Memoirs of the Faculty of Education and Human Studies
Akita University (Natural Science)
66, 13 - 17 (2011)

On Quintic Equations

Hideji ITO

We consider the quintic equation of the form $z^5 - az + 1 = 0$ $(a \in \mathbf{C})$. When $|a|$ becomes large, we show that its roots ω_k $(1 \leq k \leq 5)$ approach to $\{0, \pm a^{1/4}, \pm i\, a^{1/4}\}$ ($i = \sqrt{-1}$, $a^{1/4}$ = a 4-th root of a). As an application, we show that when $|a| \to \infty$ galois resolvents $\sum_{i=1}^{5} \xi_k \omega_k$ (the ξ_k are distinct 5-th roots of 1) will make five circles centered at the origin on the complex plane. Similar consideration can be applied to higher equations of type $z^m - az + 1 = 0$, though the distribution of galois resolvents is too complicated to describe.

Key Words: quintic equation, Bring-Jerrard normal form, approximation, galois resolvent

1 Approximate zeros

In this paper, we deal mostly with quintic equations. The reason is that for $m \geq 6$ the equations of type $z^m - az + 1 = 0$ seem to have no special bearing among general m-th degree equations, whereas any quintic equations can be transformed into $z^5 - az + 1 = 0$ as is explained in the following.

Let F be a field in characteristic 0. As is well known, by a Tschirnhaus tranformation, quintic polynomials $f(x) \in F[x]$ can be brought into Bring-Jerrard form $x^5 + Ax + B \cdots$ (1). Here the coefficients A and B are not necessarily contained in F but in some algebraic extension over F of degree 6 (see for example [7]). By further changes of variables, we get them in the forms such as $x^5 + \alpha x + \alpha \cdots$ (2) ([3]) or $x^5 - ax + 1 \cdots$ (3). ((1) $\Rightarrow$ (2) by $x \to (A^5/B^4)x$ and $\alpha = A^5/B^4$; (2) $\Rightarrow$ (3) by $x \to x/\alpha$ and $a = -\alpha^{1/5}$).

As for the approximation of the zeros of a polynomial, there are a lot of results. We quote a recent one given by Neumaier [4]. He gives a Gerschgorin type estimate without relying Gerschgorin's theorem. To state it, we need several notations as in [4]. Let $f(z)$ be a polynomial of degree n with unknown zeros $\zeta_1, \ldots, \zeta_n$:

$$f(z) = a_0 \prod_{k=1}^{n} (z - \zeta_k) \quad (a_0 \neq 0 \in \mathbf{C}).$$

Let $z_1, \ldots, z_n$ be known approximations to the zeros (with unknown accuracy). Put

$$g(z) = \prod_{k=1}^{n} (z - z_k)$$
$$p_k = f(z_k) / \prod_{\ell \neq k} (z_k - z_\ell).$$

Also put

$$D[z; r] = \{w \in \mathbf{C} \mid |w - z| \leq r\}.$$

This is the closed disk with midpoint z and radius r. Then Neumaier's theorem is as follows ([4] Theorem 3.2).

All the zeros of $f(z)$ belong to the union of the disks

$$D[z_j - np_j/2a_0; |np_j/2a_0|].$$

Moreover, every connected component of S consisting of m of these disks contains exactly m zeros of $f(z)$, if these are counted with their algebraic multiplicity.

Now applying this to the case $f(z) = z^5 - az + 1$ $(a \in \mathbf{C})$ and $g(z) = z(z^4 - a)$ (so $z_1 = 0$, $z_k (2 \leq k \leq 5) = \pm a^{1/4}, \pm i a^{1/4}$), we get the following theorem.

Theorem 1 *The roots of $z^5 - az + 1 = 0$ belong to the union of five disks*:

$$D[5/(2a); |5/(2a)|]\ ,\ D[z_k - 5/(8a); |5/(8a)|] \quad (2 \leq k \leq 5).$$

These five disks are disjoint for $|a| > (25/4)^{4/5}$.

Proof. In our case $n = 5$ and $a_0 = 1$. Since

$$\prod_{\ell \neq k} (z_k - z_\ell) = g'(z_k) = 5z_k^4 - a,$$

we readily see that $p_1 = -1/a$ and $p_k = 1/4a$ $(2 \leq k \leq 5)$.

As for the disjointness, it's enough to find out the condition between $D[5/2a; |5/2a|]$ and $D[z_2 - 5/8a; |5/8a|]$ (Note that $|z_2| = |a|^{1/4}$). Since a is a complex number, all you can say is that $D[5/2a; |5/2a|]$ is contained in $D[0; |5/a|]$, and $D[z_2 - 5/8a; |5/8a|]$ is contained in $D[z_2; |5/4a|]$. If those two circles are disjoint, we must have the inequality

$$5/|a| < |a|^{1/4} - 5/4|a|.$$

This gives us the desired condition of a.

Theorem 1 says when $|a| \to \infty$ the roots of $z^5 - az + 1 = 0$ approach to the zeros of $z^5 - az = 0$. Of course, they never coincide. The estimate of their difference is given in the following way. Put D_k $(1 \leq k \leq 5)$ be the five disks given in theorem 1 (in that order).

Theorem 2 *Suppose a root ω of $z^5 - az + 1 = 0$ is contained in a disk D_k of theorem 1. Then we have the following inequalities*:

$$|\omega - z_k| \geq 1/C(a, k)$$

Here the constant $C(a, k)$ are given as follows,

$$C(a, 1) = (|a|^{1/4} + 5/|a|)^4,$$

$$C(a, k) = (|a|^{1/4} + 5/(4|a|))(\sqrt{2}|a|^{1/4} + 5/(4|a|))^2 \times (2|a|^{1/4} + 5/(4|a|)) \quad (2 \leq k \leq 5)).$$

Proof. Suppose $z^4 = a$, i.e., z is one of the roots $\pm a^{1/4}$, $\pm i a^{1/4}$. Then we have $1 = |\omega^5 - a\omega| = |\omega||\omega^4 - z^4| = |\omega||\omega + z||\omega - z||\omega + iz||\omega - iz|$. Hence

$$|\omega - 0| = |\omega| = 1/|\omega + z||\omega - z||\omega + iz||\omega - iz|.$$

If ω is located near 0 as in the estimate of theorem 1, that is, $|\omega - 5/2a| < |5/2a|$, then at any rate ω is contained in the circle $D[0; 5/|a|]$. Hence the distance between ω and z_k $(2 \leq k \leq 5)$ is at most $|a|^{1/4} + 5/|a|$. This gives our estimate of $C(a, 1)$. By similar reasoning we get the result of $C(a, k)$ $(2 \leq k \leq 5))$.

Examples. Let $S(a)$ be the roots of $z^5 - az + 1 = 0$ and ω_k be the root located near z_k $(1 \leq k \leq 5)$. Put $T(a) = \{0, \pm a^{1/4}, \pm i a^{1/4}\}$, $D_1(a) = \{|\omega_1 - 5/2a|, |\omega_2 - 5/8a|, \ldots\}$, $D_2(a) = \{|\omega_k - z_k|\}$ $(1 \leq k \leq 5)$. Also put $E_1(a) = \{|5/2a|, |5/8a|\}$ and $E_2(a) = \{1/C(a, 1), 1/C(a, k)\}$ $(k \neq 1)$. All the values given below are approximate numbers (not rounding, but simply cutting off the rest) except $E_1(4)$ and $E_1(100)$.

(i) $a = 4$

$S(4) = \{0.250245, -1.470818, 1.343246, -0.061336 - 1.420873i, -0.061336 + 1.420873i\}$

$T(4) = \{0, -1.414213, 1.414213, -1.414213i, 1.414213i\}$

$D_1(4) = \{0.374754, 0.099645, 0.095146, 0.095146, 0.085282\}$

$D_2(4) = \{0.250245, 0.056604, 0.070967, 0.061697, 0.061697\}$

$E_1(4) = \{0.625, 0.15625\}$

$E_2(4) = \{0.019848, 0.034479\}$

(ii) $a = 100$

$S(100) = \{0.010000, -3.164772, 3.159772, -0.002499 - 3.162282i, -0.002499 + 3.162282i\}$

$T(100) = \{0, -3.162277, 3.162277, -3.162277i, 3.162277i\}$

$D_1(100) = \{0.014999, 0.0100049, 0.0099950, 0.010000016, 0.010000016\}$

$D_2(100) = \{0.010000, 0.0024950, 0.0025049, 0.00249998, 0.00249998\}$

$E_1(4) = \{0.025, 0.00625\}$

$E_2(4) = \{0.0093917, 0.00244323\}$

Remark 1 By a result of Petkovic et al [6], we have *if* $\max_{1 \leq k \leq 5} |p_k| \leq \frac{1}{5 \cdot 5} \min_{1 \leq j < k \leq 5} |z_k - z_j|$ $(\natural)$, *then the inclusion disks of roots can be chosen as* $D[z_k - p_k; (1/4)|p_k|]$.

The condition $(\natural)$ in our case means $1/|a| \leq \frac{1}{25}|a|^{1/4}$. Hence we have the following assertion;

if $|a| \geq 5^{8/5} (= 13.13\ldots)$, *then the roots* ω_k *are contained in* $D[z_k - p_k; (1/4)|p_k|]$.

This especially implies $|\omega_k - z_k| > (3/4)|p_k|$. So we get a better estimate of the difference between the roots of $z^5 - az + 1 = 0$ and those of $z^5 - az = 0$.

But we prefer Neumaier's simple method and a direct approach as in Theorem 2, because the method of Petkovic et al is rather too sophisticated.

Remark 2 We observe that when $|\alpha| \to \infty$ the roots of $z^5 + \alpha z + \alpha = 0$ approach to $\{-1, (-\alpha)^{1/4} + 1/4\}$ (note that there are four values of $(-\alpha)^{1/4}$) . Putting $g(z) = (z + 1)(z^4 + \alpha)$ and argue as before, we can prove that one root of $z^5 + \alpha z + \alpha = 0$ must approach to -1. But for other values we cannot prove the validity yet.

One might wonder why the change of variables and coefficients from $z^5 - az + 1$ to $z^5 + \alpha z + \alpha$ does not directly give approximate roots of corresponding equation. The reason is that we are dealing with intervals, not with the exact values of roots.

2 Distribution of resolvents

In this section we consider the distribution of values of galois resolvents $\Sigma_{k=1}^{5} \xi_k \omega_k$. Here the ω_k are the roots of $z^5 - az + 1 = 0$ and the ξ_k are the distinct 5-th roots of 1. Our interest lies in the behavior under $|a| \to \infty$. A typical example is shown in the following figure 1 ($a = 100$).

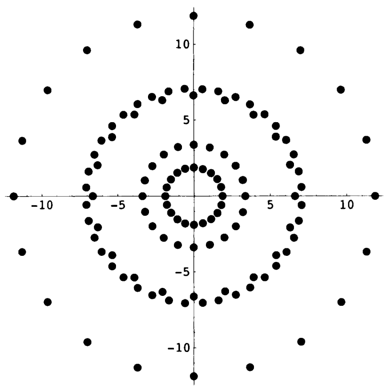

Figure 1: *Distribution of the values of galois resolvents of* $z^5 - 100z + 1 = 0$

Since the roots $\{\omega_k\}$ approach to $\{0, \pm a^{1/4}, \pm i\, a^{1/4}\}$ as $|a| \to \infty$, what we actually deal with is

$$a^{1/4}\Sigma\xi_k\eta$$

where η runs through $\{0, \pm 1, \pm i\}$. In other words (discarding $a^{1/4}$), we must consider the sum of the form

$$\xi_1 \cdot 0 + \xi_2 \cdot i + \xi_3 \cdot i^2 + \xi_4 \cdot i^3 + \xi_5 \cdot i^4.$$

We shall call the sum of above type a cyclotomic resolvent (of type (5,4)) in this paper. Let $\xi = e^{2\pi i/5}$, a primitive 5-th root of unity. For convienience, we consider S_5 (the symmetric group of degree 5) acting on the set $\{0,1,2,3,4\}$. For $\sigma \in S_5$, we set

$$S(\sigma) = \xi^{\sigma(0)} \cdot 0 + \xi^{\sigma(1)} \cdot i + \xi^{\sigma(2)} \cdot i^2 + \xi^{\sigma(3)} \cdot i^3 + \xi^{\sigma(4)} \cdot i^4.$$

Put $\gamma = i\xi$. Then γ is a primitive 20-th root of unity and any $\xi^k i^j$ can be expressed as a power of γ (for example, $\xi = \gamma^{16}$, $i = \gamma^5$). So the sum in a cyclotomic resolvent is a sum of 4 distinct powers of γ. But their powers cannot be arbitrary.

Lemma 1 *If $S(\sigma)$ is a cyclotomic resolvent, then $\gamma^m S(\sigma)$ is also a cyclotomic resolvent for all m ($1 \le m \le 20$).*

Proof. Without loss of generality, we can assume $m = 1$. Then $\gamma S(\sigma) = (\xi i)(S(\sigma)) = \xi^{\sigma(0)+1} \cdot 0 + \xi^{\sigma(4)+1} \cdot i + \xi^{\sigma(1)+1} \cdot i^2 + \xi^{\sigma(2)+1} \cdot i^3 + \xi^{\sigma(3)+1} \cdot i^4$. Since $\{\sigma(k) | 0 \le k \le 4\} = \{0,1,2,3,4\}$, we clearly have $\{\sigma(k) + 1 \bmod 5 | 0 \le k \le 4\} = \{0,1,2,3,4\}$.

The number of cyclotomic resolvents of type (5,4) is $|S_5| = 5! = 120$. Introduce an equivalence relation among them: $S(\sigma) \sim S(\tau)$ iff $S(\sigma) = \gamma^m S(\tau)$ for some $1 \le m \le 20$. By the above lemma, they are divided into 6 classes. Since each member of the same class has the same absolute value, they will make 6 circles centered at the origin on the complex plane. But as the next theorem shows, the two of them have the same radius.

Theorem 3 *On the complex plane, the distribution of galois resolvents of $z^5 - az + 1 = 0$ approaches 5 circles centered at the origin of radius $|a|^{1/4} \cdot r_k (1 \le k \le 5)$, where $r_1 = 0.595112$, $r_2 = 1.0674$, $r_3 = 2.09488$, $r_4 = 2.23607$, $r_5 = 3.75739$.*

Proof. We consider a special type of cyclotomic resolvent. Let $\varepsilon \in S_5$ with the property $\varepsilon(0) = 0$, $\varepsilon(4) = 1$. Then we put

$$S_\varepsilon = \xi^0 \cdot 0 + \xi^1 \cdot i^4 + \xi^{\varepsilon(1)} \cdot i^1 + \xi^{\varepsilon(2)} \cdot i^2 + \xi^{\varepsilon(3)} \cdot i^3.$$

There are 6 of them. To be explicit,

$$s_1 = \xi - \xi^2 + \xi^3 i - \xi^4 i = \xi(1-\xi)(1+i\xi^2)$$
$$s_2 = \xi - \xi^2 + \xi^4 i - \xi^3 i = \xi(1-\xi)(1-i\xi^2)$$
$$s_3 = \xi - \xi^4 + \xi^3 i - \xi^2 i = -\xi^2(1-\xi)(\xi^2+\xi^3+i)$$
$$s_4 = \xi - \xi^3 + \xi^2 i - \xi^4 i = \xi(1-\xi^2)(1+i\xi)$$
$$s_5 = \xi - \xi^4 + \xi^2 i - \xi^3 i = -\xi^2(1-\xi)(\xi^2+\xi^3-i)$$
$$s_6 = \xi - \xi^3 + \xi^4 i - \xi^2 i = \xi(1-\xi^2)(1-i\xi)$$

By *Mathematica*, we get their absolute values as $|s_1| = r_2$, $|s_2| = r_3$, $|s_3| = |s_5| = r_4$, $|s_4| = r_1$, $|s_6| = r_5$, r_k being the same as in the statement of theorem 3. Of course, they are only approximate numbers. The exact equality of $|s_3| = |s_5|$ is due to the fact $s_5 = -\overline{s_3}$ (the overline means the complex conjugation), which is easy to verify. Also we have $\overline{s_3} \ne \gamma^m s_3$ for all $1 \le m \le 20$. In fact, rewriting them as a sum of powers of γ, we have $s_3 = \gamma^{16} + \gamma^{14} + \gamma^{13} + \gamma^7$, $\overline{s_3} = \gamma^4 + \gamma^6 + \gamma^7 + \gamma^{13}$. Checking case by case whether $\gamma^m s_3 = \overline{s_3}$ or not, we get the result.

Remark 3 Using trigonometric functions, we can express the $|s_k|$ as follows:

$$|s_1| = 2\sqrt{(1-\cos(2\pi/5))(1-\cos(3\pi/10))}$$
$$|s_2| = 2\sqrt{(1-\cos(2\pi/5))(1-\cos(7\pi/10))}$$
$$|s_3| = |s_5| = \sqrt{2(1-\cos(2\pi/5))(2(1-\cos(3\pi/5))+1)}$$
$$|s_4| = 2\sqrt{(1-\cos(4\pi/5))(1-\cos(\pi/10))}$$
$$|s_6| = 2\sqrt{(1-\cos(4\pi/5))(1-\cos(9\pi/10))}$$

Remark 4 Figure 1 may suggest that the 40 points of absolute value $100^{1/4} r_4$ (coming from s_3, s_5 and their equivalents) are equidistributed, that is, they can be expressed as $\rho^m s_3$ ($\rho = e^{2\pi i/40}$, $1 \le m \le 40$). But that is not the case. (The reason: a sum of powers of γ is a sum of even powers of ρ. So, they cannot be connected by a multiplication by any odd power of ρ.)

A numerical calculation shows that their difference is very slight, less than 0.5 degree.

Remark 5 Just for record, in figure 2 we show the distribution of cyclotomic resolvents of type (6,5). They are of the form

$$\kappa^{\sigma(0)} \cdot 0 + \Sigma_{j=1}^{5} \kappa^{\sigma(j)} \cdot \xi^j$$

where $\sigma \in S_6$ (acting on $\{0,1,2,3,4,5\}$) and $\kappa = e^{2\pi i/6}$, $\xi = e^{2\pi i/5}$. This correponds to the distribution of the values of galois resolvents of $z^6 - nx + 1 = 0$ $(n \to \infty)$.

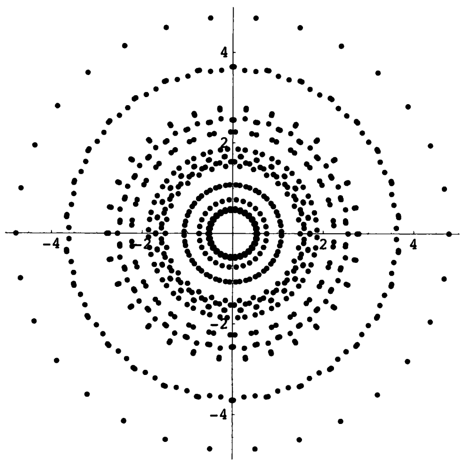

Figure 2: *Distribution of the cyclotomic resolvents of type* (6,5)

3 Algebraic properties

In this section, we assume $a = n \in \mathbf{Z}$. Let K_n be the splitting field (over $\mathbf{Q}$) of the equation

$$f_n(X) = X^5 - nX + 1 = 0.$$

Lemma 2 *Except for* $n = -1,\ 0,\ 2$, *the polynomial* $f_n(X)$ *is irreducible over* $\mathbf{Q}$.

Proof. If $f_n(X)$ has a factor of degree 1, then we clearly have $n = 0$ or 2. If $f_n(X)$ has a factor of degree 2, then writing possible factorization as $X^5 - nX + 1 = (X^2 + aX \pm 1)(X^3 + bX^2 + cX \pm 1)$ $(a, b, c \in \mathbf{Z})$, you can readily deduce $n = -1 : X^5 + X + 1 = (X^2 + X + 1)(X^3 - X^2 + 1)$.

Next we investigate the galois group $\mathrm{Gal}(K_n/\mathbf{Q})$. By Cox [2] p.383, the discriminant $\Delta(f_n)$ of f_n is

$$\Delta(f_n) = 5^5 - 2^8 n^5.$$

There are many criteria to decide the galois group of an irreducible trinomial, but in our present case, $\Delta(f_n)$ is not necessarily squarefree (for example $\Delta(f_{11}) = -3^2 \cdot 1409 \cdot 3251$) or the cases $5|n$ do occur and we assume the constant term of f_n is 1 from the start. Thus the general criteria, such as, Osada [5] (Theorem 1 or Theorem 6) or S.D.Cohen [1] (which requires some prime divides the constant term) cannot deal with all our cases of n. So we reason rather ad hoc way.

Theorem 4 *The galois group* $\mathrm{Gal}(K_n/\mathbf{Q})$ *is* S_5, *except for* $n = -1,\ 0,\ 2$.

Proof. Put $G = \mathrm{Gal}(K_n/\mathbf{Q})$. By lemma 2, $f_n(X)$ is irreducible. So we have only to deal with 5 possible galois groups (Cox [2] p.368). If $\Delta(f_n) = m^2$ $(m \in \mathbf{Z})$, then $5^5 \equiv m^2 \pmod 8$. But this is impossible because 5 is not a square residue modulo 8. Hence we have $G \not\subset A_5$.

As the case $5 \not| n$ is dealt with by Osada [5] Theorem 1, we hereafter assume $5|n$.

Suppose G is solvable. Then by Runge's theorem (Cox [2] theorem 13.2.12), we can write

$$-n^5 = 5^5\lambda/((\lambda - 1)^4(\lambda^2 - 6\lambda + 25))$$

for some $\lambda \in \mathbf{Q}$. Put $\lambda = t/s$, t, $s \in \mathbf{Z}$, $(t, s) = 1$. Then we have

$$-(n/5)^5 = ts^5/((t - s)^4(t^2 - 6ts + 25s^2)).$$

Since $t^2 - 6ts + 25s^2 = (t - 3s)^2 + 16s^2 > 16$ and $(t, s) = 1$, the fraction in the right hand side cannot be contained in $\mathbf{Z}$. This contradicts our assumption $5|n$. Thus G is not solvable. So we must have $G = S_5$.

Lemma 3 *Let* ξ *be the primitive 5-th root of 1 as before. If* $5 \not| n$ *or* $n > 0$, *then we have* $K_n(\xi) \cap \mathbf{Q}(\xi) = \mathbf{Q}$.

Proof. The fields K_n and $\mathbf{Q}(\xi)$ have unique subfield of degree 2, i.e., $\mathbf{Q}(\sqrt{5^5 - 2^8 n^5})$ and $\mathbf{Q}(\sqrt{5})$ respectively. So if $K_n(\xi) \cap \mathbf{Q}(\xi)$ contains $\mathbf{Q}$ as a strict subfield, then those two subfields must conincide. That is, we must have $5^5 - 2^8 n^5 = 5m^2$ for some $m \in \mathbf{Z}$. From this, we clearly have $5|n$. Writing $n = 5d$, we have $5^4 - 2^8 5^4 d^5 = m^2$. Hence we see $5^2|m$. Putting $m = 5^2\ell$, we have $1 - 2^8 d^5 = \ell^2$. If $d > 0$, i.e., if $n > 0$, this is impossible.

Corollary *Suppose* $n \neq -1, 0, 2$ *and* $5 \not| n$ *or* $n > 0$. *Then* $\mathrm{Gal}(K_n(\xi)/\mathbf{Q}(\xi)) = S_5$.

Remark 6. By machine computation, even when $n < 0$, we have that the equation $1 - 2^8 d^5 = \ell^2$ has no solution in rational integers at least for $d < 10^8$.

For a time above results made me suspect that there might be some relevance between the algebraic properties and the distribution of galois resolvents in section 2. But that is not true in general. In Runge's theorem you can take $\lambda - 1$ as small as possible. Then the coefficient of x (our a in section 1, 2) in tranformed polynomial can be arbitrary large. That is, the structure of the galois group makes no difference (at least in those cases).

References

[1] S.D. Cohen, Galois groups of trinomials, Acta Arith. **54** (1989), 43-49.
[2] D. Cox, Galois Theory, Wily-Interscience (2004).
[3] A. Hausner, The Bring-Jerrard Equation and Weierstrass Elliptic Functions, Amer.Math. Monthly, **69** (1962), 193-196.
[4] A. Neumaier, Enclosing clusters of zeros of polynomials, J. Comp. Applied Math. **156** (2003), 389-401.
[5] H. Osada, The Galois group of the polynomials $x^n + ax^l + b$, J. Number Theory **25** (1987), 230-238.
[6] M. Petkovic, C. Carstensen, M. Trajkovic, Weierstrass formula and zero-finding methods, Numer. Math. **69** (1995), 353-372.
[7] M. Postonikov, Foundations of Galois Theory, (1960). [Japanese translation (1964) 東京図書]

Department of Mathematics
Faculty of Education and Human Studies
Akita University
Akita 010-8502, Japan

E-mail : itoh@math.akita-u.ac.jp