Proceedings of the

NATIONAL ACADEMY OF SCIENCES

Volume 56 • Number 3 • September 15, 1966

CHARACTERIZATION OF PLANE ALGEBROID CURVES WHOSE MODULE OF DIFFERENTIALS HAS MAXIMUM TORSION

By Oscar Zariski

HARVARD UNIVERSITY

Communicated July 18, 1966

§1. Let k be an algebraically closed field of characteristic zero, let $f(X,Y)$ be an irreducible power series with coefficients in k, and let C be the plane algebroid curve defined by $f = 0$. We denote by $\mathfrak{o}(= k[[x,y]])$ the local ring of C, by $\mathfrak{m}$ the maximal ideal of $\mathfrak{o}$, and by $\mathfrak{o}d\mathfrak{o}$ the module of Kähler differentials of $\mathfrak{o}$. It is well known that $\mathfrak{o}d\mathfrak{o}(= \mathfrak{o}dx + \mathfrak{o}dy)$ is the quotient of a free module $\mathfrak{o}u + \mathfrak{o}v$ by the principal submodule generated by $f_xu + f_yv$, the images of u and v being dx and dy, respectively.

Let T be the torsion of $\mathfrak{o}d\mathfrak{o}$, i.e., the submodule consisting of the elements of $\mathfrak{o}d\mathfrak{o}$ which have a nonvanishing annihilator. It is clear *a priori* that the length $l(T)$ is finite (in the sequel, all lengths $l(M)$ are intended as lengths of $\mathfrak{o}$-modules M). Indeed, if $\omega\in T$, then $\xi\omega = 0$ for some $\xi\in\mathfrak{m}$, $\xi \neq 0$, and since $\mathfrak{o}$ is a local (noetherian) *domain, of dimension* 1, and T is finitely generated over $\mathfrak{o}$, it follows that $\mathfrak{m}^\rho T = 0$ for some integer $\rho \geqq 0$. This implies that $l(T)$ is finite.

Let $J = \mathfrak{o}f_x + \mathfrak{o}f_y$ be the Jacobian ideal of $\mathfrak{o}$.

Theorem 1. $l(T) = l(\mathfrak{o}/J)$.

Proof: Let $\mathfrak{A}_x = \{B\in\mathfrak{o}|Bf_x/f_y\in\mathfrak{o}\}$ (this is an ideal in $\mathfrak{o}$). For any B in $\mathfrak{A}_x$ we set $A = Bf_x/f_y$ and we consider the $\mathfrak{o}$-homomorphism

$$\varphi:\mathfrak{A}_x \to \mathfrak{o}d\mathfrak{o}$$

defined by $\varphi(B) = Adx + Bdy$. Since $A/f_x = B/f_y$, we have

$$f_x(Adx + Bdy) = A(f_xdx + f_ydy) = 0,$$

$$f_y(Adx + Bdy) = B(f_xdx + f_ydy) = 0.$$

Hence, $\varphi(B)\in T$. Conversely, if $\omega = Adx + Bdy\in T$ $(A,B\in\mathfrak{o})$ and if, say, $\xi\omega = 0(\xi\in\mathfrak{o},\ \xi \neq 0)$, then there exists H in $\mathfrak{o}$ such that $A\xi = Hf_x$, $B\xi = Hf_y$, and hence $A = Bf_x/f_y\in\mathfrak{o}$, showing that $B\in\mathfrak{A}_x$ and that $\omega = \varphi(B)$. We have thus shown that $\mathrm{Im}\varphi = T$. We have $\varphi(B) = 0$ if and only if $B\in\mathfrak{o}f_y$. Hence, $\mathrm{Ker}\varphi = \mathfrak{o}f_y$, and consequently

$$l(T) = l(\mathfrak{A}_x/\mathfrak{o}f_y). \tag{1}$$

Consider now the $\mathfrak{o}$-homomorphism

$$\mathfrak{o} \xrightarrow{\psi} J/\mathfrak{o}f_y \rightarrow 0$$

defined by the composition of the following $\mathfrak{o}$-homomorphisms:

$$\mathfrak{o} \rightarrow \mathfrak{o}f_x \rightarrow \mathfrak{o}f_x/(\mathfrak{o}f_x \cap \mathfrak{o}f_y) \stackrel{\approx}{\rightarrow} J/\mathfrak{o}f_y,$$

where the first arrow denotes multiplication by f_x. We have $\xi \in \mathrm{Ker}\psi \Longleftrightarrow \xi f_x \in \mathfrak{o}f_y \Longleftrightarrow \xi \in \mathfrak{A}_x$. Hence, $\mathfrak{o}/\mathfrak{A}_x \approx J/\mathfrak{o}f_y$, and consequently,

$$l(\mathfrak{o}/\mathfrak{A}_x) = l(J/\mathfrak{o}f_y). \tag{2}$$

In view of $\mathfrak{o} \supset J \supset \mathfrak{o}f_y$ and $\mathfrak{o} \supset \mathfrak{A}_x \supset \mathfrak{o}f_y$ we have $l(\mathfrak{o}/J) = l(\mathfrak{o}/\mathfrak{o}f_y) - l(J/\mathfrak{o}f_y)$ and $l(\mathfrak{A}_x/\mathfrak{o}f_y) = l(\mathfrak{o}/\mathfrak{o}f_y) - l(\mathfrak{o}/\mathfrak{A}_x)$. From this the theorem now follows, in view of (1) and (2).

Let $\mathfrak{C}$ be the conductor of $\mathfrak{o}$ in the integral closure $\bar{\mathfrak{o}}$ of $\mathfrak{o}$, and let $c = l(\mathfrak{C})$.

THEOREM 2. $l(T) \leqq c$.

Proof: The theorem is an easy consequence of the following formula due to R. Berger ["Differentialmoduln eindimensionaler lokaler Ringe," *Math. Z.*, **81**, 349 (1963), Corollary 2]:

$$l(T) = l(\bar{\mathfrak{o}}D\bar{\mathfrak{o}}/\mathfrak{o}D\mathfrak{o}) + \frac{c}{2}, \tag{3}$$

where $\bar{\mathfrak{o}}D\bar{\mathfrak{o}}$ is the module of differentials of $\bar{\mathfrak{o}}$ (regarded, according to our general stipulation, as a module over $\mathfrak{o}$) and $\mathfrak{o}D\mathfrak{o}$ is the submodule generated (over $\mathfrak{o}$) by the differentials $D\xi$, $\xi \in \mathfrak{o}$. We denote by v the natural valuation of $\bar{\mathfrak{o}}$ and by $v(\mathfrak{m})$ the set of (positive) integers $v(\xi)$, $\xi \in \mathfrak{m}$. If ν is any integer in $v(\mathfrak{m})$, and if, say, $\nu = v(\xi)$, $\xi \in \mathfrak{m}$, then $\nu - 1 = v(D\xi)$, and so $\nu - 1 \in v(\mathfrak{o}D\mathfrak{o})$. Hence, if we denote by $\mu_1, \mu_2, \ldots, \mu_{c/2}$ the positive integers which are missing in $v(\mathfrak{m})$ (the number of such integers is precisely $l(\bar{\mathfrak{o}}/\mathfrak{o})$, and it is known that $l(\bar{\mathfrak{o}}/\mathfrak{o}) = c/2$), then the set $\{\mu_1 - 1, \mu_2 - 1, \ldots, \mu_{c/2} - 1\}$ must contain all the nonnegative integers which are missing in $v(\mathfrak{o}D\mathfrak{o})$; in other words: the set $\{\mu_1 - 1, \mu_2 - 1, \ldots, \mu_{c/2} - 1\}$ must contain the complement $v(\bar{\mathfrak{o}}D\bar{\mathfrak{o}}) - v(\mathfrak{o}D\mathfrak{o})$ (here we use the fact that the characteristic of k is zero). It follows that

$$l(\bar{\mathfrak{o}}D\bar{\mathfrak{o}}/\mathfrak{o}D\mathfrak{o}) \leq \frac{c}{2}, \tag{4}$$

and this completes the proof of Theorem 2, in view of (3).

Note that in (4) [and hence also in (3)] we have equality if and only if every integer in $v(\mathfrak{o}D\mathfrak{o})$ is of the form $\nu - 1$, with $\nu \in v(\mathfrak{m})$, in other words, if and only if, given any differential Ω in $\mathfrak{o}D\mathfrak{o}$, there exists an element ξ in $\mathfrak{m}$ such that $v(\Omega) = v(D\xi)$. Upon replacing ξ by $c\xi$, where c is a suitable constant in k, we may assume that $v(\Omega - D\xi) > \nu(\Omega)$. Let $\Omega_1 = \Omega - D\xi$. By the same argument, there exists an element ξ_1 in $\mathfrak{m}$ such that $v(\Omega_1 - D\xi_1) > v(\Omega_1)$. In this fashion, we obtain a sequence $\{\xi_i\}$ in $\mathfrak{m}$ such that, if we set $\Omega_i = \Omega - D(\xi + \xi_1 + \ldots + \xi_{i-1})$, then $v(\Omega) < v(\Omega_1) < \ldots < v(\Omega_i) < \ldots$ and $v(\xi_i) = 1 + v(\Omega_i) \rightarrow +\infty$ as $i \rightarrow +\infty$. Thus, the infinite series $\sum_{i=0}^{+\infty} \xi_i (\xi_0 = \xi)$ is convergent in $\mathfrak{o}$, and if we set $\xi^* = \Sigma\xi_i$, then $\xi^* \in \mathfrak{o}$ and $\Omega = D\xi^*$. We have, therefore, the following

COROLLARY 3. $l(T) = c$ *if and only if every differential in* $\mathfrak{o}D\mathfrak{o}$ *is exact* (*i.e., is of the form* $D\xi$, $\xi \in \mathfrak{o}$).

Note: In a similar fashion, it follows easily that, quite generally, *the difference $c - l(T)$ is equal to the maximum number of linearly independent differentials in $\mathfrak{o}D\mathfrak{o}$ (over k), no linear combination of which, with nonzero coefficients in k, is exact.*

§2. The main result of this note is the following.

THEOREM 4. *$l(T) = c$ if and only if for a suitable basis $\{x,y\}$ of $\mathfrak{m}$ the equation of the curve C is of the form $y^n = x^m$ (where necessarily $(n,m) = 1$, since C is irreducible, and where we may assume that $n < m$).*

Proof: We fix a basis $\{x,y\}$ of $\mathfrak{m}$ and we denote by n the multiplicity of the local ring $\mathfrak{o}$ (whence, $n = \min\cdot\{v(x), v(y)\}$). Let, say, $v(x) = n$. Upon replacing y by $y - g(x)$, where $g(x)$ is a suitable polynomial in x, we may assume that $v(y) = m$, where $m > n$ and *m is not divisible by n* (we exclude the trivial case $n = 1$). The two integers n and m are uniquely determined by the ring $\mathfrak{o}$. Upon setting $x = t^n (t \in \bar{\mathfrak{o}})$ we have $\bar{\mathfrak{o}} = k[[t]]$ and the usual Puiseux parametric representation of the curve C:

$$x = t^n,\ y = t^m + c_1 t^{m+1} + c_2 t^{m+2} + \ldots, \tag{5}$$

where we have assumed, without loss of generality, that the coefficient of t^m is 1.

Let $n_1 < n_2 < \ldots < n_i < \ldots$ be the integers in $v(\mathfrak{m})$ which are greater than m. For each i we fix an element ξ_i in $\mathfrak{m}$ such that $v(\xi_i) = n_i$ and $v(\xi_i - t^{n_i}) > n_i$. We define, by induction on i, a Cauchy sequence $\{y_i\}$ in $\mathfrak{o}$, as follows: $y_1 = y - c_{n_1}\xi_1$ (note that we have then $y_1 = t^m + \sum_{j=1}^{\infty} c_j^{(1)} t^{m+j}$, with $c_{n_1-m}^{(1)} = 0$); assuming that $y_1, y_2, \ldots, y_i$ have already been defined and that $y_i = t^m + \sum_{j=1}^{\infty} c_j^{(i)} t^{m+j}$, with $c_{n_1-m}^{(i)} = c_{n_2-m}^{(i)} = \ldots = c_{n_i-m}^{(i)} = 0$, we set $y_{i+1} = y_i - c_{n_{i+1}-m}^{(i)}\xi_{i+1}$. Let $y^* = \lim y_i$. Then $y^* \in \mathfrak{m}$, $\{x,y^*\}$ is still a basis of $\mathfrak{m}$, and we have $y^* = t^m + \sum_{\alpha=1}^{c/2} b_\alpha t^{\mu_\alpha}$, where $\mu_1, \mu_2, \ldots, \mu_{c/2}$ are precisely the positive integers which are missing in $v(\mathfrak{m})$ (cf. with §1, proof of Theorem 2). We may therefore assume that our curve C is represented parametrically by

$$x = t^n, \qquad y = t^m + \sum_{\alpha=1}^{c/2} b_\alpha t^{\mu_\alpha}, \qquad \mu_\alpha \notin v(\mathfrak{m}). \tag{5'}$$

We call any parametric representation of C, of the form (5'), a *short representation.*

Suppose that for some basis $\{x,y\}$ of $\mathfrak{m}$, our curve C is defined by $x = t^n$, $y = t^m$. We find then that

$$x^i y^j Dx = \frac{n}{(i+1)\,n + jm} D(x^{i+1}y^j),$$

$$x^i y^j Dy = \frac{m}{in + (j+1)m} D(x^i y^{j+1}),$$

which shows that every differential in $\mathfrak{o}D\mathfrak{o}$ is exact and that consequently, $l(T) = c$ (Corollary 3). A direct verification shows that the ideal $\mathfrak{A}_x$, defined in §1, is now the ideal $\mathfrak{o}\cdot(f_y,x)$ and that the torsion elements of $\mathfrak{o}d\mathfrak{o}$ are the $(m-1)(n-1)$ $(= c)$ differentials $x^i y^j(mydx - nxdy)$ $(i = 0,1,\ldots,m-2;\ j = 0,1,\ldots,n-2)$.

Assume now that if $\{x,y\}$ is *any* basis of $\mathfrak{m}$, with $v(x) = n$ and $v(y) = m$, and if

$x = t^n$, then $y \neq t^m$. We shall show then that $l(T) < c$, by exhibiting a differential in $\mathfrak{o}D\mathfrak{o}$ which is not exact.

Our assumption implies that in any short parametric representation (5′) of C the coefficients b_α are not all zero. We fix a short representation (5′) and we denote by λ the first exponent μ_α such that $b_\alpha \neq 0$. Thus

$$x = t^n,\ y = t^m + bt^\lambda + \text{a finite sum of terms } b_\alpha t^{\mu_\alpha};$$
$$b \neq 0,\ \mu_\alpha > \lambda > m(\lambda, \mu_\alpha \not\in v(\mathfrak{m})). \quad (6)$$

We now show that if $\lambda + n$ *is of the form* $an + bm$, *with* $a \geqq 0$ *and* $b \geqq 0$, *then there exists a short parametric representation of* C:

$$x' = \tau^n, \qquad y' = \tau^m + b'\tau^{\lambda'} + \ldots,\ (b' \neq 0,\ \lambda' > m) \quad (6')$$

such that $\lambda' > \lambda$. To see this, we observe that if $\lambda + n$ is of the above-indicated form $an + bm$, then $a = 0$, for if $a \geqq 1$, then $\lambda = (a-1)n + bm \in v(\mathfrak{m})$, contrary to the definition of short representations. Hence, we have $\lambda = (j+1)m - n$, where $j \geqq 1$, since $\lambda > m$. This being so, we set

$$x' = x + ay^j = \tau^n,$$

where the constant a is to be determined. We have

$$\tau^n = t^n + at^{jm} + \text{terms of higher degree.}$$

Hence,

$$t = \tau - \frac{a}{n}t^{jm+n+1} + \ldots,$$

and

$$y = \tau^m + \left(b - \frac{am}{n}\right)\tau^\lambda + \text{terms of degree} > \lambda.$$

We set $a = \dfrac{bn}{m}$, and then, upon replacing y by a suitable element y' [following the same procedure used above in replacing y by y^*, leading from (5) to the short representation (5′)], we obtain a short representation (6′), with $\lambda' > \lambda$.

We shall now consider only such short representations (6) *in which the exponent* λ *is not of the form* $bm - n$ $(b > 0)$.

We shall now need the following

LEMMA 5. *If* ν *is an element of* $v(m)$ *and* ν *is not of the form* $an + bm$ $(a \geqq 0, b \geqq 0)$, *then* $\nu \geqq mn_1 + \lambda - m$, *where* $n_1 = n/(n,m)$.

Proof of the lemma: Let $\xi = \Sigma a_{ij}x^iy^j$ be an element of $\mathfrak{m}$ such that $v(\xi)$ is different from the value of any monomial x^ay^b. Then the power series $\Sigma a_{ij}x^iy^j$ must contain a certain set of terms $a_\alpha x^{i_\alpha}y^{j_\alpha}$, *of equal value*, such that if

$$\eta = a_1x^{i_1}y^{j_1} + a_2x^{i_2}y^{j_2} + \ldots + a_qx^{i_q}y^{j_q} \quad (q \geqq 2;\ a_\alpha \neq 0)$$

is the sum of terms of that set, then

$$v(\xi) \geqq v(\eta) > v(x^{i_\alpha}y^{j_\alpha}).$$

Let $m_1 = m/(m,n)$. From the fact that $(m_1,n_1) = 1$ and that

$$i_1n_1 + j_1m_1 = i_2n_1 + j_2m_1 = \ldots = i_qn_1 + j_qm_1,$$

it follows that if, say,

$$i_1 < i_2 < \ldots < i_q,$$

then

$$j_1 > j_2 > \ldots > j_q,$$

and

$$\eta = x^{i_1}y^{j_q}\varphi(x^{m_1},y^{n_1}),$$

where φ is a form, of degree q, in x^{m_1},y^{n_1}. Furthermore, since $v(\eta) > v(x^{i_\alpha}y^{j_\alpha})$, we must have $v(\varphi(x^{m_1},y^{n_1})) > qv(x^{m_1})(= qv(y^{n_1}))$. *This implies that* $\varphi(X, Y)$ *must be divisible by* $Y - X$. Now, $v(y^{n_1} - x^{m_1}) = mn_1 + \lambda - m_1$ by (6). Hence, $v(\eta) \geqq mn_1 + \lambda - m$, and the lemma is proved (since $v(\xi) \geqq v(\eta)$).

We now observe that $\lambda + n < mn_1 + \lambda - m$ (since $n_1 > 1$ and $n < m$). Since we have assumed that $\lambda + n$ is not of the form $an + bm$ ($a \geqq 0$, $b \geqq 0$), it follows from the above lemma that

$$\lambda + n \not\in v(\mathfrak{m}). \tag{7}$$

Now, consider the differential $\Omega = my\,Dx - nx\,Dy$ in $\mathfrak{o}D\mathfrak{o}$. We find at once that $v(\Omega) = \lambda + n - 1$. Therefore, it follows by (7) that Ω is *not* an exact differential $D\xi$, $\xi \in \mathfrak{o}$. This completes the proof of Theorem 4.

We conclude with one final observation. Consider all possible short parametric representations (6) of C such that $\lambda + n$ is not of the form $an + bm$, $a \geqq 0$, $b \geqq 0$. We have just shown that in that case $\lambda + n \not\in v(\mathfrak{m})$. The converse is obvious: if $\lambda + n \not\in v(\mathfrak{m})$, then certainly $\lambda + n$ is not of the form $an + bm$, $a \geqq 0$, $b \geqq 0$. So we can say that we are dealing with all short parametric representations (6) of C such that $\lambda + n \not\in v(\mathfrak{m})$. The exponent λ may depend *a priori* on the particular short parametric representation under consideration. However, we show that, in fact, *the integer* λ *is the same for all short parametric representations of* C *and is therefore an analytical invariant of the curve* C. We prove this by fixing a short parametric representation (6) and showing that $\lambda + n - 1$ has the following intrinsic property: *it is the smallest of all integers which belong to* $v(\mathfrak{o}D\mathfrak{o})$ *and do not belong to* $v(D\mathfrak{o})$. In other words, we shall show that if Ω is the *differential* $my\,Dx - nx\,Dy$ *introduced above, and if* Ω' *is any differential in* $\mathfrak{o}D\mathfrak{o}$ *such that* $v(\Omega')$ *is not of the form* $v(\xi) - 1$, $\xi \in \mathfrak{o}$, *then* $v(\Omega') \geqq v(\Omega)$.

To see this, let $\Omega' = ADx + BDy$ with A, B in $\mathfrak{o}$. Then it is immediate that

$$nx\Omega' = (nAx + mBy)Dx - B\Omega.$$

We cannot have $v(x\Omega') = v((nAx + mBy)Dx)$, for otherwise it would follow that $v(\Omega') = v(\xi) - 1$, with $\xi = nAx + mBy \in \mathfrak{o}$, contrary to assumption. Therefore,

$$v(x\Omega') \geqq v(B\Omega). \tag{8}$$

We assert that $B \in \mathfrak{m}$. For we have the inequalities $v(\Omega') \neq v(ADx)$ $(= v(Ax) - 1)$ and $v(\Omega') \neq v(BDy)(= v(By) - 1)$, and hence $v(ADx) = v(BDy)$, i.e., $v(A) + n = v(B) + m$. Were B a unit in $\mathfrak{o}$, it would follow that $m - n = v(A) \in v(\mathfrak{o})$, which is impossible, since every element of $v(\mathfrak{o})$ which is less than m is necessarily a multiple of n. This proves our assertion that $B \in \mathfrak{m}$. It follows that $v(B) \geqq v(x)$, and hence, by (8), $v(\Omega') \geqq \Omega$.