INTEGERS AND BASIS OF A NUMBER FIELD*

BY
N. R. WILSON

I. INTRODUCTION

The existence theorems of the standard theory of algebraic numbers do not always lead to very practicable methods of computation in individual cases. Such methods of computation form the main subject of this paper. The basis set up appears at the same time to have some advantage of simplicity for theoretical purposes. The numbers of the field are first expressed in terms of a special set of integers, from which the basis is obtained in the third section. In the remaining sections, methods of computing this special set are discussed, illustrated by the general cubic.

Let $A_n z^n + A_{n-1}z^{n-1} + \cdots + A_0 = 0$ be the equation defining the field, all A's being rational integers and $A_n \neq 0$. Let d be the greatest rational integer such that $d^r / A_{n-\gamma} A_n^{r-1}$ †for all of $r = 1,2, \cdots, n$. Then the substitution $xd = zA_n$ reduces this equation to $x^n + B_{n-1}x^{n-1} + \cdots + B_0 = 0$, the B's being rational integers. This form of the equation we call the *normal form*. Its defining features are (i) the coefficient of x^n is 1 and all B's are rational integers; (ii) there exists no rational prime p such that p^r / B_{n-r} for all of $r = 1, 2, \cdots, n$. We may, if we please, make $B_{n-1} = 0$. These transformations, being rational, do not affect the field.

To minimize the verbiage, we use the following notation and terms, the the latter mostly self-descriptive. The integers $1, x, x^2, \cdots, x^{n-1}$ we call *ordinary integers*; also the sums and differences of such. These letters and y, z, Y, Z denote algebraic integers. The remaining letters, $a, b, \cdots, w$, and the corresponding capitals, denote rational integers, p being reserved for primes and $p_1, p_2, \cdots$ denoting distinct primes. Greek letters denote rational numbers. If an algebraic integer is of the form $\alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$, $m \leqq n - 1$, $\alpha_m \neq 0$, and each α in its lowest terms, we say that it is of degree m in x, abbreviated $(\alpha_0, \alpha_1, \cdots, \alpha_m)$. If also $-\frac{1}{2} < \alpha \leqq \frac{1}{2}$ for each α and $\alpha_m = 1 \div D_m$ where $D_m > 0$, we call it a *reduced integer*. If y is a reduced integer and the denominators of the α's are powers of one and the same prime, we call y a *single-prime reduced integer*. If y is a single-prime reduced integer and $\alpha_m = 1 \div p^t$ where t is the greatest possible, we say that y is a *maximal reduced integer* in p of degree m.

* Presented to the Society, December 29, 1925; received by the editors in February, 1926.

† The symbol / throughout denotes "is a factor of."

THEOREM I. *If p^k is the highest power of p occurring in the denominator of any α of the single-prime reduced integer $\alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$, then p^{2k} is a factor of the discriminant of the field equation.**

$$\begin{vmatrix} 1 & x & x^2 & \cdots & x^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{vmatrix}$$

Let $y = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}$ be the integer and $y_2 = \alpha_0 + \alpha_1 x_2 + \cdots + \alpha_{n-1} x_2^{n-1}$, $\cdots$, $y_n = \alpha_0 + \alpha_1 x_n + \cdots + \alpha_{n-1} x_n^{n-1}$ be its conjugates. The determinant D on the left, when squared, gives the discriminant, Δ. Let α_r, $r \leqq m$, be any coefficient which contains p^k in its denominator. Multiplying the equations above by the co-factors of x^r, x_2^r, $\cdots$, x_n^r in D and adding, we obtain on the right $\alpha_r D$, and on the left a determinant D' which is not affected, except for a change of sign, if we interchange a pair of conjugate roots. Hence D'^2 also is a symmetric function of the roots; rational and, since the coefficient of x^n is 1, integral in the remaining coefficients B. Since $\Delta = D^2$ and $\Delta \neq 0$, $\alpha_r^2 = D'^2 \div D^2$ or p^{2k}/Δ.

COROLLARY 1. *If there exists a single-prime reduced integer in p of degree m in x, there exists a maximal reduced integer in p of degree m in x.*

For, since p^{2k}/Δ, k for α_m is bounded and is a rational integer. Hence k must have a rational integral maximum, t.

COROLLARY 2. *The maximal reduced integers in a given field are finite in number.*

For m is restricted to the range 0, 1, 2, $\cdots$, $n - 1$; p to the primes such that p^2/Δ. For each m and p there can be only one maximum t of the last corollary. The coefficients α are limited by the relation $-\frac{1}{2} < \alpha \leqq \frac{1}{2}$. The number of each is finite, and therefore also the number of maximal reduced integers.

II. EXPRESSION BY ORDINARY AND MAXIMAL REDUCED INTEGERS

We prove first that any integer can be expressed in terms of† ordinary and maximal reduced integers, using not more than one of the latter for

---

* The discriminant Δ of the field equation throughout this paper denotes the product of the squared differences of the roots, without the additional numerical factor of some current definitions. We suppose always that $\Delta \neq 0$.

† For simplicity, when ambiguity is not likely to arise, "expressed in terms of" is used to abbreviate "expressed as a rational linear homogeneous function, with rational integral coefficients, of" except in enunciating theorems.

each m and p. If $M = p_1^{k_1} p_2^{k_2} \cdots$ is the L. C. M. of the denominators of the coördinates in $y = (\alpha_0, \alpha_1, \cdots, \alpha_m)$; and if $u_1, u_2, \cdots$ are non-zero solutions of

$$M\left(\frac{u_1}{p_1^{k_1}} + \frac{u_2}{p_2^{k_2}} + \cdots\right) = 1$$

(the notation implying that they are rational integers); then $y = u_1 y_1 + u_2 y_2 + \cdots$, where

$$y_r = \frac{M}{p_r^{k_r}} y.$$

Each y_r contains in its denominators the same powers of p_r as in the corresponding denominators of y, and powers of p_r only. It will be sufficient therefore to prove the result for an integer y, all of whose denominators are powers of one prime p.

If y is such an integer of degree k in x, then $y - (a_1, a_2, \cdots, a_k)$ is also an integer. Hence y is the sum of ordinary integers and an integer of the form

$$y' = \left(\frac{b_0}{p^{t_0}}, \frac{b_1}{p^{t_1}}, \cdots, \frac{b_m}{p^{t_m}}\right),$$

where $-\frac{1}{2} < (b \div p^t) \leqq \frac{1}{2}$, $b_m \not\equiv 0$ and prime to p. If $ub_m + vp^{t_m} = 1$, $uy' + vx^m$, apart from ordinary integers, is a single-prime reduced integer, $(\beta_0, \beta_1, \cdots, 1 \div p^{t_m})$. Hence a maximal reduced integer in p of degree m in x exists (Theorem I, Corollary 1); viz. $Y_m = (\gamma_0, \gamma_1, \cdots, 1 \div p^t), t \geqq t_m$.

Consider the integer $y - b_m p^{t-t_m} Y_m$. The coefficient of x^m is 0, so that it is of degree $<m$ in x. If this difference is not expressible in terms of ordinary integers, we obtain in a similar manner a single-prime reduced integer, $(\beta_0', \beta_1', \cdots, b_s' \div p^{u_s})$, and a corresponding maximal reduced integer, $Y_s = (\gamma_0, \gamma_1, \cdots, 1 \div p^u)$ of degree s in $x, s < m$ and $u \geqq u_m$, and consider the difference $(y - b_m p^{t-t_m} Y_m) - b_s p^{u-u_s} Y_s$. Continuing this process so long as the difference is not expressible in terms of ordinary integers, we must, after m steps if not before, obtain a difference which is integral and of degree 0 in x; i.e., a rational integer. Hence y is expressible in terms of $Y_m, Y_s, \cdots$ and ordinary integers. As all maximal reduced integers in p of degree m in x have the same highest coefficient, any one with the same m and p may be used in making these reductions.

THEOREM IIa. *All integers of the field can be expressed as rational linear homogeneous functions with rational integral coefficients of ordinary integers and maximal reduced integers, the latter consisting of one selected arbitrarily from those in each prime and for each degree in x for which such exist.*

COROLLARY. *The difference between two integers in* p,

$$\left(\frac{a_0}{p^{t_0}}, \frac{a_1}{p^{t_1}}, \cdots, \frac{a_m}{p^v}\right)$$

and

$$\left(\frac{b_0}{p^{u_0}}, \frac{b_1}{p^{u_1}}, \cdots, \frac{a_m}{p^v}\right),$$

of the same degree in x *and with the same highest coefficient, is expressible in terms of ordinary integers and maximal reduced integers in* p, *both of lower degree in* x.

THEOREM IIb. *If* p *is a prime occurring in the denominator of some coordinate of an integer, then* (i) *there exists exactly one maximal reduced integer* Y_r, *in* p *of lowest degree* r *in* x, $r > 0$; (ii) *if* $r < n - 1$, *there exist maximal reduced integers in* p *of degrees* $r + 1, r + 2, \cdots, n - 1$ *in* x; *and* (iii) *for each* u, $0 < u < t$, *there is one and but one single-prime reduced integer,* $(\beta_0, \beta_1, \cdots, 1 \div p^u)$ *of degree* r *in* x *differing from* $p^{t-u}Y$ *by ordinary integers, where* $Y_r = (\gamma_0, \gamma_1, \cdots, 1 \div p^t)$.

As in Theorem Ia, there exists a single-prime reduced integer and therefore a maximal reduced integer in p of some degree m in x. Since m has 0 for a lower bound and is a rational integer, there exists at least one of some lowest degree r. We must have $r > 0$; for any rational number which is also an integer must be a rational integer. If there were two of this lowest degree in x, since their highest coefficients are the same, their difference leads to a single-prime reduced integer of lower degree, since $-\frac{1}{2} < \alpha \leqq \frac{1}{2}$. From Corollary 1, Theorem Ia, we should then have a maximal reduced integer of degree r', $r' < r$, the least degree in x.

If Y_r is this one and $r < n - 1$, then $xY_r, x^2Y_r, \cdots, x^{n-r+1}Y_r$ are single-prime reduced integers in p of degrees $r + 1, r + 2, \cdots, n - 1$, in x, hence, by the same corollary, there are maximal reduced integers of these degrees in x. The integer given in (iii) shows that there is at least one integer for each u; that there cannot be more than one follows exactly as in (i).

COROLLARY. *The maximal reduced integers of degree* $r + 1$ *in* x *are of the form* $Y_{r+1} + mY_r$, *where* $m = 0, 1, 2, \cdots, (p^t - 1)$ *and* Y_{r+1} *is any one of them; those of degree* $r + 2$ *in* x *of the form* $Y_{r+2} + nY_{r+1} + mY_r$, *where also* $n = 0, 1, 2, \cdots, (p^u - 1), 1 \div p^u$ *being the highest coefficient in* Y_{r+2}, *any one of them, and so on.*

THEOREM IIc. If $(a_0 \div p^{t_0}, a_1 \div p^{t_1}, \cdots, 1 \div p^{t_m})$ *is a maximal reduced integer in* p *of degree* m *in* x *then* $t_s \leqq t_m$ *for* $s < m$.

For the lowest degree r of the preceding theorem, let

$$Y_r = \left(\frac{a_0}{p^{t_0}}, \frac{a_1}{p^{t_1}}, \cdots, \frac{1}{p^{t_r}}\right).$$

If possible, let any t_s, $s < r$, be the last index exceeding t_r. Then the integer $p^{t_r}Y_r$ leads to the single-prime reduced integer $(\beta_0, \beta_1, \cdots, 1 \div p^u)$, of degree s in x, where $u = t_s - t_r$. There is therefore a maximal reduced integer of degree s in x, $s < r$, contrary to hypothesis with respect to r.

For degree $r + 1$ in x if $r < n - 1$, we have

$$xY_r = \frac{a_0}{p^{t_0}} x + \frac{a_1}{p^{t_1}} x^2 + \cdots + \frac{1}{p^{t_r}} x^{r+1}.$$

If

$$Y_{r+1} = \frac{b_0}{p^{u_0}} + \frac{b_1}{p^{u_1}} x + \cdots + \frac{b_r}{p^{u_r}} x^r + \frac{1}{p^{t_r+v}} x^{r+1}$$

is a maximal reduced integer of degree $r + 1$ in x, the difference $p^vY_{r+1} - xY_r$ is of degree $< r + 1$, and therefore of the form cY_r. Examining the coefficient of x^k, the degree of p in $(b_k \div p^{u_k-v}) - (a_{k-1} \div p^{t_{k-1}})$ cannot exceed t_r. Since $t_{k-1} \leqq t_r$, we have $u_k - v \leqq t_r$ or $u_k < t_r + a$, the index of the highest coefficient in Y_{r+1}. Replacing r by $r + 1$, the same result follows in similar fashion for Y_{r+2}, the sole change being that the difference is of the form $cY_{r+1} + dY_r$ instead of cY_r. Similarly for all degrees in x up to $n - 1$. (This property obviously does not hold for single-prime reduced integers in general unless all maximal reduced integers of degrees $< m$ in x are of degree 1 in p.)

COROLLARY. *If $t_r, t_{r+1}, \cdots, t_{n-1}$ denote the degrees of p in the highest coefficients for a series of maximal reduced integers in p, $Y_r, Y_{r+1}, \cdots, Y_{n-1}$, of the degrees in x indicated by the subscripts, then $t_r \leqq t_{r+1} \leqq \cdots \leqq t_{n-1}$; if $(n-1) \div r \geqq 2$, then $kt_r \leqq t_m$ for $m \geqq kr$, where k is any integer $\not> (n - 1) \div r$.*

For the degree of p in the highest coefficient of Y_{m+1} must be at least the degree in xY_m and therefore not less than the degree in Y_m. Also if $m \geqq kr$, the degree of p in the highest coefficient of Y_m must be at least that in Y_r^k.

THEOREM IId. *If $r, r < n - 1$, be the lowest degree in x for which a maximal reduced integer in p exists, then there exist single-prime reduced integers of every degree m in x, $r < m \leqq n - 1$, such that $\alpha_r = \alpha_{r+1} = \cdots = \alpha_{m-1} = 0$.*

For, let

$$Y_m = \left(\alpha_0, \cdots, \frac{b}{p^{t_{m-1}}}, \frac{1}{p^{t_m}}\right) \text{ and } Y_{m-1} = \left(\alpha_0, \cdots, \frac{1}{p^{u_{m-1}}}\right)$$

be maximal reduced integers of degrees m and $m-1$ in x. Then $p^v Y_m - bp^w Y_{m-1}$, where $v = t_m - t_r$ and $w = t_m - t_{m-1} + u_{m-1} - t_r$, has $\alpha_{m-1} = 0$ and is an integer, since by the preceding theorem and corollary the indices v and w are not negative. Similarly, by subtracting proper multiples of $Y_{m-2}, \cdots, Y_r$, we may reduce the coefficients $\alpha_{m-2}, \cdots, \alpha_r$ to 0. (The coefficients can obviously be given any arbitrary values, those obtained being most convenient for use with § IV.)

III. Constructing a basis

Since the number of different primes which can occur in the denominator of an integer is finite (Theorem I), and for each there is a maximal reduced integer of lowest degree r' in $x, r' > 0$, there will be a lowest degree r, $r > 0$, for which any such occurs. For any k, $r \leqq k \leqq n-1$, let

$$y_{k,1} = \left(\alpha_0, \cdots, \frac{1}{p_1^{t_1}}\right), \quad y_{k,2} = \left(\alpha_0, \cdots, \frac{1}{p_2^{t_2}}\right), \cdots$$

be any selection of maximal reduced integers of degree k in x, one for each distinct prime for which such occur. Let $P_k = p_1^{t_1} p_2^{t_2} \cdots$ and let $v_1, v_2, \cdots$ be non-zero solutions of

$$P_k\left(\frac{v_1}{p_1^{t_1}} + \frac{v_2}{p_2^{t_2}} + \cdots\right) = 1.$$

Let Z_k be the reduced integer derived from $v_1 y_{k,1} + v_2 y_{k,2} + \cdots$ by removing ordinary integers as in §II. Then Z_k is of the form $(\beta_0, \beta_1, \cdots, 1 \div P_k)$. The coefficient of x^k in $P_k Z_k$ is 1, and, by Theorem IIc, lower powers of x reduce to ordinary integers. Hence x^k is expressible in terms of Z_k and ordinary integers of degrees $< k$. Also $(P_k \div p_s^{t_s}) Z_k$ is of the form $(\beta_0', \cdots, 1 \div p_s^{t_s})$. The corresponding reduced integer,

$$Y_{k,s} = \left(\beta_0'', \cdots, \frac{1}{p_s^{t_s}}\right),$$

is therefore a maximal reduced integer in p_s. Hence $Y_{k,s}$ is expressible in terms of Z_k and ordinary integers of degrees $< k$ in x.

For the basis, $\omega_1, \omega_2, \cdots, \omega_r, \omega_{r+1}, \cdots, \omega_n$, we take $1, x, \cdots, x^{r-1}, Z_r, Z_{r+1}, \cdots, Z_{n-1}$. These are linearly independent since each contains a power of x higher than the preceding. By Theorem IIa, every integer can

be expressed in terms of ordinary integers and the maximal reduced integers, $Y_{k,1}, Y_{k,2}, \cdots$ for $r \leqq k \leqq n-1$. Ordinary integers of degrees $< r$ in x are exactly $\omega_1, \omega_2, \cdots, \omega_r$. We have proved in the preceding paragraph that x^r and $Y_{r,1}, Y_{r,2}, \cdots$ can be expressed in terms of Z_r and ordinary integers of degrees $< r$ in x; i.e. in terms of ω_{r+1}, and $\omega_r, \cdots, \omega_1$. Also that x^{r+1} and $Y_{r+1,1}, Y_{r+2,1}, \cdots$ can be expressed in terms of Z_{r+1} and ordinary integers of degree $< r+1$ in x; i.e. in terms of ω_{r+2} and $\omega_{r+1}, \omega_r, \cdots, \omega_1$. And so on. Hence the given set actually form a basis. An integer of degree m in x can in fact be expressed in terms of $\omega_1, \cdots, \omega_{m+1}$.

The usual theorems follow at once. If $\omega_i' = \sum_{j=1}^{n} c_{ij}\omega_j$, $1 \leqq i \leqq n$, are linearly independent, the c's being rational integers, we can express each ω_i rationally and integrally in terms of the set ω', provided $|c_{ij}|^2 = 1$. Hence with this condition the set ω' also form a basis. The discriminant $\Delta_1(\omega_1', \cdots, \omega_n') = |c_{ij}|^2 \Delta_1(\omega_1', \cdots, \omega_n')$, and since $|c_{ij}|$ is rational, integral and $\neq 0$, $|c_{ij}|^2 \geqq 1$. Hence $\Delta_1(\omega_1, \cdots, \omega_n)$ is a minimum, and, if any $\Delta_1(\omega_1', \cdots, \omega_n') = \Delta_1(\omega_1, \cdots, \omega_n)$, $|c_{ij}|^2 = 1$ and the set ω' form a basis. Finally, since we have seen that the minimum degree for which maximal reduced integers exist is greater than 0, 1 is always a member of a basis constructed as above.

We may deduce a relation between the discriminant of the field and of the defining equation. In the field discriminant below, $\omega_1^{(1)} = 1$, $\omega_2^{(1)} = x, \cdots, \omega_r^{(1)} = x^{r-1}$, $\omega_{r+1}^{(1)} = \alpha_0 + \alpha_1 x + \cdots + (1 \div P_r)x^r, \cdots, \omega_n^{(1)} = \delta_0 + \delta_1 x + \cdots + (1 \div P_{n-1})x^{n-1}$. The columns, $\omega_2^{(i)}, \cdots, \omega_n^{(i)}$, $1 < i \leqq n$, are obtained by replacing x by its conjugates x_i. Keeping the first row unaltered, by subtracting proper multiples of preceding rows, we obtain the second determinant, on the left. (Thus, for the sth row, $s > r$, on subtracting the proper multiple of the $(s-1)$th row, we eliminate the terms x_i^{s-1}; from the difference, the proper multiple of the $(s-2)$th row, we eliminate x_i^{s-2}; and so on.) The latter determinant on inspection is seen to be $\Delta \div P_r^2 P_{r+1}^2 \cdots P_{n-1}^2$, where Δ denotes the discriminant of the equation defining the field.

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \omega_2^{(1)} & \omega_2^{(2)} & \cdots & \omega_2^{(n)} \\ \omega_3^{(1)} & \omega_3^{(2)} & \cdots & \omega_3^{(n)} \\ \cdot & \cdot & \cdots & \cdot \\ \omega_n^{(1)} & \omega_n^{(2)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2 = \Delta_1$$

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x & x_2 & \cdots & x_n \\ \cdot & \cdot & \cdots & \cdot \\ x^{r-1} & x_2^{r-1} & \cdots & x_n^{r-1} \\ \frac{1}{p^r}x^r & \frac{1}{p^r}x_2^r & \cdots & \frac{1}{p^r}x_n^r \\ \cdot & \cdot & \cdots & \cdot \\ \frac{1}{p_{n-1}}x^{n-1} & \frac{1}{p_{n-1}}x_2^{n-1} & \cdots & \frac{1}{p_{n-1}}x_n^{n-1} \end{vmatrix}^2 = \Delta_1$$

THEOREM III. *If Δ_1, Δ denote the discriminants of the field and of the equation defining the field, and P_r, P_{r+1}, $\cdots$, P_{n-1} are the denominators of the highest coefficients of the elements of the basis as above determined, other than those which are ordinary integers, then* $\Delta = P_r^2 P_{r+1}^2 \cdots P_{n-1}^2 \Delta_1$.

Since Δ_1 must be a rational integer,

COROLLARY. *If P_r, P_{r+1}, $\cdots$, P_{n-1} are the denominators of the highest coefficients of elements of the basis as above determined, other than those which are ordinary integers,* $(P_r P_{r+1} \cdots P_{n-1})^2$ *is a factor of* Δ.

IV. RELATIONS AMONG THE COÖRDINATES OF AN INTEGER; FIRST METHOD

If $y = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}$ is an integer, consider the product-equation

$$\Pi\{y - (\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1})\} = 0,$$

where x runs through the complete set of n conjugates, the field being given by the equation $x^n - B_{n-1}x^{n-1} + \cdots + B_0 = 0$. The coefficients of this equation, arranged in powers of y, are symmetric functions of the x's. Since the coefficient of x^n is 1, they are rational integral functions of the B's. Since the α's are rational, they are rational numbers. They are also integers, being the sums and products of integers. Hence they are rational integers.

The absolute term of this equation is the eliminant of $\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}$ and $x^n + B_{n-1}x^{n-1} + \cdots + B_0$, obtained by symmetric functions. Since the coefficients of α_0^n in the eliminant thus obtained and in the eliminant obtained in the more convenient Sylvester form below are the same, the eliminants are identical. We denote this eliminant by $E(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$. The left side of the above equation in y is $E(\alpha_0 - y, \alpha_1, \cdots, \alpha_{n-1})$.

THEOREM IVa. *If $y = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}$ is an integer, then all of*

$$\frac{1}{m!}\frac{\partial^m E}{\partial \alpha_0^m} \qquad (m = 0,1,2,\cdots,n-1)$$

and all of

$$\frac{1}{2!(n-2)!}\frac{\partial^{n-1} E}{\partial \alpha_0^{n-2}\partial \alpha_r} \qquad (r = 1,2,\cdots,n-1),$$

are rational integers; conversely, if all of

$$\frac{1}{m!}\frac{\partial^m E}{\partial \alpha_0^m} \qquad (m = 0,1,2,\cdots,n-1)$$

are rational integers, then y is an integer.

$$E = \begin{vmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & 0 & 0 & 0 \\ 0 & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & 0 & 0 \\ 0 & 0 & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 & 0 \\ 0 & 0 & 0 & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ B_0 & B_1 & B_2 & B_3 & 1 & 0 & 0 \\ 0 & B_0 & B_1 & B_2 & B_3 & 1 & 0 \\ 0 & 0 & B_0 & B_1 & B_2 & B_3 & 1 \end{vmatrix}$$

On inspection of the sample determinant on the left, we have that the coefficient of α_0^n is 1 and all partial differential coefficients with respect to the α's of order higher than n vanish. Also

$$\frac{1}{2!(n-2)!}\frac{\partial^n E}{\partial \alpha_0^{n-2}\partial \alpha_r^2} (1 \leqq r \leqq n-1)$$

is a rational integer. For the terms of E which do not vanish from the differentiation are those involving $\alpha_0^{n-2}\alpha_r^2$. The factors arising from the indices on differentiating such terms will cancel $2!(n-2)!$. The remaining factors are minors from the lowest $(n-1)$ rows and therefore rational integers.

The equation for y is $E(\alpha_0 - y, \alpha_1, \cdots, \alpha_{n-1}) = 0$, or

$$y^n - \frac{1}{(n-1)!}\frac{\partial^{n-1}E}{\partial \alpha_0^{n-1}} y^{n-1} + \frac{1}{(n-2)!}\frac{\partial^{n-2}E}{\partial \alpha_0^{n-2}} y^{n-2} - \cdots \pm \frac{\partial E}{\partial \alpha_0} y \mp E = 0,$$

on expanding by Taylor's Theorem. If the coefficients of the powers of y are rational integers, y is an integer, proving the converse part of the theorem. For the reasons stated in the first paragraph, these coefficients are rational integers if y is an integer, proving the first part of the necessary conditions. Hence in particular,

$$\frac{1}{(n-2)!}\frac{\partial^{n-2}E}{\partial \alpha_0^{n-2}}$$

is a rational integer. But if $(\alpha_0, \alpha_1, \cdots, \alpha_r, \cdots, \alpha_{n-1})$ is an integer, so also is $(\alpha_0, \alpha_1, \cdots, \alpha_r + 1, \cdots, \alpha_{n-1})$. Hence we have the rational integer

$$\frac{1}{(n-2)!}\frac{\partial^{n-2}}{\partial \alpha_0^{n-2}} E(\alpha_0, \alpha_1, \cdots, \alpha_r + 1, \cdots, \alpha_{n-1})$$

$$= \frac{1}{(n-2)!}\frac{\partial^{n-2}}{\partial \alpha_0^{n-2}} E(\alpha_0, \alpha_1, \cdots, \alpha_r, \cdots, \alpha_{n-1}) + \frac{1}{(n-2)!}\frac{\partial^{n-1}E}{\partial \alpha_0^{n-2}\partial \alpha_r} + \frac{1}{2!(n-2)!}\frac{\partial^{n-2}E}{\partial \alpha_0^{n-2}\partial \alpha_r^2}.$$

Since the first and last expressions on the right are rational integers, so also is the middle expression.

In applying this result, it will be found simplest to obtain E by forming $yx, yx^2, \cdots, yx^{n-1}$, reducing to degree $(n-1)$ by the field equation.* Thus for the cubic field, $x^3 + Qx + R = 0$, we have $y = \alpha_0 + \alpha_1 x + \alpha_2 x^2$, $yx = -R\alpha_2 + (\alpha_0 - \alpha_2 Q)x + \alpha_1 x^2$, $yx^2 = -R\alpha_1 - (\alpha_1 Q + \alpha_2 R)x + (\alpha_0 - \alpha_2 Q)x^2$, and obtain the rational integers from Theorem IVa: $\alpha_0^3 - 2\alpha_0^2\alpha_2 Q + \alpha_0\alpha_1^2 Q + 3\alpha_0\alpha_1\alpha_2 R + \alpha_0\alpha_2^2 Q^2 - \alpha_1^3 R - \alpha_1\alpha_2^2 QR + \alpha_2^3 R^2$; $3\alpha_0^2 - 4\alpha_0\alpha_2 Q + \alpha_1^2 Q + 3\alpha_1\alpha_2 R + \alpha_2^2 Q^2; 3\alpha_0 - 2\alpha_2 Q; 2\alpha_1 Q + 3\alpha_2 R; \alpha_0 Q - 3\alpha_1 R$; all but the last are obtained by direct differentiation, the last being simplified by the second preceding.

COROLLARY. *The Taylor expansion of*

$$\frac{1}{m!}\frac{\partial^m}{\partial\alpha_0^m} E(\alpha_0, \cdots, \alpha_{r-1}, \alpha_r + h, \alpha_{r+1}, \cdots, \alpha_{n-1})$$

in powers of h, less the first and last terms, is a rational integer for all rational integral values of h.

The rational integers obtained by the corollary can be simplified by the linear equations obtained from the theorem as in the last case above for the cubic, or by the following theorem.

THEOREM IVb. *If $A_1 h + A_2 h^2 + \cdots + A_m h^m$ is a rational integer for m unequal rational integral non-zero values of h, then every A_k is rational, its denominator being a factor of the product of the values of h and their differences; in particular, if this expression is a rational integer for $h = 1, 2, \cdots, m$, these denominators are factors of $m\,(m-1)^2\,(m-2)^3 \cdots 2^{n-1}$.*

$$\begin{vmatrix} h_1 & h_1^2 & h_1^3 & h_1^4 \\ h_2 & h_2^2 & h_2^3 & h_2^4 \\ h_3 & h_3^2 & h_3^3 & h_3^4 \\ h_4 & h_4^2 & h_4^3 & h_4^4 \end{vmatrix} = D$$

Substituting the given values, $h_1, \cdots, h_m$, in $A_1 h + A_2 h^2 + \cdots + A_m h^m$, and solving for the A's, the numerators are rational integers and the denominator is D on the left. By inspection, $h_1, h_2, \cdots, h_m$ and all differences are seen to be factors of D, accounting for all literal factors. From the principal diagonal, the remaining numerical factor is ± 1. Hence the denominators of the A's are factors of their product. In the particular case, these give the product stated. Applied to E for the cubic $x^3 + Qx + R = 0$, we obtain the rational integer

$$h\frac{\partial E}{\partial\alpha_1} + \frac{h^2}{2!}\frac{\partial^2 E}{\partial\alpha_1^2},$$

* This is equivalent to expanding the eliminant given above by Chiò's pivotal method, applied to the 1's in the principal diagonal.

so that, by Theorem IV b, $\partial E/\partial\alpha_1$ is a rational integer or one half such. As we are concerned only with maximal reduced integers, we have that, unless $p = 2$,

$$\frac{\partial E}{\partial \alpha_1} = 2\alpha_0\alpha_1 Q + 3\alpha_0\alpha_2 R - 3\alpha_1^2 R - \alpha_2^2 QR$$

for such is a rational integer; if $p = 2$, it is a rational integer divided by 2.

We have seen that there is no maximal reduced integer of degree 0 in x (§III). If

$$Y_1 = \frac{a_0}{p^{t_0}} + \frac{1}{p^{t_1}} x$$

is a maximal reduced integer of degree 1 in x, then Y_2 is of degree at least $2t_1$ in p, Y_3 at least $3t_1, \cdots, Y_{n-1}$ at least $(n-1)t_1$ (Corollary, Theorem IIc). Hence $p^{n(n-1)t_1}/\Delta$ (Theorem III). By Theorem IVa,

$$\frac{1}{(n-1)!}\frac{\partial^{n-1}E}{\partial\alpha_0{}^{n-1}} \text{ and } \frac{1}{2!(n-2)!}\frac{\partial^{n-1}E}{\partial\alpha_0{}^{n-2}\partial\alpha_1}$$

are rational integers. If $B_{n-1} = 0$, from E as given at the beginning of this section these reduce to $n\alpha_0$ and $B_{n-2}\alpha_1$ respectively. Hence

THEOREM IVc. *For the field* $x^n + B_{n-2}x^{n-2} + \cdots + B_0 = 0$, *the maximal reduced integer* $(a_0 \div p^{t_0}, a_1 \div p^{t_1})$ *can exist only if* (i) $p^{n(n-1)t_1}/\Delta$, (ii) p^{t_1}/B_{n-2} *and* (iii) $a_0 = 0$ *or* p^{t_0}/n.

COROLLARY. *If* $Y = (\alpha_0, \cdots, 1 \div p^{tm})$ *of degree* m *in* x *is a maximal reduced integer and* $n - 1 = qm + R$, $0 \leqq R < m$, *then* p^v/Δ, *where* $v = \{mq(q-1) + 2q(r+1)\}t_m$.

For $Y_m, Y_{m+1}, \cdots, Y_{2m-1}$ are of degrees at least t_m in p; $Y_{2m}, Y_{2m+1}, \cdots, Y_{3m-1}$, at least $2t_m, \cdots$; $Y_{qm}, \cdots$ at least qt_m.

V. RELATIONS AMONG THE COÖRDINATES OF AN INTEGER; SECOND METHOD

The formulas of §IV have been determined by observing that, if y is an integer, so also is $y + x^r$. These will be found sufficient to determine the set of maximal reduced integers in numerical cases and thence a basis,

possible primes in the denominators of the former being determined by Theorem I. We may also obtain useful relations by observing that, if y is an integer, so also is yx.

THEOREM V. *When a maximal reduced integer in p of degree $n-1$ in x exists but none in p of lower degree in x, there exists a single-prime reduced integer,*

$$y = \frac{1}{p}(a_0, a_1, \cdots, a_{n-2}, 1),$$

such that either (i) *yx reduces to ordinary integers and $a_{n-2} \equiv B_{n-1}$, $a_{n-3} \equiv B_{n-2}, \cdots, a_0 \equiv B_1, 0 \equiv B_0$, all* (mod p), *or* (ii) *yx does not reduce to ordinary integers and $a_{n-2} \not\equiv B_{n-1}$, $a_{n-2}(a_{n-2} - B_{n-1}) \equiv a_{n-3} - B_{n-2}, \cdots, a_{r+1}(a_{n-2} - B_{n-1}) \equiv a_r - B_{r+1}, \cdots, a_1(a_{n-2} - B_{n-1}) \equiv a_0 - B_1, a_0(a_{n-2} - B_{n-1}) \equiv -B_0$, all* (mod p).

For on reducing x^n in yx by the field equation, we have

$$yx = -\frac{B_0}{p} + \frac{a_0 - B_1}{p}x + \cdots + \frac{a_r - B_{r+1}}{p}x + \cdots + \frac{a_{n-3} - B_{n-2}}{p}x^{n-2} + \frac{a_{n-2} - B_{n-1}}{p}x^{n-1}.$$

If $a_{n-2} \equiv B_{n-1}$ (mod p), since there is no single-prime reduced integer in p of degree $< n-1$ in x, yx reduces to ordinary integers and the remaining coefficients must be rational integers, leading to the congruences in (i). If $a_{n-2} \not\equiv B_{n-1}$, yx cannot, but $yx - (a_{n-2} - B_{n-1})y$ must reduce to ordinary integers. The coefficients of each power of y in this difference must be rational integers, leading to the congruences in (ii).

COROLLARY 1. *If $B_0 \not\equiv 0$* (mod p) *and a maximal reduced integer in p of degree $n-1$ in x exists but none in p of lower degree in x then, if any $a_r \equiv B_{r+1}$* (mod p), *$a_{r+1} = 0$.*

For, in this case, by the last congruence in (i) above, yx cannot reduce to ordinary integers; whence the result follows from (ii).

COROLLARY 2. *If p is a factor of each of $B_0, B_1, \cdots, B_{n-1}$, and a maximal reduced integer in p of degree $n-1$ in x exists but none in p of lower degree in x, then $x^{n-1} \div p$ is an integer.*

If so, yx reduces to ordinary integers. For, if not, $a_{n-2} \not\equiv B_{n-1}$ (mod p).

From the last congruence of (ii), remembering that $-\frac{1}{2} < (a_0 \div p) \leqq \frac{1}{2}$, we have that $a_0 = 0$ since p/B_0. From the second last, $a_1 = 0$ and so on to $a_{n-2} = 0$, contradicting $a_{n-2} \not\equiv B_{n-1} \pmod{p}$. If yx reduces to ordinary integers, $a_{n-2} \equiv B_{n-1} \pmod{p}$, or $a_{n-2} = 0$ since p/B_{n-1}. From the congruences of (i), we have $a_{n-3} = 0, \cdots, a_0 = 0$, whence the integer must be $x^{n-1} \div p$.

COROLLARY 3. *If p is a factor of $B_0, B_1, \cdots, B_r$, but not of B_{r+1}, and there is a maximal reduced integer in p of degree $n-1$ but none in p of lower degree in x, then $a_0 = a_1 = \cdots = a_{r-1} = 0$ and either* (i) *$a_r \not\equiv 0$ if $a_{n-2} \equiv B_{n-1} \pmod{p}$ or* (ii) *$a_r \equiv 0$, $a_{r+1} \not\equiv 0$ if $a_{n-2} \not\equiv B_{n-1} \pmod{p}$.*

The proof follows the same lines as in Corollary 2.

COROLLARY 4. *If p is a factor of B_{n-1} but not of B_0, then $a_0 \not\equiv 0$ and $a_{n-2} \not\equiv 0$.*

For yx can not reduce to ordinary integers. Hence $a_{n-2} \not\equiv B_{n-1}$, or $a_{n-2} \not\equiv 0$. Since $a_0(a_{n-2} - B_{n-1}) \equiv -B_0 \pmod{p}$, $a_0 \not\equiv 0$.

A two-fold use may be made of this theorem and its corollaries. First, many cases may be excluded on inspection before applying Theorem IVa. Second, when a maximal reduced integer in p exists, the single-prime reduced integer obtained serves as a starting point in building up the former. The theorem can be enunciated so as to cover cases in which the powers of p in the denominators are higher than the first, but, in practice, it will be found more convenient to obtain the integer of the theorem and to apply the method to obtain integers with higher powers, using Theorem IIb. Using the corollary to Theorem IIa, it may also be enunciated to cover cases in which there are maximal reduced integers of degree $< n-1$ in x. The corollary to Theorem IIc, however, furnishes a single-prime reduced integer at once, from which the maximal reduced integer can be built up. Both these methods are illustrated in the next section, the former by the case $p = 2$, etc., and the latter by the case $p = 3$.

VI. APPLICATION TO THE CUBIC FIELD

In the first instance we suppose that the cubic is reduced to $x^3 + Qx + R = 0$ in the normal form of §I. If $y = (\alpha_0, \alpha_1, \alpha_2)$ is an integer, from Theorem IVa, we have the rational integers

(Ia) $3\alpha_0 - 2\alpha_2 Q$; (Ib) $2\alpha_1 l + 3\alpha_2 R$; (Ic) $\alpha_0 Q - 3\alpha_1 R$;

(II) $3\alpha_0^2 - 4\alpha_0\alpha_2 Q + \alpha_1^2 Q + 3\alpha_1\alpha_2 R + \alpha_2^2 Q^2$;

(III) $\alpha_0^3 - 2\alpha_0^2\alpha_2 Q + \alpha_0\alpha_1^2 Q + 3\alpha_0\alpha_1\alpha_2 R + \alpha_0\alpha_2^2 Q^2 - \alpha_1^3 R - \alpha_1\alpha_2^2 QR + \alpha_2^3 R^2$.

That (Ia), (II) and (III) are rational integers is a condition sufficient to make y an integer. We use the standard notation, $(a_0 \div p^t, a_1 \div p^m, a_2 \div p^n)$ for single-prime reduced integers. The discriminant, Δ, equals $-4Q^3 - 27R^2$.

If there is a maximal reduced integer, $y = (a_0 \div p^t, a_1 \div p^m)$, of degree 1 in x, it cannot have $a_0 = 0$. For, by (II) above, p^{2m}/Q, and by (III) p^{3m}/R; which cannot occur if the equation is in the normal form. Hence further $m \not> t$; for, if so, the reduced integer derived from $p^{m-t}y$ has $a_0 = 0$. By Theorem IVc, since $a_0 \neq 0$, $p^t/3$ and p^m/Q. Hence $p = 3$, $t = 1 = m$, and $3/Q$. Since $-\frac{1}{2} < (a_0 \div 3) \leqq \frac{1}{2}$, $a_0 = \pm 1$. Substituting these values, (Ia) is satisfied, (II) is satisfied only if $Q \equiv -3 \pmod 9$, and (III) only if $R \equiv \pm(Q+1) \pmod{27}$ according as $a_0 = \pm 1$. We have therefore the maximal reduced integer $\frac{1}{3}(x \pm 1)$.

We dispose first of the cases in which there is a maximal reduced integer of degree 2 in x but none of degree 1. If both p/Q and p/R, by Corollary 2, Theorem V, $x^2 \div p$ is an integer. Conditions (Ia), (II) and (III) are satisfied if p^2/R. If $x^2 \div p$ is not maximal, by Theorem IIb, we must have an integer of the form $(a_0 \div p, a_1 \div p, 1 \div p^2)$. Since the equation is in its normal form, we cannot have p^2/Q and p^3/R. But, since $p^4/\Delta = -4Q^3 - 27R^2$ (Theorem I), p^2/Q unless $p = 2$. Hence, from (Ia), unless $p = 2, 3$, we have $a_0 = 0$ and, from (II) if $a_1 \neq 0$, or (III) if $a_1 = 0$, p^3/R. If $p = 3$, we have from (Ia) that $3^2/Q$ and we proved above that $3^2/R$. From (III), $3/\alpha_0^3$, or $a_0 = 0$. Hence, again from (III), $3^5/R^2$, so that $3^3/R$. Finally, if $p = 2$, from (Ia) $a_0 = 0$ and from (II), written as a congruence, $6a_1R + Q^2 \equiv 0 \pmod{16}$. Since $2^2/R$, $2^3/Q^2$ or $2^2/Q$; also, unless $2^3/R$, $a_1 = 0$. If so, from (III), $2^3/R$. Hence there can be no integer of the form $(a_0 \div p, a_1 \div p, 1 \div p^2)$.

If neither p/Q nor p/R, in the integer referred to in Theorem V, $a_0 \neq 0$, $a_1 \neq 0$ (Corollary 4). Hence any maximal reduced integer is homogeneous in p. Since $p^2/\Delta = -4Q^3 - 27R^2$, we cannot have $p = 2$ or 3. Conditions (Ia,b) become $3a_0 - 2Q \equiv 0$, $2a_1Q + 3R \equiv 0 \pmod{p^n}$, where p^{2n}/Δ. Substituting from these in the congruences, (mod p^{2n}) and (mod p^{3n}), derived from (II) and (III), we may omit terms congruent to 0 with these moduli, even if divided by 2, 3, Q, leaving (II′) $\Delta \equiv 0 \pmod{p^{2n}}$, and (III′) $\Delta^2 \equiv 0 \pmod{p^{3n}}$, respectively. Since p^{2n}/Δ, these are satisfied.

There remain only the cases in which $p = 2$ and $2/R$ but not $2/Q$, and in which $p = 3$ and $3/Q$ but not $3/R$. In the former, from Corollary 3, Theorem V, we must have an integer of the forms $(\frac{1}{2},0,\frac{1}{2})$ or $(0,\frac{1}{2},\frac{1}{2})$. Only

the latter satisfies (Ia), while (II) requires that $R \equiv Q + 1 \pmod 4$. If this integer is not maximal, the latter must be of the form $(a_0 \div 2^t, a_1 \div 2^n, 1 \div 2^n)$, where $a_1 \equiv 1 \pmod 2$, and $2^{2n}/\Delta = -4Q^3 - 27R^2$. Since Q is odd, $R \equiv 2 \pmod 4$, from the last, and $Q \equiv 1 \pmod 4$. From (Ia,b), $t = n - 1$, $3a_0 - Q = 2^{n-1}a$, $2a_1Q + 3R = 2^nb$. Writing $\Delta = 2^{2n}\Delta'$, from (II) and (III) we obtain (II′) $b^2 \equiv \Delta' \pmod 4$, and (III′) $6Q^2a(3b^2 + \Delta') - 3Rb(b^2 - \Delta') + 2^n\Delta'(\Delta' - b^2) \equiv 0 \pmod 8$. Hence, if b is odd, $\Delta' \equiv 1 \pmod 4$, and, if b is even, $\Delta' \equiv 0 \pmod 4$, or $2^{2n+2}/\Delta$. Hence, if Δ is of the form $2^{2k}(4s + 1)$, we have $n = k$ for the maximal, and $2a_1Q + 3R \equiv 0 \pmod{2^n}$ but $\not\equiv 0 \pmod{2^{n+1}}$; otherwise, n is the greatest index such that $2^{2n+2}/\Delta$, and $2a_1Q + 3R \equiv 0 \pmod{2^{n+1}}$.

If $p = 3$ and $3/Q$ but not $3/R$, in the integer referred to in Theorem V, $a_0 \not\equiv 0$, $a_1 \not\equiv 0$ (Corollary 4), and, if $y = \frac{1}{3}(a_0, a_1, 1)$,

$$yx = \left(-\frac{R}{3}, \frac{a_0 - Q}{3}, \frac{a_1}{3}\right) = a_1y,$$

apart from ordinary integers. Hence $a_0a_1 \equiv -R$, $a_1^2 \equiv a_0 \pmod 3$, giving $a_0 = 1$, $a_1 = \pm 1$ since $-\frac{1}{2} < (a \div 3) \leqq \frac{1}{2}$. From (III), $R \equiv \pm (Q + 1) \pmod 9$, according as $a_1 = \mp 1$, and (Ia, II) are satisfied, giving the integer $\frac{1}{3}(1, \mp 1, 1)$. This is maximal unless there is a maximal reduced integer of degree 1 in x. For, if not and $y = \frac{1}{9}(a_0, a_1, 1)$, then $3y = (1, \mp 1, 1)$, apart from ordinary integers, giving $a_0 \equiv 1$, $a_1 \equiv \pm 1 \pmod 3$. From (Ia), $Q \equiv -3 \pmod 9$. As above, $a_0a_1 \equiv \pm 2$, $a_0 + 3 \equiv a_1^2 \pmod 9$, from which we have $(a_0, a_1) = (1, \pm 2), (4, \mp 4), (-2, \mp 1)$. Substituting in (III), we obtain either a contradiction of $R \equiv \pm (Q + 1) \pmod 9$, or the condition $R \equiv \pm (Q + 1) \pmod{27}$, the condition already obtained for the existence of a maximal reduced integer of degree 1.

If there is such an integer, viz. $\frac{1}{3}(\pm 1, 1, 0)$, its square, $\frac{1}{9}(1, \pm 2, 1)$ is an integer. Since $Q \equiv -3 \pmod 9$, and $R \not\equiv 0 \pmod 3$, from (Ia,b), an integer of higher degree in 3 must be homogeneous in 3. If $(1 \div 3^n)(a_0, a_1, 1)$ is this integer, from (Ia,b), $3a_0 - 2Q = 3^na$; also $2a_1Q + 3R = 3^nb$, and from Theorem III, $3^{2n+2}/\Delta$. Writing $\Delta = 3^{2n+2}\Delta'$ and substituting in (II) and (III), we obtain (II′) $a^2 \equiv b^2 \pmod 3$, and (III′) $8Q^3a^3 + 18Q^2ab^2 - 27Rb^3 + 54Q^2\Delta'a + 243R\Delta'b \equiv 0 \pmod{3^6}$. From the latter, since $Q \equiv -3 \pmod 9$, $a^3 \equiv Rb^3 \pmod 3$, or $a \equiv \pm b \pmod 3$ according as $R \equiv \mp 2 \pmod 9$. The solutions $a \equiv \pm b \equiv \pm 1 \pmod 3$ evidently lead to values of

a_0, a_1, differing from those obtained from $a \equiv b \equiv 0 \pmod 3$ by 3^{n-1}; i.e. the integers obtained differ by $\frac{1}{3}(x \pm 1)$. As any one of the three will serve for the maximal reduced integer (Theorem IIa), we may take $a \equiv b \equiv 0 \pmod 3$, and both (II′) and (III′) are satisfied. The maximal reduced integer is therefore $(1 \div 3^n)\ (a_0, a_1, 1)$, where a_0 and a_1 are determined from $3a_0 - 2Q \equiv 0$, $2a_1Q + 3R \equiv 0 \pmod{3^{n+1}}$, n being the greatest index such that $3^{2n+2}/\Delta$.

Basis for a general cubic

For the general cubic, $A_0z^3 + A_1z^2 + A_2z + A_3 = 0$, all A's bring rational integers, we obtain $x^3 + Qx + R = 0$ in the normal form by writing $dx = A_0z + A_1, Q = 3(A_0A_2 - A_1) \div d^2, R = (A_0A_3 - 3A_0A_1A_2 + 2A_1) \div d^3$, where d is the greatest rational integer for which such division is possible; also $\Delta = -4Q^3 - 27R^2$. Then 1 is one element of the basis; $x = (A_0z + A_1) \div d$ is a second element unless $Q \equiv -3 \pmod 9$, $R \equiv \pm (Q + 1) \pmod{27}$, when $\frac{1}{3}(x \pm 1) = (A_0z + A_1 \pm d) \div 3d$ is the second element. To determine the third element, the complete set of maximal reduced integers m_i of degrees n_i in the primes p_i, where p_i^2 is a factor of Δ, is determined from the table below. The third element is $\sum u_im_i$, where the u's are rational integral non-zero solutions of $\sum (u_i \div p_i^{n_i}) = 1$. The solutions a_0 and a_1 of the congruences below are such that $-\frac{1}{2} < (a \div D) \leqq \frac{1}{2}$, where D is the denominator given.

	Max. Red. Int.	Conditions
1	$\frac{x^2}{p}$	p/Q and p^2/R; $n = 1$.
2	$\frac{a_0 + a_1x + x^2}{p^n}$	p prime to $6QR$; n greatest index such that p^{2n}/Δ; $3a_0 - 2Q \equiv 0$, $2a_1Q + 3R \equiv 0 \pmod{p^n}$.
3a	$\frac{x + x^2}{2}$	$p = 2, Q \equiv 1 \pmod 2, R \equiv Q + 1 \pmod 4$, (3b) unsatisfied; $n = 1$.
3b	$\frac{a_0}{2^n} + \frac{a_1}{2^n}x + \frac{1}{2^n}x^2$	$p = 2, Q \equiv 1, R \equiv 2 \pmod 4$; if Δ is of the form $2^{2k}(4s + 1)$, $n = k$, $2a_1Q + 3R \equiv 0 \pmod{2^n}$, but $\not\equiv 0 \pmod{2^{n+1}}$; otherwise, n is the greatest index such that $2^{2n+2}/\Delta, 2a_1Q + 3R \equiv 0 \pmod{2^{n+1}}$; $3a_0 - Q \equiv 0 \pmod{2^{n-1}}$.
4a	$\frac{1 + x + x^2}{3}$	$p = 3, Q \equiv 0 \pmod 3, R \equiv \pm (Q + 1) \pmod 9$, (4b) unsatisfied; $n = 1$.
4b	$\frac{1 + 2x + x^2}{9}$	$p = 3, Q \equiv -3 \pmod 9, R \equiv \pm (Q + 1) \pmod{27}$, (4c) unsatisfied; $n = 2$.
4c	$\frac{a_0 + a_1x + x^2}{3}$	$p = 3, 3^{2n+2}/\Delta, n > 2$; $3a_0 - 2Q \equiv 0, 2a_1Q + 3R \equiv 0 \pmod{3^{n+1}}$, where n is the greatest index such that $3^{2n+2}/\Delta$.

University of Manitoba,
Winnipeg, Canada