THE C_{ab} CURVE

RYUTAROH MATSUMOTO

ABSTRACT. We characterize the defining equation of a plane algebraic curve with exactly one rational place Q at infinity, then give a basis of $L(mQ)$ with pairwise distinct pole orders at Q. The defining equation can be regarded as a generalization of the Weierstrass form of a hyperelliptic curve.

In this informal note I give an English proof of the results of the C_{ab} curve found by Miura [4, 5, 6]. Throughout in this note, K denotes a perfect field, and a, b denote relatively prime positive integers. For a place Q of an algebraic function field, we define

$$L(\infty Q) = \bigcup_{i=1}^{\infty} L(iQ),$$

and v_Q denotes the discrete valuation at Q. We say a place Q *K-rational* if the degree of Q is one.

Theorem 1. [5, Theorem 5.17 and Lemma 5.30], [6, Appendix B and Lemma, p.1416] *Let $\overline{K}$ be the algebraic closure of K, $\chi \subset \overline{K}^2$ be a possibly reducible affine algebraic set defined over K, x, y the coordinate of the affine plane $\overline{K}^2$, and a, b relatively prime positive integers. The following 2 conditions are equivalent.*

1. *χ is an absolutely irreducible algebraic curve with exactly one K-rational place Q at infinity, and the pole divisors of x and y are aQ and bQ respectively.*
2. *χ is defined by a bivariate polynomial of form*

$$\alpha_{b,0}x^b + \alpha_{0,a}y^a + \sum_{ia+jb<ab} \alpha_{i,j}x^i y^j, \tag{1}$$

where $\alpha_{i,j} \in K$ for all i, j and $\alpha_{b,0}, \alpha_{0,a}$ are nonzero.

Proof. $(1 \Rightarrow 2)$ Let X, Y be variables over K, $F(X,Y) \in K[X,Y]$ the defining equation of χ, and $x, y \in K[X,Y]/F(X,Y)$ the elements represented by X, Y.

Consider the minimal polynomial $G(x,Y)$ of y over the subfield $K(x)$. Since $[K(x,y) : K(x)] = a$ [9, Theorem I.4.11], the degree of $G(x,Y)$ is a. The integral closure of $K[x]$ in $K(x,y)$ is $L(\infty Q)$ [9, Theorem III.2.6], and $y \in L(\infty Q)$. Thus y is integral over $K[x]$, and $G(x,Y) \in K[x,Y]$. Write $G(X,Y)$ as

$$\sum_{X,Y} \beta_{i,j} X^i Y^j.$$

If $v_Q(x^i y^j) = -ab$ and both i and j are nonnegative, then (i, j) is either $(b,0)$ or $(0,a)$. By the strict triangle inequality of a discrete valuation [9, Lemma I.1.10], for every term $\beta_{i,j}x^i y^j$ in $G(x,y)$, $v_Q(x^i y^j) \geq -ab$, and the coefficient $\beta_{b,0}$ of the term $\beta_{b,0}x^b$ is nonzero.

Date: December 17, 1998.

1991 *Mathematics Subject Classification.* Primary 14H99; Secondary 14H05, 94B27, 11T71.

The latest version of this note can be downloaded from `http://tsk-www.ss.titech.ac.jp/~ryutaroh/cab.html`.

Therefore if $\beta_{i,j}x^iy^j$ is a term in $G(x,y)$, then the exponent (i,j) is either $(b,0)$ or $(0,a)$, or $ai+bj<ab$.

Finally we have to show that $F(X,Y)$ is a constant multiple of $G(X,Y)$, and it is enough to show that $G(X,Y)$ generates the kernel of the canonical homomorphism $\varphi : K[X,Y] \to K[x,y]$. If $H(X,Y) \in \ker\varphi \setminus \{0\}$, then the degree of $H(X,Y)$ in Y is at least a, because $G(x,Y)$ is the minimal polynomial of y over $K(x)$. Thus $\{G(X,Y)\}$ is a Gröbner basis of $\ker\varphi$ with respect to the lexicographic monomial order $Y > X$ [1, Definition 5, Section 2.5], and a Gröbner basis generates the ideal [1, Corollary 6, Section 2.5].

($2 \Rightarrow 1$) Let $F(X,Y)$ be the polynomial of (1), and x,y the elements in $K[X,Y]/F(X,Y)$ represented by X,Y. By the theory of Gröbner bases [1, Proposition 4, Section 5.3], we see that

$$\{x^iy^j \mid 0 \le i,\ 0 \le j \le a-1\} \tag{2}$$

is a basis of $K[x,y]$ as a K-linear space, where $\{F(X,Y)\}$ is viewed as a Gröbner basis with respect to the lexicographic monomial order $Y > X$.

Any element f in $K[x,y]$ can be written uniquely as a polynomial

$$\sum_{i,j} \beta_{i,j}x^iy^j, \tag{3}$$

where each monomial x^iy^j belongs to the basis (2) and $\beta_{i,j} \in K$. We define a function o from $K[x,y]$ to $\mathbb{Z} \cup \{-\infty\}$ to be

$$\begin{aligned} o(0) &= -\infty, \\ o(f) &= \max\{ak+bl \mid x^ky^l \text{ is a monomial of } f \text{ written as (3).}\}, \end{aligned}$$

where f is nonzero. Then for $f,g \in K[x,y]$, $o(f) = -\infty$ iff $f = 0$ and $o(fg) = o(f) + o(g)$, where the sum of $-\infty$ and an integer is $-\infty$.

Now we can prove the absolute irreducibility of the polynomial (1). The following discussion is based on [3, Proposition 12]. Suppose that $fg = 0$ for $f,g \in K[x,y]$. Then $o(fg) = -\infty$, which implies $o(f) = -\infty$ or $o(g) = -\infty$. Thus $K[x,y]$ is an integral domain. This argument is valid if K is replaced by its algebraic closure. So the polynomial (1) is absolutely irreducible.

Next we will show that χ has exactly one place at infinity. Note that $K(x,y)/K$ is an algebraic function field with the full constant field K. We define a function v from $K(x,y)$ to $\mathbb{Z} \cup \{\infty\}$ such that for nonzero $f/g \in K(x,y)$, $v(f/g) = o(g) - o(f)$ and $v(0) = \infty$. Then v satisfies the axiom of the discrete valuation [9, Definition I.1.9]. Let Q be the place of $K(x,y)/K$ corresponding to v, and P_∞ be the pole of x in the rational function field $K(x)$. Then Q lies over P_∞, and the ramification index of Q over P_∞ is a, which equals to the extension degree $[K(x,y) : K(x)]$. Thus P_∞ is totally ramified, Q is K-rational, and the pole divisor of x in $K(x,y)$ is aQ. A similar argument shows that the pole divisor of y is bQ. Since $K[x,y] \subseteq L(\infty Q)$, the set of places at infinity is $\{Q\}$. □

Definition 2. A plane curve defined by a polynomial of the form (1) is said to be a C_{ab} *curve*.

Corollary 3. [5, Theorem 5.17], [6, Appendix B] *Let $F(X,Y) \in K[X,Y]$ be a polynomial of the form (1), Q a unique place at infinity of the C_{ab} curve defined by $F(X,Y)$. Then*

$$\{X^iY^j \bmod F(X,Y) \mid 0 \le i,\ 0 \le j \le a-1\}$$

is a K-basis of $K[X,Y]/F(X,Y)$ *and elements in the basis have pairwise distinct discrete valuations at* Q*. If the* C_{ab} *curve is nonsingular, then* $K[X,Y]/F(X,Y) = L(\infty Q)$ *and a basis of* $L(mQ)$ *is*

$$\{X^iY^j \bmod F(X,Y) \mid 0 \le i,\ 0 \le j \le a-1,\ ai+bj \le m\},$$

for a nonnegative integer m*.*

The previous corollary overlaps with [8, Proposition 13 and 14].

Corollary 4. [5, 6] *Let* F/K *is an algebraic function field with a* K*-rational place* Q*. Then there exists a* C_{ab} *curve defined over* K *with the function field* F*.*

Proof. There exist elements $x, y \in F$ such that pole divisors of x and y are aQ and bQ respectively, and a, b are relatively prime positive integers. We claim that $F = K(x,y)$. $[F : K(x)] = a$ and $[F : K(y)] = b$ by [9, Theorem I.4.11], and $[F : K(x,y)]$ divides both $[F : K(x)]$ and $[F : K(y)]$. Thus $[F : K(x,y)] = 1$.

Consider the ring homomorphism φ:

$$\begin{array}{ccc} K[X,Y] & \longrightarrow & K[x,y], \\ f(X,Y) & \longmapsto & f(x,y), \end{array}$$

where X, Y are variable over K. Then the plane curve defined by $\ker\varphi$ is a C_{ab} curve by Theorem 1. □

Historical Note 5. The results in this note are generalizations of [4], and were first officially published in [5]. The results in [6] is a subset of [5], and also contain the results in this note. In [4] Miura proved the following fact.

> Let χ be a nonsingular affine algebraic curve defined by a bivariate polynomial of the form (1). Then χ has exactly one rational place Q at infinity, the pole divisors of x and y are aQ and bQ respectively, and a basis of $L(mQ)$ is $\{x^iy^j \mid 0 \le i,\ 0 \le j \le a-1,\ ai+bj \le m\}$ for a nonnegative integer m.

In [4] it is not clear whether the affine algebraic set defined by the polynomial (1) is always irreducible.

Historical Note 6. Miura told the author that he learned the proof of the absolute irreducibility of a polynomial of the form (1) from the preprint version of Pellikaan's paper [7].

Historical Note 7. A subclass of C_{ab} curves was treated in [2, pp.1007–1009], and called "type I of plane affine curves."

References

[1] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, second ed., Springer-Verlag, Berlin, 1996.

[2] Gui-Liang Feng and T. R. N. Rao, *A simple approach for construction of algebraic-geometric codes from affine plane curves*, IEEE Trans. Inform. Theory **40** (1994), no. 4, 1003–1012.

[3] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan, *Order functions and evaluation codes*, Proc. AAECC-12, Lecture Notes in Computer Science, vol. 1255, Springer-Verlag, 1997, pp. 138–150.

[4] Shinji Miura, *Algebraic geometric codes on certain plane curves*, Trans. IEICE **J75-A** (1992), no. 11, 1735–1745 (Japanese).

[5] ______, Ph.D. thesis, Univ. Tokyo, 1997 (Japanese).

[6] ______, *Linear codes on affine algebraic curves*, Trans. IEICE **J81-A** (1998), no. 10, 1398–1421 (Japanese).

[7] Ruud Pellikaan, *On the existence of order functions*, to appear in J. Statistical Planning and Inference (1998).

[8] Keith Saints and Chris Heegard, *Algebraic-geometric codes and multidimensional cyclic codes: A unified theory and algorithms for decoding using Gröbner bases*, IEEE Trans. Inform. Theory **41** (1995), no. 6, 1733–1751.

[9] Henning Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993.

SAKANIWA LAB., DEPT. OF ELECTRICAL AND ELECTRONIC ENGINEERING, TOKYO INSTITUTE OF TECHNOLOGY, 2-12-1 OOKAYAMA, MEGURO-KU, TOKYO, 152-8552 JAPAN

E-mail address: ryutaroh@ss.titech.ac.jp

URL: http://tsk-www.ss.titech.ac.jp/˜ryutaroh/