invariant subgroup of order $1 + 3k$. Since s_1s_2 is of order 3 we have $(s_1s_2)^3 = (s_1s_2^{-1}\, s_1s_2)^3 = 1$. It is easy to prove that $s_1s_2s_1$ generates a cyclic group whose generators are commutative with their conjugates under s_1 and under s_2. That is, if a group contains a maximal subgroup of order 3 it contains an invariant abelian subgroup of index 3 which is either cyclic or of type 1^m. The groups which contain maximal subgroups of order 2 or of order 3 may therefore be regarded as determined, but those which contain maximal subgroups of order 2 are naturally considerably simpler than those which contain maximal subgroups of order 3.

[1] Cf. these PROCEEDINGS **27,** 212–216 (1941).

ON THE RIEMANN HYPOTHESIS IN FUNCTION-FIELDS

BY ANDRÉ WEIL

NEW SCHOOL FOR SOCIAL RESEARCH

Communicated June 11, 1941

A year ago[1] I sketched the outline of a new theory of algebraic functions of one variable over a finite field of constants, which may suitably be described as transcendental, in view of its close analogy with that portion of the classical theory of algebraic curves which depends upon the use of Abelian integrals of the first kind and of Jacobi's inversion theorem; and I indicated how this led to the solution of two outstanding problems, viz., the proof of the Riemann hypothesis for such fields, and the proof that Artin's non-abelian L-functions on such fields are polynomials. I have now found that my proof of the two last-mentioned results is independent of this "transcendental" theory, and depends only upon the algebraic theory of correspondences on algebraic curves, as due to Severi.[2]

Γ being a non-singular projective model of an algebraic curve over an algebraically closed field of constants, the variety of ordered couples (P, Q) of points on Γ has the non-singular model $\Gamma \times \Gamma$ (in a bi-projective space); correspondences are divisors on this model, additively written; they form a module $\mathfrak{C}$ on the ring Z of rational integers. Let Γ_A, Γ_B', Δ, respectively, be the loci of points (P, A), (B, P) and (P, P), on $\Gamma \times \Gamma$, A and B being fixed on Γ and P a generic point of Γ (in the precise sense defined by van der Waerden[3]). The intersection number (C, D) of C and D being defined by standard processes[4] for irreducible, non-coinciding correspondences C, D, will be defined for any C and D which have no irreducible component in common, by the condition of being linear both in C and in D. The degrees $r(C)$, $s(C)$, and the coincidence number $f(C)$

of C are defined as its intersection numbers with a generic Γ_A, with a generic Γ_B' and with Δ, respectively. Transformation $(P, Q) \rightarrow (Q, P)$, which is a birational, one-to-one involution of $\Gamma \times \Gamma$ into itself, transforms a correspondence C into a correspondence which will be denoted by C'. To every rational function φ on $\Gamma \times \Gamma$ is attached a divisor (the divisor of its curves of zeros and poles), i.e., a corresponding C_φ; and $(C_\varphi, D) = 0$ whenever it is defined. Let $\mathfrak{C}_0$ be the module of all correspondences of the form $C_\varphi + \Sigma a_i \Gamma_{A_i} + \Sigma b_j \Gamma_{B_j}'$: if $C \epsilon \mathfrak{C}_0$, then $f(C) = r(C) + s(C)$ (whenever $f(C)$ is defined), since this is true for $C = C_\varphi$ (both sides then being 0) and for $C = \Gamma_A$, $C = \Gamma_B'$. Put $\mathfrak{R} = \mathfrak{C} - \mathfrak{C}_0$; an element γ in $\mathfrak{R}$ is a co-set in $\mathfrak{C}$ modulo $\mathfrak{C}_0$, and it can be shown that there always is a C in this co-set for which $f(C)$, $r(C)$, $s(C)$ are defined, so that, putting $\sigma(\gamma) = r(C) + s(C) - f(C)$, $\sigma(\gamma)$ is defined as a linear function over $\mathfrak{R}$. If γ_0 in $\mathfrak{R}$ corresponds to Δ in $\mathfrak{C}$, $\sigma(\gamma_0) = 2g$, where g is the genus of Γ. If $C \epsilon \mathfrak{C}_0$, we have $C' \epsilon \mathfrak{C}_0$, and so the reciprocal relation $(C \rightleftarrows C')$ in $\mathfrak{C}$ induces a similar relation $(\gamma \rightleftarrows \gamma')$ in $\mathfrak{R}$; and $\sigma(\gamma') = \sigma(\gamma)$.

The product of correspondences now being defined essentially as in Severi, $\mathfrak{C}$ becomes a ring, with Δ as unit-element; $\mathfrak{C}_0$ is two-sided ideal in $\mathfrak{C}$, so that $\mathfrak{R}$ also can be defined as ring, with unit-element γ_0: we write $\gamma_0 = 1$. It is found that the degrees of $C \cdot D$ are $r(C) \cdot r(D)$, $s(C) \cdot s(D)$; and that (C, D) is the same as $(C \cdot D', \Delta) = f(C \cdot D')$, and hence is equal to $r(C) \cdot s(D) + r(D) \cdot s(C) - \sigma(\gamma \cdot \delta')$ if γ, δ are the elements of $\mathfrak{R}$ which correspond to C, D. It follows that $\sigma(\gamma\delta) = \sigma(\delta\gamma)$. From $\sigma(n \cdot 1) = 2ng$ it follows that ring $\mathfrak{R}$ has characteristic 0.

Defining the complementary correspondence to C as in Severi,[5] it is found that the generic complementary correspondence to C is irreducible and has degrees (g, m), where $2m = \sigma(\gamma\gamma')$: it follows that $\sigma(\gamma\gamma') \geqslant 0$, and that $\sigma(\gamma\gamma') = 0$ only if $\gamma = 0$.

Now, let k (as in my note[1]) be the Galois field with q elements; k_n its algebraic extension of degree n; $\bar{k}$ its algebraic closure. Let $K = k(x, y)$ be a separable algebraic extension of $k(x)$; $K_n = k_n(x, y)$; $\bar{K} = \bar{k}(x, y)$. Then $(x, y) \rightarrow (x^q, y^q)$ defines a correspondence I, of degrees 1, q, on a non-singular model Γ of field $\bar{K}$; I^n is the correspondence, of degrees 1, q^n, defined by $(x, y) \rightarrow (x^{q^n}, y^{q^n})$; and $I \cdot I' = q \cdot \Delta$ (more generally, any correspondence C, such that $r(C) = 1$, satisfies $C \cdot C' = s(C) \cdot \Delta$). Let ι be the element of $\mathfrak{R}$ which corresponds to I; we have $\iota \cdot \iota' = q$. The intersections of I^n with Δ, which are all found to be of multiplicity 1, are those points of Δ which have coördinates in k_n, so that the number ν_n of such points (i.e., of points on Γ with coördinates in k_n) is $f(I^n) = 1 + q^n - \sigma(\iota^n)$. But the numerator of the zeta-function $\zeta_K(s)$ of K is[6] a polynomial $P(u) = u^{2g} - (1 + q - \nu_1)u^{2g-1} + \ldots$, of degree $2g$, in $u = q^s$; and, putting $P(u) = \prod_i (u - \alpha_i)$, the numerator of the zeta-function of K_n is

$$P_n(u^n) = \prod_i (u^n - \alpha_i^n) = u^{2ng} - (1 + q^n - \nu_n)u^{n(2g-1)} + \dots,$$

so that we find that $\Sigma\alpha_i^n = 1 + q^n - \nu_n = \sigma(\iota^n)$.

Now, let $F(x) = \Sigma a_\mu x^\mu$ be any polynomial with coefficients in Z; apply $\sigma(\gamma\gamma') \geqslant 0$ to $\gamma = F(\iota)$; using $\iota\cdot\iota' = q$, $\sigma(1) = 2g$, and $\sigma(\iota'^n) = \sigma(\iota^n) = \Sigma\alpha_i^n$, we find

$$\sum_\mu a_\mu^2 \cdot 2g + 2 \sum_{\mu < \nu} a_\mu a_\nu q^\mu \cdot \sum_i \alpha_i^{\nu - \mu} \geqslant 0.$$

The functional equation of $\zeta_K(s)$ implies that to every root α_i of $P(u)$ there is a root $\alpha_i' = q/\alpha_i$, so that our inequality can be written as $\Sigma F(\alpha_i)F(\alpha_i') \geqslant 0$. The left-hand side of this is a quadratic form in the coefficients of F, which is $\geqslant 0$ for all integral values, and therefore also for all real values, of these coefficients. If α_1 is such that $\alpha_1\bar{\alpha}_1 = |\alpha_1|^2 \neq q$, i.e., $\alpha_1' \neq \bar{\alpha}_1$, suppose, first, that $\alpha_1' \neq \alpha_1$; put $\alpha_2 = \alpha_1'$; a polynomial $F(x)$ can be found, with real-valued coefficients, which vanishes for all roots of $P(u)$ except α_1, α_2, $\bar{\alpha}_1$, $\bar{\alpha}_2$, and takes prescribed values z_1, z_2 at α_1, α_2: then $\Sigma F(\alpha_i)F(\alpha_i') = z_1z_2 + \bar{z}_1\bar{z}_2$, which becomes < 0 for suitable z_1, z_2: this contradicts our previous inequality. We reason similarly if $\alpha_1' = \alpha_1$. Thus all roots of $P(u)$ must satisfy $|\alpha_i|^2 = q$, which is the Riemann hypothesis for ζ_K.

A detailed account of this theory, including the application to Artin's L-functions, and of the "transcendental" theory as outlined in my previous note, is being prepared for publication.

[1] Sur les fonctions algébriques à corps de constantes fini, C.R.t. 210 (1940), p. 592.

[2] F. Severi, *Trattato di Geometria algebrica*, vol. 1, pt. 1, Bologna, Zanichelli 1926, chapter VI. It should be observed that Severi's treatment, although undoubtedly containing all the essential elements for the solution of the problems it purports to solve, is meant to cover only the classical case where the field of constants is that of complex numbers, and doubts may be raised as to its applicability to more general cases, especially to characteristic $p \neq 0$. A rewriting of the whole theory, covering such cases, is therefore a necessary preliminary to the applications we have in view.

[3] A generic point of an irreducible variety of dimension n is a point, the coördinates of which satisfy the equations of the variety and generate a field of degree of transcendency n over the field of constants. Cf. B. L. van der Waerden, *Einführung in die algebraische Geometrie*, Berlin, Springer 1939, chap. IV, § 29.

[4] B. L. van der Waerden, "Zur algebraischen Geometrie XIII," *Math. Ann.*, **115**, 359, and XIV, *Ibid.* 619.

[5] Loc. cit.,[2] chap. VI, No. 75 (pp. 228–229) and No. 84 (pp. 259–267). Severi's treatment can be somewhat clarified and simplified at this point, as will be shown elsewhere.

[6] H. Hasse, "Über die Kongruenzzetafunktionen," *Sitz.-ber. d. Preuss. Akad. d. Wiss.* **1934**, 250.