ARKIV FÖR MATEMATIK Band 2 nr 27

Communicated 8 October 1952 by F. CARLSON and T. NAGELL

On the exceptional points of cubic curves

By GÖSTA BERGMAN

§ 1

Introduction

1. If the curve

$$y^2 = x^3 - Ax - B \qquad (4A^3 - 27B^2 \neq 0) \tag{1}$$

is represented by the elliptic $\wp$-function with the invariants $4A$ and $4B$ and a primitive pair of periods ω, ω':

$$x = \wp(u); \quad y = \tfrac{1}{2}\wp'(u),$$

a point $(x; y)$ on (1) may be called *the point* u, where u is determined mod ω, ω'.

If the points u_1, u_2, u_3 lie on a straight line, we have

$$u_1 + u_2 + u_3 \equiv 0 \qquad (\text{mod } \omega, \omega').$$

It follows that the tangent in the point u cuts the curve in $-2u$. If the number u is commensurable with a period, and if n is the smallest natural number that makes nu a period, then u is called an *exceptional point of order* n; this notion has been introduced by NAGELL [11]. The point of order 1 is the infinite point of inflexion, the points of order 2 are given by $y = 0$, and the points of order 3 are the finite points of inflexion.

Now suppose that A and B belong to a field Ω. Then u is said to be a *point in* Ω, if its coordinates belong to this field. If u_1 and u_2 are exceptional points in Ω, the same is true of $u_1 + u_2$, and in this way the exceptional points in Ω form an Abelian group, the *exceptional group in* Ω on the curve (1) (see CHÂTELET [17]). If Ω is an algebraic field, it follows from a theorem due to WEIL [16] that this group is finite. If p is a prime, the group contains at most two independent elements of order p, since there are only two independent periods (see BILLING [1], p. 29); consequently a group of order

$$p_1^{\nu_1} p_2^{\nu_2} \ldots p_r^{\nu_r},$$

where $p_1, p_2, \ldots, p_r$ are differerent primes, may be of

$$\prod_{i=1}^{r}\left(1+\left[\frac{\nu_i}{2}\right]\right)$$

types, which will be denoted by

$$(p_1^{\lambda_1}, p_1^{\nu_1-\lambda_1}, \ldots, p_r^{\lambda_r}, p_r^{\nu_r-\lambda_r}),$$

where

$$\nu_i \leqq 2\lambda_i \leqq 2\nu_i \qquad (i=1, 2, \ldots, r).$$

Two independent elements of order p cannot occur, if p is an odd prime and Ω is real (see NAGELL [10], p. 105–108).

In the case $\Omega=k(1)$ the following result has been obtained by LEVI [7], HURWITZ [6], NAGELL [10], [15], BILLING [1]–[4], MAHLER [9] and LIND [8]:

Theorem 1. *There exist curves (1), whose exceptional groups in $k(1)$ are of the following types: (1), (2), (3), (2, 2), (4), (5), (2, 3), (7), (4, 2), (8), (9), (2, 5), (2, 2, 3), (4, 3) and (8, 2). There does not exist any curve (1), whose exceptional group in $k(1)$ contains a sub-group of the type (11), (2, 7), (3, 5), (16), (2, 2, 5), (4, 5), (4, 2, 3) or (8, 3).*

If $\Omega=k(\sqrt{-3})$, we may have the group (3, 3) (NAGELL [15]).

2. Sometimes it is possible to find parametric expressions for A and B, if the exceptional group in Ω on (1) has a given sub-group. The following results are due to NAGELL [13]–[15]; some substitutions have been made in order to simplify the formulas:

Theorem 2. *If there is a point of order 3 in Ω on the curve (1), A and B are given by the following formulas, where c and d are numbers in Ω which make $4A^3-27B^2\neq 0$:*

$$A=3(9c^3-2d)c;$$

$$-B=54c^6-18c^3d+d^2;$$

$$4A^3-27B^2=27d^3(4c^3-d).$$

A point of order 3 is $(3c^2; d)$.

Theorem 3. *If there is a point of order 5 in Ω on the curve (1), A and B are given by the following formulas, where m and n are numbers in Ω which make $4A^3-27B^2\neq 0$:*

$$A=27(m^4+12m^3n+14m^2n^2-12mn^3+n^4);$$

$$-B=54(m^2+n^2)(m^4+18m^3n+74m^2n^2-18mn^3+n^4);$$

$$4A^3-27B^2=-2^8\cdot 3^{12}m^5n^5(m^2+11mn-n^2).$$

The finite points of the group are:

$$\pm u \quad [3(m^2+6mn+n^2);\ \pm 108\, mn^2];$$

$$\pm 2u\ [3(m^2-6mn+n^2);\ \pm 108\, m^2 n].$$

Theorem 4. *If there is a point of order 7 in Ω on the curve (1), A and B are given by the following formulas, where δ, m and n are numbers in Ω which make $4A^3-27B^2\neq 0$:*

$$3A=\delta^4(m^2-mn+n^2)(m^6-11m^5n+30m^4n^2-15m^3n^3-10m^2n^4+5mn^5+n^6);$$

$$-27B=2\delta^6(m^{12}-18m^{11}n+117m^{10}n^2-354m^9n^3+570m^8n^4-486m^7n^5+$$
$$+273m^6n^6-222m^5n^7+174m^4n^8-46m^3n^9-15m^2n^{10}+6mn^{11}+n^{12});$$

$$4A^3-27B^2=2^8\delta^{12}m^7n^7(m-n)^7(m^3-8m^2n+5mn^2+n^3).$$

The finite points of the group are:

$$\pm u \quad [\tfrac{1}{3}\delta^2(m^4+6m^3n-9m^2n^2+2mn^3+n^4);\ \pm 4\delta^3m^3n(m-n)^2];$$

$$\pm 2u\ [\tfrac{1}{3}\delta^2(m^4-6m^3n+15m^2n^2-10mn^3+n^4);\ \pm 4\delta^3mn^2(m-n)^3];$$

$$\pm 3u\ [\tfrac{1}{3}\delta^2(m^4-6m^3n+3m^2n^2+2mn^3+n^4);\ \pm 4\delta^3m^2n^3(m-n)].$$

NAGELL [13], [15] has also found parametric formulas corresponding to systems of the types (2, 2), (4), (2, 3), (3, 3) and (9). Under the assumption $\Omega=k(1)$ LIND [8] has investigated the cases (4, 2), (8), (2, 5), (2, 2, 3), (4, 3) and (8, 2).

3. If $B=0$, we get the *harmonic* curve

$$y^2=x^3-Ax. \tag{2}$$

Its exceptional group in $k(1)$ is given by the following theorem due to NAGELL ([11], p. 17–18):

Theorem 5. *If A is rational, the curve (2) has the following exceptional group in $k(1)$:*

$$(2), \quad \text{if } A\neq C^2,\ \neq -4C^4;$$

$$(2,2), \quad \text{if } A=C^2;$$

$$(4), \quad \text{if } A=-4C^4.$$

Here C denotes any rational number.

If $A=0$, we get the *equianharmonic* curve

$$y^2=x^3-B. \tag{3}$$

Its exceptional group in $k(1)$ is given by the following result due to FUETER [5]:

Theorem 6. *If B is rational, the curve (3) has the following exceptional group in $k(1)$:*

(1), if $B \neq C^3$, $\neq -C^2$, $\neq 432\,C^6$;

(2), if $B = C^3$, $\neq -C^6$;

(3), if $B = -C^2$ or $= 432\,C^6$ but $\neq -C^6$;

(2, 3), if $B = -C^6$.

Here C denotes any rational number.

4. In this paper we shall determine parametric expressions for A and B corresponding to groups of the types (4, 2), (8), (2, 5), (2, 2, 3), (4, 3), (4, 4), (8, 2) and (2, 3, 3). Further, we shall find the exceptional groups on the curves (2) and (3) in algebraic fields of degree n, where $n = 2, 4$ or an odd number in the harmonic case, and $n = 2, 3$ or a number indivisible by 2 and 3 in the equianharmonic case.

§ 2

Some properties of the $\wp$-function

5. If n is a natural number and the function $\psi_n(u)$ is defined by

$$\psi_n(u) = \frac{\sigma(nu)}{[\sigma(u)]^{n^2}},$$

it is known that

$$\psi_n(u) = \begin{cases} P_n[\wp(u)], & \text{if } n \text{ is odd,} \\ \wp'(u)\,Q_n[\wp(u)], & \text{if } n \text{ is even,} \end{cases}$$

where P_n and Q_n are polynomials.

As usual we put $\wp(u) = x$ and $\wp'(u) = 2y$. Then

$$4y^2 = 4x^3 - 4Ax - C, \text{ where } C = 4B,$$

$$P_1(x) = 1,\ Q_2(x) = -1,$$

$$P_3(x) = 3x^4 - 6Ax^2 - 3Cx - A^2,$$

$$Q_4(x) = -2x^6 + 10Ax^4 + 10Cx^3 + 10A^2x^2 + 2ACx - (2A^3 - C^2)$$

and

$$\begin{cases} P_{4r+1} = (4y^2)^2 Q_{2r+2} Q_{2r}^3 - P_{2r-1} P_{2r+1}^3, \\ Q_{4r+2} = P_{2r+1} [P_{2r-1} Q_{2r+2}^2 - P_{2r+3} Q_{2r}^2], \\ P_{4r+3} = P_{2r+3} P_{2r+1}^3 - (4y^2)^2 Q_{2r} Q_{2r+2}^3, \\ Q_{4r+4} = Q_{2r+2} [Q_{2r} P_{2r+3}^2 - Q_{2r+4} P_{2r+1}^2] \end{cases} \tag{4}$$

for $r > 0$. Consequently

$$P_5 = -(16y^4 Q_4 + P_3^3) = 5x^{12} - 62Ax^{10} - 95Cx^9 - 105A^2x^8 + 60ACx^7 +$$
$$+ 15(20A^3 - C^2)x^6 + 174A^2Cx^5 - 5(25A^3 - 24C^2)Ax^4 - 5(4A^3 - 5C^2)Cx^3 +$$
$$+ 5(10A^3 - 3C^2)A^2x^2 + 5(5A^3 - 2C^2)ACx + (A^6 + 2A^3C^2 - C^4),$$

$$Q_6 = P_3(Q_4^2 - P_5),$$

$$P_7 = P_5 P_3^3 + 16y^4 Q_4^3,$$

$$Q_8 = -Q_4(P_5^2 + Q_6 P_3^2)$$

and generally

$$P_n(x) = n x^{\frac{1}{2}(n^2-1)} + \alpha_{n,2} x^{\frac{1}{2}(n^2-1)-2} + \cdots + \alpha_{n,\frac{1}{2}(n^2-1)},$$

$$Q_n(x) = -\tfrac{1}{2} n x^{\frac{1}{2}(n^2-4)} + \beta_{n,2} x^{\frac{1}{2}(n^2-4)-2} + \cdots + \beta_{n,\frac{1}{2}(n^2-4)},$$

where $\alpha_{n,m}$ and $\beta_{n,m}$ are polynomials in A and C with integral coefficients.

If nu is not a period, it is also known that

$$\wp(nu) = \begin{cases} x - \dfrac{4y^2 Q_{n+1} Q_{n-1}}{P_n^2}, & \text{if } n \text{ is odd;} \\ x - \dfrac{P_{n+1} P_{n-1}}{4y^2 Q_n^2}, & \text{if } n \text{ is even.} \end{cases} \tag{5}$$

Particularly we find

$$\wp(2u) = \frac{(x^2 + A)^2 + 8Bx}{4y^2},$$

which may be written

$$\wp(2u) + 2x = \left(\frac{3x^2 - A}{2y}\right)^2.$$

In the formula

$$\wp'(u) = -\psi_2(u) = -\frac{\sigma(2u)}{[\sigma(u)]^4}$$

we change u into nu and find

$$\wp'(nu) = -\frac{\sigma(2nu)}{[\sigma(nu)]^4} = -\frac{\psi_{2n}(u)}{[\psi_n(u)]^4}.$$

If neither nu nor $2u$ is a period, it follows that

$$\frac{\wp'(nu)}{\wp'(u)} = \begin{cases} -\dfrac{Q_{2n}}{P_n^4}, & \text{if } n \text{ is odd;} \\ -\dfrac{Q_{2n}}{16\,y^4\,Q_n^4}, & \text{if } n \text{ is even.} \end{cases} \tag{6}$$

6. In the harmonic case the preceding formulas are simplified in the following way:

$$\begin{cases} P_3 = 3x^4 - 6Ax^2 - A^2; \\ Q_4 = -2(x^2+A)(x^4 - 6Ax^2 + A^2); \\ P_5 = (5x^4 - 2Ax^2 + A^2)(x^8 - 12Ax^6 - 26A^2x^4 + 52A^3x^2 + A^4); \\ Q_6 = -(3x^4 - 6Ax^2 - A^2)(x^4 + 6Ax^2 - 3A^2)(x^8 - 28Ax^6 + 6A^2x^4 - \\ \qquad - 28A^3x^2 + A^4); \\ P_7 = 7x^{24} - 7.44Ax^{22} - 7.422A^2x^{20} + 7.2836A^3x^{18} - 7.5033A^4x^{16} + \\ \qquad + 7.11752A^5x^{14} - 7.15988A^6x^{12} + 7.6024A^7x^{10} + 7.2239A^8x^8 - \\ \qquad - 7.2108A^9x^6 + 7.186A^{10}x^4 - 7.28A^{11}x^2 - A^{12}; \end{cases} \tag{7}$$

$$\wp(2u) = \left(\frac{x^2+A}{2y}\right)^2. \tag{8}$$

In the equianharmonic case we get the following expressions:

$$\begin{cases} P_3 = 3x(x^3 - C); \\ Q_4 = -2x^6 + 10Cx^3 + C^2; \\ P_5 = 5x^{12} - 95Cx^9 - 15C^2x^6 + 25C^3x^3 - C^4; \\ Q_6 = -3x(x^3 - C)(x^{12} - 55Cx^9 - 111C^2x^6 + 5C^3x^3 - 2C^4); \\ P_7 = (7x^6 + Cx^3 + C^2)(x^{18} - 141Cx^{15} - 363C^2x^{12} + 1924C^3x^9 - 741C^4x^6 + \\ \qquad + 48C^5x^3 + C^6). \end{cases} \tag{9}$$

7. If A is given the degree 2 and B the degree 3, it is easily shown by induction that P_n or Q_n is homogeneous of degree $\frac{1}{2}(n^2-1)$ or $\frac{1}{2}(n^2-4)$, according as n is odd or even.

It also follows from the formulas (4) that in the case $A=1$, $B=0$

$$P_n(0) = (-1)^{\frac{1}{4}(n-1)} \quad \text{and} \quad P_n(1) = P_n(-1) = (-1)^{\frac{1}{4}(n-1)} \cdot 2^{\frac{1}{4}(n^2-1)}.$$

Let p be an odd prime, put $p^2-1=8N$, and let $x_1, x_2, \ldots, x_{4N}$ be the roots of $P_p(x)=0$, while $\pm y_1, \pm y_2, \ldots, \pm y_{4N}$ are the corresponding values of y. Then

$$\prod_{i=1}^{4N} y_i^2 = \prod_{i=1}^{4N} (x_i^3 - A x_i - B) = c_0 A^{6N} + c_1 A^{6N-3} B^2 + \cdots + c_{2N} B^{4N}, \tag{10}$$

where $c_0, c_1, \ldots, c_{2N}$ are certain constants. Since the numbers y_i are always $\neq 0$, the last member of (10) may be written

$$k_p (4A^3 - 27B^2)^{2N}.$$

In order to determine k_p we put $A=1$ and $B=0$. Then

$$\prod_{i=1}^{4N} y_i^2 = \prod_1^{4N} x_i \prod_1^{4N} (x_i - 1) \prod_1^{4N} (x_i + 1) = \frac{1}{p^3} P_p(0) P_p(1) P_p(-1) =$$

$$= \frac{1}{p^3} (-1)^{\frac{1}{2}(p-1)} \cdot 2^{4N}, \quad \text{and hence} \quad k_p = \frac{1}{p^3} (-1)^{\frac{1}{2}(p-1)}.$$

But then

$$\pm \prod_1^{4N} y_i = \frac{1}{p^2} (4A^3 - 27B^2)^N \sqrt{(-1)^{\frac{1}{2}(p-1)} p},$$

and we have proved the following theorem:

Theorem 7. *Let p be an odd prime, and let Ω be a field which contains A and B. If the exceptional group in Ω on the curve (1) has a sub-group of the type (p, p), then the number*

$$\sqrt{(-1)^{\frac{1}{2}(p-1)} p}$$

belongs to Ω.

§ 3.

Parametric expressions for A and B corresponding to certain systems of exceptional points

8. Let A and B belong to the arbitrary field Ω, and suppose that the equation

$$z^3 - Az - B = 0 \tag{11}$$

has a solution $z = \frac{1}{3}M$ in Ω. Then we may transform the curve (1) into

$$\eta^2 = \xi^3 + M\xi^2 + N\xi \tag{12}$$

by introducing the variables

$$\xi = x - \tfrac{1}{3}M; \quad \eta = y,$$

but it must be observed that the representation (12) is not unique, if (11) has more than one root in Ω.

Conversely, if (12) is given, A and B are determined by

$$\begin{cases} 3A = M^2 - 3N; \\ -27B = M(2M^2 - 9N). \end{cases} \tag{13}$$

Further,

$$D = 4A^3 - 27B^2 = N^2(M^2 - 4N).$$

If the tangent to (12) in the point $(\xi_1; \eta_1)$ cuts the curve in $(\xi_2; \eta_2)$, we have

$$\xi_2 = \left(\frac{\xi_1^2 - N}{2\eta_1}\right)^2, \tag{14}$$

and this formula may be transformed into

$$\left[\xi_1^2 - 2\left(\xi_2 + \frac{\eta_2}{\sqrt{\xi_2}}\right)\xi_1 + N\right]\left[\xi_1^2 - 2\left(\xi_2 - \frac{\eta_2}{\sqrt{\xi_2}}\right)\xi_1 + N\right] = 0. \tag{15}$$

(Compare LIND [8], p. 19–20.)

9. We begin with five cases, where a group of order 2^ν is given. The first theorem is due to NAGELL ([13], p. 20).

Theorem 8. *If the curve (1) has a point of order 4 in a field Ω, it is given by*

$$3A = a^2(a^2 - 4ac + c^2),$$

$$-27B = a^3(a - 2c)(2a^2 - 8ac - c^2),$$

$$D = a^7 c^4 (a - 4c),$$

where a and c are numbers in Ω and $D \neq 0$.

Proof. We may use the equation (12) and suppose that the tangent in $(\xi_1; \eta_1)$ cuts the curve in $(0; 0)$. Then, by (14), $N = \xi_1^2$, and M is determined by

$$\eta_1^2 = \xi_1^3 + M\xi_1^2 + N\xi_1 = \xi_1^2(2\xi_1 + M).$$

Since $\xi_1 \eta_1 \neq 0$, we may put $\eta_1 = \xi_1 a$ and $\xi_1 = ac$, and hence

$$M = a(a - 2c); \quad N = a^2 c^2.$$

Finally A and B are given by (13).

Theorem 9. *If some exceptional points in Ω on the curve (1) form a group of the type (4, 2), the curve is given by*

$$3A = \delta^4 n^4 (m^4 - 2m^3 n + 5m^2 n^2 - 4mn^3 + n^4),$$

$$27B = \delta^6 n^6 (2m^2 - 2mn + n^2)(m^2 + 2mn - n^2)(m^2 - 4mn + 2n^2),$$

$$D = \delta^{12} m^4 n^{14} (m-n)^4 (2m-n)^2,$$

where δ, m, n are numbers in Ω and $D \neq 0$.

Proof. Let z_1, z_2, z_3 be the roots of (11). In this case these numbers belong to Ω, and hence

$$D = [(z_1 - z_2)(z_1 - z_3)(z_2 - z_3)]^2$$

is a square. Since there is also a point of order 4 in Ω, the preceding theorem may be applied, and consequently we can put

$$a(a - 4c) = e^2,$$

where a, c, e are numbers in Ω. If this curve is cut by the straight line

$$c = \frac{m}{2n}(a - e),$$

we find

$$\begin{cases} a = \delta n^2, \\ c = \delta m (n - m), \\ e = \delta n (2m - n), \end{cases}$$

where δ, m, n may be supposed to be numbers in Ω. If M is chosen as in theorem 8, the group contains the following finite points on the curve (12):

$$\pm u_1 \ [\delta^2 mn^2 (m-n);\ \pm \delta^3 mn^3 (m-n)(2m-n)];$$

$$2u_1 \ [0;\ 0];$$

$$u_2 \ [-\delta^2 m^2 n^2;\ 0];$$

$$2u_1 + u_2 \ [-\delta^2 n^2 (m-n)^2;\ 0];$$

$$\pm u_1 + u_2 \ [-\delta^2 mn^2 (m-n);\ \mp \delta^3 mn^4 (m-n)].$$

Finally,

$$M = \delta^2 n^2 (2m^2 - 2mn + n^2);$$

$$N = \delta^4 m^2 n^4 (m-n)^2.$$

Theorem 10. *If the curve (1) has a point of order 8 in Ω, it is given by*

$$3A = \delta^4 (a^8 - 8a^7 c + 12a^6 c^2 + 8a^5 c^3 - 10a^4 c^4 + 8a^3 c^5 + 12a^2 c^6 - 8ac^7 + c^8),$$

$$-27B = 2\delta^6 (a^4 - 4a^3 c - 2a^2 c^2 - 4ac^3 + c^4)(a^8 - 8a^7 c + 12a^6 c^2 + 8a^5 c^3 - 34a^4 c^4 + 8a^3 c^5 + 12a^2 c^6 - 8ac^7 + c^8),$$

$$D = 2^8 \delta^{12} a^8 c^8 (a-c)^4 (a+c)^2 (a^2 - 6ac + c^2),$$

where δ, a, c are numbers in Ω and $D \neq 0$.

Proof. Let u be a point of order 8 on the curve

$$y^2 = x^3 - A_0 x - B_0,$$

and let the point $4u$ have the abscissa $\frac{1}{3} M_0$. Then the curve may be transformed into

$$\eta^2 = \xi^3 + M_0 \xi^2 + N_0 \xi.$$

The points u and $2u$ on this curve will be denoted by $(\xi_1; \eta_1)$ and $(\xi_2; \eta_2)$, respectively. Then, by (14),

$$\xi_2 = \left(\frac{\xi_1^2 - N_0}{2\eta_1}\right)^2 \quad \text{and} \quad N_0 = \xi_2^2.$$

Since $\xi_2 \neq 0$, we may put

$$\frac{\xi_1^2 - N_0}{2\eta_1} = a \quad \text{and} \quad \xi_1 = ac,$$

and hence

$$\xi_2 = a^2; \quad N_0 = a^4; \quad 2\eta_1 = a(c^2 - a^2)$$

and

$$4c^2 M_0 = a^4 - 4a^3 c - 2a^2 c^2 - 4ac^3 + c^4.$$

In order to avoid fractional expressions for A and B we multiply a and c by $2\delta c$. The curve (12) obtained in this way will have the coefficients

$$M = \delta^2 (a^4 - 4a^3 c - 2a^2 c^2 - 4ac^3 + c^4),$$

$$N = 16\delta^4 a^4 c^4,$$

and the curve (1) is given by (13).

The group contains the following finite points on the curve (12):

$$\pm u \quad [4\delta^2 ac^3;\ \pm 4\delta^3 ac^3 (c^2 - a^2)];$$

$$\pm 2u\ [4\delta^2 a^2 c^2;\ \pm 4\delta^3 a^2 c^2 (a-c)^2];$$

$$\pm 3u\ [4\delta^2 a^3 c;\ \pm 4\delta^3 a^3 c (c^2 - a^2)];$$

$$4u\ [0;\ 0].$$

Theorem 11. *If some exceptional points in Ω on the curve (1) form a group of the type (8, 2), the curve is given by*

$$3A = \delta^4 (m^{16} - 8m^{14}n^2 + 12m^{12}n^4 + 8m^{10}n^6 + 230m^8n^8 + 8m^6n^{10} + 12m^4n^{12} - \\ - 8m^2n^{14} + n^{16}),$$

$$-27B = 2\delta^6 (m^8 - 4m^6n^2 + 22m^4n^4 - 4m^2n^6 + n^8)(m^8 - 4m^6n^2 - 26m^4n^4 - \\ - 4m^2n^6 + n^8)(m^8 - 4m^6n^2 - 2m^4n^4 - 4m^2n^6 + n^8),$$

$$D = 2^8 \delta^{12} m^8 n^8 (m+n)^8 (m-n)^8 (m^2+n^2)^4 (m^2+2mn-n^2)^2 (m^2-2mn-n^2)^2,$$

where δ, m, n are numbers in Ω and $D \neq 0$.

Proof. We use the formulas of the preceding theorem and suppose D to be a square, since the three roots of (11) belong to Ω. Thus

$$a^2 - 6ac + c^2 = e^2,$$

and if this curve is cut by the straight line

$$c - e = \frac{2m+n}{n} a,$$

we find

$$\begin{cases} a = \delta n (m-n), \\ c = \delta m (m+n), \\ e = -\delta (m^2 - 2mn - n^2), \end{cases}$$

where δ, m, n may be supposed to belong to Ω.

If M is chosen as in theorem 10, the group contains the following finite points on the curve (12):

$$\pm u_1 \ [4\delta^2 m^3 n (m+n)^3 (m-n); \\ \pm 4\delta^3 m^3 n (m+n)^3 (m-n)(m^2+n^2)(m^2+2mn-n^2)];$$

$$\pm 2u_1 \ [4\delta^2 m^2 n^2 (m^2-n^2)^2; \ \pm 4\delta^3 m^2 n^2 (m^2-n^2)^2 (m^2+n^2)^2];$$

$$\pm 3u_1 \ [4\delta^2 mn^3 (m+n)(m-n)^3; \\ \pm 4\delta^3 mn^3 (m+n)(m-n)^3 (m^2+n^2)(m^2+2mn-n^2)];$$

$$4u_1 \ [0; 0];$$

$$u_2 \ [-16\delta^2 m^4 n^4; 0];$$

$$\pm u_1 + u_2 \ [-4\delta^2 mn^3 (m+n)^3 (m-n); \\ \pm 4\delta^3 mn^3 (m+n)^3 (m-n)(m^2+n^2)(m^2-2mn-n^2)];$$

$$\pm 2\,u_1 + u_2 \;[-4\,\delta^2 m^2 n^2 (m^2-n^2)^2;$$
$$\pm 4\,\delta^3 m^2 n^2 (m^2-n^2)^2 (m^2+2\,mn-n^2)(m^2-2\,mn-n^2)];$$
$$\pm 3\,u_1 + u_2 \;[-4\,\delta^2 m^3 n (m+n)(m-n)^3;$$
$$\pm 4\,\delta^3 m^3 n (m+n)(m-n)^3 (m^2+n^2)(m^2-2\,mn-n^2)];$$
$$4\,u_1 + u_2 \;[-\delta^2 (m^2-n^2)^4;\; 0].$$

Finally,

$$M = \delta^2 (m^8 - 4\,m^6 n^2 + 22\,m^4 n^4 - 4\,m^2 n^6 + n^8);$$
$$N = 16\,\delta^4 m^4 n^4 (m^2-n^2)^4.$$

Theorem 12. *If some exceptional points in Ω on the curve (1) form a group of the type (4, 4), then Ω contains $\sqrt{-1}$, and the curve is given by*

$$3A = \delta^4 (a^8 + 14\,a^4 c^4 + c^8),$$
$$27\,B = 2\,\delta^6 (a^4+c^4)(a^2+2\,ac-c^2)(a^2-2\,ac-c^2)(a^4+6\,a^2 c^2+c^4),$$
$$D = 2^4 \delta^{12} a^4 c^4 (a^4-c^4)^4,$$

where δ, a, c are numbers in Ω and $D \neq 0$.

Proof. In this case the curve (12) may be written

$$\eta^2 = \xi (\xi - U)(\xi - V).$$

Suppose that the tangents in $(\xi_1; \eta_1)$ and $(\xi_2; \eta_2)$ cut this curve in $(U; 0)$ and $(0; 0)$, respectively. By (14)

$$\left(\frac{\xi_1^2 - U V}{2\,\eta_1}\right)^2 = U.$$

Thus $U = e^2$, and by (15) $\xi_1 = e^2 \pm e\sqrt{e^2 - V} = e(e+g)$, where $V = e^2 - g^2$.

On the other hand, the formula (14) gives

$$\xi_2^2 = U V.$$

Thus $\xi_2^2 = e^2 V$ and consequently $V = f^2$. Now e, f, and g are related by

$$e^2 = f^2 + g^2,$$

and if this curve is cut by the straight line

$$e - g = \frac{c}{a} f,$$

we find

$$\begin{cases} e = \delta (a^2 + c^2), \\ f = 2 \delta a c, \\ g = \delta (a^2 - c^2), \end{cases}$$

where δ, a, c are numbers in Ω. Now

$$M = -(U+V) = -\delta^2 (a^4 + 6 a^2 c^2 + c^4),$$
$$N = U V = 4 \delta^4 a^2 c^2 (a^2 + c^2)^2,$$

and the group contains the following finite points on the curve (12):

$$\pm u_1 \ [2 \delta^2 a^2 (a^2 + c^2);\ \pm 2 \delta^3 a^2 (a^4 - c^4)];$$
$$\pm u_2 \ [-2 \delta^2 a c (a^2 + c^2);\ \pm 2 i \delta^3 a c (a^2 + c^2) (a + c)^2];$$
$$\pm (u_1 + u_2) \ [-2 i \delta^2 a c (a + c i)^2;\ \mp 2 \delta^3 a c (a^2 - c^2) (a + c i)^2];$$
$$\pm (u_1 - u_2) \ [2 i \delta^2 a c (a - c i)^2;\ \mp 2 \delta^3 a c (a^2 - c^2) (a - c i)^2];$$
$$\pm u_1 + 2 u_2 \ [2 \delta^2 c^2 (a^2 + c^2);\ \mp 2 \delta^3 c^2 (a^4 - c^4)];$$
$$2 u_1 \pm u_2 \ [2 \delta^2 a c (a^2 + c^2);\ \mp 2 i \delta^3 a c (a^2 + c^2) (a - c)^2];$$
$$2 u_1 \ [\delta^2 (a^2 + c^2)^2;\ 0];$$
$$2 u_2 \ [0;\ 0];$$
$$2 u_1 + 2 u_2 \ [4 \delta^2 a^2 c^2;\ 0].$$

10. As was shown by LIND ([8], p. 32, 44), a point of order 16 in $k(1)$ is impossible. However, in theorem 10 we may choose $\delta = c = 1$ and $a = h^2$, where h is a rational integer different from 0 and ± 1. Let the tangent in a point $(\xi_0;\ \eta_0)$ on the curve (12) pass through the point $-u$, whose coordinates are

$$[4 h^2;\ 4 h^2 (h^4 - 1)].$$

Then (15) takes the form

$$[\xi_0^2 - 4 h (h^4 + 2 h - 1) \xi_0 + 16 h^8] [\xi_0^2 + 4 h (h^4 - 2 h - 1) \xi_0 + 16 h^8] = 0.$$

One root of this equation is

$$\xi_0 = 2 h [h^4 + 2 h - 1 + (h - 1) \sqrt{(h^4 - 1) (h^2 + 2 h - 1)}].$$

Since $-4 h \eta_0 = \xi_0^2 - N$, the point (ξ_0, η_0) belongs to the field generated by $\sqrt{(h^4 - 1) (h^2 + 2 h - 1)}$, and it is easily seen that we obtain in this way an infinity of quadratic fields:

Theorem 13. *A point of order 16 on the curve (1) is possible in an infinity of quadratic fields. We may even suppose A and B to be rational.*

If there is a group of the type (8, 4) in Ω on the curve (1), we may suppose u to be a point of order 8 and define M by $\frac{1}{3}M = \wp(4u)$. Then the abscissa of the point $2u$ on the curve (12) ought to be a square, and hence, by theorem 12,

$$2ac(a^2+c^2) = e^2,$$

where a, c, e are numbers in Ω and $ac(a^4-c^4) \neq 0$. If we put

$$\begin{cases} ai = cX, \\ e = c^2(1+i)Y, \end{cases}$$

we must have

$$Y^2 = X^3 - X.$$

According to NAGELL ([12], p. 11–19) the only solutions of this equation in $k(\sqrt{-1})$ are $X = 0, \pm 1, \pm i$, but these values cannot be used, since they make $D = 0$. It follows that the group (8, 4) is impossible in $k(\sqrt{-1})$.

However, in theorem 12 we may choose

$$\begin{cases} a = -m^2 + 2m + 1, \\ c = m^2 + 2m - 1, \\ \delta = 1, \end{cases}$$

where m is a rational integer different from 0 and ± 1. Then the point u_1 gets the following coordinates:

$$[4(m^2+1)^2(m^2-2m-1)^2;\ -32m(m^2-1)(m^2+1)^2(m^2-2m-1)^2],$$

and by (15) the tangent in (ξ_0, η_0) passes through this point, if

$$\xi_0 = 4(m^2+1)(m^2-2m-1)[m^4+2m^3-6m-1+4(m+1)\sqrt{m(1-m^2)}]$$

and

$$\frac{\xi_0^2 - N}{2\eta_0} = 2(m^2+1)(m^2-2m-1).$$

Since $\sqrt{m(1-m^2)}$ generates an infinity of quadratic fields, we have the following result:

Theorem 14. *A group of the type (8, 4) on the curve (1) is impossible in $k(\sqrt{-1})$ but exists in an infinity of quartic fields $k(\sqrt{-1}, \sqrt{d})$, where d is a natural number. We may even suppose A and B to be rational.*

11. In the remaining cases there is a point of order 6 or 10 in Ω. Theorem 15 is due to NAGELL ([10], p. 120–122).

Theorem 15. *If the curve (1) has a point of order 6 in Ω, it is given by*

$$3A = (s+t)(s^3+3s^2t-3st^2+t^3),$$

$$-27B = (s^2+2st-2t^2)(2s^4+8s^3t+2st^3-t^4),$$

$$D = s^3t^6(2s-t)^2(s+4t),$$

where s and t are numbers in Ω and $D \neq 0$.

Proof. If $(a; c)$ is a point of inflexion on the curve (12), the equation (14) gives

$$a = \left(\frac{a^2-N}{2c}\right)^2 \neq 0.$$

Thus if we put $a^2-N = 2ct$ and $c = st^2$, we find $a = t^2$ and

$$M = s^2+2st-2t^2;$$

$$N = t^3(t-2s).$$

The group contains the following finite points on the curve (12):

$$\pm u \quad [t(t-2s);\ \pm st(t-2s)];$$

$$\pm 2u\ [t^2;\ \pm st^2);$$

$$3u\ [0;\ 0).$$

Theorem 16. *If some exceptional points in Ω on the curve (1) form a group of the type (2, 2, 3), the curve is given by*

$$3A = \delta^4(m^2+mn+n^2)(m^6+3m^5n-5m^3n^3+3mn^5+n^6),$$

$$-27B = \delta^6(2m^4+4m^3n-2mn^3-n^4)(m^4+2m^3n+2mn^3+n^4)\cdot$$
$$\cdot(m^4+2m^3n-4mn^3-2n^4),$$

$$D = \delta^{12}m^6n^6(m+n)^6(m-n)^2(m+2n)^2(2m+n)^2,$$

where δ, m, n are numbers in Ω and $D \neq 0$.

Proof. Theorem 15 may be applied, but in this case D ought to be a square, since the three roots of (11) belong to Ω. Thus

$$s(s+4t) = r^2,$$

and if this curve is cut by the straight line

$$t=\frac{m}{2n}(s-r),$$

we find

$$\begin{cases} r=-\delta n(2m+n), \\ s=\delta n^2, \\ t=\delta m(m+n), \end{cases}$$

where δ, m, n may be supposed to belong to Ω. Now

$$M=\delta^2(-2m^4-4m^3n+2mn^3+n^4),$$
$$N=\delta^4 m^3(m+n)^3(m-n)(m+2n),$$

and the group contains the following finite points on the curve (12):

$$\begin{aligned}
\pm u_1 &\ [\delta^2 m(m^2-n^2)(m+2n);\ \pm\delta^3 mn^2(m^2-n^2)(m+2n)]; \\
\pm 2u_1 &\ [\delta^2 m^2(m+n)^2;\ \pm\delta^3 m^2 n^2(m+n)^2]; \\
3u_1 &\ [0;\ 0]; \\
u_2 &\ [\delta^2 m^3(m+2n);\ 0]; \\
\pm u_1+u_2 &\ [\delta^2 m^2(m^2-n^2);\ \mp\delta^3 m^2 n(m^2-n^2)(2m+n)]; \\
\pm 2u_1+u_2 &\ [\delta^2 m(m+n)^2(m+2n);\ \mp\delta^3 mn(m+n)^2(m+2n)(2m+n)]; \\
3u_1+u_2 &\ [\delta^2(m+n)^3(m-n);\ 0].
\end{aligned}$$

Theorem 17. *If the curve (1) has a point of order 12 in Ω, it is given by*

$$\begin{aligned}
3A=&\ \delta^4(m^4+2m^3n+2mn^3+n^4)(m^{12}+6m^{11}n+12m^{10}n^2+14m^9n^3+3m^8n^4- \\
&-12m^7n^5-24m^6n^6-12m^5n^7+3m^4n^8+14m^3n^9+12m^2n^{10}+ \\
&+6mn^{11}+n^{12}),
\end{aligned}$$

$$\begin{aligned}
-27B=&\ 2\delta^6(m^8+4m^7n+4m^6n^2+4m^5n^3-2m^4n^4+4m^3n^5+4m^2n^6+ \\
&+4mn^7+n^8)(m^{16}+8m^{15}n+24m^{14}n^2+40m^{13}n^3+44m^{12}n^4+ \\
&+24m^{11}n^5-32m^{10}n^6-88m^9n^7-114m^8n^8-88m^7n^9-32m^6n^{10}+ \\
&+24m^5n^{11}+44m^4n^{12}+40m^3n^{13}+24m^2n^{14}+8mn^{15}+n^{16}),
\end{aligned}$$

$$D=2^8\delta^{12}m^{12}n^{12}(m+n)^6(m-n)^2(m^2+mn+n^2)^4(m^2+n^2)^3(m^2+4mn+n^2),$$

where δ, m, n are numbers in Ω and $D\neq 0$.

Proof. Let u be a point of order 12 on the curve (1) and define M by $\frac{1}{3}M = \wp(6u)$. Then the theorems 8 and 15 may be applied and give two expressions for M and N:

$$\begin{cases} M = a^2 - 2e = s^2 + 2st - 2t^2, \\ N = e^2 = t^3(t - 2s), \end{cases}$$

where e has been substituted for ac. If e is eliminated, we get

$$4a^2t^2 + 4s(s^2 - a^2)t + (s^2 - a^2)^2 = 0,$$

and hence, since $a \neq 0$,

$$t = \frac{1}{2a^2}(s^2 - a^2)(-s \pm \sqrt{s^2 - a^2}) = \frac{1}{2a^2}(s^2 - a^2)(b - s),$$

where

$$s^2 = a^2 + b^2.$$

If this curve is cut by the straight line

$$b + s = \frac{m+n}{m-n}a,$$

we find

$$\begin{cases} a = \delta(m+n)^2(m^2 - n^2); \\ b = \delta(m+n)^2 \cdot 2mn; \\ s = \delta(m+n)^2(m^2 + n^2). \end{cases}$$

Consequently $t = -2\delta m^2 n^2$ and

$$M = \delta^2(m^8 + 4m^7 n + 4m^6 n^2 + 4m^5 n^3 - 2m^4 n^4 + 4m^3 n^5 + 4m^2 n^6 + 4mn^7 + n^8);$$

$$N = 16\delta^4 m^6 n^6 (m^2 + mn + n^2)^2.$$

The group contains the following finite points on the curve (12):

$$\pm u \quad [-4\delta^2 mn^5(m^2 + mn + n^2);\ \pm 4\delta^3 mn^5(m^2 + mn + n^2)(m^4 - n^4)];$$

$$\pm 2u\ [4\delta^2 m^2 n^2 (m^2 + mn + n^2)^2;\ \pm 4\delta^3 m^2 n^2 (m^2 + mn + n^2)^2 (m+n)^2 (m^2 + n^2)];$$

$$\pm 3u\ [-4\delta^2 m^3 n^3 (m^2 + mn + n^2);\ \pm 4\delta^3 m^3 n^3 (m^2 + mn + n^2)(m+n)^3 (m-n)];$$

$$\pm 4u\ [4\delta^2 m^4 n^4;\ \pm 4\delta^3 m^4 n^4 (m+n)^2 (m^2 + n^2)];$$

$$\pm 5u\ [-4\delta^2 m^5 n (m^2 + mn + n^2);\ \pm 4\delta^3 m^5 n (m^2 + mn + n^2)(m^4 - n^4)];$$

$$6u\ [0; 0].$$

Theorem 18. *If some exceptional points in Ω on the curve (1) form a group of the type (2, 3, 3), then $\sqrt{-3}$ belongs to Ω, and the curve is given by*

$$A = \delta^4 (s^3 - \sqrt{-3}\, s^2 t - 3 s t^2 + \sqrt{-3}\, t^3)(\sqrt{-3}\, s^3 + 3 s^2 t - \sqrt{-3}\, s t^2 - t^3) \cdot$$
$$\cdot (-\sqrt{-3}\, s^6 - 6 s^5 t + 3\sqrt{-3}\, s^4 t^2 - 3\sqrt{-3}\, s^2 t^4 - 6 s t^5 + \sqrt{-3}\, t^6),$$

$$B = 2\delta^6 (s^2 + t^2)(s^2 - 2\varrho s t - t^2)(s^2 + 2\varrho^2 s t - t^2)(s^4 - 2\sqrt{-3}\, s^3 t - 4 s^2 t^2 +$$
$$+ 2\sqrt{-3}\, s t^3 + t^4)(s^4 - 2\varrho s^3 t + 2\varrho^2 s^2 t^2 + 2\varrho s t^3 + t^4)(s^4 + 2\varrho^2 s^3 t +$$
$$+ 2\varrho s^2 t^2 - 2\varrho^2 s t^3 + t^4),$$

$$D = 2^8 (\sqrt{-3})^3 \delta^{12} s^6 t^6 (s - \varrho t)^6 (s + \varrho^2 t)^6 (s - t)^3 (s + t)^3 (\sqrt{-3}\, s + t)^3 (s - \sqrt{-3}\, t)^3,$$

where δ, s, t are numbers in Ω, $D \neq 0$ and $\varrho = \frac{1}{2}(-1 + \sqrt{-3})$.

Proof. According to theorem 15 there are on the curve

$$\eta^2 = \xi^3 + M_0 \xi^2 + N_0 \xi$$

two points of inflexion with the coordinates $(s^2; s^2 a)$ and $(t^2; t^2 b)$, where $s^2 \neq t^2$, and hence

$$M_0 = a^2 + 2as - 2s^2 = b^2 + 2bt - 2t^2;$$
$$N_0 = s^3 (s - 2a) = t^3 (t - 2b).$$

If b is eliminated, we get

$$4(s^4 + s^2 t^2 + t^4) a^2 - 4s(s^2 - t^2)(s^2 + 2t^2) a + (s^2 - t^2)^2 (s^2 + 3t^2) = 0.$$

Suppose $s^4 + s^2 t^2 + t^4 \neq 0$. Then

$$a = \frac{(s^2 - t^2)(s - \sqrt{-3}\, t)}{2(s - \varrho t)(s + \varrho^2 t)},$$

and if s and t are multiplied by $2\delta(s - \varrho t)(s + \varrho^2 t)$, we find

$$M = [2\delta(s - \varrho t)(s + \varrho^2 t)]^2 M_0 = -3\delta^2 (s^2 + t^2)(s^2 - 2\varrho s t - t^2)(s^2 + 2\varrho^2 s t - t^2);$$
$$N = [2\delta(s - \varrho t)(s + \varrho^2 t)]^4 N_0 = -16\sqrt{-3}\, \delta^4 s^3 t^3 (s - \varrho t)^3 (s + \varrho^2 t)^3.$$

If $s^4 + s^2 t^2 + t^4 = 0$, it is easy to verify that we get the same curves as if we put $s = -\varrho t$ or $s = \varrho^2 t$ in the general formulas.

The group contains the following finite points on the curve (12):

$$\pm u_1 \ [-4\sqrt{-3}\,\delta^2 s^3 t\,(s-\varrho t)\,(s+\varrho^2 t);\ \mp 4\sqrt{-3}\,\delta^3 s^3 t\,(s-\varrho t)\,(s+\varrho^2 t)\cdot$$
$$\cdot (s^2-t^2)\,(\sqrt{-3}\,s+t)];$$

$$\pm 2u_1 \ [4\delta^2 t^2 (s-\varrho t)^2 (s+\varrho^2 t)^2;\ \pm 4\delta^3 t^2 (s-\varrho t)^2 (s+\varrho^2 t)^2 (s^2-t^2)\cdot$$
$$\cdot(\sqrt{-3}\,s+t)];$$

$$\pm u_2 \ [4\delta^2 s^2 (s-\varrho t)^2 (s+\varrho^2 t)^2;\ \pm 4\delta^3 s^2 (s-\varrho t)^2 (s+\varrho^2 t)^2 (s^2-t^2)\cdot$$
$$\cdot(s-\sqrt{-3}\,t)];$$

$$3u_1 \pm u_2 \ [-4\sqrt{-3}\,\delta^2 s t^3 (s-\varrho t)\,(s+\varrho^2 t);\ \pm 4\sqrt{-3}\,\delta^3 s t^3 (s-\varrho t)\,(s+\varrho^2 t)\cdot$$
$$\cdot (s^2-t^2)\,(s-\sqrt{-3}\,t)];$$

$$\pm(2u_1+u_2) \ [4\delta^2 \varrho^2 s^2 t^2 (s-\varrho t)^2;\ \pm 4\delta^3 \varrho^2 s^2 t^2 (s-\varrho t)^2 (s-t)\,(\sqrt{-3}\,s+t)\cdot$$
$$\cdot(s-\sqrt{-3}\,t)];$$

$$\pm(2u_1-u_2) \ [4\delta^2 \varrho\, s^2 t^2 (s+\varrho^2 t)^2;\ \pm 4\delta^3 \varrho\, s^2 t^2 (s+\varrho^2 t)^2 (s+t)\,(\sqrt{-3}\,s+t)\cdot$$
$$\cdot(s-\sqrt{-3}\,t)];$$

$$\pm(u_1+u_2) \ [-4\sqrt{-3}\,\delta^2 \varrho^2 s t\,(s-\varrho t)^3 (s+\varrho^2 t);\ \mp 4\sqrt{-3}\,\delta^3 \varrho^2 s t\,(s-\varrho t)^3 (s+\varrho^2 t)\cdot$$
$$\cdot(s+t)\,(\sqrt{-3}\,s+t)\,(s-\sqrt{-3}\,t)];$$

$$\pm(u_1-u_2) \ [-4\sqrt{-3}\,\delta^2 \varrho\, s t\,(s-\varrho t)\,(s+\varrho^2 t)^3;\ \mp 4\sqrt{-3}\,\delta^3 \varrho\, s t\,(s-\varrho t)\,(s+\varrho^2 t)^3\cdot$$
$$\cdot(s-t)\,(\sqrt{-3}\,s+t)\,(s-\sqrt{-3}\,t)];$$

$$3u_1 \ [0;\ 0].$$

If $\delta=1$, $s=-\varrho$, $t=1$, we obtain the curve

$$\eta^2=\xi^3-39\,\xi^2+9.2^7\,\xi \quad \text{or} \quad y^2=x^3+645\,x+13.814.$$

Theorem 19. *If the curve (1) has a point of order 10 in Ω, it is given by*

$$3A=\delta^4(a^{12}-4a^{11}c-6a^{10}c^2+20a^9c^3+15a^8c^4-24a^7c^5-4a^6c^6+24a^5c^7+$$
$$+15a^4c^8-20a^3c^9-6a^2c^{10}+4ac^{11}+c^{12}),$$

$$-27B=2\delta^6(a^2+c^2)(a^4-2a^3c-6a^2c^2+2ac^3+c^4)(a^{12}-4a^{11}c-6a^{10}c^2+$$
$$+20a^9c^3+15a^8c^4-48a^7c^5-28a^6c^6+48a^5c^7+15a^4c^8-20a^3c^9-$$
$$-6a^2c^{10}+4ac^{11}+c^{12}),$$

$$D=2^8\delta^{12}a^{10}c^{10}(a-c)^5(a+c)^5(a^2+ac-c^2)^2(a^2-4ac-c^2),$$

where δ, a, c are numbers in Ω and $D\neq 0$.

Proof. Let u be a point of order 5 on the curve

$$\eta^2 = \xi^3 + M_0 \xi^2 + N_0 \xi$$

with the coordinates $(\xi_1; \eta_1)$, and let $(\xi_2; \eta_2)$ be the point $-2u$. Then, by (14):

$$\xi_2 = \left(\frac{\xi_1^2 - N_0}{2\eta_1}\right)^2 \quad \text{and} \quad \xi_1 = \left(\frac{\xi_2^2 - N_0}{2\eta_2}\right)^2.$$

If a and c are defined by

$$\frac{\xi_1^2 - N_0}{2\eta_1} = c \quad \text{and} \quad \frac{\xi_2^2 - N_0}{2\eta_2} = a,$$

we find

$$\begin{cases} \xi_1 = a^2 \\ \xi_2 = c^2 \end{cases} \quad \text{and} \quad \begin{cases} a^4 - N_0 = 2c\eta_1 \\ c^4 - N_0 = 2a\eta_2. \end{cases}$$

Now the relations

$$\eta_1^2 = a^2(a^4 + M_0 a^2 + N_0);$$

$$\eta_2^2 = c^2(c^4 + M_0 c^2 + N_0)$$

may be written

$$(a^4 - N_0)^2 = 4a^2c^2(a^4 + M_0 a^2 + N_0);$$

$$(c^4 - N_0)^2 = 4a^2c^2(c^4 + M_0 c^2 + N_0).$$

Here we eliminate M_0 and find

$$N_0^2 - 2a^2c^2 N_0 - a^2c^2(a^4 - 3a^2c^2 + c^4) = 0.$$

The roots of this equation are

$$ac[ac \pm (a^2 - c^2)],$$

and since a and c can be interchanged, we may write

$$N_0 = ac(a^2 + ac - c^2).$$

If a and c are multiplied by $2\delta ac$, we find

$$M = (2\delta ac)^2 M_0 = \delta^2(a^2 + c^2)(a^4 - 2a^3c - 6a^2c^2 + 2ac^3 + c^4);$$

$$N = (2\delta ac)^4 N_0 = 16\delta^4 a^5 c^5 (a^2 + ac - c^2).$$

The group contains the following finite points on the curve (12):

$$\pm u \quad [4\delta^2 a c^3 (a^2+ac-c^2);\ \pm 4\delta^3 a c^3 (a^2+ac-c^2)(a-c)^2(a+c)];$$

$$\pm 2u\ [4\delta^2 a^2 c^4;\ \mp 4\delta^3 a^2 c^4 (a-c)(a+c)^2];$$

$$\pm 3u\ [4\delta^2 a^3 c (a^2+ac-c^2);\ \mp 4\delta^3 a^3 c (a^2+ac-c^2)(a-c)(a+c)^2];$$

$$\pm 4u\ [4\delta^2 a^4 c^2;\ \pm 4\delta^3 a^4 c^2 (a-c)^2(a+c)];$$

$$5u\ [0;\ 0].$$

12. According to LIND ([8], p. 46), the groups $(4,2,3)$ and $(2,2,5)$ are impossible in $k(1)$, but if we put $\delta = n = 1$ in theorem 17 and let m be a rational integer, it is seen that $\sqrt{D}$ generates an infinity of quadratic fields. In the same way we may choose $\delta = c = 1$ in theorem 19 and let a be a rational integer. Thus we conclude:

Theorem 20. *The groups $(4,2,3)$ and $(2,2,5)$ are possible in an infinity of quadratic fields, and we may even suppose A and B to be rational.*

§ 4.

The exceptional group in the harmonic case

13. If Ω is an algebraic field and if A is a number in Ω, it is sometimes possible to determine the exceptional group in Ω on the curve

$$y^2 = x^3 - Ax. \tag{2}$$

In the case $\Omega = k(1)$ the group is given by theorem 5. NAGELL ([14], p. 6–11) has also examined the exceptional points on (2) in quadratic fields, but A is still supposed to be rational.

If α is an integer in the algebraic field K and if $\mathfrak{p}$ is a prime ideal in K, it will be convenient to introduce the notation $\mathfrak{p}^m // \alpha$, if α is divisible by $\mathfrak{p}^m$ but not by $\mathfrak{p}^{m+1}$.

14. We begin with two preliminary theorems:

Lemma 1. *If there is a point in Ω of order 7 on the curve (2), then Ω contains an algebraic field of degree 12, and in this field 2 is the square of a prime ideal.*

Proof. Let $(x; y)$ be a point of order 7 on the curve (2). Since $P_7(x) = 0$, it follows from (7) that

$$z = \frac{A}{x^2}$$

is a number in Ω satisfying

$$z^{12}+7.28\,z^{11}-7.186\,z^{10}+7.2108\,z^{9}-7.2239\,z^{8}-7.6024\,z^{7}+7.15988\,z^{6}-7.11752\,z^{5}+$$
$$+7.5033\,z^{4}-7.2836\,z^{3}+7.422\,z^{2}+7.44\,z-7=0,$$

and by Eisenstein's irreducibility criterion, z is of degree 12.

On the other hand, it follows from theorem 4 that there is a number

$$t=\frac{m}{n}$$

in Ω, which satisfies the equation

$$t^{12}-18\,t^{11}+117\,t^{10}-354\,t^{9}+570\,t^{8}-486\,t^{7}+273\,t^{6}-222\,t^{5}+174\,t^{4}-46\,t^{3}-15\,t^{2}+$$
$$+6\,t+1=0, \qquad (16)$$

and if t is a number satisfying (16), a point of order 7 is possible in $k(t)$. Consequently (16) is irreducible in $k(1)$.

If we put

$$v=\frac{t^{3}-6\,t^{2}+3\,t+1}{t\,(t-1)}\,, \qquad (17)$$

it is easy to verify that

$$v^{4}+6\,v^{3}+3\,v^{2}-46\,v+9=0, \qquad (18)$$

and since (18) is irreducible in $k(1)$, we see that $k(t)$ contains a sub-field $k(v)$ of degree 4.

Since the norms of v and $v+1$ are both odd, there is no prime ideal in $k(v)$ with the norm 2. If we put

$$s=\tfrac{1}{2}\,(v^{2}+v-1),$$

we find

$$s^{4}-10\,s^{3}+90\,s^{2}-4.41\,s-4.19=0. \qquad (19)$$

If $\mathfrak{p}$ is a prime ideal in $k(v)$ which divides 2, it follows from (19) that $\mathfrak{p}/s$. But then $\mathfrak{p}^{3}/4$ and consequently $\mathfrak{p}^{2}/2$. Since the norm of $\mathfrak{p}$ is at least equal to 4, we have $2=\mathfrak{p}^{2}$.

(17) gives the irreducible equation in $k(v)$ satisfied by t:

$$t^{3}-(v+6)\,t^{2}+(v+3)\,t+1=0, \qquad (20)$$

and the number $\xi=t^{2}+t+1$ satisfies

$$\xi^{3}-(v^{2}+11\,v+39)\,\xi^{2}+4\,(v^{2}+10\,v+30)\,\xi-(3\,v^{2}+27\,v+73)=0. \qquad (21)$$

The coefficients of (21) are divisible by $\mathfrak{p}^{2}$, $\mathfrak{p}^{4}$ and $\mathfrak{p}^{3}$, respectively. Let $\mathfrak{P}$ be a prime ideal in $k(t)$ which divides $\mathfrak{p}$. Then it is seen that $\mathfrak{P}/\xi$, and if $\mathfrak{P}^{2}/\mathfrak{p}$,

we find $\mathfrak{P}^2/\xi$. If $\mathfrak{P}^3/\mathfrak{p}$, the second term of (21) will be divisible by $\mathfrak{P}^{10}$, and hence $\mathfrak{P}^3/\xi$. It follows that $\mathfrak{p}/\xi$, and consequently the number

$$\eta = \tfrac{1}{2}\,\xi^2 - (t^3 + 2\,t^2 + t + 1) = \tfrac{1}{2}\,(t^4 - t^2 - 1)$$

is an integer. If N_1 denotes the norm relative to $k(v)$, it will be found that the numbers

$$N_1(\eta) = \tfrac{1}{2}\,(4\,v^3 + 45\,v^2 + 187\,v + 263),$$

$$N_1(\eta + 1) = \tfrac{1}{2}\,(3\,v^3 + 32\,v^2 + 124\,v + 151),$$

$$N_1(\eta + t^2) = -\,(v^3 + 9\,v^2 + 26\,v + 10),$$

$$N_1(\eta + t^2 + 1) = \tfrac{1}{2}\,(9\,v^3 + 97\,v^2 + 381\,v + 486)$$

are indivisible by $\mathfrak{p}$. However, if $\mathfrak{p}$ is not a prime ideal in $k(t)$, there must be a prime ideal $\mathfrak{P}$ in $k(t)$ with the norm 4, but this is impossible, since the five numbers

$$0,\ \eta,\ \eta + 1,\ \eta + t^2,\ \eta + t^2 + 1$$

are incongruent mod $\mathfrak{P}$. Consequently $\mathfrak{p}$ remains a prime ideal in $k(t)$.

Theorem 21. *Let Ω be an algebraic field containing the number A, and suppose that there is a point of order q in Ω on the curve*

$$y^2 = x^3 - A\,x, \tag{2}$$

where q is an odd prime. Then 2 is the square of an ideal in Ω, and if there is a prime ideal in Ω with the norm 2 or 4, we have $q \leqq 5$.

Proof. We may suppose that A is an integer and that the exceptional points in Ω on (2) have integral coordinates, for otherwise it would be sufficient to multiply A by the fourth power of a suitable natural number.

Let u_1 be a point in Ω of order q, and let $\mathfrak{p}$ be a prime ideal dividing 2. Among the points $u_1, 2\,u_1, 3\,u_1, \ldots, (q-1)\,u_1$ we choose a point u with the coordinates $(x; y)$ in such a way that x is divisible by the lowest possible power of $\mathfrak{p}$.

If $v \equiv \tfrac{1}{2}(q+1)\,u \pmod{\omega, \omega'}$, we have $2\,v \equiv u$, and then it follows from (8) that $x = z^2$, where z belongs to Ω.

Now suppose $\mathfrak{p}^m \| 2$, $\mathfrak{p}^h \| z$ and $\mathfrak{p}^a \| A$. Let P_ν and Q_ν denote the polynomials defined in § 2.

If $a < 4\,h$, we find $\mathfrak{p}^{a+2h}/y^2$ and $\mathfrak{p}^{2a} \| P_3$, and hence, by (5), $\mathfrak{p}^{2h} \nmid \varphi(2\,u)$, and if $a > 4\,h$, we find $\mathfrak{p}^{6h}/y^2$ and $\mathfrak{p}^{8h} \| P_3$, and hence $\mathfrak{p}^{2h} \nmid \varphi(2\,u)$. But the point u is chosen in such a way that $\varphi(2\,u)$ is divisible by $\mathfrak{p}^{2h}$, and consequently $a = 4\,h$.

We put $y=zt$ and find

$$t^2=z^4-A;$$

$$P_3=3t^4-4A^2;$$

$$-Q_4=2(t^2+2A)(t^4-4At^2-4A^2).$$

If $\mathfrak{p}^{4h+m}\nmid t^2$, it is seen that $\mathfrak{p}^{8h+2m}\nmid P_3$, but $\mathfrak{p}^{6h+2m}/4y^2$, and hence $\mathfrak{p}^{2h}\nmid\wp(2u)$. If $\mathfrak{p}^{4h+m+1}/t^2$, we find $\mathfrak{p}^{8h+2m}//P_3$ and $\mathfrak{p}^{6h+2m+1}/4y^2$, and then $\mathfrak{p}^{2h}\nmid\wp(2u)$. Consequently $\mathfrak{p}^{4h+m}//t^2$, and it follows that m is even. This proves the first statement of the theorem.

Put $m=2n$ and $h+n=r$. Then we know that $\mathfrak{p}^{6r}//4y^2$ and $\mathfrak{p}^{2h+n}//t$, and since $\mathfrak{p}^{2h}/\wp(2u)-z^2$, we have $\mathfrak{p}^{8h+6n}/P_3$. If we put $t^2+2A=s$, we find $\mathfrak{p}^{4h+2n}/s$ and

$$P_3=3s^2-12As+8A^2;$$

$$Q_4=-2s(s^2-8As+8A^2).$$

Since $\mathfrak{p}^{8h+6n}/P_3$, we see that $\mathfrak{p}^{4h+3n}/s$. If $\mathfrak{p}^{4h+3n+1}/s$, it is found that $\mathfrak{p}^{8h+6n}//P_3$ and $\mathfrak{p}^{12h+11n+1}/Q_4$. But then it follows from (4) that $\mathfrak{p}^{24h+18n}//P_5$, and then, by (5), $\mathfrak{p}^{2h}\nmid\wp(4u)$. Consequently $\mathfrak{p}^{4h+3n}//s$.

If $\mathfrak{p}^{8h+7n}\nmid s^2+8A^2$, we find $\mathfrak{p}^{8h+7n}\nmid P_3$ but $\mathfrak{p}^{12h+11n}/Q_4$, and hence $\mathfrak{p}^{24h+21n}\nmid P_5$ and $\mathfrak{p}^{2h}\nmid\wp(4u)$. If $\mathfrak{p}^{8h+7n+1}/s^2+8A^2$, we find $\mathfrak{p}^{8h+7n}//P_3$ but $\mathfrak{p}^{12(h+n)}/Q_4$, and hence $\mathfrak{p}^{24h+21n}//P_5$ and $\mathfrak{p}^{2h}\nmid\wp(4u)$. Consequently $\mathfrak{p}^{8h+7n}//s^2+8A^2$, $\mathfrak{p}^{8h+7n}/P_3$ and $\mathfrak{p}^{12r}//Q_4$.

If $\mathfrak{p}^{8r-c}//P_3$, where $c>0$, it follows from (4) that $\mathfrak{p}^{3(8r-c)}//P_5$, $\mathfrak{p}^{4(8r-c)}//Q_6$, $\mathfrak{p}^{6(8r-c)}//P_7$ and $\mathfrak{p}^{60r-6c}/Q_8$. Then we may suppose

$$\mathfrak{p}^{\frac{1}{8}(\nu^2-1)(8r-c)}//P_\nu, \qquad \text{if} \quad \nu \text{ is odd};$$

$$\mathfrak{p}^{\frac{1}{8}(\nu^2-4)(8r-c)}//Q_\nu, \qquad \text{if} \quad \nu\equiv 2 \pmod 4;$$

$$\mathfrak{p}^{(\nu^2-4)r-\frac{1}{8}(\nu^2-16)c}/Q_\nu, \qquad \text{if} \quad \nu\equiv 0 \pmod 4.$$

This has been verified above for $\nu\leqq 8$ and can be proved generally by induction, if the formulas (4) are used. But this implies $P_q\neq 0$, which is impossible, since u is a point of order q. Consequently $\mathfrak{p}^{8r}/P_3$.

Now suppose $q>3$. If $\mathfrak{p}^{8r+1}/P_3$, we find $\mathfrak{p}^{24r}//P_5$, $\mathfrak{p}^{32r+1}/Q_6$, $\mathfrak{p}^{48r}//P_7$, $\mathfrak{p}^{60r}//Q_8$, and the formulas

$$\mathfrak{p}^{(\nu^2-1)r}//P_\nu, \qquad \text{if } 3\nmid\nu \text{ and } \nu \text{ is odd};$$

$$\mathfrak{p}^{(\nu^2-4)r}//Q_\nu, \qquad \text{if } 3\nmid\nu \text{ and } \nu \text{ is even};$$

$$\mathfrak{p}^{(\nu^2-1)r+1}/P_\nu, \qquad \text{if } 3/\nu \text{ and } \nu \text{ is odd};$$

$$\mathfrak{p}^{(\nu^2-4)r+1}/Q_\nu, \qquad \text{if } 3/\nu \text{ and } \nu \text{ is even}$$

are easily proved by induction. But this contradicts $P_q=0$, and consequently $\mathfrak{p}^{8r}//P_3$.

As yet we have not supposed anything about the norm of $\mathfrak{p}$. Now we shall examine the two simplest cases and begin with $N(\mathfrak{p})=2$ and $q>5$. Then it follows from (4) that $\mathfrak{p}^{24r+1}/P_5$, $\mathfrak{p}^{32r}//Q_6$, $\mathfrak{p}^{48r}//P_7$, $\mathfrak{p}^{60r}//Q_8$, $\mathfrak{p}^{80r}//P_9$, $\mathfrak{p}^{96r+1}/Q_{10}$ and generally

$$\mathfrak{p}^{(\nu^2-1)r}//P_\nu, \quad \text{if } 5\nmid\nu \text{ and } \nu \text{ is odd};$$

$$\mathfrak{p}^{(\nu^2-4)r}//Q_\nu, \quad \text{if } 5\nmid\nu \text{ and } \nu \text{ is even};$$

$$\mathfrak{p}^{(\nu^2-1)r+1}/P_\nu, \quad \text{if } 5\mid\nu \text{ and } \nu \text{ is odd};$$

$$\mathfrak{p}^{(\nu^2-4)r+1}/Q_\nu, \quad \text{if } 5\mid\nu \text{ and } \nu \text{ is even}.$$

But this contradicts $P_q=0$, and consequently $q\leqq 5$, if there is a prime ideal in Ω with the norm 2.

Next suppose $N(\mathfrak{p})=4$ and $q>7$. Let α represent a primitive residue class mod $\mathfrak{p}$; then

$$\alpha^2\equiv\alpha+1 \pmod{\mathfrak{p}} \quad \text{and} \quad \alpha^3\equiv 1 \pmod{\mathfrak{p}}.$$

Let π be an integer satisfying $\mathfrak{p}^{4r}//\pi$. Then

$$P_3\equiv\pi^2, \ \equiv\alpha\pi^2 \quad \text{or} \quad \equiv\alpha^2\pi^2 \pmod{\mathfrak{p}^{8r+1}},$$

and since $\alpha\pi$ or $\alpha^2\pi$ may be substituted for π, we may suppose

$$P_3\equiv\pi^2 \pmod{\mathfrak{p}^{8r+1}}.$$

Further,

$$16y^4\equiv\pi^3, \ \equiv\alpha\pi^3 \quad \text{or} \quad \equiv\alpha^2\pi^3 \pmod{\mathfrak{p}^{12r+1}},$$

but since α and α^2 may be interchanged, it is sufficient to consider the first two cases.

First suppose $16y^4\equiv\pi^3 \pmod{\mathfrak{p}^{12r+1}}$. If $Q_4\equiv\pi^3 \pmod{\mathfrak{p}^{12r+1}}$, we find $P_5\equiv 0 \pmod{\mathfrak{p}^{24r+1}}$, $Q_6\equiv\pi^8 \pmod{\mathfrak{p}^{32r+1}}$, $P_7\equiv\pi^{12} \pmod{\mathfrak{p}^{48r+1}}$, $Q_8\equiv\pi^{15} \pmod{\mathfrak{p}^{60r+1}}$ and generally

$$P_\nu\equiv\pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if } 5\nmid\nu \text{ and } \nu \text{ is odd};$$

$$Q_\nu\equiv\pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if } 5\nmid\nu \text{ and } \nu \text{ is even};$$

$$P_\nu\equiv 0 \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if } 5\mid\nu \text{ and } \nu \text{ is odd};$$

$$Q_\nu\equiv 0 \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if } 5\mid\nu \text{ and } \nu \text{ is even},$$

but this is impossible, since $P_q=0$ and $q>5$. If $Q_4\not\equiv\pi^3 \pmod{\mathfrak{p}^{12r+1}}$, we may suppose $Q_4\equiv\alpha\pi^3 \pmod{\mathfrak{p}^{12r+1}}$, but then it will be found that

$$P_\nu \equiv \pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 1 \pmod{18};$$

$$P_\nu \equiv \alpha\pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 7 \pmod{18};$$

$$P_\nu \equiv \alpha^2\pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 5 \pmod{18};$$

$$Q_\nu \equiv \pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 2 \pmod{18};$$

$$Q_\nu \equiv \alpha\pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 4 \pmod{18};$$

$$Q_\nu \equiv \alpha^2\pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 8 \pmod{18};$$

$$P_\nu \equiv \pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv 3 \pmod{6};$$

$$Q_\nu \equiv 0 \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv 0 \pmod{6},$$

and this contradicts $P_q = 0$.

Consequently $16y^4 \equiv \alpha\pi^3 \pmod{\mathfrak{p}^{12r+1}}$. Then we must distinguish three cases, according as $Q_4 \equiv \pi^3$, $\equiv \alpha\pi^3$ or $\equiv \alpha^2\pi^3 \pmod{\mathfrak{p}^{12r+1}}$:

If $Q_4 \equiv \pi^3 \pmod{\mathfrak{p}^{12r+1}}$, the formulas (4) give the following result:

$$P_\nu \equiv \pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 1, \pm 3, \pm 7 \pmod{24};$$

$$P_\nu \equiv \alpha\pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 9 \pmod{24};$$

$$P_\nu \equiv \alpha^2\pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 5, \pm 11 \pmod{24};$$

$$Q_\nu \equiv \pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 2, \pm 4, \pm 10 \pmod{24};$$

$$Q_\nu \equiv \alpha\pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 6, 12 \pmod{24};$$

$$Q_\nu \equiv 0 \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 8, 0 \pmod{24},$$

and this is impossible.

If $Q_4 \equiv \alpha\pi^3 \pmod{\mathfrak{p}^{12r+1}}$, we get the following congruences:

$$P_\nu \equiv \pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 1, \pm 3, \pm 13 \pmod{42};$$

$$P_\nu \equiv \alpha\pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 5, \pm 15, \pm 19 \pmod{42};$$

$$P_\nu \equiv \alpha^2\pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 9, \pm 11, \pm 17 \pmod{42};$$

$$P_\nu \equiv 0 \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 7, 21 \pmod{42};$$

$$Q_\nu \equiv \pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 2, \pm 6, \pm 16 \pmod{42};$$

$$Q_\nu \equiv \alpha\pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 4, \pm 10, \pm 12 \pmod{42};$$

$$Q_\nu \equiv \alpha^2\pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 8, \pm 18, \pm 20 \pmod{42};$$

$$Q_\nu \equiv 0 \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 14, 0 \pmod{42},$$

but this is impossible, since $q > 7$.

If $Q_4 \equiv \alpha^2 \pi^3 \pmod{\mathfrak{p}^{12r+1}}$, it will be found that

$$P_\nu \equiv \pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 1, \pm 3, \pm 11 \pmod{30};$$

$$P_\nu \equiv \alpha \pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 7, \pm 13 \pmod{30};$$

$$P_\nu \equiv \alpha^2 \pi^{\frac{1}{4}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 9 \pmod{30};$$

$$P_\nu \equiv 0 \pmod{\mathfrak{p}^{(\nu^2-1)r+1}}, \quad \text{if} \quad \nu \equiv \pm 5, 15 \pmod{30};$$

$$Q_\nu \equiv \pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 2, \pm 8 \pmod{30};$$

$$Q_\nu \equiv \alpha \pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 6 \pmod{30};$$

$$Q_\nu \equiv \alpha^2 \pi^{\frac{1}{4}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 4, \pm 12, \pm 14 \pmod{30};$$

$$Q_\nu \equiv 0 \pmod{\mathfrak{p}^{(\nu^2-4)r+1}}, \quad \text{if} \quad \nu \equiv \pm 10, 0 \pmod{30},$$

and this is impossible, too.

It follows that $q \leqq 7$, if there is a prime ideal in Ω with the norm 4. However, lemma 1 shows that $q = 7$ is impossible. Thus $q \leqq 5$, and theorem 21 is proved.

15. Theorem 21 may be applied to any field, whose degree is 2, 4 or an odd number, and we shall now examine these cases in detail.

If the degree of Ω is odd, the order of the exceptional group in Ω on the curve (2) is a power of 2. If there is a point of order 4, we may put $B = 0$ in theorem 8, and this requires

$$a - 2c = 0$$

or

$$2a^2 - 8ac - c^2 = 0.$$

Since Ω does not contain $\sqrt{2}$, the latter possibility is excluded. Consequently $a = 2c$ and $A = -4c^4$, and the curve is equivalent to

$$y^2 = x^3 + 4x. \tag{22}$$

Since this curve has only one point of order 2 in Ω, the only points of order 4 are $(2; \pm 4)$, and there is no point of order 8, since otherwise 2 ought to be a square, according to (8).

We have reached the following result, which is quite analogous to theorem 5:

Theorem 22. *Let Ω be an algebraic field of odd degree. If A is a number in Ω, the curve*

$$y^2 = x^3 - Ax$$

has the following exceptional group in Ω:

$$(2), \quad \text{if} \quad A \neq C^2, \ \neq -4C^4;$$

$$(2,2), \quad \text{if} \quad A = C^2;$$

$$(4), \quad \text{if} \quad A = -4C^4.$$

Here C denotes any number in Ω.

16. Now let Ω be a quadratic field. If $\Omega + k(\sqrt{2})$ and if the curve (2) has a point of order 4 in Ω, it is equivalent to (22), and among the points of order 4 on this curve $(2; \pm 4)$ and possibly $(-2; \pm 4i)$ belong to Ω. The remaining 8 points of order 4 do not belong to Ω, since the abscissa of one of them is $2i(1+\sqrt{2})$. If u is a point of order 8, we must have $\wp(2u) = \pm 2$, but this is impossible, since then (5) gives an irreducible equation of degree 4:

$$(x^2-4)^2 = \pm 8x(x^2+4).$$

If $\Omega = k(\sqrt{2})$ and if the curve (2) has a point of order 4 in Ω, it follows from theorem 8 that the curve is equivalent to (22) or to

$$y^2 = x^3 - x.$$

In the first case there is only one point of order 2 and no point of order 8. In the second case there are 3 points of order 2, and the points of order 4 are $[1+\sqrt{2}; \pm(\sqrt{2}+2)]$ and $[1-\sqrt{2}; \pm(\sqrt{2}-2)]$. No point of order 8 belongs to Ω, since $1 \pm \sqrt{2}$ is not a square in this field.

If there is a point of order 3 in Ω, it follows from theorem 2 that $\Omega = k(\sqrt{3})$ and that (2) is equivalent to one of the curves

$$y^2 = x^3 + (3 \pm 2\sqrt{3})x.$$

We may choose the upper sign and then have the points of inflexion $[1; \pm(1+\sqrt{3})]$, and since Ω does not contain $\sqrt{-3}$, theorem 7 implies that the other points of order 3 do not belong to Ω. If u is a point of order 9 with the abscissa x and if $\wp(3u) = 1$, we get by (5):

$$(1-x)P_3^2(x) = 4x(x^2 + \varepsilon\sqrt{3})Q_4(x), \tag{23}$$

where $\varepsilon = 2+\sqrt{3}$ and

$$P_3(x) = 3(x^4 + 2\varepsilon\sqrt{3}x^2 - \varepsilon^2);$$

$$Q_4(x) = -2(x^2 - \varepsilon\sqrt{3})(x^4 + 6\varepsilon\sqrt{3}x^2 + 3\varepsilon^2).$$

Let $\mathfrak{p}$ be a prime ideal in $\Omega(x)$, which divides $\sqrt{3}$. Since $\mathfrak{p}/P_3$, it is seen that $\mathfrak{p}/x$, since otherwise $\mathfrak{p}$ would not divide the right member of (23). Suppose $\mathfrak{p}^h//\sqrt{3}$; then $\mathfrak{p}^{2h}//P_3$. If $\mathfrak{p}^h/x^2$, we find $\mathfrak{p}^{3h}/Q_4$, and the right member of (23) would be divisible by $\mathfrak{p}^{4h+1}$, which is impossible. Thus if $\mathfrak{p}^k//x$, we have $2k<h$, $\mathfrak{p}^{6k}//Q_4$ and $\mathfrak{p}^{3k}//x(x^2+\varepsilon\sqrt{3})$. Consequently $4h=9k$, and hence $h=9$. But this implies that $\Omega(x)$ is of degree 18.

If there is a point of order 5 in Ω, it follows from theorem 3 that $\Omega=k(\sqrt{-1})$ and that (2) is equivalent to one of the curves

$$y^2=x^3-(1\pm 2i)\,x.$$

It is easy to show that there are 10 exceptional points in Ω in this case (see NAGELL [13], p. 12). If the upper sign is chosen, the points of order 5 are $[1;\ \pm(1-i)]$ and $[-1;\ \pm(1+i)]$.

We have proved the following theorem:

Theorem 23. *If A belongs to the quadratic field Ω, the curve*

$$y^2=x^3-Ax$$

has the following exceptional group in Ω:

1. $\Omega\neq k(\sqrt{-1}),\ \neq k(\sqrt{2}),\ \neq k(\sqrt{3})$.

   (2), if $A\neq C^2,\ \neq -4C^4$;

   (2, 2), if $A=C^2$;

   (4), if $A=-4C^4$.

2. $\Omega=k(\sqrt{-1})$.

   (2), if $A\neq C^2,\ \neq(1\pm 2i)C^4$;

   (2, 2), if $A=C^2,\ \neq C^4$;

   (4, 2), if $A=C^4$;

   (2, 5), if $A=(1\pm 2i)C^4$.

3. $\Omega=k(\sqrt{2})$.

   (2), if $A\neq C^2,\ \neq -4C^4$;

   (2, 2), if $A=C^2,\ \neq C^4$;

   (4), if $A=-4C^4$;

   (4, 2), if $A=C^4$.

4. $\Omega = k(\sqrt{3})$.

(2), if $A \neq C^2, \neq -4C^4, \neq -(3 \pm 2\sqrt{3})C^4$;

(2, 2), if $A = C^2$;

(4), if $A = -4C^4$;

(2, 3), if $A = -(3 \pm 2\sqrt{3})C^4$.

Here C denotes any number in Ω.

17. Finally let Ω be a quartic field. If the curve (2) has a point of order 4 in Ω, it is equivalent to

$$y^2 = x^3 + 4x \tag{22}$$

or to

$$y^2 = x^3 - x. \tag{24}$$

In the former case we may suppose that $\sqrt{-1}$ does not belong to Ω, since -4 is a fourth power in $k(\sqrt{-1})$.

First consider the curve (22). The only points of order 4 in Ω are $(2; \pm 4)$. If u is a point of order 8 with the abscissa x and if $\wp(2u) = 2$, we find

$$x = 2[1 + \sqrt{2} \pm \sqrt{2(1+\sqrt{2})}] \quad \text{or} \quad x = 2[1 - \sqrt{2} \pm \sqrt{2(1-\sqrt{2})}].$$

Thus if x belongs to Ω, the field is $k(\sqrt{1+\sqrt{2}})$ or $k(\sqrt{1-\sqrt{2}})$ and then, by (6), y also belongs to Ω.

Since the exceptional groups on the curve (22) in two conjugate fields are isomorphic, it is sufficient to examine the case $\Omega = k(\sqrt{1+\sqrt{2}})$. The points of order 8 are

$$[2(\varepsilon^3 + \varepsilon^2 - \varepsilon);\ \pm 4(\varepsilon^3 + \varepsilon^2 + 1)] \quad \text{and} \quad [2(-\varepsilon^3 + \varepsilon^2 + \varepsilon);\ \pm 4(-\varepsilon^3 + \varepsilon^2 + 1)],$$

where $\varepsilon = \sqrt{1+\sqrt{2}}$. If there were a point of order 16 in Ω, the abscissa of each point of order 8 would be a square (according to (8)), and hence

$$z^2 = \varepsilon^3 + \varepsilon^2 - \varepsilon,$$

where z belongs to Ω. But this equation may be written

$$(z-1)(z+1) = (1+\varepsilon)\sqrt{2},$$

and if we define the ideal $\mathfrak{p} = (1+\varepsilon)$, we find $\mathfrak{p}^4 = 2$ and hence $\mathfrak{p}^3 // (z-1)(z+1)$, which is impossible.

Now consider the curve (24). If ω is the least positive period and if ω' is the least positive-imaginary period, the points of order 2 are

$$\tfrac{1}{2}\omega'(-1;0); \quad \tfrac{1}{2}(\omega+\omega')(0;0); \quad \tfrac{1}{2}\omega(1;0),$$

and the points of order 4 are

$$\mp\tfrac{1}{4}\omega \qquad [1+\sqrt{2};\ \pm(2+\sqrt{2})]; \quad \pm\tfrac{1}{4}(\omega-\omega')\,[i;\ \pm(1-i)];$$

$$\pm\tfrac{1}{4}\omega+\tfrac{1}{2}\omega' \ [1-\sqrt{2};\ \pm(2-\sqrt{2})]; \quad \pm\tfrac{1}{4}(\omega+\omega')\,[-i;\ \pm(1+i)];$$

$$\mp\tfrac{1}{4}\omega' \qquad [-1-\sqrt{2};\ \pm i(2+\sqrt{2})];$$

$$\pm\tfrac{1}{4}\omega'+\tfrac{1}{2}\omega \ [-1+\sqrt{2};\ \pm i(2-\sqrt{2})].$$

If there is a point of order 8, the abscissa of one of the points of order 4 must be a square, and hence $\Omega=k(\sqrt{1\pm\sqrt{2}})$ or $\Omega=k(\sqrt{2},\sqrt{-1})$. First suppose $\Omega=k(\sqrt{1+\sqrt{2}})$ and let u be a point of order 8 with the abscissa x. Then $\wp(2u)=1+\sqrt{2}$ and consequently by (5),

$$(x^2-2x-1)^2=4x(x^2-1)\sqrt{2}. \tag{25}$$

Suppose that x belongs to Ω and put $\mathfrak{p}=(1+\sqrt{1+\sqrt{2}})$. By (25), $\mathfrak{p}^5/x^2-2x-1$, and hence $\mathfrak{p}^4//x^2-1$ and, if (25) is used once again, $\mathfrak{p}^7//x^2-2x-1$. But this is impossible, since

$$x^2-2x-1=(x-1+\sqrt{2})(x-1-\sqrt{2}),$$

and if one of these factors is divisible by $\mathfrak{p}^4$, the same is true of the other.

Next suppose $\Omega=k(\sqrt{2},\sqrt{-1})$ and let u be a point of order 8 with the abscissa x. Then we may put $\wp(2u)=i$ and hence

$$4ix(x^2-1)=(x^2+1)^2.$$

One root of this equation is

$$x=i(1-\sqrt{2})+\sqrt{2(\sqrt{2}-1)},$$

and since Ω does not contain $\sqrt{\sqrt{2}-1}$, x is of degree 8.

Consequently no point of order 8 on the curve (24) belongs to Ω, and we have reached the following result:

Lemma 2. *If Ω is a quartic field, the points of order 2^ν $(\nu\geqq 0)$ in Ω on the curve (2) form the following group:*

1. *Ω contains neither $\sqrt{2}$ nor $\sqrt{-1}$.*

(2), if $A\neq C^2,\ \neq -4C^4$;

(2,2), if $A=C^2$;

(4), if $A=-4C^4$.

2. *Ω contains $\sqrt{-1}$ but is $\neq k(\sqrt{2}, \sqrt{-1})$.*

(2), if $A \neq C^2$;

$(2,2)$, if $A = C^2, \neq C^4$;

$(4,2)$, if $A = C^4$.

3. *Ω contains $\sqrt{2}$ but is $\neq k(\sqrt{2}, \sqrt{-1})$ and $\neq k(\sqrt{1 \pm \sqrt{2}})$.*

(2), if $A \neq C^2, \neq -4C^4$;

$(2,2)$, if $A = C^2, \neq C^4$;

(4), if $A = -4C^4$;

$(4,2)$, if $A = C^4$.

4. *$\Omega = k(\sqrt{2}, \sqrt{-1})$.*

(2), if $A \neq C^2$;

$(2,2)$, if $A = C^2, \neq C^4$;

$(4,4)$, if $A = C^4$.

5. *$\Omega = k(\sqrt{1 \pm \sqrt{2}})$.*

(2), if $A \neq C^2, \neq -4C^4$;

$(2,2)$, if $A = C^2, \neq C^4$;

$(4,2)$, if $A = C^4$;

(8), if $A = -4C^4$.

Here C denotes any number in Ω.

18. Suppose that there is a point of order 3 in Ω on the curve (2). Then it follows from theorem 2 that the curve is equivalent to

$$y^2 = x^3 + (3 \pm 2\sqrt{3})\, x,$$

and these two curves are inequivalent except in the case $\Omega = k(\sqrt{3}, \sqrt{-1})$, since

$$\frac{3 + 2\sqrt{3}}{3 - 2\sqrt{3}} = -(2 + \sqrt{3})^2 = [\tfrac{1}{2}(1 + i)(1 + \sqrt{3})]^4.$$

We may choose the upper sign and then find the following finite points of inflexion:

$$[1;\ \pm(1+\sqrt{3})]; \qquad [i(2+\sqrt{3});\ \pm(1-i)(2+\sqrt{3})];$$

$$[-1;\ \pm i(1+\sqrt{3})]; \quad [-i(2+\sqrt{3});\ \pm(1+i)(2+\sqrt{3})].$$

If u is a point of order 9 with the abscissa x, we have, by (5),

$$[\wp(3u)-x]\,P_3^2(x) = 4x(x^2+3+2\sqrt{3})\,Q_4(x),$$

where $\wp(3u) = \pm 1$ or $= \pm i(2+\sqrt{3})$. It was shown above that this is impossible in the case $\wp(3u)=1$, if Ω is a field of degree <18, and the proof is the same in the other cases.

This discussion may be summed up in the following way:

Lemma 3. *If Ω is a quartic field, the points of order 5^ν $(\nu \geqq 0)$ in Ω on the curve (2) form the following group:*

1. *Ω does not contain $\sqrt{3}$.*

   (1).

2. *Ω contains $\sqrt{3}$ but is $\neq k(\sqrt{3}, \sqrt{-1})$.*

   (1), if $A \neq -(3 \pm 2\sqrt{3})\,C^4$;

   (3), if $A = -(3 \pm 2\sqrt{3})\,C^4$.

3. *$\Omega = k(\sqrt{3}, \sqrt{-1})$.*

   (1), if $A \neq -(3+2\sqrt{3})\,C^4$;

   (3, 3), if $A = -(3+2\sqrt{3})\,C^4$.

Here C denotes any number in Ω.

19. Finally suppose that a point of order 5 belongs to Ω. According to theorem 3 we have to distinguish two cases. Either Ω contains $\sqrt{-1}$, and the curve is equivalent to

$$y^2 = x^3 - (1 \pm 2i)\,x, \tag{26}$$

or $\Omega = k(\sqrt{10+2\sqrt{5}})$, and the curve is equivalent to

$$y^2 = x^3 - 2\,[1 + 35\sqrt{5} \pm 6(1-2\sqrt{5})\sqrt{10+2\sqrt{5}}]\,x \tag{27}$$

or

$$y^2 = x^3 - 2\,[1 - 35\sqrt{5} \pm 6(1+2\sqrt{5})\sqrt{10-2\sqrt{5}}]\,x. \tag{28}$$

First consider the curves (26). If they were equivalent in Ω, this field would contain a number C satisfying

$$C^4 = \frac{1+2i}{1-2i} = \tfrac{1}{5}(1+2i)^2. \tag{29}$$

Hence $\Omega = k(\sqrt{5}, \sqrt{-1})$, but in this field there are two different prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ satisfying $\mathfrak{p}\mathfrak{p}' = \sqrt{5}$, since 5 is the product of two different ideals in $k(\sqrt{-1})$, and then it is seen that the right member of (29) is not the fourth power of an ideal in Ω.

Now we choose the upper sign in (26). Four points of order 5 are

$$[1;\ \pm(1-i)] \quad \text{and} \quad [-1;\ \pm(1+i)], \tag{30}$$

and by (7) it is seen that one of the others has the abscissa

$$x = \frac{1+2i}{\sqrt{5}} = C^2,$$

where C is a number satisfying (29). But then

$$y = \pm(1+i)\,C^3,$$

and consequently this point cannot belong to Ω, since C is of the eighth degree. Thus (30) are the only points of order 5 in Ω.

Suppose that a point (x, y) of order 25 belongs to Ω. Then, by (5),

$$[x - \wp(5u)]\,P_5^2(x) = 4y^2\,Q_4(x)\,Q_6(x), \tag{31}$$

where $\wp(5u) = \pm 1$ and Q_4, P_5, Q_6 are given by (7). Let $\mathfrak{p}$ be a prime ideal in Ω dividing A and define m and h by $\mathfrak{p}^m \| A$ and $\mathfrak{p}^h \| x$; then $\mathfrak{p}^m \| 5$. If $2h > m$, we find $\mathfrak{p}^{2m} \| P_3$; $\mathfrak{p}^{3m} \| Q_4$; $\mathfrak{p}^{h+m} \| y^2$; $\mathfrak{p}^{6m} \| P_5$; $\mathfrak{p}^{8m} \| Q_6$, and it is seen by (31) that this is impossible. If $2h < m$, we have $h = 0$, since $m \leqq 2$, but then $\mathfrak{p} \| P_5$, while $\mathfrak{p} \nmid y^2 Q_4 Q_6$, and this is also impossible. Hence $2h = m = 2$. Then $\mathfrak{p}^2 \| y$, which implies $\mathfrak{p}^3 \| x^2 - A$, but then we find $\mathfrak{p}^{12} \| P_5$, while $\mathfrak{p}^6 \| Q_4$ and $\mathfrak{p}^{16} \| Q_6$, and it follows from (31) that this is impossible.

Next consider the curves (27) and (28). Since

$$\frac{1+35\sqrt{5}+6(1-2\sqrt{5})\sqrt{10+2\sqrt{5}}}{1+35\sqrt{5}-6(1-2\sqrt{5})\sqrt{10+2\sqrt{5}}} = \{\tfrac{1}{2}[9+\sqrt{5}-3\sqrt{10+2\sqrt{5}}]\}^4,$$

the curves (27) are equivalent, and the same is true of the curves (28). However, (27) is not equivalent to (28), since

$$1-35\sqrt{5}-6(1+2\sqrt{5})\sqrt{10-2\sqrt{5}} < 0 < 1+35\sqrt{5}-6(1-2\sqrt{5})\sqrt{10+2\sqrt{5}}$$

and Ω is real. Thus if we put

$$\sqrt{10+2\sqrt{5}}=2\alpha; \quad \sqrt{10-2\sqrt{5}}=2\alpha',$$

we have two inequivalent curves given by

$$A = 2[1+35\sqrt{5}+12(1-2\sqrt{5})\alpha]$$

and

$$A' = 2[1-35\sqrt{5}+12(1+2\sqrt{5})\alpha'].$$

Since $A'<0$, A' is no square in Ω, and since A and A' are conjugates, the same is true of A. Since $A>0$, A is not of the form $-4C^4$, and consequently the same is true of A'.

Since Ω is real, there are only 4 points of order 5 in Ω. If we choose the upper sign in (27), one of them is

$$\{(3+\sqrt{5})(2-\alpha); 2[6\alpha-(9+\sqrt{5})]\}.$$

Now let u be a point of order 25 with the coordinates (x, y) and

$$\wp(5u)=(3+\sqrt{5})(2-\alpha).$$

Let $\mathfrak{p}$ denote the ideal (α); then $\mathfrak{p}^4=5$, and every integer in Ω is $\equiv 0, \pm 1$ or $\pm 2 \pmod{\mathfrak{p}}$. We find $A\equiv 2$ and $\wp(5u)\equiv 1 \pmod{\mathfrak{p}}$. Consider the equation

$$[x-\wp(5u)]P_5^2=4y^2P_3Q_4(Q_4^2-P_5). \tag{32}$$

If $\mathfrak{p}/x$, $\mathfrak{p}$ will divide only the right member of (32), and if $x\equiv\pm 1 \pmod{\mathfrak{p}}$, $\mathfrak{p}$ will divide only the left member. If $x\equiv\pm 2 \pmod{\mathfrak{p}}$, we find $y^2\equiv\mp 1$; $P_3\equiv 1$; $Q_4\equiv 1$; $P_5\equiv -2$, and the two members of (32) become incongruent. Thus there is no point of order 25 in Ω, and we have the following result:

Lemma 4. *If Ω is a quartic field, the points of order 5^ν $(\nu\geqq 0)$ in Ω on the curve (2) form the following group:*

1. *Ω does not contain $\sqrt{-1}$, and $\Omega\neq k(\sqrt{10+2\sqrt{5}})$.*

   (1).

2. *Ω contains $\sqrt{-1}$.*

   (1), if $A\neq(1\pm 2i)C^4$;

   (5), if $A=(1\pm 2i)C^4$.

3. $\Omega = k(\sqrt{10+2\sqrt{5}})$.

(1), if $A \neq 2[1 \pm 35\sqrt{5} + 6(1 \mp 2\sqrt{5})\sqrt{10 \pm 2\sqrt{5}}]C^4$;

(5), if $A = 2[1 \pm 35\sqrt{5} + 6(1 \mp 2\sqrt{5})\sqrt{10 \pm 2\sqrt{5}}]C^4$.

Here C denotes any number in Ω.

20. If the three lemmas are combined, we get the following theorem:

Theorem 24. *If A belongs to the quartic field Ω, the curve*

$$y^2 = x^3 - Ax$$

has the following exceptional group in Ω:

1. *Ω does not contain any of the numbers $\sqrt{-1}$, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{10+2\sqrt{5}}$.*

(2), if $A \neq C^2$, $\neq -4C^4$;

(2, 2), if $A = C^2$;

(4), if $A = -4C^4$.

2. *Ω contains $\sqrt{-1}$ but is $\neq k(\sqrt{2}, \sqrt{-1})$, $\neq k(\sqrt{3}, \sqrt{-1})$, $\neq k(\sqrt{1 \pm 2i})$.*

(2), if $A \neq C^2$, $\neq (1 \pm 2i)C^4$;

(2, 2), if $A = C^2$, $\neq C^4$;

(4, 2), if $A = C^4$;

(2, 5), if $A = (1 \pm 2i)C^4$.

3. *Ω contains $\sqrt{2}$ but is $\neq k(\sqrt{2}, \sqrt{-1})$, $\neq k(\sqrt{2}, \sqrt{3})$, $\neq k(\sqrt{1 \pm \sqrt{2}})$.*

(2), if $A \neq C^2$, $\neq -4C^4$;

(2, 2), if $A = C^2$, $\neq C^4$;

(4), if $A = -4C^4$;

(4, 2), if $A = C^4$.

4. *Ω contains $\sqrt{3}$ but is $\neq k(\sqrt{3}, \sqrt{-1})$, $\neq k(\sqrt{3}, \sqrt{2})$, $\neq k(\sqrt{-(3 \pm 2\sqrt{3})})$.*

(2), if $A \neq C^2$, $\neq -4C^4$, $\neq -(3 \pm 2\sqrt{3})C^4$;

(2, 2), if $A = C^2$;

(4), if $A = -4C^4$;

(2, 3), if $A = -(3 \pm 2\sqrt{3})C^4$.

5. $\Omega = k(\sqrt{2}, \sqrt{-1})$.

(2), if $A \neq C^2$, $\neq (1 \pm 2i)\, C^4$;

$(2, 2)$, if $A = C^2$, $\neq C^4$;

$(4, 4)$, if $A = C^4$;

$(2, 5)$, if $A = (1 \pm 2i)\, C^4$.

6. $\Omega = k(\sqrt{3}, \sqrt{-1})$.

(2), if $A \neq C^2$, $\neq -(3 + 2\sqrt{3})\, C^4$, $\neq (1 \pm 2i)\, C^4$;

$(2, 2)$, if $A = C^2$, $\neq C^4$;

$(4, 2)$, if $A = C^4$;

$(2, 3, 3)$, if $A = -(3 + 2\sqrt{3})\, C^4$;

$(2, 5)$, if $A = (1 \pm 2i)\, C^4$.

7. $\Omega = k(\sqrt{2}, \sqrt{3})$.

(2), if $A \neq C^2$, $\neq -4\, C^4$, $\neq -(3 \pm 2\sqrt{3})\, C^4$;

$(2, 2)$, if $A = C^2$, $\neq C^4$;

(4), if $A = -4\, C^4$;

$(4, 2)$, if $A = C^4$;

$(2, 3)$, if $A = -(3 \pm 2\sqrt{3})\, C^4$.

8. $\Omega = k(\sqrt{1 \pm \sqrt{2}})$.

(2), if $A \neq C^2$, $\neq -4\, C^4$.

$(2, 2)$, if $A = C^2$; $\neq C^4$;

$(4, 2)$, if $A = C^4$;

(8), if $A = -4\, C^4$.

9. $\Omega = k(\sqrt{-(3 \pm 2\sqrt{3})})$.

(2), if $A \neq C^2$, $\neq -4\, C^4$, $\neq -(3 \mp 2\sqrt{3})\, C^4$;

$(2, 2)$, if $A = C^2$, $\neq -(3 \pm 2\sqrt{3})\, C^4$;

(4), if $A=-4C^4$;

(2, 3), if $A=-(3\mp 2\sqrt{3})C^4$;

(2,2,3), if $A=-(3\pm 2\sqrt{3})C^4$.

10. $\Omega=k(\sqrt{1\pm 2i})$ *(two different fields).*

(2), if $A\neq C^2,\ \neq(1\mp 2i)C^4$;

(2, 2), if $A=C^2,\ \neq C^4,\ \neq(1\pm 2i)C^4$;

(4, 2), if $A=C^4$;

(2, 5), if $A=(1\mp 2i)C^4$;

(2,2,5), if $A=(1\pm 2i)C^4$.

11. $\Omega=k(\sqrt{10+2\sqrt{5}})$.

(2), if $A\neq C^2,\ \neq -4C^4,\ \neq 2[1\pm 35\sqrt{5}+6(1\mp 2\sqrt{5})\sqrt{10\pm 2\sqrt{5}}]C^4$;

(2, 2), if $A=C^2$;

(4), if $A=-4C^4$;

(2, 5), if $A=2[1\pm 35\sqrt{5}+6(1\mp 2\sqrt{5})\sqrt{10\pm 2\sqrt{5}}]C^4$.

Here C denotes any number in Ω.

§ 5.

The exceptional group in the equianharmonic case

21. If B is a rational number, the exceptional group in $k(1)$ on the curve

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

is given by theorem 6, and NAGELL ([14], p. 11–15) has found the exceptional group on (3) in quadratic fields.

We shall now generalize these results and begin with a preliminary theorem:

Theorem 25. *Let Ω be an algebraic field containing the number B, and suppose that there is a point of order q in Ω on the curve*

$$y^2=x^3-B,$$

where q is a prime >3. Then 3 is the square of an ideal in Ω, and if there is a prime ideal in Ω with the norm 3, we have $q=7$.

Proof. Since the number of exceptional points in Ω is finite, their coordinates may be supposed to be integral. Let u be a point of order q with the coordinates $(x; y)$, and let $\mathfrak{p}$ be a prime ideal in Ω dividing 3. Suppose

$$\mathfrak{p}^m \| 3; \quad \mathfrak{p}^b \| B; \quad \mathfrak{p}^h \| x; \quad \mathfrak{p}^k \| y.$$

We may choose u in such a way that $\mathfrak{p}^h \nmid \wp(\nu u)$ $(\nu = 2, 3, \ldots, q-1)$. The polynomials $P_3(x)$ and $Q_4(x)$ may be written in the following manner:

$$\begin{aligned} P_3 &= 3x(y^2 - 3B); \\ Q_4 &= -2(y^4 - 18By^2 - 27B^2). \end{aligned} \tag{33}$$

If $b \neq 3h$, we find

$$2k \leqq b; \quad 2k \leqq 3h; \quad \mathfrak{p}^{m+h+2k} \| P_3; \quad \mathfrak{p}^{4k} \| Q_4; \quad \mathfrak{p}^{2k-2m-2h} \| \wp(3u) - x,$$

but $2k - 2m - 2h < h$, and this is impossible, since we have supposed $\mathfrak{p}^h \nmid \wp(3u)$. Hence $b = 3h$.

If $2k \leqq 3h + m$, we find $\mathfrak{p}^{m+h+2k} \mid P_3$, $\mathfrak{p}^{4k} \| Q_4$ and $\mathfrak{p}^h \nmid \wp(3u)$. Consequently $2k > 3h + m$ and $\mathfrak{p}^{2(2h+m)} \| P_3$.

If $4k > 3(2h+m)$, we find $\mathfrak{p}^{3(2h+m)} \| Q_4$, $\mathfrak{p}^{6(2h+m)} \| P_5$, $\mathfrak{p}^{8(2h+m)} \mid Q_6$ and generally

$$\mathfrak{p}^{\frac{1}{3}(\nu^2-1)(2h+m)} \| P_\nu, \quad \text{if } \nu \text{ is odd};$$

$$\mathfrak{p}^{\frac{1}{3}(\nu^2-4)(2h+m)} \mid Q_\nu, \quad \text{if } \nu \text{ is even},$$

but this is impossible, since $P_q = 0$.

If $4k < 3(2h+m)$, we find $\mathfrak{p}^{8k+1} \mid P_3^3$, $\mathfrak{p}^{4k} \| Q_4$, $\mathfrak{p}^{8k} \| P_5$, $\mathfrak{p}^{8k} \mid \frac{Q_6}{P_3}$ and generally

$$\mathfrak{p}^{\frac{1}{3}(\nu^2-1)k} \| P_\nu, \quad \text{if } \nu \equiv \pm 1 \pmod 6;$$

$$\mathfrak{p}^{\frac{1}{3}(\nu^2-4)k} \| Q_\nu, \quad \text{if } \nu \equiv \pm 2 \pmod 6;$$

$$\mathfrak{p}^{\frac{1}{3}(\nu^2-9)k} \mid \frac{P_\nu}{P_3}, \quad \text{if } \nu \equiv 3 \pmod 6;$$

$$\mathfrak{p}^{\frac{1}{3}(\nu^2-12)k} \mid \frac{Q_\nu}{P_3}, \quad \text{if } \nu \equiv 0 \pmod 6,$$

and this is impossible.

Consequently $4k = 3(2h+m)$, but then m must be an even number, and the first part of the theorem is proved.

Now suppose $N(\mathfrak{p}) = 3$ and $q \neq 7$. Since k is divisible by 3, we may put $k = 3n$. Then $m = 2(2n - h)$ and $n \geqq 1$. We have $\mathfrak{p}^{8n} \| P_3$ and $\mathfrak{p}^{12n} \mid Q_4$.

If $\mathfrak{p}^{12n+1}/Q_4$, we find $\mathfrak{p}^{24n}//P_5$, $\mathfrak{p}^{32n}//Q_6$, $\mathfrak{p}^{48n}//P_7$, $\mathfrak{p}^{60n+1}/Q_8$ and generally

$$\mathfrak{p}^{(\nu^2-1)n}//P_\nu, \quad \text{if} \quad \nu \equiv \pm 1 \pmod 4;$$

$$\mathfrak{p}^{(\nu^2-4)n}//Q_\nu, \quad \text{if} \quad \nu \equiv 2 \pmod 4;$$

$$\mathfrak{p}^{(\nu^2-4)n+1}/Q_\nu, \quad \text{if} \quad \nu \equiv 0 \pmod 4,$$

and this is impossible. Hence $\mathfrak{p}^{12n}//Q_4$. But it follows from (33) that

$$Q_4 \equiv y^4 - 27B^2 \pmod{\mathfrak{p}^{12n+1}},$$

and since the norm of $\mathfrak{p}$ is 3, we must have $y^4 \equiv -27B^2 \pmod{\mathfrak{p}^{12n+1}}$. Then, by (33), $P_3^3 \equiv -y^8 \pmod{\mathfrak{p}^{24n+1}}$, $Q_4 \equiv -y^4 \pmod{\mathfrak{p}^{12n+1}}$, and we find

$$P_\nu \equiv y^{\frac{1}{8}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)n+1}}, \quad \text{if} \quad \nu \equiv 1, 11, 23, 25, 29, 37 \pmod{42};$$

$$P_\nu \equiv -y^{\frac{1}{8}(\nu^2-1)} \pmod{\mathfrak{p}^{(\nu^2-1)n+1}}, \quad \text{if} \quad \nu \equiv 5, 13, 17, 19, 31, 41 \pmod{42};$$

$$\frac{P_\nu}{P_3} \equiv y^{\frac{1}{8}(\nu^2-9)} \pmod{\mathfrak{p}^{(\nu^2-9)n+1}}, \quad \text{if} \quad \nu \equiv 3, 27, 33 \pmod{42};$$

$$\frac{P_\nu}{P_3} \equiv -y^{\frac{1}{8}(\nu^2-9)} \pmod{\mathfrak{p}^{(\nu^2-9)n+1}}, \quad \text{if} \quad \nu \equiv 9, 15, 39 \pmod{42};$$

$$P_\nu \equiv 0 \pmod{\mathfrak{p}^{(\nu^2-1)n+1}}, \quad \text{if} \quad \nu \equiv 7, 35 \pmod{42};$$

$$\frac{P_\nu}{P_3} \equiv 0 \pmod{\mathfrak{p}^{(\nu^2-9)n+1}}, \quad \text{if} \quad \nu \equiv 21 \pmod{42};$$

$$Q_\nu \equiv y^{\frac{1}{8}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)n+1}}, \quad \text{if} \quad \nu \equiv 10, 20, 26, 34, 38, 40 \pmod{42};$$

$$Q_\nu \equiv -y^{\frac{1}{8}(\nu^2-4)} \pmod{\mathfrak{p}^{(\nu^2-4)n+1}}, \quad \text{if} \quad \nu \equiv 2, 4, 8, 16, 22, 32 \pmod{42};$$

$$\frac{Q_\nu}{P_3} \equiv y^{\frac{1}{8}(\nu^2-12)} \pmod{\mathfrak{p}^{(\nu^2-12)n+1}}, \quad \text{if} \quad \nu \equiv 18, 30, 36 \pmod{42};$$

$$\frac{Q_\nu}{P_3} \equiv -y^{\frac{1}{8}(\nu^2-12)} \pmod{\mathfrak{p}^{(\nu^2-12)n+1}}, \quad \text{if} \quad \nu \equiv 6, 12, 24 \pmod{42};$$

$$Q_\nu \equiv 0 \pmod{\mathfrak{p}^{(\nu^2-4)n+1}}, \quad \text{if} \quad \nu \equiv 14, 28 \pmod{42};$$

$$\frac{Q_\nu}{P_3} \equiv 0 \pmod{\mathfrak{p}^{(\nu^2-12)n+1}}, \quad \text{if} \quad \nu \equiv 0 \pmod{42}.$$

But it is seen that this contradicts $P_q = 0$, since $q \nmid 42$, and the theorem is proved.

22. Let Ω be an algebraic field, whose degree is indivisible by 2 and 3, and let B be a number in Ω. Then there is at most one point of order 2 in Ω on the curve (3), since Ω does not contain $\sqrt{-3}$, and it follows from theorem 8 that there is no point of order 4 in Ω, since $\sqrt{3}$ does not belong to Ω.

According to theorem 7, at most two finite points of inflexion belong to Ω, since Ω does not contain $\sqrt{-3}$. If these points have the abscissa 0, it is seen that $B=-C^2$, where C is a number in Ω. Let u be a point of order 9 with $\wp(u)=x$ and $\wp(3u)=0$. Then, by (5),

$$x P_3^2(x)+4(x^3+C^2)Q_4(x)=0,$$

that is

$$t^3+3t^2-24t+1=0,$$

where $t=\frac{4C^2}{x^3}$. Thus x does not belong to Ω, since t is of the third degree.

If $(\xi;\eta)$ is a point of inflexion in Ω and $\xi\neq 0$, the expression for P_3 given in (9) shows that $\xi^3=4B$ and hence

$$B=432\left(\frac{\eta}{3\xi}\right)^6.$$

Thus the curve is equivalent to

$$y^2=x^3-432,$$

whose rational points of order 3 are $(12;\pm 36)$. Let u be a point of order 9 with $\wp(u)=12z$ and $\wp(3u)=12$. Then, by (5),

$$12(1-z)P_3^2(12z)=4.432(4z^3-1)Q_4(12z),$$

that is

$$9z^2(z-1)^3(z^2+z+1)^2=(4z^3-1)(2z^6-10z^3-1). \tag{34}$$

Let $\mathfrak{p}$ be a prime ideal in $k(z)$ which divides 3, and suppose $\mathfrak{p}^m\,||\,3$. If we put $z=1+v$, (34) is transformed into

$$9v^3(v+1)^2(v^2+3v+3)^2=$$

$$=(4v^3+12v^2+12v+3)(2v^6+12v^5+30v^4+30v^3-18v-9). \tag{35}$$

Suppose $\mathfrak{p}^h\,||\,v$, and denote the left and right members of (35) by L and R, respectively. If $3h<m$, we find $\mathfrak{p}^{7h+2m}\,|\,L$, while $\mathfrak{p}^{9h}\,||\,R$, and this is impossible, since $7h+2m>9h$. If $3h>m$, $\mathfrak{p}^{3h+2m}\,|\,L$ and $\mathfrak{p}^{3m}\,||\,R$, which is also impossible. Consequently $3h=m$ and $\mathfrak{p}^{13h}\,||\,L$. We may, however, write

$$R=\tfrac{1}{8}(4z^3-1)[(4z^3-1)^2-18(4z^3-1)-27].$$

Suppose $\mathfrak{p}^k\,||\,4z^3-1$; then $k\geqq 3h$. If $2k\geqq 9h$, we find $\mathfrak{p}^{13h+1}\,|\,R$. Thus $2k<9h$, but then $\mathfrak{p}^{3k}\,||\,R$, and hence $3k=13h$. But this implies $h=3$ and $m=9$, and it follows that (34) is irreducible in $k(1)$.

We have reached the following result, which is quite analogous to theorem 6:

Theorem 26. *Let Ω be an algebraic field, whose degree is indivisible by 2 and 3. If B is a number in Ω, the curve*

$$y^2 = x^3 - B$$

has the following exceptional group in Ω:

(1), if $B \neq C^3$, $\neq -C^2$, $\neq 432\,C^6$;

(2), if $B = C^3$, $\neq -C^6$;

(3), if $B = -C^2$ or $= 432\,C^6$ but $\neq -C^6$;

(2, 3), if $B = -C^6$.

Here C denotes any number in Ω.

23. Now let Ω be a quadratic field. If there is a point of order 4 in Ω, theorem 8 may be used to show that $\Omega = k(\sqrt{3})$ and that the curve is equivalent to

$$y^2 = x^3 + (3 \pm 2\sqrt{3})^3;$$

these two curves are inequivalent. We choose the upper sign and find the points

$$[3 + \sqrt{3};\ \pm 3\,(3 + 2\sqrt{3})]$$

of order 4. Let u be a point of order 8 with $\wp(u) = x$ and $\wp(2u) = 3 + \sqrt{3}$, and put $\varepsilon = 2 + \sqrt{3}$. Then by (5),

$$4\,[x^3 + (\sqrt{3})^3\,\varepsilon^3]\,[x - \sqrt{3}\,(1 + \sqrt{3})] = 3\,x\,[x^3 + 4\,(\sqrt{3})^3\,\varepsilon^3]. \tag{36}$$

Suppose that x belongs to $k(\sqrt{3})$ and put $\mathfrak{p} = (1 + \sqrt{3})$; then $\mathfrak{p}^2 = 2$. If the two members of (36) are denoted by L and R, we see that $\mathfrak{p} \mid L$ and hence $\mathfrak{p} \mid x$, but if $\mathfrak{p} \parallel x$, we find $\mathfrak{p}^5 \mid L$ and $\mathfrak{p}^4 \parallel R$, and if $\mathfrak{p}^2 \mid x$, we find $\mathfrak{p}^5 \parallel L$ and $\mathfrak{p}^6 \mid R$. Thus x does not belong to $k(\sqrt{3})$.

A point of order 9 in Ω is impossible, as was shown in no. **22**. If the 8 finite points of inflexion belong to Ω, we have $\Omega = k(\sqrt{-3})$, and it was seen in no. **22** that the curve is equivalent to

$$y^2 = x^3 - 16.27,$$

but now this curve may be replaced by

$$y^2 = x^3 + 16,$$

since -27 is the sixth power of a number in Ω.

In order to determine the conditions for a point of order 7 in Ω we put $A=0$ in theorem 4. If t is a number satisfying

$$\varphi(t)=t^6-11t^5+30t^4-15t^3-10t^2+5t+1=0,$$

and if $z=\dfrac{t^3-3t+1}{t(t-1)}$, we find

$$z^2-11z+25=0;$$

hence $k(t)$ contains $\sqrt{21}$. Let $\mathfrak{p}$ be a prime ideal in $k(t)$ which divides 3. Since $\varphi(0)=\varphi(1)=1$ and $\varphi(-1)=43$, $\mathfrak{p}$ does not divide any of the numbers $t, t\pm1$. Consequently the norm of $\mathfrak{p}$ is >3 and $k(t)\neq k(\sqrt{21})$. It follows that $\varphi(t)$ is irreducible in $k(1)$.

Now theorem 4 shows that if there is a point of order 7 in Ω on the curve (3), then $\Omega=k(\sqrt{-3})$, and the curve is equivalent to

$$y^2=x^3\pm8(\sqrt{-3})^3(1\pm3\sqrt{-3}).$$

These two curves are inequivalent in $k(\sqrt{-3})$. If we choose the upper sign, the points of order 7 are $(4\sqrt{-3};\ \pm12\varrho^2\sqrt{-3})$, $(4\varrho\sqrt{-3};\ \pm12\varrho^2\sqrt{-3})$ and $(4\varrho^2\sqrt{-3};\ \pm12\varrho^2\sqrt{-3})$, where $\varrho=\frac{1}{2}(-1+\sqrt{-3})$. It is easy to show that there are only 7 exceptional points in Ω in this case (see NAGELL [13], p. 12).

We have proved the following theorem:

Theorem 27. *If B belongs to the quadratic field Ω, the curve*

$$y^2=x^3-B$$

has the following exceptional group in Ω:

1. $\Omega\neq k(\sqrt{3}),\ \neq k(\sqrt{-3})$.

   (1), if $B\neq C^3,\ \neq -C^2,\ \neq 432\,C^6$;

   (2), if $B=C^3,\ \neq -C^6$;

   (3), if $B=-C^2$ or $=432\,C^6$ but $\neq -C^6$;

   (2, 3), if $B=-C^6$.

2. $\Omega=k(\sqrt{3})$.

   (1), if $B\neq C^3,\ \neq -C^2,\ \neq 432\,C^6$;

   (2), if $B=C^3,\ \neq -C^6,\ \neq -(3\pm2\sqrt{3})^3\,C^6$;

   (4), if $B=-(3\pm2\sqrt{3})^3\,C^6$;

   (3), if $B=-C^2$ or $=432\,C^6$ but $\neq -C^6$;

   (2, 3), if $B=-C^6$.

3. $\Omega = k(\sqrt{-3})$.

(1), if $B + C^3, \neq -C^2, \neq \pm 8(\sqrt{-3})^3 (1 \mp 3\sqrt{-3})\, C^6$;

(2, 2), if $B = C^3, \neq -C^6$;

(3), if $B = -C^2, \neq -16\, C^6, \neq -C^6$;

(3, 3), if $B = -16\, C^6$;

(2,2,3), if $B = -C^6$;

(7), if $B = \pm 8(\sqrt{-3})^3 (1 \mp 3\sqrt{-3})\, C^6$.

Here C denotes any number in Ω.

24. Finally let Ω be a cubic field. It follows from theorem 8 that there is no point of order 4 in Ω on the curve (3), and since Ω does not contain $\sqrt{-3}$, there cannot be more than one point of order 2 and two points of order 3.

If $-B$ is not a square in Ω, it was shown in no. **22** that no point of order 9 belongs to Ω. If $B = -C^2$ and if u is a point of order 9 with the coordinates $(x; y)$ and $\wp(3u) = 0$, we have seen in no. **22** that

$$t^3 + 3t^2 - 24t + 1 = 0,$$

where $t = \frac{4C^2}{x^3}$. It is convenient to substitute $t = 3s - 1$; then

$$s^3 - 3s + 1 = 0. \tag{37}$$

It will be found that

$$B = -\frac{16t}{(t+4)^3}\left(\frac{y}{x}\right)^6,$$

and if we choose $\frac{y}{x} = 3$, we get

$$\begin{aligned} B &= -144(4s^2 - 7s + 2); \quad C = \pm 12(s^2 - s); \\ x &= -4(s^2 - s - 2); \qquad y = -12(s^2 - s - 2). \end{aligned} \tag{38}$$

The remaining roots of (37) are

$$s' = s^2 - 2;$$

$$s'' = -s^2 - s + 2,$$

and if these numbers are substituted for s, we get

$$B' = 144(11s^2 + 4s - 32);$$

$$B'' = -144(7s^2 + 11s - 4).$$

The three curves obtained in this way are, however, equivalent, since

$$\frac{B}{B'} = s^6 \quad \text{and} \quad \frac{B'}{B''} = (s')^6.$$

We choose the curve given by (38).

Since s and $s+1$ are both odd, the ideal 2 is a prime ideal in $k(s)$. Hence C is not a cube, since it is divisible by 2 but not by 8, and consequently there is no point of order 2 in Ω.

The number $\pi = s+1$ satisfies

$$\pi^3 - 3\pi^2 + 3 = 0;$$

hence (π) is a prime ideal $\mathfrak{p}$ satisfying $\mathfrak{p}^3 = 3$. Suppose that u is a point of order 27 in $k(s)$ with $\wp(u) = 4z$ and $\wp(3u) = -4(s^2 - s - 2) = -4\pi(\pi - 3)$. Then the equation (5)

$$[\wp(3u) - 4z] P_3^2(4z) = 4[(4z)^3 - B] Q_4(4z)$$

may be written

$$9z^2[z + \pi(\pi-3)](z^3 + 9\varepsilon^2)^2 = (4z^3 + 9\varepsilon^2)(2z^6 + 90\varepsilon^2 z^3 - 81\varepsilon^4), \tag{39}$$

where $\varepsilon = s^2 - s = (\pi - 1)(\pi - 2)$; the two members of (39) will be denoted by L and R. It is seen that $\mathfrak{p}^2 // z$; then $\mathfrak{p}^{24} / L$, and since

$$8R = (4z^3 + 9\varepsilon^2)[(4z^3 + 9\varepsilon^2)^2 + 162(4z^3 + 9\varepsilon^2)\varepsilon^2 - 3^7\varepsilon^4],$$

we have $\mathfrak{p}^8 / 4z^3 + 9\varepsilon^2$. If $z \equiv \pi^2 \pmod 3$, it will, however, be found that $\mathfrak{p}^6 // 4z^3 + 9\varepsilon^2$, and hence $z = 3\alpha - \pi^2$, where α is an integer. Then $\mathfrak{p}^9 / z^3 + 9\varepsilon^2$ and $\mathfrak{p}^{31} / L$. But if $\mathfrak{p}^{31} / R$, we must have $\mathfrak{p}^{11} / 4z^3 + 9\varepsilon^2$ and hence $\mathfrak{p}^9 // z^3 + 9\varepsilon^2$. Now $\mathfrak{p}^{32} / R$ and consequently $\mathfrak{p}^4 / z + \pi(\pi - 3)$, which implies $\mathfrak{p} / \alpha$. But then

$$4z^3 + 9\varepsilon^2 = 27[4\alpha^3 - 4\pi^2\alpha^2 + 4(3\pi^2 - \pi - 3)\alpha - (8\pi^2 + \pi - 15)]$$

is not divisible by $\mathfrak{p}^{11}$.

Consequently no point of order 27 belongs to Ω, and we have proved the following theorem:

Theorem 28. *If B belongs to the cubic field Ω, the curve*

$$y^2 = x^3 - B$$

has the following exceptional group in Ω:

1. $\Omega \neq k(\sqrt[3]{2}),\ \neq k(\varrho\sqrt[3]{2}),\ \neq k(\varrho^2\sqrt[3]{2})$ *and* $\neq k(s)$, *where* $s^3-3s+1=0$.

   (1), if $B \neq C^3,\ \neq -C^2,\ \neq 432\,C^6$;

   (2), if $B = C^3,\ \neq -C^6$;

   (3), if $B = -C^2$ or $= 432\,C^6$ but $\neq -C^6$;

   (2, 3), if $B = -C^6$.

2. $\Omega = k(\sqrt[3]{2})$ *or* $= k(\varrho\sqrt[3]{2})$ *or* $= k(\varrho^2\sqrt[3]{2})$.

   (1), if $B \neq C^3,\ \neq -C^2$;

   (2), if $B = C^3,\ \neq -C^6,\ \neq 27\,C^6$;

   (3), if $B = -C^2,\ \neq -C^6$;

   (2, 3), if $B = -C^6$ or $= 27\,C^6$.

3. $\Omega = k(s)$, *where* $s^3-3s+1=0$ (*a normal field*).

   (1), if $B \neq C^3,\ \neq -C^2,\ \neq 432\,C^6$;

   (2), if $B = C^3,\ \neq -C^6$;

   (3), if $B = -C^2$ or $= 432\,C^6$ but $\neq -C^6,\ \neq -144\,(4s^2-7s+2)\,C^6$;

   (9), if $B = -144\,(4s^2-7s+2)\,C^6$;

   (2, 3), if $B = -C^6$.

Here C *denotes any number in* Ω, *and* $\varrho = \frac{1}{2}(-1+\sqrt{-3})$.

BIBLIOGRAPHY

[1] BILLING, G. Beiträge zur arithmethischen Theorie der ebenen kubischen Kurven vom Geschlecht Eins, Nova Acta Reg. Soc. Sci. Ups., Ser. IV, vol. 11, n:o 1, Uppsala 1938.

[2] BILLING, G. and MAHLER, K. On exceptional points on cubic curves, Journal London Math. Soc., vol. 15 (1940), p. 32–43.

[3] BILLING, G. A diophantine equation with seven solutions, Arkiv f. matematik, astronomi och fysik, band 27 A, n:o 14 (1940).

[4] ——. A diophantine equation with nine solutions, Arkiv f. matematik, astronomi och fysik, band 27 B, n:o 8 (1940).

[5] FUETER, R. Über kubische diophantische Gleichungen, Commentarii Mathematici Helvetici, vol. 2 (1930), p. 69.

[6] HURWITZ, A. Über ternäre diophantische Gleichungen dritten Grades, Mathematische Werke, Bd. 2, p. 446.

[7] LEVI, B. Saggio per una teoria aritmetica delle forme cubiche ternarie, Atti Accademia di Torino 41 (1906), p. 739; 43 (1908), p. 99, 413, 672; Atti del IV Congresso internazionale dei matematici Roma 1908, 2, p. 173.

[8] LIND, C. E. Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins, Inaugural-Dissertation, Uppsala 1940.
[9] MAHLER, K. and BILLING, G. On exceptional points on cubic curves, Journal London Math. Soc., vol. 15 (1940), p. 32—43.
[10] NAGELL, T. Sur les propriétés arithmétiques des cubiques planes du premier genre, Acta mathematica, vol. 52 (1928), p. 93.
[11] ——. Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre, Skrifter utg. av det Norske Videnskaps-Akademi i Oslo, 1935, Mat.-naturv. kl., n:o 1.
[12] ——. Sur la résolubilité des équations diophantiennes cubiques à deux inconnues dans un domaine relativement algébrique, Nova Acta Reg. Soc. Sci. Ups., Ser. IV, vol. 13, n:o 3, Uppsala 1942.
[13] ——. Les points exceptionnels sur les cubiques planes du premier genre, Nova Acta Reg. Soc. Sci. Ups., Ser. IV, vol. 14, n:o 1, Uppsala 1946.
[14] ——. Les points exceptionnels sur les cubiques planes du premier genre II, Nova Acta Reg. Soc. Sci. Ups., Ser. IV, vol. 14, n:o 3, Uppsala 1947.
[15] ——. Recherches sur l'arithmétique des cubiques planes du premier genre dans un domaine de rationalité quelconque, Nova Acta Reg. Soc. Sci. Ups., Ser. IV, vol. 15, n:o 4, Uppsala 1952.
[16] WEIL, A. L'arithmétique sur les courbes algébriques, Acta mathematica, vol. 52 (1929), p. 281.
[17] CHÂTELET, F. Points exceptionnels d'une cubique de Weierstrass, Comptes rendus des séances de l'Académie des Sciences, Paris, t. 210 (1940), p. 90.

Tryckt den 2 juli 1953

Uppsala 1953. Almqvist & Wiksells Boktryckeri AB