairs of allowed indices. Since $g(x, y)$ belongs to $\mathfrak{F}(x, y)$, every symmetrical function of

$$\varepsilon^{k_1}\varphi_{h_1}(x)^{1/N},\ \varepsilon^{k_2}\varphi_{h_2}(x)^{1/N},\ \ldots,\ \varepsilon^{k_n}\varphi_{h_n}(x)^{1/N}$$

and so also every symmetrical function of

$$\varphi_{h_1}(x),\ \varphi_{h_2}(x),\ \ldots, \varphi_{h_n}(x)$$

belongs to $\mathfrak{F}(x)$. The polynomial

$$f^*(x, y) = \prod_{l=1}^{n} (y - \varphi_{h_l}(x))$$

in y has therefore coefficients in $\mathfrak{F}(x)$ and belongs itself to $\mathfrak{F}(x, y)$. Now $f^*(x, y)$ has at least one zero $\varphi_{h_1}(x)$ in common with $f(x, y)$, and it is moreover normed and of the same degree in y as $f(x, y)$. Hence

$$f^*(x, y) \equiv f(x, y)$$

by the irreducibility of $f(x, y)$. This relation implies that $h_1, h_2, \ldots, h_n$ form a permutation of the indices $1, 2, \ldots, n$. Hence, on defining the Nth roots

$$\varphi_1(x)^{1/N},\ \varphi_2(x)^{1/N},\ \ldots,\ \varphi_n(x)^{1/N}$$

suitably, the formula (12) takes the simpler form

$$g(x, y) = \prod_{h=1}^{n} (y - \varphi_h(x)^{1/N}).$$

[9] In (13), the zero $\varphi_1(x)$ of $f(x, y)$ is an algebraic function of x, and it is by hypothesis not a constant; hence $\varphi_1(x)$ vanishes for at least one value $x = \xi$ of x. If we choose the prime N sufficiently large, then $\varphi_1(x)^{1/N}$ has at $x = \xi$ a branch point at least of degree N, and so it assumes at least N different values in suitable points $x = \xi^*$ near to $x = \xi$. All these values

$$\eta^* = \varphi_1(\xi^*)^{1/N}$$

satisfy the equation

$$g(\xi^*, \eta^*) = 0,$$

so that a contradiction arises as soon as N is greater than n.

[10] We can now prove the following result.

Iemma 1 : Let F $(x, y) \neq 0$ be a polynominal in x and y with coefficients in $\mathfrak{F}$, wich is irreducible over $\mathfrak{F}$ and not of the form

$$F(x, y) = ax + b$$

where $a \neq 0$ and b are in $\mathfrak{F}$. If N is a sufficiently large prime, any if $\alpha \neq 0$ is any element of $\mathfrak{F}$, then the polynomial $F(x, \alpha y^N)$ is likewise irreducible over $\mathfrak{F}$.

Proof : Write

$$F(x, y) = A_0(x)y^n + A_1(x)y^{n-1} + \ldots + A_n(x)$$

where

$$(14) \qquad A_0(x) \neq 0,\ A_1(x),\ \ldots,\ A_n(x)$$

are polynomials in x with coefficients in $\mathfrak{F}$. Assume that N is a very large prime number, and that $F(x, \alpha y^N)$, hence also $F(x, y^N)$, is reducible over $\mathfrak{F}$. Then

$$F(x, y^N) = G(x, y)H(x, y)$$

where both $G(x, y)$ and $H(x, y)$ are non-constant polynomials in x and y. Both these polynomials contain the variable y. For if for instance $G(x, y)$ is a polynomial in x alone, then $G(x, y)$ divides all polynomials (14), and so it also divides $F(x, y)$, contrary to hypothesis.

The normed element

$$f(x, y^N) = \frac{F(x, y^N)}{A_0(x)}$$

of $\mathfrak{F}(x, y]$ is therefore reducible over $\mathfrak{F}(x)$. By what we have proved in [2]-[9], this requires that also

$$f(x, y) = \frac{F(x, y)}{A_0(x)}$$

is reducible over $\mathfrak{F}(x)$. But then, by a well-known theorem [1], $f(x, y)$ is reducible over $\mathfrak{F}$, contrary to the hypothesis.

II. *Numbers divisible by only a finite number of prime ideals.*

[11] Let $\mathfrak{K}$ be a field of finite degree over the field of all rational numbers, and let

$$\mathfrak{P} = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s\}$$

be any finite set of prime ideals in $\mathfrak{K}$. We denote by $\langle\mathfrak{P}\rangle$ the set of all integers $\alpha \neq 0$ in $\mathfrak{K}$ which are divisible by no prime ideals except those in $\mathfrak{P}$. We need the following well-known result.

Lemma 2 : Let N be an arbitrary positive integer. Then every element α of $\langle\mathfrak{P}\rangle$ can be written as

$$\alpha = \alpha_\tau \alpha^{*N}$$

where α_τ is one of a finite number of elements

$$\alpha_1, \alpha_2, \ldots, \alpha_t$$

of $\langle\mathfrak{P}\rangle$, and α^* also belongs to $\langle\mathfrak{P}\rangle$.

(1) B. L. van der Waerden, *Moderne Algebra,* 2nd ed., 23.

[12] For the proof, select a system of units

$$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$$

of $\mathfrak{K}$ such that every unit ε in this field is of the form

$$\varepsilon = \varepsilon_1^{e_1}\varepsilon_2^{e_2}, \ldots \varepsilon_r^{e_r}$$

with rational integral exponents $e_1, e_2, \ldots, e_r$. Each such exponent can be written as

$$e_\rho = f_\rho N + g_\rho \qquad (\rho = 1, 2, \ldots; r)$$

where $f_1, f_2, \ldots, f_r$ are arbitrary integers, while $g_1, g_2, \ldots, g_r$ belong to the set of integers

$$0, 1, 2, \ldots, N\text{-}1.$$

On putting

$$\vartheta = \varepsilon_1^{f_1}\varepsilon_2^{f_2}, \ldots, \varepsilon_r^{f_t}, \; \theta = \varepsilon^{g_1}\varepsilon^{g_2}, \ldots, \varepsilon_r^{g}{}_r,$$

ε takes the form

$$\varepsilon = \vartheta\, \theta,$$

where ϑ is an arbitrary unit, while θ is a unit which can assume only a finite number of values, say the values

$$\theta = \theta_1, \theta_2, \ldots, \theta_u$$

[13] If α belongs to $\langle\mathfrak{P}\rangle$, the principal ideal (α) may be written in the form

$$(\alpha) = \mathfrak{p}^{a_1}\mathfrak{p}^{a_2}, \ldots, \mathfrak{p}^{a_s}$$

where, $a_1, a_2, \ldots, a_s$ are non-negative integers. On dividing these exponents by hN, where h is the class number of $\mathfrak{K}$, we get

$$a_\sigma = b_\sigma hN + c_\sigma \qquad (\sigma = 1, 2, \ldots, s)$$

where $b_1, b_2, \ldots, b_s$ are non-negative integers, while $c_1, c_2, \ldots, c_s$ belong to the set of integers

$$0, 1, 2, \ldots, hN\text{-}1$$

Put

$$\mathfrak{b} = (\mathfrak{p}_1{}^{b}{}_1\mathfrak{p}_2{}^{b_2}\mathfrak{p}_s{}^{b_s})^h, \; \mathfrak{c} = \mathfrak{p}_1{}^{c_1}\mathfrak{p}_2{}^{c_2}\mathfrak{p}_s{}^{c_s}$$

so that

$$(\alpha) = \mathfrak{b}^N\mathfrak{c}.$$

As the h-th power of an ideal, $\mathfrak{b} = (\beta)$ is principal, hence also $\mathfrak{c}$ as it lies in the inverse ideal class :

$$\mathfrak{c} = (\gamma) \text{ where } \gamma = \frac{\alpha}{\beta^N};$$

here both β and γ are integers in $\mathfrak{K}$. Since $\mathfrak{c}$ is one of a finite number of ideals, γ can be chosen so as to assume only a finite number of values, the values

$$\gamma = \gamma_1, \gamma_2, \ldots, \gamma_v$$

in $\mathfrak{K}$, say

[14] Since $(\alpha) = (\beta^N\gamma)$, we have

$$\alpha = \beta^N\gamma\varepsilon$$

where ε is a unit in $\mathfrak{K}$. By [12], this unit may be written in the form

$$\varepsilon = \vartheta^N\theta$$

where ϑ is an arbitrary unit, and θ is one of the finite set of units

$$\theta = \theta_1, \theta_2, \ldots, \theta_u.$$

Put now

$$\alpha^* = \beta\vartheta,$$

and denote by

$$\alpha_1, \alpha_2, \ldots, \alpha_t$$

the numbers

$$\gamma_\varkappa\theta_\lambda \qquad (\varkappa = 1, 2, \ldots, v; \lambda = 1, 2, \ldots, u)$$

in an arbitrary order. Then

$$\alpha = \alpha_\tau\alpha^{*N}$$

as asserted.

III. *The main theorems.*

[15] Let $F(x, y) \neq 0$ be a polynomial with algebraic coefficients which is irreducible over the field $\mathfrak{F}$ of all complex numbers [(1)].

Denote by $\mathfrak{K}$, as before, any field of finite degree over the field of all rational numbers, and give to $\mathfrak{P}$ and $\langle\mathfrak{P}\rangle$ the same meaning as in [11].

We assume that the equation

$$F(x, y) = 0$$

admits an infinite set Σ of solutions (x, y) in integers

$$x = \xi, \qquad y = \eta$$

in $\mathfrak{K}$ such that y belongs to $\langle\mathfrak{P}\rangle$.

The equations

$$x - \alpha = 0$$

where α is an integer in $\mathfrak{K}$, and

$$y - \beta = 0$$

both have these properties. In order to exclude such trivial cases, we assume from now on that $F(x, y)$ contains both variables x and y to at least the first power. Then both x and y assume infinitely many different values for the elements of Σ.

---

(1) One shows easily that this condition is satisfied if $F(x, y)$ is irreducible over the field of all algebraic numbers.

We make the further assumption that all coefficients of $F(x, y)$ are contained in $\mathfrak{K}$. This leads to no loss of generality, because if the hypothesis is satisfied for $\mathfrak{K}$, then it also holds for any finite extention of $\mathfrak{K}$.

[16] Denote by N a sufficiently large prime number, so that, by Lemma 1, $F(x, \alpha y^N)$ is irreducible over $\mathfrak{F}$ for every $\alpha \neq 0$ in $\mathfrak{K}$ (or even in $\mathfrak{F}$). By Lemma 2, the second coordinate η of every element

$$x = \xi, \qquad y = \eta$$

can be written in the form

$$\eta = \alpha_\tau \alpha^{*N}$$

where α_τ is one of a finite number of elements

$$\alpha_1, \alpha_2, \ldots, \alpha_t$$

of $\langle\mathfrak{P}\rangle$, and α^* likewise belongs to this set and so also to the integers of $\mathfrak{K}$. Now Σ is an infinite set, and every infinite subset has the same properties. We may therefore assume, without loss of generality, that

$$\alpha_\tau = \alpha_0 \neq 0$$

retains one fixed value α_0 for all points (x, y) of Σ.

[17] We have thus obtained the result that not only the curve

$$C : F(x, y) = 0,$$

but also every curve

$$C_N(\alpha) : F(x, \alpha y^N) = 0,$$

contains infinitely many points with coordinates integral in $\mathfrak{K}$; here N is an arbitrarily large prime, and $\alpha = \alpha_0 \neq 0$ is an integer in $\mathfrak{K}$ which depends on N.

[18] Now Siegel's theorem states [1] :

«Let the irreductible equation $F(x, y) = 0$ with coefficients in $\mathfrak{K}$ have infinitely many solutions in integers of $\mathfrak{K}$. Then the equation can be satisfied identically in a parameter z by two expressions,

$$x = P(z) = a_m z^m + a_{m-1} z^{m-1} + \ldots + a_{-m} z^{-m},$$
$$y = Q(z) = b_m z^m + b_{m-1} z^{m-1} + \ldots + b_{-m} z^{-m},$$

where $P(z)$ and $Q(z)$ are not both constants. Moreover, the parameter z can be chosen as a rational function of x and y.»

On applying this theroem to the two curves C and $C_N(\alpha)$, we obtain the following representations.

(*a*) *The coordinates* x, y *of a point on* $C : F(x, y) = 0$ *may be written as*

$$(15) \qquad x = P(z) = \sum_{h=-m}^{+m} a_h z^h, \quad y = Q(z) = \sum_{h=-m}^{+m} b_h z^h,$$

where both rational functions on the right-hand side are non-constant because C *does not contain any line parallel to either coordinate axis. Further*

$$(16) \qquad z = r(x, y)$$

is a rational function of x *and* y.

Since a similar representation is obtained on replacing z by $1/z$, and since $Q(z)$ is not a constant, there is no loss of generality in assuming that at least one coefficient b_h with $h > 0$ is different from zero.

Analogous formulae hold for the coordinates x, Y on the curve

$$C_N(\alpha) : F(x, \alpha Y^N) = 0.$$

Therefore, on putting $y = \alpha Y^N$, we obtain the following parameter representation of C :

(b) *If* N *is a sufficiently large prime, then the coordinates of a point* (x, y) *on* $C : F(x, y) = 0$ *may also be written as*

$$(17) \qquad x = P_N(Z) = \sum_{h=-m_N}^{+m_N} a_h^{(N)} Z^h,$$

$$y^{1/N} = Q_N(Z) = \sum_{h=-m_N}^{+m_N} b_h^{(N)} Z^h,$$

(*where neither of the rational functions* $P_N(Z)$, $Q_N(Z)$ *is a constant, and where the parameter* Z *is a rational function*

$$18) \qquad Z = r_N(x, y^{1/N})$$

of x *and* $y^{1/N}$.

As above, there is no loss of generality in assuming that at least one coefficient $b_h^{(N)}$ with $h > 0$ does not vanish.

[19] Since z is a rational function of x and y, and since x and y are rational functions of Z, the parameter z is a rational function

$$(19) \qquad z = T_N(Z)$$

of Z; this function is evidently not a constant.

From

$$(20) \qquad y = Q(z) = Q_N(Z)^N$$

we obtain the identity

$$(21) \qquad Q(T_N(Z)) = Q_N(Z)^N.$$

By (17), $Q_N(Z)$ has poles at most at $Z = 0$ and $Z = \infty$, Since further $b_h \neq 0$ for at least one index $h > 0$,

---

[1] See note [1], page 47.

$Q(z)$ has a pole at $z=\infty$. Hence $T_N(Z)$ may have poles only at $Z=0$ and $Z=\infty$, and so is of the form

$$(22) \qquad T_N(Z)=Z^{g_N}\,\Pi_N(Z),$$

where g_N is a rational integer, and $\Pi_N(Z)$ is a polynomial in Z satisfying

$$(23) \qquad \Pi_N(0)\neq 0.$$

[20] By hypothesis, there is at least one positive index h for which $b_h\neq 0$. **Suppose now that $Q(z)$ is not a polynomial,** hence that there exists also at least one negative index h' satisfying $b_{h'}\neq 0$. This means that $Q(z)$ has a pole at $z=0$. Hence, by (21), $T_N(Z)$ may now vanish only for $Z=0$ and $Z=\infty$, and so, by (23), is of the form

$$T_N(Z)=\rho_N Z^{g_N}$$

where $\rho_N\neq 0$ is a constant, while g_N is now an integer different from zero since $T_N(Z)$ is not a constant.

Since $Q(z)$ consists of at least two terms, there exists a finite value $z=z_1\neq 0$ such that

$$Q(z_1)=0.$$

Determine a number Z_1 by

$$z_1=T_N(Z_1)1=\rho_N Z_1^{g_N};$$

this number is likewise finite and different from zero. Therefore the derivative

$$T'_N(Z)=\frac{dP_N(Z)}{dZ}=\rho_N g_N Z^{g_N-1}$$

does not vanish at $Z=Z_1$.

On putting $Z=Z_1$ in the identity (21), the left-hand side

$$Q(T_N(Z_1))=Q(z_1)$$

vanishes, hence also the right-hand side

$$Q_N(Z_1)^N.$$

As the Nth power of a regular function, the function $Q_N(Z)^N$ has then a zero at least of order N at $Z=Z_1$, and therefore all its derivatives up to the $(N-1)$st order vanish at this point. Since $T'_N(Z_1)\neq 0$, this implies that the derivatives

$$\frac{d^\nu Q(z)}{dz^\nu} \qquad (\nu=0,1,2,\ldots,N-1)$$

are likewise all zero at $z=z_1$; $Q(z)$ vanishes therefore at least to the order N at this point. But

$$z^m Q(z)=\sum_{h=-m}^{+m} b_h z^{h+m}$$

is a polynomial of degree not greater than $2m$ and does not vanih identically. Hence our hypothesis leads to a contradiction if the prime N is greater than $2m$.

This we assume from now on; we know then that **$Q(z)$ is a non-constant polynomial in z.**

[21] Factorize this polynomial in the form

$$(24) \qquad Q(z)=b\prod_{l=1}^{p}(z-\zeta_l)^{d_l}$$

where $b\neq 0$ is a constant,

$$\zeta_1,\zeta_2,\ldots,\zeta_p$$

are the different zeros of $Q(z)$, and

$$d_1,d_2,\ldots,d_p$$

are positive integers. Then

$$Q(T_N(Z))=b\prod_{l=1}^{p}\{T_N(Z)-\zeta_l\}^{d_l}$$

must be the Nth power of the rational function $Q_N(Z)$.

We distinguish two cases, according as to whether $T_N(Z)$ is a polynomial, or has a pole at $Z=0$.

[22] If $T_N(Z)$ is a polynomial, then $Q_N(Z)$ is likewise one. In the identity

$$Q(T_N(Z))=b\prod_{l=1}^{p}\{T_N(Z)-\zeta_l\}^{d_l}=Q_N(Z)^N,$$

no two of the polynomials

$$T_N(Z)-\zeta_l \qquad (l=1,2,\ldots,p)$$

have a zero in common. Hence, if N is chosen greater than the largest of the exponents d_l, there exist p polynomials

$$(25) \qquad P_l(Z) \qquad (l=1,2,\ldots,p)$$

such that

$$(26) \qquad T_N(Z)-\zeta_l=P_l(Z)^N \qquad (l=1,2,\ldots,p)$$

identically in Z. Moreover, none of the polynomials (25) can be a constant because $T_N(Z)$ is not one.

[23] If $T_N(Z)$ is not a polynomial, then the exponent g_N in (22) can be written as

$$g_N=-h_N$$

where h_N is a positive integer. The identity (21) takes now the form

$$(27) \qquad b\prod_{l=1}^{p}\{\Pi_N(Z)-\zeta_l Z^{h_N}\}^{d_l}=Z^{h_N\sum_{l=1}^{p}d_l}\,Q_N(Z)^N.$$

Here none of the polynomials

$$\Pi_N(Z) - \zeta_l Z^{h_N} \quad (l = 1, 2, \ldots, p)$$

vanishes at $Z = 0$, and no two of them have a zero in common. Hence there exist p polynomials

(28) $$P_l(Z) \quad (l = 1, 2, \ldots, p)$$

such that

(29) $$\Pi_N(Z) - \zeta_l Z^{h_N} = P_l(Z)^N \quad (l = 1, 2, \ldots, p)$$

identically in Z.

The left-hand side of (27), hence also the right-hand side, is a polynomial; the exponent

$$h_N \sum_{l=1}^{N} d_l$$

of Z is therefore a multiple of N. Hence, if we assume now that the prime N is larger than

$$\sum_{l=1}^{N} d_l,$$

then h_N is divisible by N, thus of the form

(30) $$h_N = N j_N$$

where j_N is a positive integer. Since $T_N(Z)$ is not a constant, none of the rational functions

$$\{T_N(Z) - \zeta_l\}^{1/N} = \frac{P_l(Z)}{Z^{j_N}} \quad (l = 1, 2, \ldots, p)$$

can be a constant.

[24] We next show that $Q(z)$ cannot be divisible by two or more different linear factors $z - \zeta_l$.

For assume that $p \geq 2$. Then, according as to whether $P_N(Z)$ is, or is not, a polynomial, we have by (26), or by (29) and (30), the identities

$$T_N(Z) - \zeta_1 = P_1(Z)^N, \quad T_N(Z) - \zeta_2 = P_2(Z)^N,$$

or

$$T_N(Z) - \zeta_1 = \left(\frac{P_1(Z)}{Z^{j_N}}\right)^N, \quad P_N(Z) - \zeta_2 = \left(\frac{P_2(Z)}{Z^{j_N}}\right)^N,$$

respectively. Hence, on putting in the first case

$$u = P_1(Z), \quad u_2 = P_2(Z),$$

and in the second case

$$u = \frac{P_1(Z)}{Z^{j_N}}, \quad u_2 = \frac{P_2(Z)}{Z^{j_N}}.$$

we obtain a solution of the equation

$$u^N - v^N = \zeta_2 - \zeta_1$$

in rational, non-constant functions of a parameter Z. But this curve has no singular points because $\zeta_2 - \zeta_1 \neq 0$ and is therefore of positive genus if $N \geq 3$. The assumption that $p \geq 2$ leads therefore to a contradiction as soon as N is sufficiently large.

[25] We have thus found that $Q(z)$ is of the form

$$Q(z) = b(z - \zeta)^d$$

where $b \neq 0$ and ζ are complex numbers and d is a positive integer.

Denote by $\beta \neq 0$ an arbitrary complex number, and introduce the new parameter

$$z^* = \sqrt[d]{\frac{b}{\beta}}(z - \zeta)$$

and the new rational function

$$T^*_N(Z) = \sqrt[d]{\frac{b}{\beta}}\{T_N(Z) - \zeta\}.$$

Then $Q(z)$ is transformed into the simpler function

$$Q(z) = Q^*(z^*) = \beta z^{*d},$$

while the parameters z^* and Z are now connected by the relation

$$z^* = T^*_N(Z).$$

Let us now again omit the asterisk (1). We have then the following parameter representation of the curve

$$C : F(x, y) = 0.$$

The coordinates x and y are given by the formulae,

(31) $$\begin{cases} x = P(z) = \sum_{h=-m}^{+m} a_h z^h, \\ y = Q(z) = \beta z^d, \end{cases}$$

where $\beta \neq 0$ may be any complex number, while d is a fixed positive integer. Moreover, $P(z)$ is not a constant.

[26] By hypothesis, there exists an infinite set Σ of different points (x, y) on C for which x is an integer in $\mathfrak{K}$, and y lies in $\langle\mathfrak{P}\rangle$. For these points, the coordinate y may, by Lemma 2, be written in the form

$$y = \alpha_\tau \eta^d$$

where both α_τ and η belong to $\langle\mathfrak{P}\rangle$, and where α_τ has only a finite number of possible values. As we may, if necessary, replace Σ by an infinite subset, there is no loss of generality in assuming that α_τ has a fixed value

$$\alpha_\tau = \alpha \neq 0$$

(1) That this is permitted when $P(z)$ is a polynomial is obvious. If $P(z)$ has a pole at $z = 0$, then a proof similar to that in [30] may be used to show that $\zeta = 0$.

for all points (x, y) in Σ. For the same reason, we may restrict the discussion to the following two cases :

(i) For all elements (x, y) of Σ, y has the form

$$y = \alpha\eta^d$$

where η is a unit in $\mathfrak{K}$.

(ii) For all elements (x, y) of Σ, y has the form

$$y = \alpha\eta^d$$

where the norm of η is not bounded.

In either case, identify the constant β in (31) with the new constant α, and put

$$z = \eta.$$

Then z has an infinity of integral values in $\mathfrak{K}$, and for all these values the number $x = P(z)$ is an integer in $\mathfrak{K}$. Hence, in case (i), the coefficients a_h are elements of $\mathfrak{K}$, not necessarily integral. In case (ii), these coefficients are likewise in $\mathfrak{K}$; but now $P(z)$ is a polynomial

$$P(z) = \sum_{h=0}^{m} a_h z^h$$

in z. For suppose, on the contrary, that $P(z)$ contains a term $a_{h_0} z^{h_0}$ with $a_{h0} \neq 0$ and $h_0 < 0$. We may then choose this index in such a way that

$$z^{-h_0} P(z) = P_1(z)$$

is a polynomial with the constant term $S_{h0} \neq 0$. Since the norm of η is not bounded in Σ, η is divisible by an arbitrarily large power of one of the primes in $\mathfrak{P}$, say the prime ideal $\mathfrak{p}_1$. But then $P_1(z)$ is divisible at most by the highest power of $\mathfrak{p}_1$ which divides the numerator of a_{h0}, and therefore the denominator of $P(z)$ is divisible by arbitrarily high powers of $\mathfrak{p}_1$, contrary to the assumption that $x = P(z)$ is an integer in $\mathfrak{K}$ for all the points (x, y) of Σ.

[27] The long discussion has led us to the following result :

Theorem 1 : **Let $\mathfrak{K}$ be a field of finite degree over the rational field, and let $F(x,y)$ be a polynomial with coefficients in $\mathfrak{K}$ which is irreducible over the field of all complex numbers. Assume that the curve**

$$C : F(x, y) = 0$$

is not a line parallel to either of the coordinate axes.

(A) **If there are infinitely many points (x, y) on C for which x is an integer and y a unit in $\mathfrak{K}$, then the curve may be expressed parametrically in the form,**

$$x = P(z) = \sum_{h=-m}^{+m} a_h z^h, \quad y = Q(z) = \beta z^d$$

where m and d are two positive integers, all coefficients a_h and $\beta \neq 0$ are in $\mathfrak{K}$, and where $P(z)$ is not a constant.

(B) **If there are infinitely many points (x, y) on C such that x and y are intergers in $\mathfrak{K}$, the norm of y is unbounded, and y is divisible only by a finite set**

$$\mathfrak{P} = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s\}$$

of prime ideals, then the curve can be expressed parametrically in the form

$$x = P(z) = \sum_{h=0}^{m} a_h z^h, \quad y = Q(z) = \beta z^d$$

where m and d are two positive integers, all coefficients a_h and $\beta \neq 0$ are in $\mathfrak{K}$, and $P(z)$ is not a constant.

[28] As an application of Theorem 1, let now C satisfy the more rigorous condition that both coordinates x and y belong to $\mathfrak{P}$ when (x, y) runs over Σ. We can then express the coordinates of a point (x, y) on C in two ways parametrically, namely,

$$(32) \qquad \begin{cases} x = \alpha z^c = \displaystyle\sum_{h=-m}^{+m} a_h z'^h, \\ y = \displaystyle\sum_{h=-m}^{+m} b_h z^h = \beta z'^d; \end{cases}$$

here $\alpha \neq 0$, a_h, b_h, and $\beta \neq 0$ are elements of $\mathfrak{K}$, c and d are positive integers, and neither of the rational functions

$$\sum_{h=-m}^{+m} a_h z'^h \quad \text{and} \quad \sum_{h=-m}^{+m} b_h z^h$$

is a constant. Further both parameters z and z' are rational functions of x and y, hence also of one another. This means that there are four constants A, B, A′, B′ with $AB' - A'B \neq 0$ such that

$$z' = \frac{Az + B}{A'z + B'}, \quad z = \frac{B'z' - B}{-A'z' + A}.$$

On substituting in (32), we obtain the identities

$$\alpha\left(\frac{B'z' - B}{A'z' + A}\right)^c = \sum_{h=-m}^{+m} a_h z'^h$$

and

$$\beta\left(\frac{Az + B}{A'z + B'}\right)^d = \sum_{h=-m}^{+m} b_h z^h.$$

Since the right-hand sides have poles only at 0 and ∞, at least one of the two numbers A and A$'$, and at least one of the two numbers A$'$ and B$'$, must be zero. Hence

either $A = B' = 0$ **and** $A' \neq 0,\ B \neq 0,$ **or** $A' = 0$

[29] In the first case, the relation between z and z' becomes

$$z' = \frac{B}{A'} z^{-1}$$

and the curve C has therefore the parameter form

(33) $$x = \alpha z^c, \qquad y = \gamma z^{-d}$$

where $\alpha \neq 0$ and $\gamma = \beta \left(\frac{B}{A'}\right)^d \neq 0$ are elements of $\mathfrak{K}$, and c and d are positive integers. This case evidently arises only when the norms of x and y are bounded for all points (x, y) in Σ, this, for instance, when x and y are units in $\mathfrak{K}$.

[30] In the less simple second case when $A' = 0$, the relation between z and z' may be written in the form

(34) $$z' = Az + B$$

where $A = 0$. Hence the curve C now allows a representation

(35) $$x = \alpha z^c, \qquad y = \beta(Az + B)^d$$

where $\alpha \neq 0$, $\beta \neq 0$, $A \neq 0$, and B, are elements of $\mathfrak{K}$, while c and d are positive integers. The parameter z may still be replaced by τz where $\tau \neq 0$ is an arbitrary constant. It may therefore be assumed, without loss of generality, that A, B, and z, are integers in $\mathfrak{K}$, and that z belongs to $\langle\mathfrak{P}\rangle$. The coefficient $\beta \neq 0$ lies likewise in $\mathfrak{K}$, but may be fractional. Since y belongs to $\langle\mathfrak{P}\rangle$, $Az + B$ necessarily belongs to $\langle\mathfrak{P}^*\rangle$, where $\mathfrak{P}^*$ is obtained from $\mathfrak{P}$ by joining to this set all the different prime ideals dividing the numerator of β.

Hence both z and $Az + B$ belong to $\langle\mathfrak{P}^*\rangle$, and z assumes infinitely many different values when the point (x, y) runs over Σ. Select now an arbitrarily large positive integer N. By Lemma 2, we have then

$$z = U_\sigma \Xi^N, \qquad Az + B = V_\tau H^N$$

where U_σ and V_τ each have only a finite number of possible values in $\langle\mathfrak{P}^*\rangle$, while Ξ and H both assume infinitely many different values in this set. We can again assume that U_τ and V_σ have fixed values

$$U_\sigma = U \neq 0, \quad V_\tau = V \neq 0$$

for the points of Σ. Therefore, finally, the relation

$$AU\Xi^N + B = VH^N$$

has an infinity of different solutions in integers Ξ. H of $\mathfrak{K}$. If now B were different from zero, the curve

$$AUX^N + B = VY^N$$

would be of positive genus for $N \geq 3$, and so we should obtain a contradiction to Siegel's theorem. Therefore $B = 0$, and the representation (35) of C has the simpler form

(36) $$x = \alpha z^c, \quad y = \beta_1 z^d \quad (\beta_1 = \beta A^d \neq 0)$$

where $\beta_1 \neq 0$ and $\alpha \neq 0$ are elements of $\mathfrak{K}$, and c and d are positive integers. The result is thus quite similar to that in [29].

[31] Let us now combine the results in the last two sections. We have found that the curve C is either of the form (33) when

$$x^d y^c = \alpha^d \gamma^c,$$

or of the form (36) when

$$\beta_1{}^c y^c = \alpha^d x^d.$$

The proof assumed, however, that C was not a line

$$x = a \quad \text{or} \quad y = b.$$

Hence our final result may be stated in the following form :

Theorem 2 : **Let $\mathfrak{K}$ be a field of finite degree over the rational field, and let $F(x, y)$ be a polynomial with coefficients in $\mathfrak{K}$ which is irreducible over the complex field. Let the ourve**

$$C : F(x, y) = 0$$

contain an infinite set of points (x, y) where x and y are units in $\mathfrak{K}$, or where, more generally, both x and y are divisible only by a finite set of given prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ in $\mathfrak{K}$. Then the polynomial $F(x, y)$ consists of exactly two non-vanishing terms.