East-West J. of Mathematics: Vol. 14, No 2(2012) pp. 201-207

ARITHMETIC DYNAMICS AND DYNAMICAL UNITS

Chatchawan Panraksa* and **Lawrence Washington**

*Department of Mathematics Mahidol University
Center of Excellence in Mathematics, Bangkok 10400, Thailand
e-mail: sccpr@mahidol.ac.th

†Department of Mathematics, University of Maryland-College Park
Mathematics Building, University of Maryland, College Park, MD 20742-4015, USA
e-mail:lcw@math.umd.edu

Abstract

For a point of order two and a point of order three for a rational function defined over a number field with good reduction outside a set S, it is known that the bilinear form $B([x_1, y_1], [x_2, y_2]) = x_1y_2 - x_2y_1$ yields a unit in the ring of S-integers of a number field. We prove that this is essentially the only bilinear form with this property.

1 Introduction

Fix the n^{th} root of unity $\mu = e^{2\pi i/n}$. The cyclotomic units can be constructed using $1 - \mu^j$ for $1 \leq j \leq n-1$. Let K be a field. One of our goals is to study this theory for the periodic points of a rational function $\phi \in K(z)$, or equivalently of a rational map $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$. In other words, we will study units in the fields generated by the periodic points of ϕ . By analogy with the cyclotomic theory and in recognition of the dynamical study of periodic points of rational maps, we will call the units constructed by periodic points *dynamical units*. Some of these were originally constructed by Narkiewicz [1], then was reformulated and generalized by Morton and Silverman [2].

Key words: good reduction, periodic points, S-integers, dynamical units
2010 AMS Subject Classification: 37C25

2 Background

We study dynamics of rational maps ϕ over fields K with valuations that have "good reduction." This means that the reduction of ϕ modulo the maximal ideal of the ring of integers of K is a "well-behaved" rational map $\widetilde{\phi}$ over the residue field k of K. Thus, studying the dynamics of $\widetilde{\phi}$ over k allows us to derive information about the dynamics of ϕ over K. We set the following notation:
K a field with normalized discrete valuation $v : K^* \to \mathbb{Z}$
$|\cdot| = c^{-v(x)}$ for some $c > 1$, an absolute value associated to v.
$R = \{\alpha \in K : v(\alpha) \geq 0\}$, the ring of integers of K.
$\mathfrak{p} = \{\alpha \in K : v(\alpha) \geq 1\}$, the maximal ideal of R.
$R^* = \{\alpha \in K : v(\alpha) = 0\}$, the group of units of R.
$k = R/\mathfrak{p}$, the residue field of R.
$\sim$ reduction modulo $\mathfrak{p}$, i.e., $R \to k, a \mapsto \widetilde{a}$.

The following theorem will provide the notion of "good reduction", see [3].

Definition 1. *Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map and write*

$$\phi = [F(X,Y), G(X,Y)]$$

with homogeneous polynomials $F, G \in K[X,Y]$ and $gcd(F,G) = 1$. We say that the pair (F,G) is ***normalized****, or has been written in* ***normalized form****, if $F, G \in R[X,Y]$ and at least one coefficient of F or G is in R^*.*

Equivalently, $\phi = [F,G]$ is normalized if

$$F(X,Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_{d-1}XY^{d-1} + a_dY^d$$

and

$$G(X,Y) = b_0X^d + b_1X^{d-1}Y + \cdots + b_{d-1}XY^{d-1} + b_dY^d$$

satisfy

$$\min\{v(a_0), v(a_1), \ldots, v(a_d), v(b_0), v(b_1), \ldots, v(b_d)\} = 0.$$

Definition 2. *Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map defined over a field K with nonarchimedean absolute value $|\cdot|_v$. Write $\phi = [F,G]$ using a pair of normalized homogeneous polynomials $F, G \in R[X,Y]$. The resultant of ϕ is the quantity $Res(\phi) = Res(F,G)$.*

Theorem 1. *[3] Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map defined over K and write $\phi = [F,G]$ in normalized form. The following are equivalent:*

(a) *$deg(\phi) = deg(\widetilde{\phi})$.*

(b) *The equation $\widetilde{F}(X,Y) = \widetilde{G}(X,Y) = 0$ has no solution $[\alpha,\beta] \in \mathbb{P}^1(\overline{k})$.*

(c) $Res(\phi) \in R^*$.

(d) $Res(F, G) \neq 0$.

Definition 3. *A rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ defined over K is said to have **good reduction (modulo v)** if it satisfies any one (hence all) of the conditions of Theorem 1.*

Since, in general, periodic points might not lie in the base field, one sometimes need to study the points in the extension of the base field. The following theorem enables one to study the extensions of a field with valuation.

Theorem 2. *[4] Let K be a subfield of a field L. Then a valuation on K has an extension to a valuation on L.*

3 Periodic Points and Dynamical Units

Recall that the chordal metric on $\mathbb{P}^1(\mathbb{C})$, which we now denote by ρ_∞, is defined by the formula

$$\rho_\infty(P_1, P_2) = \frac{|X_1Y_2 - X_2Y_1|}{\sqrt{|X_1|^2 + |Y_1|^2}\sqrt{|X_2|^2 + |Y_2|^2}}$$

for points $P_1 = [X_1, Y_1]$ and $P_2 = [X_2, Y_2]$ in $\mathbb{P}^1(\mathbb{C})$. In the case of a field K having a nonarchimedean absolute value $|\cdot|_v$, it is convenient to use a metric given by a slightly different formula.

Definition 4. *Let K be a field with a nonarchimedean absolute value $|\cdot|_v$, and let $P_1 = [X_1, Y_1]$ and $P_2 = [X_2, Y_2]$ be points in $\mathbb{P}^1(K)$. The **v-adic chordal metric** on $\mathbb{P}^1(K)$ is*

$$\rho_v(P_1, P_2) = \frac{|X_1Y_2 - X_2Y_1|_v}{\max\{|X_1|_v, |Y_1|_v\} \max\{|X_2|_v, |Y_2|_v\}}.$$

It is clear from the definition that $\rho_v(P_1, P_2)$ is independent of the choice of homogeneous coordinates for P_1 and P_2.

The following proposition will confirm that ρ_v is indeed a metric. In fact, it is an ultrametric, i.e., it satisfies the nonarchimedean triangle inequality.

Proposition 1. *[3]*

(a) $1 \geq \rho_v(P_1, P_2) \geq 0$ *for all* $P_1, P_2 \in \mathbb{P}^1(K)$.

(b) $\rho_v(P_1, P_2) = 0$ *if and only if* $P_1 = P_2$.

(c) $\rho_v(P_1, P_2) = \rho_v(P_2, P_1)$.

(d) $\rho_v(P_1, P_3) \leq \max\{\rho_v(P_1, P_2), \rho_v(P_2, P_3)\}$.

Lemma 1. *[3] Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map that has good reduction. Then the map ϕ is everywhere nonexpanding:*

$$\rho_v(\phi(P_1), \phi(P_2)) \leq \rho_v(P_1, P_2)$$

for all $P_1, P_2 \in \mathbb{P}^1(K)$.

As their name suggests, rational maps with good reduction behave well when they are reduced. For the proof of the following theorem see [3].

Theorem 3. *[3] Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map that has good reduction. Then*

(a) $\widetilde{\phi}(\widetilde{P}) = \widetilde{\phi(P)}$ *for all $P \in \mathbb{P}^1(K)$*

(b) *Let $\psi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be another rational map with good reduction. Then the composition $\phi \circ \psi$ has good reduction, and $\widetilde{\phi \circ \psi} = \widetilde{\phi} \circ \widetilde{\psi}$.*

Proposition 2. *[3] Let $\phi(z) \in K(z)$ be a rational function of degree $d \geq 2$ with good reduction.*

(*a*) *Let $P \in \mathbb{P}^1(K)$ be a point of period n for ϕ. Then $\rho_v(\phi^i P, \phi^j P) = \rho_v(\phi^{i+k} P, \phi^{j+k} P)$ for all $i, j, k \in \mathbb{Z}$, where for $i < 0$ we use the periodicity $\phi^n P = P$ to define $\phi^i P$.*

(*b*) *Let $P \in \mathbb{P}^1(K)$ be a point of exact period n for ϕ. Then $\rho_v(\phi^i P, \phi^j P) = \rho_v(\phi P, P)$ for all $i, j \in \mathbb{Z}$ satisfying $\gcd(i - j, n) = 1$.*

(*c*) *Let $P_1, P_2 \in \mathbb{P}^1(K)$ be periodic points for ϕ of exact period n_1 and n_2, respectively. Assume that $n_1 \nmid n_2$ and $n_2 \nmid n_1$. Then $\rho_v(P_1, P_2) = 1$.*

Theorem 4. *[3, 2] Let $\phi \in K(z)$ be a rational map of degree $d \geq 2$ with good reduction. Let $n_1, n_2 \in \mathbb{Z}$ be integers with $n_1 \nmid n_2$ and $n_2 \nmid n_1$, let $P_1, P_2 \in \mathbb{P}^1(K)$ be periodic points of exact periods n_1 and n_2, respectively, and write $P_i = [x_i, y_i]$ in normalized form. Then $x_1 y_2 - x_2 y_1 \in R^*$.*

Remark: Theorem 4 can be extended to the preperiodic points by the following.

Proposition 3. *Let $\phi(z) \in K(z)$ be a rational function of degree $d \geq 2$ with good reduction. Let $P_1, P_2 \in \mathbb{P}^1(K)$ be preperiodic points for ϕ of exact periods n_1 and n_2, respectively. Assume that $n_1 \nmid n_2$ and $n_2 \nmid n_1$. Then $\rho_v(P_1, P_2) = 1$.*

Proof Since P_1, P_2 are preperiodic points, there is $k \in \mathbb{N}$ such that $\phi^k(P_1)$ and $\phi^k(P_2)$ are periodic points of exact periods n_1 and n_2, respectively. By Proposition 2,
$\rho_v(\phi^k(P_1)_1, \phi^k(P_2)) = 1$. By Proposition 1(a) and Lemma 1, $\rho_v(P_1, P_2) = 1$. □

Theorem 5. *Let $\phi(z) \in K(z)$ be rational function of degree $d \geq 2$ with good reduction. Let $n_1, n_2 \in \mathbb{N}$ with $n_1 \nmid n_2$ and $n_2 \nmid n_1$, let $P_1, P_2 \in \mathbb{P}^1(K)$ be preperiodic points for ϕ of exact periods n_1 and n_2, respectively, and write $P_i = [x_i, y_i]$ in normalized form. Then*

$$x_1y_2 - x_2y_1 \in R^*.$$

Moreover, if ϕ is even, then $x_1y_2 \pm x_2y_1 \in R^*$.

Proof Since P_i are in normalized form, the chordal metric is given by

$$\rho_v(P_1, P_2) = \mid x_1y_2 - x_2y_1 \mid_v .$$

The assumptions on n_1 and n_2 and Proposition 3 imply that $\rho_v(P_1, P_2) = 1$, and hence $x_1y_2 - x_2y_1$ is a unit. Now assume that ϕ is even. Thus, $-x_2$ is also a preperiodic point. Then $x_1y_2 \pm x_2y_1 \in R^*$. □

Morton and Silverman show in [2] that we can use periodic points of rational functions to produce units over fields with valuations. We will consider the converse problems of the results in [2]. To be more precise, we consider the following question:
What are the forms that we can use to produce units from periodic points of rational functions over fields with valuations?
We will prove that, under certain conditions, the form that can be used to generate the units is unique.

Proposition 4. *Let K be a number field and let T be a finite set of places of K that includes the archimedean places. Let $\widetilde{T}$ be the set of places of $\overline{\mathbb{Q}}$ lying over the places of T. Let $a, b \in K$. Suppose p is a prime number and ζ_p is a primitive pth root of unity such that*

$$a^{p^m}\zeta_p + b^{p^m}$$

is a $\widetilde{T}$-unit of $K(\zeta_p)$ for infinitely many positive integers m. Then each of a, b is a T-unit or 0. If $ab \neq 0$ then a/b is a root of unity.

Proof For each m as in the statement, write

$$u_m^{-1}a^{p^m}\zeta_p + u_m^{-1}b^{p^m} = 1,$$

where u_m is a T-unit. Let S be the set of primes occuring in the factorizations of a and b plus the places in T. The S-unit theorem (applied to $K(\zeta_p)$) says that $u+v=1$ has only finitely many solutions in S-units u and v (see [5, 6]). Therefore, there are indices $m_1 \neq m_2$ such that

$$u_{m_1}^{-1} a^{p^{m_1}} = u_{m_2}^{-1} a^{p^{m_2}}.$$

This implies that a power of a is a T-unit, hence a is a T-unit. Similarly, b is a T-unit.
Let T' be the set of places of $K(\zeta_p)$ above T. The group of T'-units of $K(\zeta_p)$ is finitely generated, so there are finitely many cosets mod p-th powers. Write each u_m in the form wv_m^p with w from a finite set of representatives mod pth powers. Some w, call it w_0, occurs for infinitely many m. Therefore, for these m,

$$w_0^{-1}(a^{p^{m-1}} v_m^{-1})^p \zeta_p + w_0^{-1}(b^{p^{m-1}} v_m^{-1})^p = 1.$$

The S-unit theorem implies that there are indices m' and m'' such that

$$a^{p^{m'-1}} v_{m'}^{-1} = a^{p^{m''-1}} v_{m''}^{-1}$$

and

$$b^{p^{m'-1}} v_{m'}^{-1} = b^{p^{m''-1}} v_{m''}^{-1}.$$

The ratio of these two relations (if $ab \neq 0$) yields

$$(a/b)^{p^{m'-1} - p^{m''-1}} = 1.$$

Therefore, if $ab \neq 0$ then a/b is a root of unity. □

We can now prove a converse to Theorem 4.

Theorem 6. *Let K be number field and let T be finite set of places of K that includes the archimedean places. Let $\widetilde{T}$ be a set of places of $\overline{\mathbb{Q}}$ lying above the places in T. Suppose $a, b, c, d \in K$ are such that*

$$B([x_1, y_1], [x_2, y_2]) = ax_1x_2 + bx_1y_2 + cx_2y_1 + dx_2y_2$$

is a $\widetilde{T}$-unit whenever ϕ is a rational function of degree at least 2 defined over K with everywhere good reduction, $[x_1, y_1] \in \mathbb{P}^1(\overline{\mathbb{Q}})$ is a normalized point of order 2 and $[x_2, y_2] \in \mathbb{P}^1(\overline{\mathbb{Q}})$ is a normalized point of order 3 for ϕ. Then $a = 0 = d$ and $b = -c$. Moreover, b and c are T-units.

Proof Let $p \equiv 1 \pmod 3$ be prime. Let $m \geq 1$ and let n have order 6 in $(\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$. Let k be an integer and let $\phi(x) = k + (x-k)^{-n}$. Then $[x_1, y_1] = [k, 1]$ and $[1, 0]$ have order 2 for ϕ and $[k+\zeta, 1]$ has order 3, where ζ

is any primitive p^{m+1}st root of unity.
We have that

$$B([1,0],[k+\zeta,1]) = a\zeta + (ak+b)$$

is a $\widetilde{T}$-unit in $K(\zeta)$ for each primitive p^{m+1}-th root of unity ζ. Fix one such ζ. The product

$$u_m = \prod_{j=1}^{p^m} (a\zeta^{1+jp} + (ak+b)) = a^{p^m}\zeta_p + (ak+b)^{p^m}$$

is a $\widetilde{T}$-unit (where $\zeta_p = \zeta^{p^m}$). If $a \neq 0$ then $ak+b \neq 0$ for sufficiently large k. The proposition implies that $(ak+b)/a$ is a root of unity for large k. Absolute values show that this is impossible. Therefore $a = 0$. Therefore, b is a T-unit. Now conjugate ϕ by $(1/x)$ to obtain

$$\psi(x) = \frac{(1-kx)^n}{k(1-kx)^n + x^n}.$$

Then $[x_1, y_1] = [1, k]$ and $[0, 1]$ have order 2 for ψ and $[1, k+\zeta]$ has order 3, where ζ is any primitive p^{m+1}st root of unity. We find that $d = 0$ and c is a T-unit.
Now compute

$$B([k,1],[k+\zeta,1]) = (b+c)k + c\zeta.$$

If $b + c \neq 0$, we find that $(b+c)k/c$ is a root of unity for all $k > 0$. This is impossible. Therefore, $b = -c$. □

References

[1] W. Narkiewicz. Polynomial cycles in algebraic number fields. *Colloq. Math.* **58**(1), 151-155, 1989.

[2] P. Morton and J. H. Silverman. Periodic points, multiplicity and dynamical units. *J. Reine Angew. Math.* **461**, 81-122, 1995.

[3] J. H. Silverman. *The Arithmetic of Dynamical Systems.* Springer, 2007.

[4] S. Lang. *Algebra, Third Edition.* Springer, 2002.

[5] K. Mahler. On algebraic relations between two units of an algebraic field, Algèbre et Théorie des Nombres. *Colloques Internationaux du Centre National de la Recherche Scientifique.* **24**, 47-55, 1950.

[6] C. L. Siegel. Approximation algebraischer Zahlen. *Math. Z.* **10**, 173-213, 1921.