Commun. Korean Math. Soc. **28** (2013), No. 2, pp. 209–224
http://dx.doi.org/10.4134/CKMS.2013.28.2.209

CUBIC FORMULA AND CUBIC CURVES

Sung Sik Woo

Abstract. The problem of finding rational or integral points of an elliptic curve basically boils down to solving a cubic equation. We look closely at the cubic formula of Cardano to find a criterion for a cubic polynomial to have a rational or integral roots. Also we show that existence of a rational root of a cubic polynomial implies existence of a solution for certain Diophantine equation. As an application we find some integral solutions of some special type for $y^2 = x^3 + b$.

1. Introduction

We can find a rational solution of an elliptic curve is basically the same as solving a cubic equation. In fact, to find the rational solution of rational cubic equation

$$y^2 = a_3x^3 + a_2x^2 + a_1x + a_0$$

we need to solve the simultaneous equation

$$\begin{cases} y^2 = a_3x^3 + a_2x^2 + a_1x + a_0, \\ y = \alpha x + \beta \end{cases}$$

with $\alpha, \beta \in \mathbb{Q}$ which amounts to solving a cubic equation.

In §2 we recall Cardano's cubic formula which gives the zeros of $f(x) = x^3 + ax + b$. And we show that a cubic f has a rational root if and only if the quantity

$$\omega = \frac{-27}{2}b + \frac{3}{2}\sqrt{-3D},$$

where D is the discriminant of f, is a cube in the splitting field of f. Also we show that existence of rational root of f implies existence of rational solution of a Diophantine equation.

In §3 we consider an integral cubic of the form $f(x) = x^3+ax+b$ and we find criteria for f to have an integral root in terms of ω. When the class number of $\mathbb{Q}(\sqrt{-3D})$ is not divisible by 3 we give a criterion for f to have an integral root in terms of prime factorization of ω in the ring of integers of $\mathbb{Q}(\sqrt{-3D})$.

Received March 10, 2012.
2010 *Mathematics Subject Classification.* 11D25, 14G05, 11G05.
Key words and phrases. cubic equation, rational solution, integral point of an elliptic curve.

In the last section, we consider the zeros of the integral cubic of the form $f(x) = x^3 + ax^2 + b$. We give criteria for f to have an integral root which are similar to those in §3. As an application we find solutions of some special type for $y^2 = x^3 + b$.

2. Cubic equation

The contents of this section are probably well known since ancient times. For completeness we record whatever we need later.

To solve a cubic equation $y = a_3x^3 + a_2x^2 + a_1x + a_0$ we make a change of variable $x \mapsto (X - \frac{a_2}{3a_3})$ to get the equation of the form

$$f(X) = X^3 + aX + b \in \mathbb{Q}[X].$$

Let α, β, γ be the roots of f. The discriminant of f is defined by

$$D = D(f) = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.$$

Also it is well known that the discriminant is given by

$$D = -4a^3 - 27b^2$$

and if $D > 0$, then f has 3 distinct real roots; if $D < 0$, then f has one real and two complex roots (conjugate each other). If $D = 0$, then f has a (real) repeated root and no complex root.

Lemma 2.1. *Let α be a root of $f(X)$ be a monic cubic polynomial and let $f(X) = (X - \alpha)g(X)$ for some quadratic polynomial $g(X)$. Then*

$$D(f) = g(\alpha)^2 D(g).$$

Proof. If β, γ are the roots of g, then $g(X) = (X - \beta)(X - \gamma)$ and $D(g) = (\beta - \gamma)^2$. And $g(\alpha)^2 = (\alpha - \beta)^2(\beta - \gamma)^2$. Hence $D(f) = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = g(\alpha)^2 D(g)$. □

Let

$$\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3},\ \rho^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3} = \bar{\rho}$$

be two primitive cube roots of unity and

$$A = \sqrt[3]{\frac{-27}{2}b + \frac{3}{2}\sqrt{-3D}}, \qquad B = \sqrt[3]{\frac{-27}{2}b - \frac{3}{2}\sqrt{-3D}},$$

where the cube roots are chosen so that $AB = -3p$ (If $b = 0$, then $A = \sqrt{3a}, B = -\sqrt{3a}$). Then the roots of cubic polynomial $f(X)$ is given by the Cardano's formula [8]:

$$\alpha = \frac{1}{3}(A + B), \quad \beta = \frac{1}{3}(\rho^2 A + \rho B), \quad \gamma = \frac{1}{3}(\rho A + \rho^2 B).$$

We will give the conditions for the cubic polynomials $f(X) = X^3 + aX + b \in \mathbb{Q}[X]$ to have rational roots. We start with an obvious fact:

Lemma 2.2. *Let $f(X) = X^3 + pX + q \in \mathbb{Q}[X]$. Then f has a rational root if and only if the splitting field of f is an extension of $\mathbb{Q}$ of degree ≤ 2.*

Proof. The cubic f is reducible if and only if $f(X) = (X - \alpha)g(X)$ in $\mathbb{Q}[X]$ where g is of degree 2. Hence f is reducible if and only if the splitting field of f is the same as the splitting field of g. And obviously this is equivalent to that the splitting field of g is of degree ≤ 2. □

Now we want to determine the quadratic extension in the lemma when the rational cubic $f(X) = X^3 + aX + b$ is reducible in $\mathbb{Q}[X]$ in terms of the splitting field of f.

Proposition 2.3. *Let $f(X) = X^3 + aX + b \in \mathbb{Q}[X]$ with $D = -4a^3 - 27b^2$. Then f has a rational root if and only of the splitting field of f is $\mathbb{Q}(\sqrt{D})$.*

Proof. First suppose $D < 0$ and f is reducible. In this case, since $f(X)$ is reducible in $\mathbb{Q}[X]$ we see that $f(X)$ has one rational root and two complex roots which are conjugate. Let $\alpha \in \mathbb{Q}$ be a rational root of f. Then we can write $f(X) = X^3 + aX + b = (X - \alpha)g(X)$ where $\alpha \in \mathbb{Q}$ and $g(X)$ is a monic quadratic rational polynomial with $D(g) < 0$ by Lemma 2.1. Also note that irreducibility of g implies $b \neq 0$ and hence $\alpha \neq 0$. Let $\alpha, \beta, \gamma = \bar{\beta}$ be the roots of f. Let $\beta = g + \sqrt{h}$, $\gamma = g - \sqrt{h}$ $(g, h \in \mathbb{Q},\ h < 0)$. Then

$$\sqrt{D} = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) = 2\sqrt{h}\left(h - (\alpha - g)^2\right).$$

Since $\alpha + \beta + \gamma = 0$ we have

$$\alpha = -(\beta + \gamma) = -2g$$

which means that the rational root determines the real part of the two complex roots. On the other hand, since $\alpha\beta\gamma = -b$ we have $\alpha(g^2 - h) = -b$. Hence we have

$$h = \frac{\alpha g^2 + b}{\alpha}.$$

Thus

$$\sqrt{D} = 2\sqrt{h}[h - (\alpha - g)^2] = 2\sqrt{h}(h - 9g^2).$$

Now the expression in the square bracket of the last term is a rational number. Hence

$$\sqrt{h} = \frac{\sqrt{D}}{2(h - 9g^2)} = \frac{1}{2}(\beta - \gamma). \tag{1}$$

Hence $\alpha, \beta, \gamma \in \mathbb{Q}(\sqrt{D})$.

Next suppose $D > 0$. Let $f(X) = (X - \alpha)g(X)$ with $\alpha \in \mathbb{Q}$ and $g(X)$ is a monic quadratic rational polynomial with $D(g) > 0$. Let $\alpha, \beta = g + \sqrt{h}, \gamma = g - \sqrt{h}$ $(g, h \in \mathbb{Q}, h > 0)$. Then similar computation yields the equality (1) which also shows that $\alpha, \beta, \gamma \in \mathbb{Q}(\sqrt{D})$.

If $D = 0$ and if $f(X) = X^3 + aX + b \in \mathbb{Q}[X]$ is reducible, then by direct computation, we can easily see that f has three rational roots.

Conversely assume the splitting field of the cubic polynomial $f(X) = X^3 + aX + b \in \mathbb{Q}[X]$ is $\mathbb{Q}(\sqrt{D})$. If D is a square in $\mathbb{Q}$, then the splitting field of f is $\mathbb{Q}$ which says f has three rational roots. Hence f is reducible of course. If D is not a square in $\mathbb{Q}$, then the Galois group of f is cyclic of order 2 whose generator permutes two roots and fixes the other one. Thus f is reducible in this case too. □

We saw that the cubic equation $f(X)$ has a rational root if and only if the splitting field of f is $\mathbb{Q}(\sqrt{D})$. We will show that this is equivalent to that $A, B \in \mathbb{Q}(\sqrt{-3D})$.

Theorem 2.4. *Let $f(X) = X^3 + aX + b$ be a rational cubic polynomial. Let*

$$\omega = \frac{-27}{2}b + \frac{3}{2}\sqrt{-3D}$$

with $D = -4a^3 - 27b^2$. Then f has a rational root if and only if ω is a cube in $\mathbb{Q}(\sqrt{-3D})$, i.e., $A \in \mathbb{Q}(\sqrt{-3D})$.

In this case, if $\alpha \in \mathbb{Q}, \beta, \gamma$ are the roos of f, then $A = x + y\sqrt{-3D}$ is given by

$$x = \frac{-3(\beta+\gamma)}{2}, \quad y = \frac{-1}{2(2\beta+\gamma)(\beta+2\gamma)}. \tag{2}$$

Proof. First consider the case $D = 0$. In this case, it is easy to show that f is reducible in $\mathbb{Q}[X]$ if and only if f has three rational roots. And the latter condition is equivalent to $A = B \in \mathbb{Q}$.

Now consider the case $D \neq 0$. Assume $f \in \mathbb{Q}[X]$ is reducible and let $\alpha, \beta, \gamma \in \mathbb{Q}(\sqrt{D})$ be its roots. First suppose $D < 0$. Then A, B are real numbers. Suppose $\alpha \in \mathbb{Q}$ and β, γ are complex conjugates. And

$$\begin{aligned} 3\beta &= \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)A + \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)B \\ &= -\frac{1}{2}(A+B) + \frac{\sqrt{3}}{2}i(A-B). \end{aligned}$$

On the other hand,

$$3\beta = \frac{3}{2}(\beta+\gamma) + \frac{3}{2}(\beta-\gamma).$$

Hence we have

$$\begin{aligned} A &= -\frac{3}{2}(\beta+\gamma) + \frac{\sqrt{-3}}{2}(\beta-\gamma), \\ B &= -\frac{3}{2}(\beta+\gamma) - \frac{\sqrt{-3}}{2}(\beta-\gamma). \end{aligned} \tag{3}$$

Therefore $A, B \in \mathbb{Q}(\sqrt{-3D})$.

Now suppose $D > 0$ and α, β, γ are three real roots. We see that A, B are complex conjugates say by De Moivre's law. Since f is reducible, we may assume $\alpha \in \mathbb{Q}$. Similar computation yields the same equation (3).

Conversely suppose $A, B \in \mathbb{Q}(\sqrt{-3D})$. And let α, β, γ be three roots of f. Then since $\frac{-27}{2}b + \frac{3}{2}\sqrt{-3D}$ and $\frac{-27}{2}b - \frac{3}{2}\sqrt{-3D}$ are cubes in $\mathbb{Q}(\sqrt{-3D})$ we can write

$$A = \sigma + \tau\sqrt{-3D},\ B = \sigma - \tau\sqrt{-3D} \text{ with } \sigma, \tau \in \mathbb{Q}.$$

Then

$$\alpha = \frac{1}{3}(A + B) = \frac{3}{2}\sigma$$

is a rational root.

If $D < 0$, then

$$\begin{aligned} 3\beta &= \rho A + \rho^2 B \\ &= \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)(\sigma + \tau\sqrt{-3D}) + \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)(\sigma - \tau\sqrt{-3D}) \\ &= -\sigma + 3\tau\sqrt{D}. \end{aligned}$$

Similar computation shows $3\gamma = -\sigma - 3\tau\sqrt{D}$.

If $D > 0$, then

$$3\beta = \rho A + \rho^2 B = -\sigma - 3\tau\sqrt{D}$$

and $3\gamma = -\sigma + 3\tau\sqrt{D}$. Hence in either case, we conclude that $\alpha \in \mathbb{Q}$ and $\beta, \gamma \in \mathbb{Q}(\sqrt{D})$.

Hence we showed that f is reducible if and only if $A, B \in \mathbb{Q}(\sqrt{-3D})$. But the latter condition is equivalent to $A \in \mathbb{Q}(\sqrt{-3D})$.

For the last part, by (1) and (3) using the notation of the proof of the proposition above, we get

$$A = -3g + \frac{\sqrt{-3D}}{2(h - 9g^2)}.$$

Using the identity

$$h = \left(\frac{\beta - \gamma}{2}\right)^2, \quad g = \left(\frac{\beta + \gamma}{2}\right)$$

we obtain our result. □

Corollary 2.5. *Let $f(X) = X^3 + aX + b \in \mathbb{Q}[X]$ and let $\omega = \frac{-27}{2}b + \frac{3}{2}\sqrt{-3D}$. If $b \neq 0$, then $f(X)$ has three rational root if and only if*

(1) $\omega = \frac{-27}{2}b + \frac{3}{2}\sqrt{-3D} = (x + y\sqrt{-3D})^3$ for some $x, y \in \mathbb{Q}$ and

(2) $D = d^2$ for some $d \in \mathbb{Q}$.

If $b = 0$, then f has three rational roots if and only if (2) holds.

Proof. Clear from the proof of theorem. □

In [7] we saw that reducibility of a polynomial is equivalent to existence of a common solution of the Diophantine equations. In case of cubics we have:

Corollary 2.6. *Let* $f(X) = X^3 + aX + b \in \mathbb{Q}[X]$ *with* $D = -4a^3 - 27b^2$. *Assume* $-3D$ *is not a square in* $\mathbb{Q}^*$. *Then* $f = 0$ *has a rational solution if and only if the Diophantine equations*

$$\begin{cases} X^3 - 9DXY^2 = -\dfrac{27}{2}b, \\ X^2Y - DY^3 = \dfrac{1}{2} \end{cases} \tag{4}$$

have a common rational solution.

Proof. Since f is reducible if and only if $\omega = \frac{-27}{2}b + \frac{3}{2}\sqrt{-3D}$ is a cube in $\mathbb{Q}(\sqrt{-3D})$, i.e., $\omega = (x + y\sqrt{-3D})^3$ with $x, y \in \mathbb{Q}$. Now simply observe that

$$\begin{aligned} \frac{-27}{2}b + \frac{3}{2}\sqrt{-3D} &= (x + y\sqrt{-3D})^3 \\ &= x^3 - 9Dxy^2 + \sqrt{-3D}(3x^2y - 3Dy^3). \end{aligned}$$ □

If we take the differences we have:

Corollary 2.7. *Let* $D = -4a^3 - 27b^2$ *with* $a, b \in \mathbb{Q}$ *and* $-3D$ *is not a square in* $\mathbb{Q}^*$. *Then the cubic*

$$X^3 - X^2Y - 9DXY^2 + DY^3 = -\frac{1}{2}(27b + 1)$$

has a rational solution if $\omega = \frac{-27}{2}b + \frac{3}{2}\sqrt{-3D}$ *is a cube in* $\mathbb{Q}(\sqrt{-3D})$. *The solution is given by* (2) *of* Theorem 2.4.

Remark. Let D, b be nonzero rational numbers. Let

$$\begin{cases} F(X,Y,Z) = X^3 - 9DXY^2 + \dfrac{27b}{2}Z^3, \\ G(X,Y,Z) = X^2Y - DY^3 - \dfrac{1}{2}Z^3. \end{cases}$$

Then the cubic curves $F = 0$ and $G = 0$ are nonsingular curves of genus 1 with the obvious rational points $F(0,1,0) = 0, G(1,0,0) = 0$. Also the cubic

$$H(X,Y,Z) = X^3 - X^2Y - 9DXY^2 + DY^3 + \frac{1}{2}(27b + 1)Z^3$$

is nonsingular unless $D = -\frac{1}{27}$.

3. Cubics with integer coefficients

In this section we consider the cubic polynomials $f(X) = X^3 + aX + b$ with integer coefficients and let $D = -4a^3 - 27b^2$ be its discriminant. Let

$$\omega = \frac{-27}{2}b + \frac{3}{2}\sqrt{-3D}.$$

To see whether f has a rational root we need to see if ω is a cube in $\mathbb{Q}(\sqrt{-3D})$. The rational solution must an integer since it satisfies a monic integral polynomial.

For a square free d the ring of integers $A = \mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{d})$ is given by [3]

$$A = \begin{cases} \mathbb{Z} + \mathbb{Z} \cdot \sqrt{d} & d \equiv 2, 3(4), \\ \mathbb{Z} + \mathbb{Z} \cdot \dfrac{-1+\sqrt{d}}{2} & d \equiv 1(4) \end{cases}$$

and for $n \in \mathbb{Z}$ we define, the square free part $d = d(n)$ of n, by $n = b^2 d$ for some $b \in \mathbb{Z}$ and d is a square free integer.

Lemma 3.1. *Let $f(X) = X^3 + aX + b \in \mathbb{Z}[X]$ with the discriminant $D = -4a^3 - 27b^2$. Let d be the square free part of $-3D$ and $K = \mathbb{Q}(\sqrt{d})$ with the ring of integers $\mathcal{O}_K$. Then*
(1) *$\omega \in \mathcal{O}_K$ and*
(2) *$f = 0$ has an integer solution if and only if ω is a cube in $\mathcal{O}_K$.*

Proof. We know $\omega \in O_K$ if and only if the norm and the trace of ω are integers [3]. For $\omega = \frac{-27}{2} b + \frac{3}{2}\sqrt{-3D}$, we have $N(\omega) = \frac{27}{4}(27b^2 - D) = (-3a)^3 \in \mathbb{Z}$ and $\mathrm{tr}(\omega) = -27b \in \mathbb{Z}$. Hence $\omega \in \mathcal{O}_K$.

By Theorem 2.4, f has a rational root if and only if ω is a cube and since f is monic with the integer coefficients the rational root must be an integer. ☐

We want to find the conditions for ω to be a cube in $\omega \in \mathcal{O}_K$. To fix our notation we briefly summarize factorization of prime ideals of a ring of integers of a number field from Chapter 12 of [3]. Let K be a finite Galois extension of $\mathbb{Q}$ of degree n with the group G. Let $A = \mathcal{O}_K$ be the ring of integers. Then any ideal of A can be written uniquely as a product of prime ideals of A. If $\mathfrak{p}$ is a prime ideal of A, then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal say $(p) = \mathfrak{p} \cap \mathbb{Z}$. On the other hand, if $(p) \subseteq \mathbb{Z}$ is a prime ideal, then $(p)A$ is an ideal which has a factorization into prime ideals say $(p)A = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}$ and since $K/\mathbb{Q}$ is Galois, all e_i's are the same and the residue extension degree $f = [A/\mathfrak{p}_i : \mathbb{Z}/(p)]$'s are the same (independs of $\mathfrak{p}_i$). Hence if we let r to be the number of primes lying above (p), then

$$(p)A = (\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r)^e, \quad erf = n.$$

The norm of a prime ideal $\mathfrak{p}$ is defined by $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^f$ where $f = [A/\mathfrak{p} : \mathbb{Z}/p]$. Further,

$$N_{K/\mathbb{Q}}(\mathfrak{p})\mathcal{O}_K = \prod_{\sigma \in G} \sigma\mathfrak{p} = (\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r)^{ef} \text{ and}$$
$$N_{K/\mathbb{Q}}(\mathfrak{b}) = |N_{K/\mathbb{Q}}(b)| \text{ if } \mathfrak{b} = (b) \text{ is a principal fractional ideal.}$$

If $K = \mathbb{Q}(\sqrt{d})$ (d is square free) is a quadratic extension of $\mathbb{Q}$, then $e, r, f \in \{1, 2\}$. Let $\mathcal{O}_K = A$ be the ring of integers. Let $p \in \mathbb{Z}$ be a prime. Then $(p)A$ is a product of prime ideals. Since $2 = erf$ we have the following three cases:

$$pA = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 \text{ where } p \text{ splits if; } & e = f = 1, r = 2, \\ \mathfrak{p}^2 \text{ where } p \text{ ramifies; } & r = f = 1, e = 2, \\ \mathfrak{p} \text{ where } p \text{ remains prime; } & e = r = 1, f = 2. \end{cases}$$

We know that p ramifies if and only if p divides the discriminant of K. The criteria which prime ramifies, splits or remains prime is given in ([3], §13.1). Finitely many primes ramifies and about the half of the rest split and the other half inert.

We will use a generalization of Eisenstein criterion proved in [2].

Theorem 3.2. *Let A be an integral domain with classical ideal theory and let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ be a polynomial in $A[X]$. Let $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be an ideal of A with $r > 0, e_j > 0$, assume that $\mathfrak{a}$ divides each coefficient a_j of $f(X)$ and that $p_i^{e_i}$ exactly divides a_n. Assume finally that the greatest common divisor of $n, e_1, \dots, e_r$ is 1, i.e., $(n, e_1, \dots, e_r) = 1$. Then $f(X)$ is irreducible.*

We need a special case of this:

Corollary 3.3. *Let A be a ring of integers of a number field and $f(X) = X^n - a \in A[X]$. If $(a) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and $(n, e_1, e_2, \dots, e_r) = 1$, then $f(X)$ is irreducible.*

The following result is a slight generalization of [1] (Lemma 5, p. 543).

Lemma 3.4. *Let $f(X) = X^p - a \in K[X]$ for a field K and a prime p. Then f is reducible if and only if f has a root in K, i.e., f is irreducible if and only if f has no root in K.*

Proof. First suppose f is reducible and assume $p \nmid \mathrm{char}(K)$. Let ζ be a primitive p-th root of unity and let α be a root of f. Then the roots of f are $\alpha, \alpha\zeta, \alpha\zeta^2, \dots, \alpha\zeta^{p-1}$. Since f is reducible write $f = gh$. The constant term of g is of the form $d = \alpha^i\zeta^j$. Hence $d^p = \alpha^{ip} = a^i$. Write $1 = ix + py$. Then $a = a^{ix+py} = d^{px}a^{py}$. Hence a is a p-power. Thus f has a root in K.

Now suppose $p = \mathrm{char}(K)$. Then since $f' = 0$ we see $f(X) = h(X^p)$ with $h(t) = t - a$ which is separable. In this case, every root of f has multiplicity p. Hence $f(X) = (X - \alpha)^p$. Since f is reducible, $(X - \alpha)^i$ divides f; $\alpha^i \in K$ for some i. If $ai + bp = 1$ $(a, b \in \mathbb{Z})$, then $\alpha = \alpha^{ai+bp} = (\alpha^i)^a(\alpha^p)^b \in K$. Hence f has a root in K.

The converse is obvious. □

Corollary 3.5. *Let $f(X) = X^p - a \in K[X]$ be reducible. Let ζ be a primitive p-th root of unity. Suppose $f(\alpha) = 0$. If $p \nmid \mathrm{char}(K)$, there is an i such that $\zeta^i\alpha \in K$. If $p = \mathrm{char}(K)$, then $\alpha \in K$ and has multiplicity p.*

Proof. In the proof Lemma 3.4 when $\mathrm{char}(K) \neq p$, the root of f are of the form $\zeta^i\alpha$ and at least one of them belongs to K. The other case is obvious. □

Lemma 3.6. *Let A be a Dedekind domain with a quotient field K. Let $f(X) = X^p - a \in A[X]$ where p is a prime. Then f is reducible in $K[X]$ if and only if f has a root in A.*

Proof. Suppose f is reducible in $K[X]$. By Lemma 3.4 above, f has a root say $\alpha \in K$. Since $\alpha^p - a = 0$ we see α is integral over A. Therefore $\alpha \in A$ since A is integrally closed. □

Lemma 3.7. *Let K be a number field with the ring of integer A and let h_K be the class number of K. Let $a \in A$ and let $(a) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ with $p \mid e_i$. Then either there is a unit u of K such that ua is a p-th power in A; or $p \mid h_K$. Conversely, if $a \in A$ is a p-th power and $(a) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, then $p \mid e_i$.*

Proof. Let $e_i = p\epsilon_i$ and let $\mathfrak{a} = \mathfrak{p}_1^{\epsilon_1} \cdots \mathfrak{p}_r^{\epsilon_r}$. If $\mathfrak{a} \neq (b)$ for any $b \in A$, then $\mathfrak{a}$ is a nontrivial element in the class group of K of order p. Hence $p \mid h_K$. If $\mathfrak{a} = (b)$ for some $b \in A$, then $ua = b^p$ for some unit $u \in A^*$.

For the converse, let $a = b^p$ and $(b) = \mathfrak{p}_1^{\epsilon_1} \cdots \mathfrak{p}_r^{\epsilon_r}$. Then $(a) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} = (b^p) = \mathfrak{p}_1^{p\epsilon_1} \cdots \mathfrak{p}_r^{p\epsilon_r}$. By uniqueness of decomposition of an ideal into prime ideals we see that $e_i = \epsilon_i p$. As required. □

Lemma 3.8. *Let $K/\mathbb{Q}$ be a quadratic extension with the class number h_K and the ring of integers A and $a \in A$. Let $(a) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}$ with $\mathfrak{p}_i \cap \mathbb{Z} = (p_i)$ and let $p_1 \leq p_2 \leq \cdots \leq p_r$. Let p be an odd prime with $p \nmid h_K$. Suppose $N_{K/\mathbb{Q}}(a)$ is a p-th power and*

(†) *whenever $p_i = p_{i+1}$ (i.e., p_i splits) we have $p \mid e_i$ and $p \mid e_{i+1}$.*

Then there is a unit $u \in A^*$ such that ua is a p-th power.

Proof. Let $N_{K/\mathbb{Q}}((a)) = p_1^{e_1 f_1} p_2^{e_2 f_2} \cdots p_r^{e_r f_r}$. If $p_j \neq p_{j+1}$, then $p_j^{e_j f_j} p_{j+1}^{e_{i+1} f_{i+1}}$ is a factor of $N_{K/\mathbb{Q}}((a))$ and since the norm is a p-power and $f_i = 1$ or 2 we see that $p|e_j, e_{j+1}$. If $p_i = p_{i+1}$, then $p_i^{e_i f_i + e_{i+1} f_{i+1}}$ is a factor of $N_{K/\mathbb{Q}}((a))$. In this case we assumed $p \mid e_i$, $p \mid e_{i+1}$. In all cases we have $p \mid e_i$. Hence $(a) = (\mathfrak{p}_1^{\epsilon_1}\mathfrak{p}_2^{\epsilon_2} \cdots \mathfrak{p}_r^{\epsilon_r})^p$. If $\mathfrak{p}_1^{\epsilon_1}\mathfrak{p}_2^{\epsilon_2} \cdots \mathfrak{p}_r^{\epsilon_r}$ is not principal, then the class group contains an element of order p which contradict to the fact that h_K is not divisible by p. Hence $(\mathfrak{p}_1^{\epsilon_1}\mathfrak{p}_2^{\epsilon_2} \cdots \mathfrak{p}_r^{\epsilon_r})$ is principal, say equal to (α) for some $\alpha \in K$. Hence $v\alpha^p = a$ for some unit $v \in A^*$ by Lemma 3.7. Hence $v^{-1}a$ is a p-th power in K^*, say $\alpha^p = v^{-1}a$. That is α is a root of $X^p - v^{-1}a \in A[X]$; α is integral over A. Therefore $\alpha \in A$ and ua is a p-th power in A with $u = v^{-1}$. □

By Lemma 3.1, reducibility of $f(X) = X^3 + aX + b \in \mathbb{Z}[X]$ is equivalent to that $\omega = \frac{-27}{2}b + \frac{3}{2}\sqrt{-3D}$ is a cube in $K = \mathbb{Q}(\sqrt{-3D})$. And by Lemma 3.7, ω being a cube depends on the prime factorization of $\omega = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. If all the exponents e_i's are multiples of 3, then ω is a cube up to a unit of $K = \mathbb{Q}(\sqrt{-3D})$ under the condition $3 \nmid h_K$.

It is well known that $a \in A$ is a unit if and only if $N_{K/\mathbb{Q}}(a) = \pm 1$ and the group of units $U(d)$ of the quadratic field $\mathbb{Q}(\sqrt{d})$ is given by ([3] p. 191).

$$U(d) = \begin{cases} \{\pm 1, \pm i\} \approx \mathbb{Z}/4 & (d = -1) \\ \{\pm 1, \pm\rho, \pm\rho^2 \mid \rho^3 = 1\} \approx \mathbb{Z}/6 & (d = -3) \\ \{\pm 1\} \approx \mathbb{Z}/2 & (d \leq -2, d \neq -3) \\ \{\pm\epsilon^m\} \approx \mathbb{Z} & (d > 0) \end{cases}$$

where ϵ in the last case is the fundamental unit.

Let $f(X) = X^3 + aX + b \in \mathbb{Z}[X]$ with $D = -4a^3 - 27b^2$ and $\omega = \frac{-27}{2}b + \frac{3}{2}\sqrt{-3D}$ as usual. For an integer n we let $\pi(n)$ be the set of (positive) prime factors of n.

Theorem 3.9. *Let $f(X) = X^3 + aX + b$ be an integral cubic polynomial with the discriminant $D = -4a^3 - 27b^2$. Let d be the square free part of $-3D$ and let $K = \mathbb{Q}(\sqrt{d})$ with the class number h_K. Suppose $d < -3$ or $d = -2$.*

If $3 \nmid h_K$ and the primes of $\pi(3a)$ satisfy the condition (†) of Lemma 3.8, then f has an integral solution. Moreover, the solution is given by $\frac{2\sigma}{3}$ where $\sigma + \tau\sqrt{d} \in \mathcal{O}_K$ is a root of $x^3 = \frac{1}{2}(-27b + 3\sqrt{-3D})$.

Proof. Let $\omega = \frac{1}{2}(-27b + 3\sqrt{-3D})$. We know that f has an integral root if and only if ω is a cube in $\mathcal{O}_K$ by Lemma 3.1. Now $N(\omega) = \frac{27}{4}(27b^2 - D) = (-3a)^3 = N(A^3)$. Hence $\omega = uA^3$ with $u = \pm 1$ by the conditions on d; $\omega = A^3$ or $\omega = -A^3$. In either case ω is a cube in $\mathcal{O}_K$. Now by Theorem 2.4, $f = 0$ has a rational root. Since the rational root satisfy a monic integral polynomial it must be an integer. To find the solution we simply note that $A = \sigma + \tau\sqrt{d}$ and $B = \sigma - \tau\sqrt{d}$ and then $\alpha = \frac{1}{3}(A + B)$ is a rational solution.

Since $N(\omega) = (-3a)^3$ the prime factors of $3a$ lies below the prime factors of ω. If they satisfy the condition (†) of Lemma 3.8, then the condition $3 \nmid h_K$ together with the fact that $N(\omega)$ is a cube implies that ω is a cube in O_K. □

Corollary 3.10. *Under the same assumptions on d, h_K and $\pi(3a)$ of Theorem 3.9,*

(i) *when $d \equiv 1 \pmod 4$ there is an $A \in O_K$ with $A^3 = \omega$ if and only if $-12a - |d|$ is a square of an odd integer.*
(ii) *when $d \equiv 2, 3 \pmod 4$ there is an $A \in O_K$ with $A^3 = \omega$ if and only if $X^2 + |d|Y^2 = -3a$ has an integral solution.*

Proof. When $d \equiv 1 \pmod 4$ we have $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \frac{-1+\sqrt{d}}{2}$. Hence any element of $\mathcal{O}_K$ is of the form $A = \frac{(2k+1)+\sqrt{d}}{2}$. Hence $N(A) = \frac{1}{4}(2k+1)^2 + \frac{1}{4}|d| = -3a$ if and only if $(2k+1)^2 = -12a - |d|$. As required.

When $d \equiv 2, 3 \pmod 4$ we have $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Hence any element of $\mathcal{O}_K$ is of the form $A = r + s\sqrt{d}$. Thus $N(A) = r^2 + |d|s^2 = -3a$ if and only if $X^2 + |d|Y^2 = -3a$ has an integral solution. □

Remark. When $d \equiv 1 \pmod 4$ it is not hard to see if $4a^2 - |d|$ is a square of an odd integer. But when $d \equiv 2, 3 \pmod 4$ it is not so easy to decide whether there is an integral solution for $X^2+|d|Y^2 = a^2$. In Chapter 19 of [4] there are many cases when such a Diophantine equation has an integral solution.

Theorem 3.11. *Let $D = -4a^3 - 27b^2$ for some $a, b \in \mathbb{Z}$. Let d be the square free part of $-3D$ and let $K = \mathbb{Q}(\sqrt{d})$ with the class number h_K. Suppose $d < -3$ or $d = -2$.*

(1) *If there is an $A \in \mathcal{O}_K$ with $N(A) = -3a$, then*

$$X^3 - 9DXY^2 - X^2Y + DY^3 = \frac{1}{2}(-27b - 1) \tag{5}$$

has a rational solution. If $\omega = (\sigma+\tau\sqrt{-3D})^3$, then $X = \sigma, Y = \tau$ is a solution.

(2) *If the primes of $\pi(3a)$ satisfy the condition (†) of Lemma 3.8 and $3 \nmid h_K$, then there is such an A.*

Proof. As in the proof of Theorem 3.9, $A = \sigma + \tau\sqrt{-3D} \in \mathcal{O}_K$ such that $A^3 = \omega$ where $\omega = \frac{1}{2}(-27b + 3\sqrt{-3D})$. As before,

$$\begin{aligned}\frac{-27}{2}b - \frac{3}{2}\sqrt{-3D} &= (\sigma + \tau\sqrt{-3D})^3 \\ &= \sigma^3 - 9D\sigma\tau^2 + \sqrt{-3D}(3\sigma^2\tau - 3D\tau^3).\end{aligned}$$

Comparing the first and the last expression we see that there is a common solution for

$$\begin{cases} X^3 - 9DXY^2 = -\dfrac{27}{2}b, \\ 3X^2Y - 3DY^3 = \dfrac{1}{2}. \end{cases}$$

Now take the differences of the equations to get our result.

The last statement is similar to the last statement of Theorem 3.9. □

Corollary 3.12. *Under the same assumptions* (1) *or* (2) *of Theorem 3.11.*

(i) *when $d \equiv 1 \pmod 4$ the equation* (5) *has a rational solution if $-12a-|d|$ is a square of an odd integer.*

(ii) *when $d \equiv 2, 3 \pmod 4$ the equation* (5) *has a rational solution if $X^2 + |d|Y^2 = -3a$ has an integral solution.*

Proof. The proof is the same as Corollary 3.10. □

Mordell ([4], p. 7) gave a family of cubics of similar type without rational solutions.

Theorem 3.13. *The integral equation*

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3 = 1$$

has no rational solutions if

$$a \equiv d \equiv 4 \pmod 9, \quad b \equiv 0 \pmod 3, \quad c \equiv \pm 1 \pmod 3.$$

4. Integral points of some elliptic curves

In this section we consider cubics of the form $f(x) = x^3 + ax^2 + b \in \mathbb{Z}[x]$ with the same method of the previous sections. Using this idea we can consider the integral solution of $y^2 = x^3 + b$ of some special type namely the solution of the simultaneous equation:

$$\begin{cases} y^2 = x^3 + b, \\ y = mx. \end{cases}$$

Let

$$f(x) = x^3 + ax^2 + b. \tag{6}$$

If we make the change of variable $x \mapsto (X - \frac{a}{3})$, then we have

$$Y = X^3 + pX + q \tag{7}$$

with

$$p = \frac{-a^2}{3}, \quad q = \frac{2a^3 + 27b}{27}$$

Any cubic polynomial can bring into the form (6) by a change of coordinate with coefficients in a quadratic extension $\mathbb{Q}$.

The discriminant of (6) is given by $D = -4a^3b - 27b^2$. We let

$$A = \sqrt[3]{\frac{-2a^3 - 27b}{2} + \frac{3}{2}\sqrt{-3D}}, \quad B = \sqrt[3]{\frac{-2a^3 - 27b}{2} - \frac{3}{2}\sqrt{-3D}}$$

the three roots of cubic (6) are then given by

$$\alpha = -\frac{a}{3} + \frac{1}{3}(A + B), \quad \beta = -\frac{a}{3} + \frac{1}{3}(\rho^2 A + \rho B), \quad \gamma = -\frac{a}{3} + \frac{1}{3}(\rho A + \rho^2 B).$$

Now let $x^3 + ax^2 + b \in \mathbb{Z}[x]$ and let

$$\omega = \frac{-2a^3 - 27b}{2} + \frac{3}{2}\sqrt{-3D}.$$

Then since $N(\omega) = \frac{1}{4}[(2a^3 + 27b)^2 + 27D] = a^6 \in \mathbb{Z}$ and $\mathrm{tr}(\omega) = -2a^3 - 27b \in \mathbb{Z}$ we see that $\omega \in O_K$.

Theorem 4.1. *Let $f(x) = x^3 + ax^2 + b \in \mathbb{Z}[x], D = -4a^3b - 27b^2$ and let d be the square free part of $-3D$. Let $K = \mathbb{Q}(\sqrt{d})$ with the class number h_K. Suppose $d < -3$ or $d = -2$.*

(1) *If there is an $A \in \mathcal{O}_K$ with $N(A) = a^2$, then the cubic equation $f = 0$ has an integral solution. If $\omega = (\sigma + \tau\sqrt{d})^3$ with $\sigma + \tau\sqrt{d} \in \mathcal{O}_K$, then the solution is given by $\alpha = \frac{2\sigma - a}{3}$.*

(2) *If $3 \nmid h_K$ and the primes of $\pi(a)$ satisfy the condition (†) of Lemma 3.8 and $3 \nmid h_K$, then there is such an A.*

Proof. The proof of this is similar to Theorem 3.9 with minor change $N(\omega) = a^6$ and we omit it. □

The corresponding statement to Corollary 3.10 is:

Corollary 4.2. *Under the same assumptions of* (1) or (2) *of Theorem 4.1.*

(i) *when* $d \equiv 1 (\bmod 4)$ *there is an* $A \in O_K$ *with* $A^3 = \omega$ *if and only if* $4a^2 - |d|$ *is a square of an odd integer.*
(ii) *when* $d \equiv 2, 3 (\bmod 4)$ *there is an* $A \in O_K$ *with* $A^3 = \omega$ *if and only if* $X^2 + |d|Y^2 = a^2$ *has an integral solution.*

Proof. The proof is similar to Corollary 3.10 with minor change of $N(\omega) = a^6$. □

Theorem 4.3. *Let* $D = -4a^3 - 27b^2$ *for some* $a, b \in \mathbb{Z}$. *Let* d *be the square free part of* $-3D$ *and let* $K = \mathbb{Q}(\sqrt{d})$ *with the class number* h_K. *Suppose* $d < -3$ *or* $d = -2$.

If there is an $A \in \mathcal{O}_K$ *with* $N(A) = a^2$, *then*

$$X^3 - 9DXY^2 - X^2Y + DY^3 = \frac{1}{2}(2a^3 + 27b + 1) \tag{8}$$

has a rational solution. If $\omega = (\sigma + \tau\sqrt{-3D})^3$, *then* $X = \sigma, Y = \tau$ *is a solution.*

If $3 \nmid h_K$ *and the primes of* $\pi(a)$ *satisfy the condition* (†) *of Lemma 3.8, then there is such an* A.

Proof. The proof of this is similar to Theorem 3.11 and we omit it. □

The corresponding statement to Corollary 3.12 is:

Corollary 4.4. *Under the same assumptions* (1) *or* (2) *of Theorem 4.3.*

(i) *when* $d \equiv 1 (\bmod 4)$ *the equation* (8) *has a rational solution if* $4a^2 - |d|$ *is a square of an odd integer.*
(ii) *when* $d \equiv 2, 3 (\bmod 4)$ *the equation* (8) *has a rational solution if* $X^2 + |d|Y^2 = a^2$ *has an integral solution.*

Proof. We omit the proof. □

We apply our idea to get a solution of the equation $y^2 = x^3 + b$ of some special type. Rosen ([3], 17.10.2) gave the necessary sufficient condition for the equation to have an integer solution when $b < -1$ and $3 \nmid h_K$ and gave an explicit solution. We know that there are only finitely many solutions for such equation by Siegel Theorem [5].

Example 4.5. To find a solution of $y^2 = x^3 + b$ we consider some special type namely the solution of y is a integral multiple of a solution of x. For this we solve the simultaneous equation

$$\begin{cases} y^2 = x^3 + b & (b \in \mathbb{Z}) \\ y = mx & (m \in \mathbb{Z}) \end{cases}$$

which boils down to solving the cubic equation

$$x^3 - m^2x^2 + b = 0. \tag{9}$$

The discriminant and ω of the cubic (9) is

$$D = 4m^6 b - 27b^2 \text{ and } \omega = \frac{2m^6 - 27b}{2} + \frac{3}{2}\sqrt{-3D} \in \mathcal{O}_K.$$

The norm of ω is $N(\omega) = m^{12}$. All the information needed in this example is in [3] especially Chapter 13.

Consider

$$y^2 = x^3 + 9. \tag{10}$$

To find the common solution (10) and $y = 2x$ we need to consider the cubic $f(x) = x^3 - 4x^2 + 9$ where we take $b = 9, m = 2$. Then we have

$$D = 3^2 13,\ -3D = -3^3 13,\ d = -3 \cdot 13 = \begin{pmatrix} \text{square free} \\ \text{part of} - 3D \end{pmatrix},\ d \equiv 1 (\operatorname{mod} 4).$$

Let $K = \mathbb{Q}(\sqrt{-39})$. Then $\delta_K = d = -39$ since $d \equiv 1(\operatorname{mod} 4)$ and $h_K = 4$ by [6]. Now

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \frac{-1 + \sqrt{-39}}{2},\ \omega = \frac{-115}{2} + \frac{9}{2}\sqrt{-39},\ N(\omega) = 2^{12}.$$

Hence $(2) \subseteq \mathbb{Z}$ is the only prime lie below the prime ideals in the decomposition of ω. Since $d \equiv 1(\operatorname{mod} 8)$ we see (2) splits in K. We have decomposition

$$(2) = \left(2, \frac{1 + \sqrt{-39}}{2}\right)\left(2, \frac{1 - \sqrt{-39}}{2}\right).$$

Let $\mathfrak{p} = \left(2, \frac{1+\sqrt{-39}}{2}\right)$, $\mathfrak{q} = \left(2, \frac{1-\sqrt{-39}}{2}\right)$, $\sigma = \frac{1+\sqrt{-39}}{2}$. If there is A with $A^3 = \omega$, then we must have $N(A) = 2^4$. If we let $A = \frac{5+\sqrt{-39}}{2}$, then $A^3 = \omega$ (Theorem 4.1).

Then $(A) = \mathfrak{p}^a \mathfrak{q}^b$ with $a + b = 4$ since $N(A) = 2^4$. The possibilities are $(a, b) = (0, 4), (1, 3), (3, 1), (4, 0)$. The pair $(2, 2)$ is impossible for $(A) = (\mathfrak{p}\mathfrak{q})^2 = (4)$ which is not true. Since $h_K = 4$ we have $\mathfrak{p}^4 = (16, 4\sigma^2, \sigma^4)$ is principal and see if $\mathfrak{p}^4 = (A)$. Now we compute

$$16 = A\bar{A}; 4\sigma^2 = -38 + 2\sqrt{-39} = A \cdot \frac{-7 + 3\sqrt{-39}}{2},$$
$$\sigma^4 = \frac{161 - 19\sqrt{-39}}{2} = A \cdot \frac{2 - 8\sqrt{-39}}{2}.$$

Thus $\mathfrak{p}^4 \subseteq (A)$ but as they have the same norm we see $\mathfrak{p}^4 = (A)$. Thence $(\omega) = \mathfrak{p}^{12}$ which is the required condition (†) of Lemma 3.8. Incidentally, our computation shows that the class group of $\mathbb{Q}(\sqrt{-39})$ is isomorphic to $\mathbb{Z}/4$.

Since $x^3 - 4x^2 + 9 = (x - 3)(x^2 - x - 3)$ has roots $\alpha = 3, \beta, \gamma = \frac{1 \pm \sqrt{13}}{2}$, $f(x) = 0$ has the integral solution $x = 3$ and the equation (10) has an integral solution $x = 3, y = \pm 6$.

Now to the Diophantine equation problem: If we let $x = \frac{5}{2}, y = \frac{1}{6}$, then

$$\begin{aligned} A^3 &= \left(\frac{5}{2} + \frac{\sqrt{-39}}{2}\right)^3 \\ &= (x + y\sqrt{-3D})^3 \\ &= (x^3 - 9Dxy^2) + (3x^2 - 3Dy^3)\sqrt{-3D} \\ &= \frac{-115}{2} + \frac{3}{2}\sqrt{-3D} = \omega. \end{aligned}$$

Hence the equation

$$\begin{cases} x^3 - 9Dxy^2 = -\dfrac{115}{2}, \\ 3x^2y - 3Dy^3 = \dfrac{3}{2}. \end{cases}$$

has solution $x = \frac{5}{2},\ y = \frac{1}{6}$. If we subtract these equations we see that the equation

$$x^3 - 9Dxy^2 - 3x^2y + 3Dy^3 = -56 \quad \text{where } D = 3^2 13$$

has the same solution $x = \frac{5}{2},\ y = \frac{1}{6}$.

On the other hand, if we take $m = 2$, then $D = 3^7 \cdot 11; -3D = -3^8 \cdot 11; d = -11 \equiv 1 (\operatorname{mod} 4)$. But $4a^2 - |d| = 313$ which is a prime. Hence there is no integral solution to $x^3 - 9x^2 - 9 = 0$.

Remark. The solutions of $y^2 = x^3 + b$ $(b > 0)$ with $y = mx$ satisfies $b = |x^3 - m^2x^2| \geq |x|^2$. Hence $|x| \leq \sqrt{b}$ which is far smaller than expected by Hall's conjecture [5]

$$|x| \leq C_\epsilon b^{2+\epsilon}.$$

We plan to apply our method with $y = x + m$ instead of $y = mx$ in which the computation will get more complicated whereas we get more general solutions.

References

[1] N. C. Ankeny and C. A. Rogers, *A conjecture of Chowla*, Ann. of Math. (2) **53** (1951), 541–550.

[2] H. Flanders, *Generalization of a theorem of Ankeny and Rogers*, Ann. of Math. (2) **57** (1953), 392–400.

[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York Berlin, 1990.

[4] L. J. Mordell, *Diophantine Equation*, Academic Press, 1969.

[5] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer-Verlag, New York Berlin, 2009.

[6] N. Sloane, *Sequences*; *A013658*, in "The On-Line Encyclopedia of Integer Sequences".

[7] S. S. Woo, *Irreducibility of polynomials and Diophantine equations*, J. Korean Math. Soc. **47** (2010), no. 1, 101–112.

[8] B. L. Van der Waerden, *Algebra*, 4th ed., Frederick Ungar Publishing Co., New York, 1967.

Department of Mathematics
College of Natural Science
Ewha Womans University
Seoul 120-750, Korea
E-mail address: sswoo@ewha.ac.kr