Commun. Korean Math. Soc. **28** (2013), No. 4, pp. 723–733
http://dx.doi.org/10.4134/CKMS.2013.28.4.723

BACHET EQUATIONS AND CUBIC RESOLVENTS

Sung Sik Woo

Abstract. A Bachet equation $Y^2 = X^3 + k$ will have a rational solution if and only if there is $b \in \mathbb{Q}$ for which $X^3 - b^2X^2 + k$ is reducible. In this paper we show that such cubics arise as a cubic resolvent of a biquadratic polynomial. And we prove various properties of cubic resolvents.

1. Introduction

We will call the equation of the form

$$Y^2 = X^3 + k \ (k \in \mathbb{Z}) \tag{1}$$

a *Bachet equation* ([2] Chapter 17). If the equation (1) has a rational solution (a, ab) then, by replacing $Y = bX$, the cubic polynomial

$$h(X) = X^3 - b^2X^2 + k \tag{2}$$

will have a rational root a and conversely. Hence to find a Bachet equation (1) having a rational solution we need to find the cubic polynomial of the form (2) having a rational root. We will call a cubic of the form (2) with $b, k \in \mathbb{Q}$ a *cubic of Bachet type*. It is well known that a cubic resolvent of an irreducible quartic has a rational root if and only if its Galois group is isomorphic to a subgroup of D_4 [1, 4]. Motivated by this fact we try to realize the cubic of a Bachet type as a cubic resolvent of a rational quartic whose Galois group is isomorphic to a subgroup of D_4. Guided by the computations of cubic resolvents, we will define a bijective map between certain classes of cubics which will play the fundamental role in proving our main result.

In §2, we recall definitions of two cubic resolvents of quartics, one due to Ferrari [1] and the other one given by van der Waerden [4]. We prove various properties of resolvents and give relations between the two resolvents. Motivated by computations of cubic resolvents in the previous section, we define in §3 certain classes of polynomials and a function between them (Theorem 3.4). Using the function, we find a necessary and sufficient condition for a cubic of

Received December 17, 2012; Revised March 20, 2013.
2010 *Mathematics Subject Classification.* 14G05, 11D25.
Key words and phrases. Bachet equation, rational solution, resolvent cubi.

Bachet type to have a rational root. Also we show that the cubics of Bachet type come from a resolvent of a quartic.

2. Cubic resolvents of quartics

There are two kinds of cubic resolvents for a quartic which we introduce both of them. The first one is due to Ferrari [1] and the second one is introduced by van der Waerden [4]. Let

$$f(X) = X^4 + aX^3 + bX^2 + cX + d \tag{3}$$

be a quartic. If r_1, r_2, r_3, r_4 are the roots of $f(X)$, then the *Ferrari's resolvent* $R_F(f)$ of $f(X)$ is defined by a cubic having the roots

$$\eta_1 = r_1r_2 + r_3r_4,\ \eta_2 = r_1r_3 + r_2r_4,\ \eta_3 = r_1r_4 + r_2r_3$$

and it is given by [1]

$$R_F(f) = X^3 - bX^2 + (ac - 4d)X - (a^2d + c^2 - 4bd). \tag{4}$$

There is another resolvent which we call *van der Waerden's resolvent* having roots

$$\theta_1 = (r_1 + r_2)(r_3 + r_4),\ \theta_2 = (r_1 + r_3)(r_2 + r_4),\ \theta_3 = (r_1 + r_4)(r_2 + r_3)$$

which is given in [4]

$$R_W(f) = X^3 - 2bX^2 + (b^2 + ac - 4d)X + (a^2d + c^2 - abc). \tag{5}$$

If the coefficient of X^3 of f is 0, then the roots $\theta_1, \theta_2, \theta_3$ of $R_W(f)$ and the roots r_1, r_2, r_3, r_4 of f satisfy the relations [4]:

$$\begin{aligned} 2r_1 &= \sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}, \\ 2r_2 &= \sqrt{-\theta_1} - \sqrt{-\theta_2} - \sqrt{-\theta_3}, \\ 2r_3 &= -\sqrt{-\theta_1} + \sqrt{-\theta_2} - \sqrt{-\theta_3}, \\ 2r_4 &= -\sqrt{-\theta_1} - \sqrt{-\theta_2} + \sqrt{-\theta_3}. \end{aligned} \tag{6}$$

Proposition 2.1. *Let $f(X) = X^4 + bX^2 + d$ and let $f^\beta(X) = f(X + \beta)$. Then*

$$\begin{aligned} R_F(f^\beta) &= R_F(f) - 6\beta^2X^2 + 4\beta^2(b + 3\beta^2)X + 4\beta^2(4d - b\beta^2 - 2\beta^4), \\ R_W(f^\beta) &= R_W(f) + 12\beta^2X^2 + (-4b\beta^2 + 48\beta^4)X + b^2 - 4d + 32\beta^4 + 64\beta^6. \end{aligned}$$

Proof. Let r_1, r_2, r_3, r_4 be the roots of $f(X) = X^4 + bX^2 + d$ so that we have

$$\begin{aligned} &r_1 + r_2 + r_3 + r_4 = 0, \\ &r_1r_2 + r_3r_4 + r_1r_3 + r_2r_4 + r_1r_4 + r_2r_3 = b, \\ &\begin{pmatrix} (r_1r_2 + r_3r_4)(r_1r_3 + r_2r_4)+ \\ (r_1r_2 + r_3r_4)(r_1r_4 + r_2r_3)+ \\ (r_1r_3 + r_2r_4)(r_1r_4 + r_2r_3) \end{pmatrix} = ac - 4d = -4d. \end{aligned}$$

For $R_F(f^\beta)$, note that if $f(r)=0$, then $f^\beta(r-\beta)=0$. Hence

$$\begin{aligned}
R_F(f^\beta) &= (X-[(r_1-\beta)(r_2-\beta)+(r_3-\beta)(r_4-\beta)])\\
&\quad\times(X-[(r_1-\beta)(r_3-\beta)+(r_2-\beta)(r_4-\beta)])\\
&\quad\times(X-[(r_1-\beta)(r_4-\beta)+(r_2-\beta)(r_3-\beta)])\\
&= R_F(f)-2\beta^2\begin{pmatrix}(X-r_1r_2+r_3r_4)(X-r_1r_3+r_2r_4)\\ +(X-r_1r_2+r_3r_4)(X-r_1r_4+r_2r_3)\\ +(X-r_1r_3+r_2r_4)(X-r_1r_4+r_2r_3)\end{pmatrix}\\
&\quad+4\beta^4(3X-(r_1r_2+r_3r_4+r_1r_3+r_2r_4+r_1r_4+r_2r_3))-8\beta^6\\
&= R_F(f)-2\beta^2(3X^2-2bX-4d)+4\beta^4(3X-b)-8\beta^6\\
&= R_F(f)-6\beta^2X^2+4\beta^2(b+3\beta^2)X+4\beta^2(4d-b\beta^2-2\beta^4),
\end{aligned}$$

since

$$\begin{pmatrix}(X-r_1r_2+r_3r_4)(X-r_1r_3+r_2r_4)\\ +(X-r_1r_2+r_3r_4)(X-r_1r_4+r_2r_3)\\ +(X-r_1r_3+r_2r_4)(X-r_1r_4+r_2r_3)\end{pmatrix}=3X^2-2bX-4d.$$

Now, for $R_W(f^\beta)$, we compute

$$\begin{aligned}
R_W(f^\beta) &= \begin{bmatrix}(X-(r_1+r_2-2\beta)(r_3+r_4-2\beta))\\ \times(X-(r_1+r_3-2\beta)(r_2+r_4-2\beta))\\ \times(X-(r_1+r_4-2\beta)(r_2+r_3-2\beta))\end{bmatrix}\\
&= \begin{bmatrix}(X-(r_1+r_2)(r_3+r_4)+4\beta^2)\\ \times(X-(r_1+r_3)(r_2+r_4)+4\beta^2)\\ \times(X-(r_1+r_4)(r_2+r_3)+4\beta^2)\end{bmatrix}\\
&= R_W(f)+4\beta^2\begin{pmatrix}(X-(r_1+r_2)(r_3+r_4))(X-(r_1+r_3)(r_2+r_4))\\ \times(X-(r_1+r_3)(r_2+r_4))(X-(r_1+r_4)(r_2+r_3))\\ \times(X-(r_1+r_3)(r_2+r_4))(X-(r_1+r_4)(r_2+r_3))\end{pmatrix}\\
&\quad+16\beta^4[(X-(r_1+r_2)(r_3+r_4))+(X-(r_1+r_3)(r_2+r_4))\\
&\quad+(X-(r_1+r_4)(r_2+r_3))]+64\beta^6\\
&= R_W(f)+4\beta^2(3X^2-4bX+(b^2-4d))+16\beta^4(3X+2b)+64\beta^6\\
&= R_W(f)+12\beta^2X^2+(-4b\beta^2+48\beta^4)X+b^2-4d+32\beta^4+64\beta^6. \quad \square
\end{aligned}$$

Now we want to find the relation between $R_F(f)$ and $R_W(f)$.

Proposition 2.2. *Let $R_F(f)=X^3+\alpha X^2+\beta X+\gamma$. Then the van der Waerden's resolvent is given by*

$$R_W(f)=X^3+2\alpha X^2+(\alpha^2+\beta)X+\alpha\beta-\gamma.$$

Let $R_W(f)=X^3+\lambda X^2+\mu X+\nu$. Then the Ferrari resolvent is given by

$$R_F(f)=X^3+\frac{\lambda}{2}X^2+\frac{1}{4}(-\lambda^2+4\mu)X+\frac{1}{8}(-\lambda^3+4\lambda\mu-8\nu).$$

Proof. Let r_1, r_2, r_3, r_4 be the roots of (3). And let η_1, η_2, η_3 be the roots of $R_F(f)$ and $\theta_1, \theta_2, \theta_3$ be the roots of $R_W(f)$. Then

$$\begin{aligned}
\theta_1 &= \eta_2 + \eta_3,\\
\theta_2 &= \eta_1 + \eta_3,\\
\theta_3 &= \eta_1 + \eta_2,\\
\eta_1 &= \frac{1}{2}(-\theta_1 + \theta_2 + \theta_3),\\
\eta_2 &= \frac{1}{2}(\theta_1 - \theta_2 + \theta_3),\\
\eta_3 &= \frac{1}{2}(\theta_1 + \theta_2 - \theta_3).
\end{aligned}$$

We will use the identities

$$\begin{aligned}
&\theta_1 + \theta_2 + \theta_3 = 2(\eta_1 + \eta_2 + \eta_3),\\
&\theta_1\theta_2 + \theta_2\theta_3 + \theta_1\theta_3 = (\eta_2 + \eta_3)(\eta_1 + \eta_3) + (\eta_1 + \eta_3)(\eta_1 + \eta_2)\\
&\qquad\qquad + (\eta_2 + \eta_3)(\eta_1 + \eta_2)\\
&\qquad = (\eta_1 + \eta_2 + \eta_3)^2 + (\eta_1\eta_2 + \eta_2\eta_3 + \eta_1\eta_3),\\
&\theta_1\theta_2\theta_3 = (\eta_1 + \eta_2)(\eta_1 + \eta_3)(\eta_2 + \eta_3)\\
&\qquad = (\eta_1 + \eta_2 + \eta_3)(\eta_1\eta_2 + \eta_2\eta_3 + \eta_1\eta_3) - \eta_1\eta_2\eta_3.
\end{aligned}$$

Let

$$R_F(f) = X^3 + \alpha X^2 + \beta X + \gamma = (X - \eta_1)(X - \eta_2)(X - \eta_3).$$

By the computation above, we have

$$\begin{aligned}
R_W(f) &= (X - (\eta_1 + \eta_2))(X - (\eta_1 + \eta_3))(X - (\eta_2 + \eta_3))\\
&= X^3 - (\eta_1 + \eta_2 + \eta_1 + \eta_3 + \eta_2 + \eta_3)X^2\\
&\quad + [\eta_1 + \eta_2)(\eta_1 + \eta_3) + (\eta_1 + \eta_3)(\eta_2 + \eta_3) + (\eta_1 + \eta_2)(\eta_2 + \eta_3)]X\\
&\quad - (\eta_1 + \eta_2)(\eta_1 + \eta_3)(\eta_2 + \eta_3)\\
&= X^3 + 2\alpha X^2 + (\alpha^2 + \beta)X + \alpha\beta - \gamma.
\end{aligned}$$

Now suppose

$$R_W(f) = (X - \theta_1)(X - \theta_2)(X - \theta_3) = X^3 + \lambda X^2 + \mu X + \nu.$$

Then

$$-(\theta_1 + \theta_2 + \theta_3) = \lambda,\ \theta_1\theta_2 + \theta_2\theta_3 + \theta_1\theta_3 = \mu,\ -\theta_1\theta_2\theta_3 = \nu$$

and

$$\begin{aligned}
R_F(f) &= (X - \eta_1)(X - \eta_2)(X - \eta_3)\\
&= X^3 - (\eta_1 + \eta_2 + \eta_3)X^2 + (\eta_1\eta_2 + \eta_2\eta_3 + \eta_1\eta_3)X - \eta_1\eta_2\eta_3\\
&= X^3 + \frac{\lambda}{2}X^2 + \left(\mu - \left(\frac{\lambda}{2}\right)^2\right)X + \frac{\lambda}{2}\left(\mu - \left(\frac{\lambda}{2}\right)^2\right) - \nu
\end{aligned}$$

$$= X^3 + \frac{\lambda}{2}X^2 + \frac{1}{4}(-\lambda^2 + 4\mu)X + \frac{1}{8}(-\lambda^3 + 4\lambda\mu - 8\nu). \qquad \square$$

Motivated by these facts we define operations on cubic polynomials. Let

$$g(X) = X^3 + \alpha X^2 + \beta X + \gamma,$$
$$h(X) = X^3 + \lambda X^2 + \mu X + \nu.$$

We define

$$g_W(X) = X^3 + 2\alpha X^2 + (\alpha^2 + \beta)X + \alpha\beta - \gamma,$$
$$h_F(X) = X^3 + \frac{\lambda}{2}X^2 + \frac{1}{4}(-\lambda^2 + 4\mu)X + \frac{1}{8}(-\lambda^3 + 4\lambda\mu - 8\nu).$$

Hence, with these notations, we obtain the following result.

Proposition 2.3. (i) *If η_1, η_2, η_3 are the roots of a cubic $g(X)$, then the roots of $g_W(X)$ are $\theta_1 = \eta_2 + \eta_3, \theta_2 = \eta_1 + \eta_3, \theta_3 = \eta_1 + \eta_2$.*

If $\theta_1, \theta_2, \theta_3$ are roots of a cubic $h(X)$, then the roots of $h_F(X)$ are given by $\eta_1 = \frac{1}{2}(-\theta_1 + \theta_2 + \theta_3), \eta_2 = \frac{1}{2}(\theta_1 - \theta_2 + \theta_3), \eta_3 = \frac{1}{2}(\theta_1 + \theta_2 - \theta_3)$.

(ii) *Suppose g, h are monic rational cubics having one* (*resp. three*) *rational root*(*s*). *Then g_W and h_F have one* (*resp. three*) *rational root*(*s*).

(iii) *We have*

$$(g_W)_F = g \text{ and } (h_F)_W = h.$$

Proof. (ii) follows from (i). The other results are obvious from the previous computation. $\square$

We will frequently consider biquadratic polynomial $f(X) = X^4 + pX^2 + r$. The following fact is a special case of [3] Lemma 23, p. 151.

Lemma 2.4. *Let K be a field. A biquadratic $X^4 + pX^2 + r \in K[X]$ is reducible if and only if it is either of the form*

$$(X^2 + a)(X^2 + b) = X^4 - (a + b)X^2 + ab$$

or

$$(X^2 + a)^2 - b^2X^2 = X^4 + (2a - b^2)X^2 + a^2$$

for some $a, b \in K$.

Now we want to recover a quartic f from $R_W(f)$ when f is a biquadratic.

Proposition 2.5. *Let BQ be the set of all monic biquadratic polynomials over a field and let B_0 be the set of monic cubics of the form $h(X) = X^3 + \alpha X^2 + \beta X$. If $f \in BQ$, then $R_W(f) \in B_0$. And if we let*

$$R^-(h) = X^4 - \frac{\alpha}{2}X^2 + \left(\frac{\alpha^2}{16} - \frac{\beta}{4}\right),$$

then $R_W(R^-(h)) = h$ and $R_W : BQ \to B_0$ is a bijection with the inverse R^-.

Further $R^-(h)$ is reducible if and only if β is a square or $t^4 - \alpha t^2 + \beta = 0$ has a rational root t.

Proof. The first statement is straight forward to check. Next we have to prove the statement about reducibility of f. By Lemma 2.4 we see that f is irreducible if and only if the corresponding quadratic has discriminant which is a square or it is of the second type. The discriminant of the corresponding quadratic is $(\frac{\alpha}{2})^2 - 4(\frac{\alpha^2}{16} - \frac{\beta}{4}) = \beta$ is a square.

Now consider the possibility of f being the second type of Lemma 2.4. Note that f is of the second type if and only if $b^2 - 2a = \frac{\alpha}{2}, a^2 = \frac{\alpha^2}{16} - \frac{\beta}{4}$ has a rational solution in a, b. And this is equivalent to $\alpha = 2b^2 - 4a, \alpha^2 - 4\beta = 16a^2$ has a rational solution. That is $b^4 - \alpha b^2 + \beta = 0$ has a rational root. $\square$

3. Bachet equations and cubic resolvents

If a Bachet equation $Y^2 = X^3 + k$ $(k \in \mathbb{Z})$ has a rational solution (a, ab), then the cubic polynomial

$$h(X) = X^3 - b^2X^2 + k$$

will have a rational root a and conversely. Hence to find a Bachet equation having a rational solution we need to find the cubic polynomial of Bachet type having a rational root with the integer constant term.

If a biquadratic polynomial is irreducible, then the splitting field will be of degree that divides 8. And if the Galois group of a rational quartic f has order that divides 8, then the Galois group of f is isomorphic to either D_4 or $\mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$. Also in this case, it is well known that the cubic resolvent of f has a rational solution [1] (Ferrari's resolvent was used in [1], but by Proposition 2.3, the result can be also stated in terms of Waerden's resolvent). Therefore we want to find conditions of a quartic that becomes biquadratic by a change of a variable whose cubic resolvent is a cubic of Bachet type.

Consider a rational quartic

$$f(X) = X^4 + aX^3 + bX^2 + cX + d \in \mathbb{Q}[X].$$

We make a change of variable $X \mapsto X - \frac{a}{4}$ to make the coefficient of X^3 to be zero and we denote the resulting quartic by f^+. Then the equation becomes

$$f^+(X) = f(X - \frac{a}{4}) = X^4 + pX^2 + qX + r$$

and its resovents becomes

$$\begin{aligned} R_F(f^+) &= X^3 - pX^2 - 4rX - (q^2 + 4pr), \\ R_W(f^+) &= X^3 - 2pX^2 + (p^2 - 4r)X + (q^2 - 4pr), \end{aligned}$$

where

$$\begin{aligned} p &= \frac{1}{8}(-3a^2 + 8b), \\ q &= \frac{1}{8}(a^3 - 4ab + 8c), \\ r &= \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d). \end{aligned}$$

We have the following elementary fact.

Lemma 3.1. *Let* $f(X) = X^4+pX^2+r \in \mathbb{Q}[X]$*. Then the resolvents* $R_F(f)$ *and* $R_W(f)$ *of the biquadratic polynomial* f *has a rational root* p *and* 0*, respectively.*

Proof. Let r_1, r_2, r_3, r_4 be the roots of f. Let $\bar{f}(t) = t^2+pt+r$ and $a\pm\sqrt{b}$ $(a, b \in \mathbb{Q})$ be the roots of $\bar{f}$. Then we can choose $r_1 = \sqrt{a+\sqrt{b}}, r_2 = \sqrt{a-\sqrt{b}}, r_3 = -\sqrt{a+\sqrt{b}}, r_4 = \sqrt{a-\sqrt{b}}$. Then $\eta_1 = r_1r_3 + r_2r_4 = -2a = p$ which is a root of $R_F(f)$. On the other hand, $\theta_2 = (r_1 + r_3)(r_2 + r_4) = 0$ is a root of $R_W(f)$. □

By Lemma 3.1, resolvent cubics of a rational biquadratic polynomial has a rational root. Motivated by this fact we choose the coefficients of the quartic in the following way.

(1) To make the coefficient of X^2 in the resolvent to be b^2 we replace $b \to b^2$ for R_F (resp. $b \to \frac{b^2}{2}$ for R_W).

(2) To make the coefficient of X in f^+ to be 0 we let $q = 0$; i.e., $c = \frac{a}{8}(4b^2 - a^2)$ for R_F (resp. $c = \frac{a}{8}(2b^2 - a^2)$ for R_W).

(3) To make the coefficient of X in $R(f)$ to be 0:
(The coefficient of X in $R_F(f)$)$=ac - 4d = 0$; $d = \frac{1}{4}ac = \frac{a^2}{32}(4b^2 - a^2)$,
(The coefficient of X in $R_W(f)$)$=b^2 + ac - 4d = 0$; $d = \frac{1}{32}(-a^4 + 2a^2b^2 + 2b^4)$.

Ferrari's resolvent
If we make the substitution for Ferrari's resolvent above, then we get:

$$\begin{aligned} f_F(X) &= X^4 + aX^3 + b^2X^2 + \frac{a}{8}(4b^2 - a^2)X + \frac{a^2}{32}(-a^2 + 4b^2), \\ f_F^+(X) &= f_F(X - \frac{a}{4}) = X^4 + \frac{1}{8}(-3a^2 + 8b^2)X^2 + \frac{a^2}{2^8}(-3a^2 + 16b^2), \end{aligned} \tag{7}$$

and their Ferrari's resolvents are

$$\begin{aligned} R_F(f) =& X^3 - b^2X^2 + \frac{1}{2^6}a^2(a^2 - 4b^2)^2, \\ R_F(f^+) =& X^3 + \frac{1}{8}(3a^2 - 8b^2)X^2 + \frac{a^2}{2^6}(a^2 - 16b^2)X \\ &+ \frac{a^2b^2}{2^9}(3a^2 - 8b^2)(3a^2 - 16b^2). \end{aligned} \tag{8}$$

Waerden's resolvent
If we make the substitution for Waerden's resolvent above, then we get:

(9)
$$\begin{aligned} f_W(X) &= X^4 + aX^3 + \frac{b^2}{2}X^2 + \frac{a}{8}(2b^2 - a^2)X + \frac{1}{32}(-a^4 + 2a^2b^2 + 2b^4), \\ f_W^+(X) &= f_W(X - \frac{a}{4}) = X^4 + \frac{1}{8}(-3a^2 + 4b^2)X^2 + \frac{1}{2^8}(-3a^4 + 8a^2b^2 + 16b^4) \end{aligned}$$

and their Waerden's resolvents are

$$
(10)\qquad \begin{aligned} R_W(f) &= X^3 - b^2X^2 + \frac{a^4}{64}(-a^2+4b^2),\\ R_W(f^+) &= X^3 - \frac{1}{4}(-3a^2+4b^2)X^2 + \frac{a^2}{16}(3a^2-8b^2)X. \end{aligned}
$$

Lemma 3.2. *Let $f_F(X)$ and $f_W(X)$ be the quartics given in* (7), (9). *Then $R_F(f_F)$ has a root $-\frac{a^2}{4}+b^2$ and $R_W(f_W)$ has a root $\frac{a^2}{4}$. In particular, $R_F(f_F)+R_W(f_W)=b^2$.*

Proof. Let r_1,r_2,r_3,r_4 be the roots of f^+. Then since $f^+(X)=f(X-\frac{a}{4})$, the roots of f are $r_i-\frac{a}{4}$ and hence the roots of $R_F(f)$ are

$$
\begin{aligned}
(r_1-\frac{a}{4})(r_2-\frac{a}{4})+(r_3-\frac{a}{4})(r_4-\frac{a}{4}) &= (r_1r_2+r_3r_4)+\frac{a^2}{8} = s_1+\frac{a^2}{8},\\
(r_1-\frac{a}{4})(r_3-\frac{a}{4})+(r_2-\frac{a}{4})(r_4-\frac{a}{4}) &= (r_1r_3+r_2r_4)+\frac{a^2}{8} = s_2+\frac{a^2}{8},\\
(r_1-\frac{a}{4})(r_4-\frac{a}{4})+(r_2-\frac{a}{4})(r_3-\frac{a}{4}) &= (r_1r_4+r_2r_3)+\frac{a^2}{8} = s_3+\frac{a^2}{8}
\end{aligned}
$$

since $r_1+r_2+r_3+r_4=0$ as they are the roots of a biquadratic polynomial. Now since $R_F(f^+)$ has a root $p=\frac{1}{8}(-3a^2+8b^2)$ by the previous result, we see that $p+\frac{a^2}{8}=\frac{-3a^2}{8}+b^2+\frac{a^2}{8}=-\frac{a^2}{4}+b^2$ is a root of $R_F(f)$.

Similarly for R_W we compute:

$$
\begin{aligned}
[(r_3-\frac{a}{2})(r_4-\frac{a}{4})] &= [(r_1+r_2)-\frac{a}{2}][(r_3+r_4)-\frac{a}{2}]\\
&= (r_1+r_2)(r_3+r_4)-\frac{a}{2}((r_1+r_2+r_3+r_4)+\frac{a^2}{4}\\
&= s_1+\frac{a^2}{4}.
\end{aligned}
$$

Now since $R_W(f^+)$ has a root 0, we have the desired result. □

Example 3.3. Let $a=2, b^2=25$ so that $c=24$ (These are chosen so that there are no X^3, X terms in f^+ and no X in $R_F(f)$. $f^+(X)=X^4+23.5X^2+\frac{97}{16}+24$). Now $f(X)=X^4+2X^3+25X^2+24X+12$ which is irreducible since f^+ is irreducible by Lemma 2.4. Its resolvent is $R_F(f)=X^3-25X^2+576=(X-24)(X^2-X-24)$. Further $k=\frac{1}{64}a^2(4b-a^2)^2=576=24^2$. The coefficient p of X^2 in f^+ is $p=\frac{1}{8}(-3a^2+8b)=23.5$ which is a root of $R_F(f^+)$, i.e., $R_F(f^+)(p)=0$. Hence the rational root of $R_F(f)$ is $p+\frac{a^2}{8}=23.5+\frac{1}{2}=24$. Hence we conclude that the Bachet equation $Y^2=X^3+576$ has a rational, in fact an integral solution $X=24, Y=120$.

Motivated by the comparison $R_W(f)$ with $R_W(f^+)$ we define

$$
\begin{aligned}
B &= \{X^3+\theta X^2+\eta \in \mathbb{Q}[X] \text{ having a rational root}\},\\
B^+ &= \{X^3+\alpha X^2+\beta X \in \mathbb{Q}[X] \text{ with } \alpha^2-3\beta \text{ is a square in } \mathbb{Q}\}
\end{aligned}
$$

so that B contains all $R_W(f)$'s and B^+ contains all $R_W(f^+)$'s of (10). We will prove that there is a bijection between them which will be the crux in determining the Bachet equations having a rational solution.

Theorem 3.4. *For the rational cubics*

$$f(X) = X^3 + \theta X^2 + \eta \text{ with } f(a) = 0,\ a \in \mathbb{Q},$$
$$g(X) = X^3 + \alpha X^2 + \beta X \text{ with } \alpha^2 - 3\beta = \gamma^2\ (\gamma \in \mathbb{Q},\ \gamma < 0),$$

we define

$$\phi(f) = X^3 + (3a+\theta)X^2 + a(3a+2\theta)X,$$
$$\psi(g) = X^3 + \gamma X^2 - \frac{1}{27}(\alpha-\gamma)^2(\alpha+2\gamma).$$

Then $\phi : B \to B^+$ and $\psi : B^+ \to B$ are inverses to each other.

Proof. First we check that $\phi(f) \in B^+$ and $\psi(g) \in B$. For this, we observe that $(3a+\theta)^2 - 3a(3a+2\theta) = \theta^2$ and $\psi(g)$ has a root $\frac{\alpha-\gamma}{3}$. Hence $\phi(f) \in B^+$ and $\psi(g) \in B$.

Now we want to show ϕ and ψ are inverses to each other. Since a is a root of $f(X)$, we have $X^3+\theta X^2+\eta = (X-a)(X^2+(\theta+a)X+a(\theta+a))$. Therefore $\eta = -a^2(\theta+a)$. We check:

$$\begin{aligned}\psi\phi(f) &= \psi(X^3 + (3a+\theta)X^2 + a(3a+2\theta)X)\\ &= X^3 + \theta X^2 + \frac{1}{27}(-\theta+(3a+\theta))^2((-3a-\theta)-2\theta)\\ &= X^3 + \theta X^2 - a^2(a+\theta) = f(X).\end{aligned}$$

Next let g be the cubic as above. Then as we noted above, $\psi(g)$ has a root $\dfrac{\alpha-\gamma}{3}$. Hence

$$\begin{aligned}\phi\psi(g) &= \phi(X^3 + \gamma X^2 - \frac{1}{27}(\alpha-\gamma)^2(\alpha+2\gamma))\\ &= X^3 + (3\cdot\frac{\alpha-\gamma}{3} + \gamma)X^2 + \frac{\alpha-\gamma}{3}(\alpha-\gamma+2\gamma)\\ &= X^3 + \alpha X^2 + \frac{1}{3}(\alpha^2-\gamma^2) = g(X),\end{aligned}$$

where the last equality follows from $\alpha^2 - 3\beta = \gamma^2$. □

The following statement is straight forward to check. However we derive it using Theorem 3.4 to illustrate the theorem. The reason why we choose $\gamma < 0$ will become obvious.

Corollary 3.5. *The cubic equation $Y^2 = X^3 + k$ $(k \in \mathbb{Q})$ has a rational solution if and only if there are $a, b \in \mathbb{Q}$ such that $k = -a^2(a-b^2)$. In this case, the solution is given by (a, ab).*

Proof. First suppose k is of the form $k = -a^2(a-b^2)$. It is trivial to check that $X^3 - b^2X^2 + k$ has a root a. Hence there is a rational solution (a, ab) for $Y^2 = X^3 + k$ $(k \in \mathbb{Q})$.

Now suppose $Y^2 = X^3 + k$ $(k \in \mathbb{Q})$ has a solution (a, ab). Then $h(X) = X^3 - b^2X^2 + k$ has a root $a \in \mathbb{Q}$. Then by Theorem 3.4, $\phi(h) = X^3 + (3a - b^2)X^2 + a(3a-2b^2)X \in B^+$. And with the notation of Theorem 3.4, we have $\gamma^2 = b^4, \alpha = 3a - b^2$ and choose $\gamma = -b^2$. Now

$$\begin{aligned}\psi\phi(h) &= X^3 + \gamma X^2 - \frac{1}{27}(\alpha-\gamma)^2(\alpha+2\gamma)\\ &= X^3 - b^2X^2 - a^2(a-b^2) = h.\end{aligned}$$

Hence k is of the form $-a^2(a-b^2)$ as required. $\square$

Corollary 3.6. *For $h(X) = X^3 - b^2X^2 - a^2(a-b^2)$, we have*

$$\phi(h) = X^3 + (3a-b^2)X^2 + a(3a-2b^2)X = h(X+a).$$

Further the rational cubic $h(X)$ has three rational roots if and only if $D = (a-b^2)(-3a-b^2)$ is a square in $\mathbb{Q}$.

Proof. We only need to check the last part. First we have

$$h(X) = (X-a)(X^2 + (a-b^2)X + a(a-b^2))$$

and the quadratic factor has discriminant $D = (a-b^2)(-3a-b^2)$. Hence the roots of h are $\theta_1 = a, \theta_2 = \frac{1}{2}(-a+b^2) + \sqrt{D}, \theta_2 = \frac{1}{2}(-a+b^2) - \sqrt{D}$.

On the other hand,

$$\phi(h) = X(X^2 + (3a-b^2)X + a(3a-2b^2))$$

and the quadratic factor has the same discriminant D; the roots of $\phi(h)$ are $\eta_1 = 0, \eta_2 = \frac{1}{2}(-3a-b^2) + \sqrt{D}, \eta_3 = \frac{1}{2}(-3a-b^2) - \sqrt{D}$. $\square$

Let BQ be the set of all rational monic biquadratic polynomials and BQ^0 be the monic quartics f for which $f^+ \in BQ$, where, as before f^+ is the quartic without X^3 term obtained by making a linear change of variable. Also we write $f^\beta(X) = f(X+\beta)$. We have a map $\rho : BQ^0 \to BQ$ defined by $\rho(f) = f^+$. Now we have a diagram:

$$\begin{array}{ccc} BQ^0 & \xrightarrow{\rho} & BQ \\ {\scriptstyle R_W}\downarrow & & \downarrow{\scriptstyle R_W} \\ B & \xrightarrow{\phi} & B^+ \end{array} \tag{11}$$

Proposition 3.7. *The diagram* (11) *is commutative.*

Proof. Let $f \in BQ^0$ and let $R_W(f) = X^3 - b^2X^2 - a^2(a-b^2)$ with roots $\{a = \theta_1, \theta_2, \theta_3\}$. Then $\phi(R_W(f))$ has roots $\{0 = \theta_1 - a,\ \theta_2 - a, \theta_3 - a\}$.

Now $\rho(f) = f^{\beta}$ for some $\beta \in \mathbb{Q}$ and $R_W(\rho(f)) = R_W(f^{\beta})$ has roots $\{0 = \theta_1 - 4\beta^2,\ \theta_2 - 4\beta^2,\ \theta_3 - 4\beta^2\}$. Since $\theta_1 - a = 0 = \theta_1 - 4\beta^2$, we see that $a = 4\beta^2$ and hence $\phi(R_W(f))$ and $R_W(\rho(f))$ have the same roots. Therefore $\phi(R_W(f)) = R_W(\rho(f))$. □

Next we show that a Bachet type cubic $h(X)$ is a resolvent of a quartic over a quadratic extension of $\mathbb{Q}$.

Theorem 3.8. *Let $h(X) = X^3 - b^2X^2 + k$ be a cubic with $k = -a^2(b - b^2)$ $(a, b \in \mathbb{Q})$. Then $h(X)$ is a cubic resolvent of a rational quartic which becomes a biquadratic by a linear change of variable if and only if a is a square in $\mathbb{Q}$.*

In this case, if $h(X) = X^3 - b^2X^2 - a^4(a^2 - b^2)$, then the quartic and the corresponding biquadratic polynomials are given by

$$f(X) = X^4 + 2aX^3 + \frac{b^2}{2}X^2 + \frac{a}{4}(b^2 - 2a^2)X + \frac{1}{16}(-8a^4 + 4a^2b^2 + b^4),$$
$$f^{+}(X) = X^4 + \frac{1}{2}(-3a^2 + b^2)X^2 + \frac{1}{2^4}(-3a^4 + 2a^2b^2 + b^4).$$

Proof. The last statement follows from (9) and (10) by replacing a by $2a$.

For the first statement let $h(X) = X^3 - b^2X^2 - a^2(a - b^2) \in B$. Choose a quartic f for which $R_W(f) = h$. Let $\{\theta_1 = a, \theta_2, \theta_3\}$ be the roots of $R_W(f)$ as in Corollary 3.6 and let f^{β} be the biquadratic. Then as in Lemma 3.2, we see that $R_W(f^{\beta})$ has roots $\{a - 4\beta^2, \theta_2 - 4\beta^2, \theta_3 - 4\beta^2\}$. Since f^{β} is biquadratic $R_W(f^{\beta})$ has 0 as a rational root, we have $a = 4\beta^2$ which is a square of a rational number 2β. □

References

[1] D. A. Cox, *Galois Theory*, Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, 2004.
[2] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.
[3] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of mathematics and its applications 77, Cambridge University Press, Cambridge, 2000.
[4] 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