ON THE DERIVATION OF BASES FOR THE CUBIC AND QUARTIC.

S.A.Lischinsky.

1928 - 1929.

Presented to the Department of Mathematics of the University of Manitoba as a partial requirement for the degree of Master of Arts.

I wish to express my sincerest thanks to Professor N. R. Wilson, who not only suggested the problem but helped me through-out the solution.

S. A. K.

PART I.

ON THE DERIVATION OF BASIS FOR THE CUBIC

$$X^3+PX^2+R = 0.$$

CHAPTER I.

Sec. I: Introduction

This part of my thesis will consider concurrently two methods of deriving a basis for the general cubic above. The first method uses the set of integral expressions derived by N.R.Wilson in his paper on " Integers and Bases of a Number Field "*. The second method of approach is based on some general theorems to be published shortly. My adaptation will appear in the next section under general relations. A departure from the original is made in the matter of elimination. Here the term of first degree in "x" is eliminated, thus preserving more obviously certain relations for the equation under differentiation.

Sec. 2: General Relations (A)

Multiplying $y = \alpha_0 + \alpha_1 x + \eta_1 x^2$, by "x" and "$x^2$", and eliminating by means of the field equation terms exceeding degree two, we obtain the following expressions necessarily integral and of which the first three are suffivient.#

---

* Transactions of American Mathematical Society. Vol. XXIX (pp. 111-126)

Theorem IV (p 118) ibidem.

$$\alpha_0^3 - \alpha_0^2\alpha_1 P + \alpha_0^2\alpha_2 P^2 + 3\alpha_0\alpha_1\alpha_2 R - 2\alpha_0\alpha_2^2 PR + \alpha_1^2\alpha_2 PR - \alpha_1^3 R + \alpha_2^3 R^2 \quad \ldots\ldots(1)$$

$$3\alpha_0^2 - 2\alpha_0\alpha_1 P + 2\alpha_0\alpha_2 P^2 + 3\alpha_1\alpha_2 R - 2\alpha_2^2 PR \quad \ldots\ldots(2)$$

$$3\alpha_0 - \alpha_1 P + \alpha_2 P^2 \quad \ldots\ldots(3)$$

$$2\alpha_0 P - 3\alpha_2 R \quad \ldots\ldots(4)$$

$$2\alpha_0 P^2 + 3\alpha_1 R - 4\alpha_2 PR \quad \ldots\ldots(5)$$

From the same paper we have also,

$$P_2^2 P_3^2 \mid \Delta, \quad \text{where} \quad \Delta = -R(4P^3 + 27R) \quad \ldots\ldots(6)$$

$$P_2^2 \mid 2P^2 \quad \ldots\ldots(7)$$

The use of the above relations comprises the first method.

Sec. 3: General Relations (B)

Whereas in the foregoing the coefficients are separately determined, in this second method, the numerator as a whole is obtained from the special form in which the equation is written. For an element of the second degree, consider

$$f(x) = aq^2 + bp^u q + cp^{2u} .$$

where a and q are of the first degree in x. On multiplication by a, we obtain by inspection that aq/p^u is an integer. By Theorem VII of the aforementioned general theorems we have that an element is of the form $(aq + rp^\omega)/p^{u+\omega}$, where p^W represents the rise. It will be shown moreover in the discussion of the first degree integer that the only possible case of such rise (for the cubic) is when "p" is equal to 3. Hence for cases other than p = 3 we may take "aq" as derived from above to be

CHAPTER II.

ELEMENTS OF DEGREE ONE

Sec. I: Method No. I.

Here "α_1" is 0, so that our equations (Sec. 2 Chap. 1) become

$$\alpha_0^3 - \alpha_0^2 P - R \quad \ldots\ldots\ldots\ldots\ldots\ldots (1')$$

$$3\alpha_0^2 - 2\alpha_0 P \quad \ldots\ldots\ldots\ldots\ldots\ldots (2')$$

$$3\alpha_0 - P \quad \ldots\ldots\ldots\ldots\ldots\ldots (3')$$

$$2\alpha_0 P \quad \ldots\ldots\ldots\ldots\ldots\ldots (4')$$

An element of the first degree is of the form $x + a/P_2$. The occurrence of this integer implies the existence of $\left[x + a/P_2\right]^2$ so that from (6), $P_2^6 \mid \Delta$. By (7'), since $P_2 \mid P$, we have that $P_2 \mid 3a$. Consider $P_2 = p^\nu$, hence for $\nu > 1$, $p \mid a$, which is impossible by (1'), since $R \not\equiv 0$, mod p^3 when $p \mid P$. For the same reason "p" = 3, so that our element is $x \pm 1/3$ according as $R + P \mp 1 \equiv 0$, mod. 27 (from (1') and $2P \pm 3 \equiv 0$, mod. 9 from (2') which gives us our sufficiency. If these conditions are not satisfied, the second element of the basis is "x".

Sec. 2: Method No. II.

If we have $x + a/p^\nu = y$, an integer, we have from the definition of an integer, the existence of an equation in y, of the form $y^s + c_1 y^2 + c_2 y + c_3 = 0$, whereupon, substituting the above value for y, we get, clearing of fractions,

$$(x+a)^3 + c_1 (x+a)^2 p^\nu + c_2 (x+a) p^{2\nu} + c_3 p^{3\nu} = 0.$$

whence by inspection and successive differentiation, we get

Furthermore, we shall break up the denominators into their constituent primes, a valid procedure, because we should, were we to multiply through by the undesired primes, obtain an integer involving only the one in question, so that the conditions must hold.

Sec. 1: Case I. (p|P and p|R) Method No. I.

We shall assume to begin with that P and R contain p only once but shall increase the power as we find it necessary. Consider equation (1).

$$a^3 - a^2bP + a^2P^2 + 3abR - 2aPR + b^2PR - b^3R + R^2 \equiv 0, \text{ mod. } p^{3v}.$$

By inspection, since all terms but the first contain p at least once, $a \equiv 0$, mod. p. Using this relation, we find next that b^3R is the only term containing p only once. Therefore either $R \equiv 0$ mod. p^2, or $b \equiv 0$ mod. p. It is immaterial which possibility we consider first, for the adoption of either immediately necessitates the introduction of the other in the next step and thereby satisfying the congruence for $v=1$. If $v>1$, since all terms but a^3 contain p^4, we must have $a \equiv 0$ mod. p^2. We are now left with a single term containing p^4, namely R^2, and since it is impossible to raise the divisibility of R beyond the power two, solutions for $v>1$ are impossible. Hence our element is

$$\frac{x^2+bx+a}{p}, \text{ where a,b, and P contain p at least once, and } R \equiv 0, \text{ mod } p^2.$$

Note: If in the above p is the only prime occurring, a and b can be taken to be 0. e.g. $x^3+2x^2+4=0$, Element is $\frac{x^2}{2}$.

our element. A slight modification will be introduced in our discussion when "p" is equal to three.

Sec.4: Notation.

The letter "p" will be taken to denote separate primes. Capital "p" i.e. "P" suffixed by 2 or 3 denotes the whole denominator of the first and second degrees respectively. Δ represents the discriminant with the factor $-R$ divided out. "α_2" is of the form $1/P$, "α_1" is of the form b/P, except in the case of the first degree integer where b is equal to one, and "α_2" $= 0$. "α_0" shall be taken to be a/P. "K", "S", and "T", are used in the sense of rational integers. The symbol $[v/2]$ means the greatest integer in $v/2$.

Note:

Since the form of the equation permits of the elimination of all factors p such that $p^3 | R$ and $p | P$, we shall assume this to have been done.

CHAPTER II.

$$f(x) \equiv 0, \text{ mod. } p^{3v} \quad \ldots\ldots(a)$$

$$f'(x) \equiv 0, \text{ mod. } p^{2v} \quad \ldots\ldots(b)$$

$$f''(x) \equiv 0, \text{ mod } p^{v} \quad \ldots\ldots(c)$$

Where $f(x)$ is of course $x^3+Px^2+R \equiv 0$. The fact that $P_2|P$ belongs to this method also, so that by (a), $x \not\equiv 0$, mod p. Hence by (c), $p = 2$ or 3. The former is disallowed by (b), leaving as our only possibility, 3, which gives us an element of the form $x \pm 1/3$. As before, the existence of this implies the integer $\left[x \pm 1/3\right]^2$, so that $3^6 | \triangle$. By substitution of $y = x \pm 1/3$ into $f(x)$, our equation in y is

$$27y^3 + (27 + 9P)y^2 + (6P \pm 9)y + (R + P \mp 1) = 0.$$

Since y is an integer this equation can be reduced to one with leading coefficient 1, hence,

$$6P \pm 9 \equiv 0, \text{ mod. } 27$$

$R + P \mp 1 \equiv 0$, mod. 27, according as our element is $x \pm 1/3$. This result we see, is identical with that obtained in the preceding section by means of the first method.

ELEMENTS OF DEGREE TWO.

Preliminary Note:

Since the discussion in the case of the second degree is rather involved, we shall divide it up into the following cases.

Case I $p|P$ and $p|R$

Case II. $p \nmid P$ and $p|R$

Case III. $p|P$ and $p \nmid R$

Case IV. $p \nmid P$ and $p \nmid R$.

Sec. 2: Case I. Method No. II.

Writing our equation as has been indicated in the first chapter, we have,

$$f(x) \equiv (x+P-2a)(x+a)^2 + (x+a)(3a^2-2aP) + R + a^2P - a^3 = 0,$$

where for our element we find the maximum "u" so that

$$3a^2 - 2aP \equiv 0, \text{ mod. } p^u \ldots\ldots (m)$$

$$R + a^2P - a^3 \equiv 0, \text{ mod. } p^{2u} \ldots (n)$$

Since $p|R$ and $p|P$, $p|a$ by (n). If $u > 1$, then by (n) $p^3|R$, $\therefore$ $u = 1$, is maximum. Hence our element is aq/p which is in this case x^2/p, the other factors containing p, having been deleted. Our conditions are here as in the preceding, $p^2|R$. It is to be observed that the complication arising out of the possibility of $p = 3$ can not arise here, for under the conditions of this case $R + P \pm 1 \equiv 0$, mod. 27 is impossible.

Sec.3: Case II ($p \nmid P$ and $p|R$) Method No. I.

As in the preceding, consider an element of the form $x^2 + bx + a/p^u$, where until shown impossible, 2u is the highest power of p that divides $\triangle$.

First taking the case where $p \neq 2$, we have from an inspection of the discriminant that $p^{2u}|R$. By (4) $p^u|a$, whence from (3), $b - P \equiv 0$, mod. p^u. Writing (2) as

$$3a^2 - 2aP(b-P) + 3bR - 2PR$$

it is congruent to 0, mod p^{2u} on inspection. Following the same system of factoring, (1) satisfies at once also, thus giving a sufficiency for the above element. Assembling our conditions we have $R \equiv 0$, mod. p^{2u} and $a \equiv 0$, mod p^u $b = P$.

Since the discussion when p is 2 is complicated, we shall divide it into three cases according as $v \lessgtr 1$, where $2^v \| R$.

a) $v = 1$.

From an inspection of (2), we find that since all terms but the first contain 2, so must it, hence $2 \| a$. Reconsidering the same equation, we find that 3bR conatins 2 once only, whereas all the others contain it at least twice. From (3) we have that $b \not\equiv 0$, mod. 2, hence there is no solution under these conditions.

b) $v = 2$.

From(3), $3a \equiv P(b - P)$, mod 2^u. This allows us to put $3a = K.2^u + P(b - P)$.

$$3a^2 - 2abP + 2aP^2 + 3bR - 2PR \equiv 0, \text{ mod. } 2^{2u} \ldots (2)$$

$$2aP^2 + 3bR - 4PR \equiv 0, \text{ mod, } 2^u \ldots\ldots\ldots (5)$$

$$\therefore \quad 3a^2 - 2abP + 2PR \equiv 0, \text{ mod } 2^u. \text{ (on subtraction)}$$

$$3a^2 - abP + aP^2 \equiv 0, \text{ mod } 2^u. \quad (3) \times a.$$

giving

$$-abP + 2PR - aP^2 \equiv 0, \text{ mod } 2^u.$$

Multiplying by 3 and dividing by P, we get,

$$-3ab + 6R - 3aP \equiv 0, \text{ mod. } 2^u.$$

Adding $4aP - 6R \equiv 0$, mod. 2^{u+1} ....(4)x2, gives

$$-3ab + aP \equiv 0, \text{ mod } 2^u.$$

Since by (4) $a \equiv 0$, mod. 2 and no more, we have, on dividing the above through by a, $3b - P \equiv 0$, mod. 2^{u-1}, permitting us to write $3b = S.2^{u-1} + P$.

Consider (2). Multiplying by 3, we get

$$9a^2 - 6abP + 6aP^2 + 9bR - 6PR \equiv 0, \text{ mod } 2^{2u}.$$

Making the above substitution re "a", we have

$$\left\{K2^u + P(b - P)\right\}^2 - 2bP\left\{K2^u + P(b - P)\right\} + 9bR - 6PR \equiv 0, \text{ mod. } 2^{2u}.$$

$$= - b^2P^2 - 9P^4 + 18bP^3 + 81bR - 54PR \equiv 0, \text{ mod. } 2^{2u}.$$

Multiplying by 9 and putting $3b = S2^{u-1} + P$, the above becomes,

$$- P^2S^2 2^{2u-2} + 4P^3 S2^{u-1} + 27RS2^{u-1} - 81PR - 4P^4 \equiv 0, \text{ mod. } 2^{2u}.$$

$$= - P^2S^2 2^{2u-2} - P(4P^3 + 27R) + S2^{u-1}(4P^3 + 27R) \equiv 0, \text{ mod. } 2^{2u}.$$

Consider the last term. If $u > 2$ it satisfies the congruence at once. If $u = 2$, then the minimum power of 2 that will divide Δ' is 3, since it consists of two factors each containing 2^2 exactly, so that the last term satisfies for all values of u. This leaves on division by P

$$- PS^2 2^{2u-2} - (4P^3 + 27R) \equiv 0, \text{ mod. } 2^{2u}.$$

Or, writing more handily,

$$PS^2 2^{2u-2} + \Delta' \equiv 0, \text{ mod. } 2^{2u}.$$

If Δ contains 2 an odd number of times, then each term must singly satisfy the congruence and the maximum u that can occur is where $2^{2u+3} | \Delta$. If Δ contains 2 an even number of times we find, on putting $\Delta' = 2^{2u-2}.4D \pm 1$, that the above depends for solution upon the fact that $P = 4P' \mp 1$ according as $\Delta' = 2^{2u-2}(4D \pm 1)$. If these conditions fail we must decrease our u by one.

Turning to (1), we multiply by 27 and put $3a = K2^u + P(b-P)$ to get, disregarding terms containing 2^{3u} or over,

$$3K^2 2^{2u}\left[P(b-P)\right] + 3K2^u P^2(b-P)^2 - 3bP\left[K^2 2^{2u} + 2K2^u P(b-P)\right] + P^3(b-P)^3$$
$$+ 3P^2\left[K^2 2^{2u} + 2P(b-P)K2^u + P^2(b-P)^2\right] + 27bR\left[K2^u + P(b-P)\right]$$
$$- 18PR\left[K2^u + P(b-P)\right] + 27b^2PR - 27b^3R + 27R^2 \equiv 0, \text{ mod. } 2^{3u}.$$

Simplifying and multiplying by 27 we get,

$$- 81b^2P^2K2^u + 162P^3bK2^u - 81P^4K2^u - 54P^3b^3 + 162bP^5 + 54P^6$$
$$+ 162P^4b^2 + 729bRK2^u + 1458PRb^2 - 1215bRP^2 - 486PRK2^u + 486RP^3$$
$$- 729Rb^3 + 729R^2 \equiv 0, \text{ mod. } 2^{3u}.$$

Putting $3b = S2^{u-1} + P$, gives

$$729R^2 + 216RP^3 - 243PRK2^u - 36KP^4 2^u + 16P^6 + 36KP^3 S2^{2u-1} - 12SP^5 2^u$$
$$+ 243RKS2^{2u-1} + 12P^4 S^2 2^{2u-2} + 81RPS^2 2^{2u-2} - 9PKS^2 2^{3u-2} - 27RS^3 2^{3u-3}$$
$$- P^3 S^3 2^{3u-2} \equiv 0, \text{ mod. } 2^{3u}.$$

$$= (4P^3 + 27R)^2 - 9KP2^u(4P^3 + 27R) - 3P^2 S2^u(4P^3 + 27R) +$$
$$+ 3PS^2 2^{2u-2}(4P + 27R) - 9KP^2 S^2 2^{3u-2} - 27RS^3 2^{3u-3} - P^3 S^3 2^{3u-2} \equiv 0, \text{ mod. } 2$$
$$= \Delta^2 - 9KP2^u\Delta + 3PS^2 2^{2u-2}\Delta - 9KP^2 S^2 2^{3u-2} - 27RS^3 2^{3u-3}$$
$$- 3SP^2 2^u\Delta - P^3 S^3 2^{3u-2} \equiv 0, \text{ mod. } 2^{3u}.$$

$$= \Delta\left[\Delta + 3PS^2 2^{2u-2}\right] + \left[P2^u\Delta + P^2 S^2 2^{3u-2}\right](9K + 3PS)$$
$$+ P^3 S^3 2^{3u-1} - 27RS^3 2^{3u-3} \equiv 0, \text{ mod. } 2.$$

While dealing with equation (2) immediately above, we saw that if Δ contains 2 an even number of times $u > 2$; hence the first term satisfies at once. As for the second term, each factor composed as it is of the sum of two odd numbers will contribute at least one 2, which, with the apparent 2^{3u-2} renders the product congruent to 0, mod. 2^{3u}. The last two terms consist of two numbers each containing 2^{3u-1} exactly, hence together they satisfy the congruence. Having thus satisfied equation (1), we have established a sufficiency.

Rewriting our results, we have that if

$2^{2u+3} \mid \Delta$ the element is $\frac{x^2 + bx + a}{2^u}$, where $3b - P \equiv 0, \text{ mod. } 2^{u-1}$

and $3a \equiv P(b - P), \text{ mod. } 2^u$.

If $2^{2u} \mid \Delta$, and $P = 4P' \mp 1$ according as $\Delta' = 2^{2u-2} \cdot 4D \pm 1$,

element is $\frac{x^2 + bx + a}{2^u}$, where a and b fulfill the same conditions as above.

If the above requirement re P and Δ' is not fulfilled we must decrease our u by one.

c) $v > 2$ (Where $2^v \mid R$).

From a consideration of the condition imposed by the discriminant it is evident on inspection that the maximum u possible is where $u = \left[\frac{v}{2}\right] + 1$. By (4) $2aP - 3R \equiv 0, \text{ mod. } 2^u$

$\therefore$ $2aP \equiv 0, \text{ mod. } 2^u$ so that $a \equiv 0, \text{ mod. } 2^{\left[\frac{v}{2}\right]}$. From (3),

$3a - P(b - P) \equiv 0, \text{ mod } 2^u$ giving us that $b - P \equiv 0, \text{ mod } 2^{\left[\frac{v}{2}\right]}$.

$$6a^2 - 2abP + 2aP^2 \equiv 0, \text{ mod. } 2^{2u} \ldots . (3) \times 2a.$$

$$\underline{3a - 2abP + 2aP + 3bR - 2PR \equiv 0, \text{ mod. } 2^{2u}.} \quad (2)$$

$$\therefore \quad 3a^2 - 3bR + 2PR \equiv 0, \text{ mod. } 2^{2u}.$$

Consider this last equation. If v is odd, then 3bR can never unite with the term in a^2 to form a higher power of two than that contained by either of them hence they must each satisfy the congruence separately giving as our maximum denominator 2^u, where $2^{2u+1} \mid R$. Furthermore, a , and hence b - P are congruent to 0, mod. 2^u, from the last equation. Using these relations in (1), disregarding terms obviously containing 2^{3u} or over, we get

$$- a^2bP + a^2P^2 + 3abR - 2aPR + b^2PR - b^3R + R^2 \equiv 0, \text{ mod. } 2^{3u}$$

$= -a^2P(b - P) - b^2R(b - P) + 3abR - 2aPR + R^2 \equiv 0$, mod. 2^{3u}.
The above is obviously true. Hence our element on deleting a which contains 2^u, is

$$\frac{x(x + P)}{2^u}, \quad R \equiv 0, \text{ mod. } 2^{2u+1}.$$

e. g. $x^3 + 9x^2 + 128 = 0$. Here the integer of second degree is $\frac{x(x + P)}{2^3}$.

If v is even, still considering

$$3a^2 + 2PR - 3bR \equiv 0, \text{ mod. } 2^{v+2}$$

$$= 3a^2 - PR - 3R(b - P) \equiv 0, \text{ mod. } 2^{v+2}.$$

The last term satisfies at once leaving $3a^2 - PR \equiv 0$, mod. 2^{v+2}. This can be written more explicitly as $3 \pm P \equiv 0$, mod 4, according as R contains the factor $4R' \mp 1$.

Turning to equation (1), consider the expressions $b^2PR - b^3R$, and $bP^2R - P^3R$. On factoring they become $b^2\left[(P - b)R\right]$ and $P^2\left[(b - P)R\right]$. Subtracting and rearranging factors we get $\left[(b + P)(b - P)^2\right]R$, which is congruent to 0, mod. 2^{2v+1}, and hence for $v \nless 4$ each expression may replace the other in equations which are to be congruent to 0, mod. 2^{3u}, where $u = (\frac{v}{2} + 1)$. Hence, replacing $b^2PR - b^3R$ by $bP^2R - P^3R$ in (1), we can factor the latter as follows;

$$(a - bP + P^2)(a^2 + PR) + R\left[R + 3a(b - P)\right] \equiv 0, \text{ mod. } 2^{3u}.$$

As for the first term, we have from above, that $3a^2 - PR \equiv 0$, mod. 2^{v+2}, hence, $a^2 + PR = 4a^2 - (3a^2 - PR) \equiv 0$, mod. 2^{v+2}; since $a - bP + P^2 = (3a - bP + P^2) - 2a$, it contains $2^{\frac{v}{2}+1}$. Thus the first term satisfies the congruence. The bracketed part of the second term, being the sum of two factors each containing 2^v

exactly, the whole term contains 2^{v+1}; R outside the bracket contributes 2^{v} and since for $v \nless 4$ $2v+1 > \frac{3v}{2} + 3$, this also satisfies, establishing a sufficiency for the element

$$\frac{x^2 + bx + a}{2^u}, \text{ where } 2^{2u-2} | R,\ b \equiv P, \text{ mod. } 2^{u-1}$$

$P \pm 3 \equiv 0$, mod. 4 according as R contains the factor $4R' \mp 1$. $a \equiv 0$, mod. 2^{u-1}.

E. g. $x^3 + x^2 - 16 = 0$. Element is $\frac{x^2 + 3x - 4}{8}$.

Sec. 4: Case II. Method No. II:

Our congruences are,

$$3a^2 - 2aP \equiv 0, \text{ mod. } p^u \ldots\ldots (m)$$

$$R + a^2(P - a) \equiv 0, \text{ mod. } p^{2u} \ldots (n)$$

If $p \neq 2$, then since $p | \triangle$, $p^{2u} | R$. Looking at the above, if $a \not\equiv 0$, mod. p, then from (n), $P - a \equiv 0$, mod. p^{2u}. From (m), $3a - 2P \equiv 0$, mod. p^u. Multiplying the former by 3 and adding to the latter gives $P \equiv 0$, mod. p^u, an impossibility in this case, hence $p | a$. Using this relation with (n), we get that $p^u | a$ which also satisfies (m). Thus we have a sufficiency for an element of the form

$$\frac{x(x + P)}{p^u}, \text{ where } R \equiv 0, \text{ mod. } p^{2u}.$$

If $p = 2$, our congruences are

$$3a^2 - 2aP \equiv 0, \text{ mod. } 2^u \ldots\ldots (m)'$$

$$R + a^2(P - a) \equiv 0, \text{ mod. } 2^{2u} \ldots\ldots (n)'.$$

By (n)' $a \equiv 0$, mod. $2^{\left[\frac{v}{2}\right]}$ where $2^v | R$. Consider case when v is odd. By (n)' $v > 1$. Since the power of 2 contributed by a^2 is necessarily even , each term of (n)' must separately satisfy

the congruence. Hence $u = \left[\frac{v}{2}\right]$, and our element is

$$\frac{x(x+P)}{2^u}, \text{ where } 2^{2u+1} \mid R.$$

If v is even and greater than 2, put $u = \frac{v}{2} + 1$. (m)' is at once satisfied, and from (n)', $R + a^2P \equiv 0$, mod. 2^{v+2}. This is possible when $P \pm 1 \equiv 0$, mod. 4 according as R contains the factor $4R' \pm 1$. Our element is under these conditions

$$\frac{x^2 + (P+a)x + aP}{2^u}, \text{ where } a \equiv 0, \text{ mod. } 2^{u-1},$$

and $R \equiv 0$, mod. 2^{2u-2}.

If R contains 2^2 and no higher, then by inspection of (n)', $a \equiv 0$, mod. 2 and no higher, so that (m)' may be rewritten as

$$3a - 2P \equiv 0, \text{ mod. } 2^{u-1} \ldots . \quad (m)''.$$

Cubing the above and subtracting 27(n)' we have on rearranging $\triangle' - 3P(3a - 2P)^2 \equiv 0$, mod. 2^{2u}, for $u \geq 3$. If $\triangle$ contains an odd power of 2, solution is impossible, unless we decrease our u by one, upon which all conditions are satisfied when $3a - P$ contains 2^u, and $2^{2u+3} \mid \triangle$ for an element of the form

$$\frac{(x+a)(x+P-2a)}{2^u}.$$

If $\triangle' \equiv 0$, mod. 2^{2u-2} exactly, put $\triangle = 2^{2u}K \pm 2^{2u-2}$, and $3a - 2P = S_0 2^u + 2^{u-1}$ in the above equation. Disregarding terms of 2^{2u} or over we get

$$2^{2u-2} - 3P(2^{2u-2}) \equiv 0, \text{ mod. } 2^{2u}.$$

This is the case, obviously when and only when $P \pm 1 \equiv 0$, mod. 4 according as $\triangle' = 2^{2u-2} \cdot 4D \pm 1$. If u is less than 3, since by inspection conditions are satisfied for u = 1, the only case presenting any difficulty is when u = 2. This possibility arises only when $\triangle \not\equiv 0$, mod 2^6, or when $2^6 \mid \triangle$ but $P \pm 1$ does

not contain 4 according as

not contain 4 according as Δ' contains $4D' \pm 1$. In the event of of the former it resolves itself at once into the case where ν is odd, for we have already shown in a previous discussion that the least power of 2 that Δ can contain is 5, thus giving the highest solution for $u = 1$. The latter admits at once $u = 2$ Hence our element is

$$\frac{(x + a)(x + P - 2a)}{2^u}$$, where $R \equiv 0$, mod. 4

$3a - 2P \equiv 0$, mod. 2^{u-1}

$P \pm 1 \equiv 0$, mod. 4 according

Δ' contains $4D \pm 1$.

Sec. 5: Case III. Method No. I.

Since $p|\Delta$, $p = 3$. Multiplying (4) by P, we have

$$2aP^2 - 3PR \equiv 0, \text{ mod. } 3^{u+1}.$$

$$\underline{2aP^2 + 3bR - 4PR} \equiv 0, \text{ mod. } 3^u \ldots(5)$$

$\therefore$ $R(3b - P) \equiv 0$, mod. 3^u and since $R \not\equiv 0$, mod. 3

we may write $3b - P \equiv 0$, mod. 3^u.

$$6a^2 - 2abP \; 2aP^2 \equiv 0, \text{ mod. } 3^u \ldots.(3)\times 2a$$

$$\underline{3a^2 - 2abP + 2aP^2 + 3bR - 2PR \equiv 0}, \text{ mod. } 3^{2u}..(2).$$

$\therefore$ $3a^2 - 3bR + 2PR \equiv 0$, mod. 3^u on subtraction. Or,

$(3a^2 + PR) - R(3b - P) \equiv 0$, mod. 3^u. Whereupon,

using the above relation re $3b - P$, we have that

$3a^2 + PR \equiv 0$, mod. 3^u. Multiplication by 3 gives

$9a^2 + 3PR \equiv 0$, mod. 3^{u+1}

$$\underline{2aP^2 - 3PR} \equiv 0, \text{ mod. } 3^{u+1} \ldots.(4)\times P$$

$\therefore$ $9a - 2P^2 \equiv 0$, mod. 3^{u+1} on subtraction and division by a which does not contain 3. Putting $3b - P \equiv 0$, mod. 3^u

in (3) to get $a + 2b^2 \equiv 0$, mod. 3^{u-1}. Using this relation in (2) gives us $a + 2b^2 \equiv 0$, mod. 3^u.

The above congruences enable us to write

$$a = \frac{1}{9}\left[K.3^{u+1} - 2P^2\right]$$

$$b = \frac{1}{3}\left[S.3^u + P\right]$$

$$4P^3 = T.3^{2v} - 27R.\text{ (Assuming that } 3^{2v} \mid \Delta \text{ .}$$

Substituting for a and b as above in

$$3a^2 - 2abP + 2aP^2 + 3bR + 2PR \equiv 0, \text{ mod. } 3^{2u} \ldots\ldots(2)$$

we have

$$K^2.3^{2u-1} - 2PSK3^{2u-2} + 4SP^3 3^{u-3} - 4P^4 3^{-3} - PR + RS3^u \equiv 0, \text{ mod. } 3^{2u}.$$

Substitution for $4P^3$ gives

$$-PT3^{2v-3} + K3^{3u-1} + 2PSK3^{2u-2} + ST3^{2v+u-3} \equiv 0, \text{ mod. } 3^{2u}.$$

Consider $u > 1$. Since the degrees in 3 of the two lowest multiples of 3 must be equal or all terms must singly satisfy the congruence, we have here, remembering that P contains 3 at least once, that $2v-2 = 2u-1$. Hence $3^{2u+1} \mid \Delta$. As a result of this the last term of the above congruence satisfies at once keeping in mind that $u > 1$. This leaves

$$-PT3^{2v-3} + K^2 3^{2u-1} - 2PSK3^{2u-2} \equiv 0, \text{ mod. } 3^{2u} \ldots\ldots(a)$$

Consider the last two terms. Dropping one K and factoring, we get

$$3^{u-2}\left[K3^{u+1} - 2PS3^u\right],$$

or, on returning to original symbols,

$$= 3^{u-2}\left[9a + 4P^2 - 6bP\right].$$

Substituting in the above $a \equiv -2b^2$, mod. 3^u, it becomes,

$$3^{u-2}(4P^2 - 6bP - 18b^2)$$

$$= -3$$

$$= - 3^{u-2}\left[2(3b - P)^2 + 6P(3b - P)\right].$$

This is congruent to 3^{2u} on inspection. Hence, deleting these two terms from (a) above, we have from the remainder that $3^{2u+2} \mid \Delta$, as a necessary condition for the satisfaction of equation (2).

Making the same substitutions in (1), we get after our usual manipulations,

$$K3^{3u-3} - RS^3 3^{3u-3} - PSK^2 3^{3u-3} \equiv 0, \text{ mod. } 3^{3u}.$$

$$\text{i.e. } K^3 - RS^3 - PSK^2 \equiv 0, \text{ mod. } 3^3.$$

This last equation depends for solution upon the fact that

$$R + P \pm 1 \equiv 0, \text{ mod. } 27, \text{ and}$$

$$6P \mp 9 \equiv 0, \text{ mod. } 27, \text{ both easily demonstrable requirements for } u > 1.$$

If $u = 1$, a and b can be taken equal to 1 or 0. By (1),

$$a^3 - b^3R + R^2 \equiv 0, \text{ mod. } 3$$

By inspection, if $b \not\equiv 0$, then $a = +1$. Consider $b = 0$. Then by the above, $a = -1$. Substituting these values in (1), we get

$$R^2 + 2PR + P^2 - 1 \equiv 0, \text{ mod. } 27.$$

$$\text{i.e. } (P + R - 1)(P + R + 1) \equiv 0, \text{ mod. } 27.$$

Since in the above product the factors differ by 2 both can not contain 3, hence we may write

$$(P + R \pm 1) \equiv 0, \text{ mod. } 27.$$

But this implies that $3^6 \mid \Delta$ allowing $u = 2$. Hence the above is impossible and $b \not\equiv 0$. Substitution of $a = 0$, gives directly that $P + R \pm 1 \equiv 0$, mod. 27, so that $a \not\equiv 0$. Hence, by the above, $a = +1$, and $b = \pm 1$. Substituting these values in (1), we have

$$(R \pm 1)^2 + P\left[P - (R \pm 1)\right] \equiv 0, \text{ mod. } 27.$$

These conditions satisfy (2) at sight.

If $P \equiv 0$, mod. 9 it is evident from the discriminant that $u = 1$ is the maximum. In this case $R \pm 1 \equiv 0$, mod. 9.

Sec.6: Case III; Method No. II:

Since the discriminant allows only $p = 3$, our congruences are

$$3a^2 - 2aP \equiv 0, \text{ mod } 3^u \ldots\ldots\ldots(m)$$

$$R + a^2(P - a) \equiv 0, \text{ mod. } 3^{2u} \ldots\ldots(n)$$

Since an examination of (n) reveals that $a \not\equiv 0$, mod. 3, (m) can be written

$$3a - 2P \equiv 0, \text{ mod. } 3^u \ldots\ldots\ldots(m)'$$

Consider first where there is an element of the first degree. Then, since $P_2^2 P_3^2 \mid \Delta$, we have that $3^{2u+2} \mid \Delta$. By actual multiplication we have that

$$(m)'^3 + 27(n) = \Delta' - 3P(m)'^2 \ldots\ldots\ldots(a)$$

Since the existence of an integer of the first degree requires $u > 1$, the above is at once satisfied with (m)'. The integer thus obtained is also an element since $3^{2u+2} \mid \Delta$ and no more. #

If there is no integer of the first degree, we obtain our element directly from the above congruences. Since the u now refers to the element we have from (a) that $3^{2u+2} \mid \Delta$ and

---

Reference to General Relations (B) will explain the necessity for this proviso.

$3a - 2P \equiv 0$, mod. 3^u are necessary and sufficient conditions for the element

$$\frac{(x + a)(x + P - 2a)}{3^u}$$

E.g. $x^3 + 3x^2 + 725 = 0$. Element is $\frac{(x - 1)(x + 2)}{3^3}$

If $u = 1$, (m) is satisfied identically and our necessary and sufficient condition obtained from (n) is that

$$R + P \pm 1 \equiv 0, \text{ mod. } 9.$$

This is obtained by putting $a = 3a' \pm 1$. Deleting the known multiples of 3 from the coefficients of our element, we have in the numerator

$$x^2 - ax - 2a^2.$$

Since $a = \pm 1$, this can be written

$x^2 \pm x + 1$; a form identical with that obtained by the first method.

Sec.7: Case IV ($p \nmid P$ and $p \mid R$) Method No. I.

Since $p^{2u} \mid \Delta$ $p \neq 2$ or 3, hence in our manipulations multiplication or divisions by these factors or by P and R will not affect in so far as divisibility by p is concerned.

$$2aP - 3R \equiv 0, \text{ mod. } p^u \ldots\ldots (4)$$

or, we may put $2aP^2 - 3PR \equiv 0$, mod $p^u \ldots\ldots (4) \times P$

$$2aP^2 + 3bR - 4PR \equiv 0, \text{ mod. } p^u. (5)$$

$\therefore$ $R(3b - P) \equiv 0$, mod. p^u on subtraction, or,

since p is prime to R we may write $3b - P \equiv 0$, mod. p^u.

$$3a^2 - 2abP + 2aP^2 + 3bR - 2PR \equiv 0, \text{ mod. } p^{2u} \ldots (2)$$

Put $3b = K.p^u + P$, and from (4), $2aP = S.p^u + 3R$, in the above, first multiplying by $12P^2$ to avoid fractions. This will give, disregarding terms containing p^{2u} or over,

$$54SRp + 81R + 8P^3Sp + 12P^3R \equiv 0, \text{ mod. } p^{2u}.$$

$$= 2Sp^u\Delta - 3\Delta \equiv 0, \text{ mod. } p^{2u}.$$

The truth of this appears on inspection. Thus (2) is satisfied.

Multiplying (1) by $216P^3$, we get

$$216a^3P^3 - 216a^2bP^4 + 216a^2P^5 + 648abRP^3 - 432aP^4R + 216b^2P^4R$$
$$- 216P^3b^3R + 216P^3R^2 \equiv 0, \text{ mod. } p^{3u}.$$

Making the same substitutions and disregarding terms of p^{3u} or over, we get,

$$243RS^2p^{2u} + 729R^2Sp^u + 729R^3 + 162P^2R^2Kp^u + 36P^3S^2p^{2u} + 108P^3RSp^u$$
$$+ 216P^3R^2* + 24P^5RKp^u + 16P^6R* \equiv 0, \text{ mod. } p^{3u}.$$

Reduction by the relation $4P^3 \equiv -27R$, mod. p^u, leaving the terms marked * intact gives

$$729R^3 + 16RP^6 + 216P^3R^2 \equiv 0, \text{ mod. } p^{3u}.$$

$$= R\Delta^2 \equiv 0, \text{ mod. } p^{3u}.$$

This is evident, so that the conditions for a and b satisfy (1). This establishes a sufficiency for the element

$$\frac{x^2 + bx + a}{p^u}, \text{ where } 2aP - 3R \equiv 0, \text{ mod. } p^u$$
$$3b \equiv P, \text{ mod. } p^u.$$
$$p^{2u} \mid \Delta.$$

If it is so desired, a and b may be eliminated from the final result. The above would then be written

$$\frac{6Px^2 + 2P^2x + 9R}{6Pp^u}.$$

All elements lend themselves to such treatment.

Sec. 8: Case IV: Method No. II:

Rewriting our congruences for convenience in reference , we have

$$R + a^2(P - a) \equiv 0, \text{ mod. } p^{2u} \ldots\ldots (n)$$

$$3a^2 - 2aP \equiv 0, \text{ mod. } p^u \ldots\ldots (m)$$

Since $R \not\equiv 0$, mod p, (n) gives $a \not\equiv 0$, mod. p, allowing us to write (m) as

$$3a - 2P \equiv 0, \text{ mod. } p^u \ldots\ldots\ldots (m)'$$

Furthermore we can show that(n) is dependent upon (m) and the discriminant, for writing

$$27(n) = \Delta - 3P(m)'^2 - (m)'^3$$

it is at once apparent. Hence our element is

$$\frac{(x + a)(x + P - 2a)}{p^u} \quad \text{where } p^{2u} \mid \Delta \text{ and } 3a - 2P \equiv 0, \text{ mod. } p^u.$$

If we were to eliminate a in the manner indicated in the foregoing section, we would get

$$\frac{9x^2 + 3Px - 2P^2}{9p^u}.$$

The identity of this with the form obtained by the first method can be made apparent by multiplying thru by 2P and putting $-4P^3 \equiv 27R \text{ mod. } p^{3u}$.

Applying to the numerical example $x^3 + 4x^2 + 222 = 0$, we get

$$\frac{x^2 - 7x + 2}{25}.$$

Table for all cases of the cubic

$$x^3 + Px^2 + R = 0.$$

	Element of degree two.	Conditions.
I	$\frac{x^2}{p}$	$p \mid P$ and $p^2 \nmid R$
II.	$\frac{6Px^2 + 2P^2x + 9R}{6Pp^u}$	$p^{2u} \mid \Delta$. "p" prime to 6PR.
III.	$\frac{x(x+P)}{p^{2u}}$	$p^{2u} \mid R$. "p" $\neq 2$.
IVa	$\frac{x^2 + bx + a}{2^u}$	$2^{2u} \mid \Delta$. $R \equiv 0$, mod. 4. $3b \equiv P$, mod. 2^{u-1}. $3a \equiv P(b-P)$ mod. 2^u. Δ contains $4D \pm 1$, acc. as $P \pm 1 \equiv 0$, mod. 4.
IVb	$\frac{x(x+P)}{2^u}$	$R \equiv 0$ mod. 2^{2u+1}
IVc	$\frac{x^2 + bx + a}{2^u}$	$b \equiv P$ mod. 2^{u-1}; $a \equiv 0$, mod. 2^{u-1}. $P \pm 1 \equiv 0$, mod. 4, acc. as R is $2^{2u-2} \cdot 4R' \pm 1$.
V	$\frac{(x+a)(x+P-2a)}{3^u}$	$3^{2u+2} \mid \Delta$. $3a - 2P \equiv 0$, mod. 3^u. $u > 1$.