MATH. SCAND. 2 (1954), 227–236

THE EXCEPTIONAL POINTS OF A CUBIC CURVE WHICH IS SYMMETRIC IN THE HOMOGENEOUS VARIABLES

ERNST S. SELMER

1. Introduction. In his well-known paper on cubic curves, Hurwitz [5] studied the exceptional points in the case

$$ax^3 + by^3 + cz^3 + dxyz = 0 , \tag{1.1}$$

with rational integral coefficients. He showed that there are no such points if all the numbers $|ab|$, $|ac|$ and $|bc|$ are *squarefree* and > 1. Special results were given when two or all three of the numbers a, b and c are equal to 1. The method of the proof is simple: Let (x, y, z) be a rational point of (1.1), with no common factor for all the three integral coordinates. We define the *weight* of the point as $|xyz|$, and show that the *tangential* of (x, y, z) — with a possible common factor removed — has a *greater* weight than (x, y, z), which consequently cannot be an exceptional point.

In the last 25 years, the theory of exceptional points has been developed mainly by Nagell and his pupils; for references, see Nagell [8] [9] and Bergman [1]. The work has mostly been concentrated on the Weierstrass normal form

$$y^2 = x^3 - Ax - B , \tag{1.2}$$

for which Nagell [7] has proved that the exceptional points must have *integral* coordinates (x, y), and that $y^2 \,|\, 4A^3 - 27B^2$ if $y \neq 0$ (assuming that the field of reference is the rational field $K(1)$).

The exceptional points of a cubic curve of genus one, in an algebraic field Ω, form a *finite group*. Examples of many different groups have been given, including parametric representations of the invariants A and B in (1.2), and other group-structures have been proved impossible. In particular, the rank r of the exceptional group is $\leqq 2$ if Ω is real. When $r = 2$, the number of exceptional points is divisible by 4, and one

Received November 12, 1954.

generator is of order 2. — The known cases of possible and impossible groups in $K(1)$ are summarized by Bergman [1, p. 490].

The forming of *tangentials* is of course equally important for the equation (1.2), but now usually in *inhomogeneous* coordinates. In the present paper, I will show how the original method of Hurwitz, based on the weight of a point in homogeneous coordinates (x, y, z), can be applied to a cubic curve which is *symmetric* in x, y and z. This is not such a heavy restriction as it may seem, since we shall see that the symmetric case will represent *all cubic curves with three rational inflections.*

2. The symmetric curve. When the equation is symmetric in x, y and z, it can be written as

$$a(x+y+z)^3 + b(xy+xz+yz)(x+y+z) + cxyz = 0 \,. \tag{2.1}$$

In what follows, we shall assume that the coefficients and variables are *rational integers.* Several of the results will clearly be valid also in an arbitrary algebraic field Ω.

The following conditions are easily established: Let $d=27a+9b+c$ and $e=b^3+b^2c-ac^2$. Then the curve (2.1) is *unicursal,* with the singular point $(1, 1, 1)$, if $d=0$, $e\neq 0$. The curve contains the line $x+y+z=0$ if $c=0$, and degenerates into three (real) lines if $e=0$. These lines have the common point $(1, 1, 1)$ if also $d=0$.

We will therefore assume that

$$cde = c(27a+9b+c)(b^3+b^2c-ac^2) \neq 0 \,, \tag{2.2}$$

in which case (2.1) represents a non-degenerate curve of genus one.

Theorem 1. *If $c\neq -3b$, the curve* (2.1) *can be given the form*

$$A(X+Y+Z)^3 + CXYZ = 0 \tag{2.3}$$

by the linear symmetric substitution

$$X = cx + b(x+y+z), \quad Y = cy + b(x+y+z), \quad Z = cz + b(x+y+z) \,.$$

The determinant $c^2(3b+c)\neq 0$, and we find

$$A = b^3+b^2c-ac^2, \qquad C = -(3b+c)^3 \,.$$

Here $A\neq 0$ by the condition (2.2), which now takes the form

$$AC(27A+C) \neq 0 \,. \tag{2.4}$$

The equation (2.3) is really a *Weierstrass* normal form; this is immediately seen if we put $Z=1$ and rotate the XY-system 45° (assuming

Cartesian coordinates). For later use, we shall consider the special transformation

$$8AX = CX_1 - CY_1 - 4A, \qquad 8AY = CX_1 + CY_1 - 4A ,$$

taking (2.3) into

$$Y_1^2 = X_1^3 + (X_1 - 4A/C)^2 . \tag{2.5}$$

All symmetric curves (2.1) *have the rational inflections*

$$(0, -1, 1), \quad (-1, 0, 1), \quad (1, -1, 0) , \tag{2.6}$$

and the *inflectional tangents* are just the new axes $X = 0$, $Y = 0$ and $Z = 0$ in the transformation of Theorem 1. In the excluded case $c = -3b$, these tangents will pass through one point (1, 1, 1), showing that we must have an *equianharmonic* case. This is also directly verified by the substitution

$$3x = x_1 - y_1 + fz_1, \quad 3y = x_1 + y_1 + fz_1, \quad 3z = x_1 - 2fz_1;$$

$$f = \frac{9a + 2b}{2b} \neq 0 .$$

With $c = -3b$, (2.1) is then transformed into

$$y_1^2 = x_1^3 + f^2, \tag{2.7}$$

where we have put $z_1 = 1$.

The equianharmonic case is, of course, well known. The curve (2.7) will usually have just 3 exceptional points, and 6 such points only if f is a rational cube. In what follows, we can therefore concentrate on the reduced symmetric form (2.3), for which we have the important

THEOREM 2. *Any rational cubic curve of genus one, with three rational inflections, is equivalent to a curve* (2.3) *if the inflectional tangents do not pass through one point.*

This is a well-known result from algebraic geometry, cf. Hilton [4, Ch. XIV, § 5]. The linear substitution in question uses the inflectional tangents as the new triangle of reference, and the line through the inflections as the new unit line.

Theorem 2 also follows from a result of Nagell [8, p. 5], that any cubic curve with three rational inflections is equivalent to one of the forms

$$y^2 = x^3 + (x + \alpha)^2 \quad \text{or} \quad y^2 = x^3 + \beta^2$$

(α and β rational), which coincide with (2.5) and (2.7) above.

The importance of Theorem 2 was already pointed out by Hurwitz [5, p. 222], who also gives

$$A_1 Z^3 + B_1 XY(X+Y) = 0$$

as a normal form for the equianharmonic case $c = -3b$.

We shall give below parametric expressions for cubic curves with an exceptional sub-group of 6, 9 or 12 points. It follows from Theorem 2 that these expressions will be *general.*

3. The tangential. For the general symmetric curve (2.1), the tangential of any point (x, y, z) has the coordinates

$$(3.1) \qquad \begin{cases} x' = (y-z)\,[b\,F(x,y,z) + cx(y-z)^2] \\ y' = (z-x)\,[b\,F(x,y,z) + cy(z-x)^2] \\ z' = (x-y)\,[b\,F(x,y,z) + cz(x-y)^2] \end{cases}$$

where

$$F(x,y,z) = (x+y+z)^3 - 3(xy+xz+yz)(x+y+z)\,.$$

The formulae are rather complicated, but take a much simpler form for the reduced curve (2.3):

$$(3.2) \quad X' = X(Y-Z)^3, \qquad Y' = Y(Z-X)^3, \qquad Z' = Z(X-Y)^3.$$

The tangential is one of the inflections (2.6) *if and only if two coordinates of the original point are equal.* This is immediately clear for the form (3.2), but is also easy to show in the general case (3.1). We shall call a tangential "proper", if it is not an inflection.

To examine the *weight* of a proper tangential (3.2), compared to the weight $|XYZ|$ of the original point, we must determine possible common factors in the expressions for X', Y' and Z'. We assume that $(X, Y, Z) = 1$, and put

$$(3.3) \quad \begin{gathered} (Y,Z) = d_1, \qquad (Z,X) = d_2, \qquad (X,Y) = d_3 \\ X = d_2 d_3 u, \qquad Y = d_3 d_1 v, \qquad Z = d_1 d_2 w \\ (Y-Z, Z-X, X-Y) = d, \qquad (d_1 d_2 d_3, d) = 1\,. \end{gathered}$$

Then $(X', Y', Z') = d_1 d_2 d_3 d^3$, and the weight of the reduced tangential is given by

$$(3.4) \qquad |XYZ| \left| \frac{Y-Z}{d_1 d} \cdot \frac{Z-X}{d_2 d} \cdot \frac{X-Y}{d_3 d} \right|^3 .$$

The weight of a proper tangential (3.2) *is never smaller than the weight of the original point.* If the two weights are to be *equal,* we must have

$$(3.5) \qquad Y-Z = d_1 d, \qquad Z-X = d_2 d, \qquad X-Y = d_3 d\,.$$

We may assume $d > 0$, let these relations determine the signs of d_1, d_2 and d_3, and finally get the signs of u, v and w by (3.3).

From (3.3) and (3.5) we get the necessary and sufficient conditions

$$d_1+d_2+d_3 = 0, \qquad u+v+w = 0\,.$$

One and only one term in each equation must be *even*. Since $XYZ = d_1^2 d_2^2 d_3^2 uvw$, and $d_1 d_2 d_3$ is prime to $S = X+Y+Z$, it follows from the given equation (2.3) that $d_1^2 d_2^2 d_3^2 | A$, i.e. in particular $4|A$. We cannot conclude that uvw is prime to S, but since S is odd, the factor 2 from uvw must also divide A, i.e. $8|A$.

It follows from the above that $d_1 X + d_2 Y + d_3 Z = 0$. Then $(d_1, X) = 1$ together with $d_1^2 | XYZ$ implies $d_1 | Y$, $d_1 | Z$, and similarly for d_2 and d_3. We can therefore formulate the results in the following

THEOREM 3. *A point (X, Y, Z) of the curve* (2.3) *will have a proper tangential of the same weight $|XYZ|$ if and only if there are three coprime integers d_1, d_2 and d_3 such that*

$$d_1+d_2+d_3 = 0, \qquad d_1^2 d_2^2 d_3^2 | A\,,$$
$$d_1 X + d_2 Y + d_3 Z = 0, \qquad (d_1, X) = (d_2, Y) = (d_3, Z) = 1\,.$$

In particular, this is impossible if $8 \nmid A$.

There will be a limited number of possibilities for d_1, d_2 and d_3, depending on the squared factors of A. For each possibility, one must examine if a homogenous *binary* cubic equation has integral solutions.

It is clear that the above considerations, especially the weight-formula (3.4), will make it easy to examine *whether a given point is the tangential of another point.*

4. Sub-group of order nine. In the following sections, we shall study exceptional sub-groups of varying structures. The study is based on the "tangential properties", that is how the points are connected by means of the formation of tangentials. These properties are easy to establish, for instance by a theorem of Billing [2, pp. 33–34] on the basis of the exceptional group.

Because of the symmetry, the points (X, Y, Z) determined by Theorem 3 will occur in *sets of six points*, with permutation of the coordinates within each set. (The same property will of course hold in general for the points of the curve (2.1) for which $x \neq y \neq z \neq x$.) An exceptional subgroup of order nine (*cyclic* in a real field) must contain the inflections (2.6) and *one* such set of exceptional points. This set must have the additional property that *the tangential of any point is obtained by a cyclic permutation of the coordinates of the given point.* With the notation of Section 3, it is easy to see that this will be the case if and only if u, v and w represent a cyclic permutation of d_1, d_2 and d_3, for instance

$$u = d_2, \quad v = d_3, \quad w = d_1 .$$

Hence from (3.3):

$$(4.1) \quad X = d_2^2 d_3 = -d_2^2(d_1+d_2), \qquad Y = d_3^2 d_1 = d_1(d_1+d_2)^2, \qquad Z = d_1^2 d_2 .$$

The other cyclic permutation of u, v and w can be represented by an interchange of d_1 and d_2.

From the given equation (2.3), we conclude that

$$(4.2) \qquad \begin{cases} A = -XYZ = [d_1 d_2 (d_1+d_2)]^3 \\ C = (X+Y+Z)^3 = [d_1^3 + 3d_1^2 d_2 - d_2^3]^3, \end{cases}$$

since these expressions have no common factor when $(d_1, d_2) = 1$. The condition (2.4) is clearly satisfied, and we have consequently found the

THEOREM 4. *Any rational cubic curve with a cyclic exceptional sub-group of order nine is equivalent to the form* (2.3), *where* A *and* C *are given by* (4.2), *with coprime positive integers* d_1 *and* d_2. *The exceptional points are the three inflections* (2.6) *and the six points obtained by permutation of the coordinates* (4.1).

The corresponding parametric representation for the Weierstrass form (1.2) has been given by Nagell [8, pp. 16-17]. His formulae are much more complicated.

The simplest numerical illustration of Theorem 4 corresponds to $d_1 = d_2 = 1$, i.e. the curve

$$8(X+Y+Z)^3 + 27XYZ = 0 .$$

The exceptional points are the inflections (2.6) and the six points (4, 1, -2) etc., and it is easily verified that there are no others. It is interesting to note that the corresponding Weierstrass curve is

$$y^2 = x^3 - 219x + 1654 .$$

In this form, Billing [3] has proved that the nine exceptional points are *all the rational points* of the curve.

5. Sub-group of order six. It seems extremely difficult to conclude from Theorem 3 whether or not *more than one set* of 6 exceptional points can exist. On the other hand, we can prove the

THEOREM 5. *If there is no point satisfying the conditions of Theorem* 3, *then the number of exceptional points is* 3, 6 *or* 12. *In particular, this is the case if* $8 \nmid A$.

Under the condition of the theorem, all exceptional points must *lead to an inflection by repeated forming of tangentials.* The exceptional group, of order n, can consequently not contain a sub-group of order p^k, p an odd prime, where $k \geqq 1$ for $p > 3$ and $k \geqq 2$ for $p = 3$. It follows that we must have $n = 3 \cdot 2^h$, $h = 0, 1, 2, \ldots$. However, Lind [6] has shown that $24 \nmid n$, which concludes the proof.

There are always at least three exceptional points (the inflections) on the symmetric curve. We shall now give parametric representations for the cases $n = 6$ and $n = 12$.

An exceptional sub-group of order 6 will contain the inflections (2.6) and three more points

$$(s, t, t), \quad (t, s, t), \quad (t, t, s)\,, \tag{5.1}$$

which have the inflections as tangentials. Substituting this in (2.3), we see that the equation

$$A(s+2t)^3 + Cst^2 = 0 \tag{5.2}$$

must have integral solutions s, t. We can then transform the points (5.1) into

$$(1, 0, 0), \quad (0, 1, 0), \quad (0, 0, 1) \tag{5.3}$$

by the symmetric substitution

$$X = s\xi+t\eta+t\zeta, \qquad Y = t\xi+s\eta+t\zeta, \qquad Z = t\xi+t\eta+s\zeta\,. \tag{5.4}$$

The determinant $(s-t)^2(s+2t) \neq 0$, and we find

$$\beta(\xi\eta+\xi\zeta+\eta\zeta)(\xi+\eta+\zeta) + \gamma\xi\eta\zeta = 0\,, \tag{5.5}$$

where $\beta = t$, $\gamma = s-t$.

The transformation (5.4) can of course be applied directly to the general symmetric curve (2.1) if this contains the rational points (5.1), leading again to an equation of the type (5.5). In particular, the *equianharmonic* case $c = -3b$ (which cannot be reduced to the form (2.3)) gives

$\beta = 1, \gamma = -3$. The curve (5.5) is then equivalent to the Weierstrass form (2.7) with $f = 1$.

The condition (2.2) takes the form

$$\beta\gamma(\beta+\gamma)(9\beta+\gamma) \neq 0 \,. \tag{5.6}$$

Theorem 6. *Under the condition* (5.6), *the form* (5.5) *will represent the general cubic curve with an exceptional sub-group of order six. The exceptional points are given by* (2.6) *and* (5.3).

A parametric representation of the invariants A and B in (1.2) for $n = 6$ has been given by Nagell [8, pp. 10–11]. Simpler expressions for the form

$$y^2 = x^3 + Mx^2 + Nx \tag{5.7}$$

were obtained by Lind [6, pp. 36-37].

6. Sub-groups of order twelve. An exceptional sub-group of order 12 can be cyclic or non-cyclic. In the latter case, *each inflection must be the tangential of three other points.* Substituting $\xi = \sigma$, $\eta = \zeta = \tau$ in (5.5), we find one root $\tau = 0$, corresponding to the points (5.3). The remaining roots are determined by the equation

$$2\beta\sigma^2 + (5\beta+\gamma)\sigma\tau + 2\beta\tau^2 = 0 \,,$$

of discriminant $(\beta+\gamma)(9\beta+\gamma) \neq 0$ by (5.6).

Theorem 7. *The general cubic curve with a non-cyclic exceptional sub-group of order twelve is represented by the form* (5.5), *satisfying* (5.6) *and with the further condition that* $(\beta+\gamma)(9\beta+\gamma)$ *is a square.*

This formulation makes it simple to decide if such a sub-group exists. As parametric representation, we may choose

$$\beta = 8^{-\varepsilon}(\lambda^2 - \mu^2), \qquad \gamma = 8^{-\varepsilon}(9\mu^2 - \lambda^2) \,. \tag{6.1}$$

Here λ and μ are coprime integers, subject to some obvious conditions obtained from (5.6). The exponent $\varepsilon = 1$ if λ and μ are both odd, and $= 0$ otherwise.

The corresponding representation for the form (1.2), as given by Bergman [1, p. 503], is very complicated. However, the formulae of Lind [6, p. 44] for the curve

$$y^2 = (x + U)(x + V)x$$

are quite simple (degree 4 in the parameters).

We now turn to the *cyclic* sub-group of order 12. There must then be a set of 6 exceptional points (ξ, η, ζ), with $\xi \neq \eta \neq \zeta \neq \xi$, such that each of the points (5.3) is *the tangential of two points* from the set.

We must determine ξ, η and ζ by the formulae (3.1) such that for instance

$$\beta\, F(\xi, \eta, \zeta) + \gamma \xi (\eta - \zeta)^2 = \beta\, F(\xi, \eta, \zeta) + \gamma \eta (\zeta - \xi)^2 = 0\,.$$

It is easily seen that these two equations, in connection with the given curve (5.5), are equivalent to the system

$$\xi\eta = \zeta^2, \qquad \beta(\xi+\eta+\zeta)^2 + \gamma\zeta^2 = 0\,.$$

We conclude that $(\zeta, \xi+\eta+\zeta) = (\zeta, \xi+\eta) = 1$. Assuming $\beta > 0$ (no restriction), we must consequently have

$$\beta = \beta_1^2, \quad \gamma = -\gamma_1^2; \qquad \xi+\eta+\zeta = \gamma_1, \quad \zeta = \beta_1\,.$$

It follows that ξ and η are the roots of an equation

$$\vartheta^2 + (\beta_1 - \gamma_1)\vartheta + \beta_1^2 = 0\,,$$

of discriminant $(\gamma_1+\beta_1)(\gamma_1-3\beta_1) \neq 0$ by (5.6).

THEOREM 8. *The general cubic curve with a cyclic exceptional sub-group of order twelve is represented by the form* (5.5), *satisfying* (5.6) *and with the further condition that* $\beta = \beta_1^2$, $\gamma = -\gamma_1^2$, *where* $(\gamma_1+\beta_1)(\gamma_1-3\beta_1)$ *is a square.*

A parametric representation is given by

$$(6.2) \qquad \beta = 16^{-\varepsilon}(\lambda^2 - \mu^2)^2, \qquad \gamma = -16^{-\varepsilon}(3\lambda^2 + \mu^2)^2,$$

with the same remarks as after (6.1).

The corresponding representation for the form (1.2), as given by Bergman [1, p. 504], is extremely complicated. The formulae of Lind [6, pp. 36–37] for the curve (5.7) are simpler, but still rather complicated.

We conclude with a weak but very simple theorem, reminiscent of the results obtained by Hurwitz for the curve (1.1). — It is clear from (5.2) that $t = \pm 1$ if all prime factors of A occur in odd powers. The transformation (5.4) gave $\beta = t$ in (5.5), but neither (6.1) nor (6.2) will represent $\beta = \pm 1$ under the condition (5.6), except in the one case $\lambda = 1$, $\mu = 3$ in (6.1), which implies $A = 3^2$. Combining this result with Theorem 5, we get the following

THEOREM 9. *If A is squarefree, the curve* (2.3) *has three or six exceptional points.*

REFERENCES

1. G. Bergman, *On the exceptional points of cubic curves*, Ark. Mat. 2 (1953), 489–535.
2. G. Billing, *Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht Eins*, Nova Acta Soc. Sci. Upsaliensis (4) 11 No. 1 (1938), 1–165.
3. G. Billing, *A diophantine equation with nine solutions*, Ark. Mat. Astr. Fys. 27B No. 8 (1940), 1–5.
4. H. Hilton, *Plane algebraic curves*, 2. ed., London, 1932.
5. A. Hurwitz, *Über ternäre diophantische Gleichungen dritten Grades*, Vierteljahrschr. Naturforsch. Ges. Zürich 62 (1917), 207–229.
6. C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Inaugural-Dissertation, Uppsala, 1940.
7. T. Nagell, *Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre*, Skr. Norske Vid. Akad. Oslo, Mat.-Naturv. Kl. No. 1 (1935), 1–25.
8. T. Nagell, *Recherches sur l'arithmétique des cubiques planes du premier genre dans un domaine de rationalité quelconque*, Nova Acta Soc. Sci. Upsaliensis (4) 15 No. 6 (1952), 1–66.
9. T. Nagell, *Sur la division des pèriodes de la fonction $\wp u$ et les points exceptionnels des cubiques*, Nova Acta Soc. Sci. Upsaliensis (4) 15 No. 8 (1953), 1–28.

UNIVERSITY OF OSLO, NORWAY