REPRESENTATION OF INTEGERS BY CERTAIN TERNARY CUBIC FORMS*

BY F. S. NOWLAN

1. *Introduction.* Apart from Eisenstein's theory relating to his canonical form† comparatively few results are available on representation of integers by ternary cubic forms. By methods differing from those employed by Eisenstein, this paper develops theory relating to two such forms. One form and the associated theory is, however, obtainable from Eisenstein's results. The other form cannot be so obtained.

2. *Rational Prime Factors of Norms of Integers of Cubic Number Fields.* Let $K(x)$ be the algebraic number field defined by a root x of an irreducible cubic. Consider any integer π of $K(x)$. Its norm, $N(\pi)$, is a rational integer. We seek the properties of its rational prime factors.

Let $N(\pi) = p_1^i p_2^j \cdots$, where $p_1, p_2, \cdots$ are rational primes and $i, j, \cdots$ are positive integers. Let π_1 be a prime factor of π. Then π_1 divides $N(\pi)$ and hence divides one of its rational prime factors, say p_1. It could not divide two such factors, for then it would divide their greatest common divisor and hence would be a unit.

Let us set $p_1 = \pi_1\alpha$, where α is an integer of $K(x)$. Then $N(\pi_1) \cdot N(\alpha) = N(p_1) = p_1^3$. Four apparent possibilities arise:

$$(1) \qquad N(\pi_1) = \pm 1, \qquad N(\alpha) = \pm p_1^3.$$

This must be excluded, as it would make π_1 a unit.

$$(2) \qquad N(\pi_1) = \pm p_1, \qquad N(\alpha) = \pm p_1^2.$$

Then $\pi_1 \pi_1' \pi_1'' = \pm p_1 = \pm \pi_1 \alpha$. It follows that $\alpha = \pm \pi_1' \pi_1''$, where π_1' and π_1'' are the conjugates of π_1. In this case p_1 is the norm of a prime of $K(x)$.

$$(3) \qquad N(\pi_1) = \pm p_1^2, \qquad N(\alpha) = \pm p_1.$$

[*] Presented to the Society, December 29, 1925.

† Journal für Mathematik, vol. 28, pp. 302–303.

Then $N(\pi_1) = \pm N(\alpha^2)$. Hence π_1 is associated with α^2 and so is not a prime. Accordingly we exclude this case.

$$(4) \qquad N(\pi_1) = \pm p_1^3, \qquad N(\alpha) = \pm 1.$$

Here α must be a unit and hence p_1 is a prime of $K(x)$. We therefore state

THEOREM I. *A rational integer, which may be represented by the norm of the general integer in a cubic number field $K(x)$, has its rational prime factors either* (a) *primes of the field, or else* (b) *norms of primes of the field. In case* (a) *these primes enter to powers which are multiples of three and in* (b), *such primes are themselves represented by the given norm.*

3. *Certain Properties of Two Galois Number Fields.* We consider the Galois fields defined by roots of the irreducible cyclic cubics

$$\text{(i)} \qquad x^3+x^2-2x-1=0,$$

and

$$\text{(ii)} \qquad x^3-3x+1=0.$$

For either equation we denote the roots by x, x' and x'' and the corresponding cubic fields by $K_1(x)$ and $K_2(x)$, respectively. For both (i) and (ii), we have

$$x'=x^2-2\ , \qquad x''=x'^2-2\ , \qquad \text{and} \quad x=x''^2-2\ .$$

These relations arise* through giving a negative sign to the square root of the discriminant Δ in the formula

$$x'=\frac{1}{2\sqrt{\Delta}}[(6Q-2P^2)x^2-(9R-7PQ+2P^3+\sqrt{\Delta})x$$
$$+(4Q^2-P^2Q-3PR-P\sqrt{\Delta})]\ ,$$

where P, Q, and R relate to the general cubic $x^3+Px^2+Qx+R=0$.

PROPERTY I. *For both $K_1(x)$ and $K_2(x)$, integral algebraic numbers are given by*

$$A=\alpha_0+\alpha_1x+\alpha_2x^2$$

with α_0, α_1, and α_2 rational integers.

* Serret, *Cours d'Algèbre Supérieure*, vol. 2, pp. 467–469.

Property II. *Unique factorization holds for the integers of both $K_1(x)$ and $K_2(x)$, since a sufficient condition in a cubic number field is that the class number of ideals shall be $h=1$.*[*] *This condition is satisfied for the two cubic fields.*

Property III. *The norm of the general integer $A=\alpha_0+\alpha_1 x+\alpha_2 x^2$ of $K_1(x)$ is given by the ternary cubic form*

$$(5)\quad F_1=\alpha_0^3-\alpha_0^2\alpha_1-5\alpha_0^2\alpha_2-2\alpha_0\alpha_1^2-\alpha_0\alpha_1\alpha_2+6\alpha_0\alpha_2^2-\alpha_1^3-\alpha_1^2\alpha_2$$
$$-2\alpha_1\alpha_2^2+\alpha_2^3\,.$$

The norm of the general integer of $K_2(x)$ is

$$(6)\quad F_2=\alpha_0^3+6\alpha_0^2\alpha_2-3\alpha_0\alpha_1^2+3\alpha_0\alpha_1\alpha_2+9\alpha_0\alpha_2^2-\alpha_1^3+3\alpha_1\alpha_2^2+\alpha_2^3\,.$$

4. *Representation of Rational Primes as Norms of Integers of $K_1(x)$.* Lemma (a). *The cubic form*

$$F=x^3+x^2y-2xy^2-y^3$$

is congruent (mod 7) *to* 0 *or to* ± 1.

(b) *The congruence $x^3+x^2-2x-1\equiv 0$* (mod p), *with p a rational prime, has solutions for $p=7$, or any prime of the form $7m\pm 1$.*

In proof of (a), we note that if $x\equiv y\equiv 0$ (mod 7), then $F\equiv 0$ (mod 7). If $y\equiv 0$ (mod 7) and $x\not\equiv 0$ (mod 7), then $F\equiv x^3\equiv \pm 1$ (mod 7). If $y\not\equiv 0$ (mod 7), we let $x\equiv zy$ (mod 7) and get $F\equiv y^3(z^3+z^2-2z-1)\equiv \pm(z^3+z^2-2z-1)$ (mod 7). On letting z be congruent (mod 7) to $0, 1, \cdots, 6$, we obtain $F\equiv 0$ or ± 1 (mod 7).

Proof of (b) is given by Cailler, Intermédiaire des Mathématiciens, vol. 16 (1909), pp. 185-7.

We are now able to prove the following theorem.

Theorem II. *For the field $K_1(x)$, defined by a root of $x^3+x^2-2x-1=0$, the norm of a prime not associated with a rational prime is either 7 or a rational prime of the form*

[*] L. W. Reid, *Tafel der Klassenanzahlen für kubische Zahlkörper*, pp. 60 and 74.

$7m \pm 1$. *In case the prime is associated with a rational prime, the norm is the cube of the rational prime and is thus of the form* $7m \pm 1$. *Rational primes of the forms* $7m \pm 2$ *and* $7m \pm 3$ *are primes of the field. Further, every rational prime* $7m \pm 1$ *is factorable into three conjugate primes of the field and thus is the norm of a prime of the field.*

We note first that $N(1+x+x^2)=7$. Hence 7 is not a prime of $K_1(x)$, but may be represented in the form F_1 of (5). Let $\pi = \alpha_0 + \alpha_1 x + \alpha_2 x^2$ be a prime of the field which is not associated with a rational prime. Then

$$\begin{aligned} N(\pi) &= \alpha_0^3 - \alpha_0^2\alpha_1 + 5\alpha_0^2\alpha_2 - 2\alpha_0\alpha_1^2 - \alpha_0\alpha_1\alpha_2 + 6\alpha_0\alpha_2^2 + \alpha_1^3 - \alpha_1^2\alpha_2 \\ &\qquad - 2\alpha_1\alpha_2^2 + \alpha_2^3 \\ &= (\alpha_0)^3 + (-\alpha_1 - 2\alpha_2)(\alpha_0)^2 - 2(-\alpha_1 - 2\alpha_2)^2(\alpha_0) \\ &\quad - (-\alpha_1 - 2\alpha_2)^3 + 7\alpha_2(\alpha_0^2 + \alpha_0\alpha_1 + 2\alpha_0\alpha_2 - \alpha_1^2 - 2\alpha_1\alpha_2 - \alpha_2^2) \ . \end{aligned}$$

Hence $N(\pi)$ is congruent (mod 7) to an expression of the form*

$$x^3 + x^2y - 2xy^2 - y^3,$$

which by the lemma is congruent (mod 7) either to 0 or to ± 1. Hence if $N(\pi) \neq 7$, we must have $N(\pi) \equiv \pm 1$ (mod 7) and thus $N(\pi)$ equals 7 or a rational prime of the form $7m \pm 1$.

Rational primes $7m \pm 2$ and $7m \pm 3$ are primes of the field, for a rational prime p is factorable into conjugate primes of $K_1(x)$ only when it is 7 or of the form $7m \pm 1$.

To prove the last statement of the theorem, we note that

$$N(\alpha - x) = \alpha^3 + \alpha^2 - 2\alpha - 1.$$

Now let p be a rational prime of the form $7m \pm 1$ and suppose p is a prime of the field. We have

$$\begin{aligned} (\alpha - x)(\alpha - x')(\alpha - x'') &= (\alpha - x)(\alpha + 2 - x^2)(\alpha - 1 + x + x^2) \\ &= \alpha^3 + \alpha^2 - 2\alpha - 1 \equiv 0 \pmod{p}, \end{aligned}$$

* Writing $N(\pi) = (\alpha_0 + 2\alpha_1 + 4\alpha_2)^3 - 7(\alpha_0^2\alpha_1 + \alpha_0^2\alpha_2 + 2\alpha_0\alpha_1^2 + 7\alpha_0\alpha_1\alpha_2 + 6\alpha_0\alpha_2^2 + \alpha_1^3 + 7\alpha_1^2\alpha_2 + 14\alpha_1\alpha_2^2 + 9\alpha_2^3)$, we might dispense with Lemma (a). This method would, however, not apply to the form F_2.

by part (b) of the lemma. Hence p, a prime of $K_1(x)$, must divide one of the factors $\alpha - x$, $\alpha + 2 - x^2$ or $\alpha - 1 + x + x^2$. We would thus have a relation as $\alpha - x = p(\beta_0 + \beta_1 x + \beta_2 x^2)$. In this case $p\beta_1 = -1$, which is impossible since p and β_1 are rational integers and $p > 1$.

Hence no rational prime of the form $7m \pm 1$ can be a prime of the field. But $p = 7m \pm 1$ divides $N(\alpha - x)$ and accordingly, by Theorem I, must be the norm of a prime of $K_1(x)$.

We may state the following corollary.

COROLLARY. *The form*

$$F_1 = \alpha_0^3 - \alpha_0^2\alpha_1 + 5\alpha_0^2\alpha_2 - 2\alpha_0\alpha_1^2 - \alpha_0\alpha_1\alpha_2 + 6\alpha_0\alpha_2^2 + \alpha_1^3 - \alpha_1^2\alpha_2$$
$$- 2\alpha_1\alpha_2^2 - \alpha_2^3$$

represents 1, 7, *all primes of the form* $7m \pm 1$ *and all products whose prime factors are* 7 *and primes* $7m \pm 1$. *It cannot represent primes* $7m \pm 2$ *and* $7m \pm 3$ *and has such primes as divisors only when they divide each of* α_0, α_1, *and* α_2; *and then they appear in powers which are multiples of* 3.

5. *Representation of Rational Primes as Norms of Integers of* $K_2(x)$. Analogous to the lemma of §3, we have the following lemma.

LEMMA (a). *The cubic form*

$$F = x^3 - 3xy^2 + y^3$$

is congruent to 0 (mod 3), *or else is congruent to* ± 1 (mod 9).

(b) *The congruence* $x^3 - 3x + 1 \equiv 0$ (mod p), *with* p *a rational prime, has solutions for* $p = 3$, *or any prime of the form* $9m \pm 1$.

Proof of (a) is obtained readily as in §3.

Proof of (b) follows from the proof for the corresponding statement with reference to $y^3 - 3y - 1 \equiv 0$ (mod p), as given by L. Aubry in the INTERMÉDIAIRE DES MATHÉMATICIENS for November and December, 1924.

By analogy to Theorem 2, we have the following theorem.

THEOREM III. *For the field $K_2(x)$, defined by a root of $x^3-3x+1=0$, the norm of a prime not associated with a rational prime; is either* 3 *or a rational prime of the form* $9m\pm 1$. *In case the prime is associated with a rational prime, the norm is the cube of the rational prime, and is thus of the form* $9m\pm 1$. *Rational primes, other than* 3 *or those of the form* $9m\pm 1$ *are primes of the field. Further, every rational prime* $9m\pm 1$ *is factorable into three conjugate primes of the field and so is the norm of a prime of the field.*

In proof, we note first that

$$N(-1-x)=3.$$

Hence 3 is not a prime of $K_2(x)$, but may be represented in the form F_2 of (6). Now let $\pi=\alpha_0+\alpha_1x+\alpha_2x^2$ be a prime of the field which is not associated with a rational prime.

$$\begin{aligned} N(\pi) &= \alpha_0^3+6\alpha_0^2\alpha_2-3\alpha_0\alpha_1^2+3\alpha_0\alpha_1\alpha_2+9\alpha_0\alpha_2^2-\alpha_1^3+3\alpha_1\alpha_2^2+\alpha_2^3 \\ &= (\alpha_0+2\alpha_2)^3-3(\alpha_0+2\alpha_2)(-\alpha_1-\alpha_2)^2+(-\alpha_1-\alpha_2)^3 \\ &\quad +9\alpha_1\alpha_2(\alpha_0+\alpha_1+\alpha_2)\ . \end{aligned}$$

Thus $N(\pi)$ is congruent (mod 9) to an expression of the form

$$x^3-3xy^2+y^3,$$

which by the lemma is congruent to zero (mod 3), or else is congruent to ± 1 (mod 9). Hence if $N(\pi)\neq 3$, we must have $N(\pi)\equiv\pm 1$ (mod 9), and thus $N(\pi)$ equals 3 or a rational prime of the form $9m\pm 1$.

Rational primes, other than 3 and those of the form $9m\pm 1$, are primes of the field, for a rational prime p is factorable into conjugate primes of $K_2(x)$ only when it is 3 or of the form $9m\pm 1$.

Finally, we note that

$$N(\alpha-x)=\alpha^3-3\alpha+1.$$

Let p be a rational prime of the form $9m\pm 1$ and suppose p is a prime of the field. We have

$$\begin{aligned} (\alpha-x)(\alpha-x')(\alpha-x'') &= (\alpha-x)(\alpha+2-x^2)(\alpha-2+x+x^2) \\ &= \alpha^3-3\alpha+1\equiv 0 \pmod{p}, \end{aligned}$$

by part (b) of the lemma. Hence p, a prime of $K_2(x)$, divides one of $\alpha-x$, $\alpha+2-x^2$, or $\alpha-2+x+x^2$. As in Section 3, this is readily seen to be impossible. Hence no rational prime of the form $9m\pm 1$ can be a prime of the field. Whence by Theorem I, such primes are norms of primes of $K_2(x)$.

COROLLARY. *The form*

$$F_2=\alpha_0^3+6\alpha_0^2\alpha_2-3\alpha_0\alpha_1^2+3\alpha_0\alpha_1\alpha_2+9\alpha_0\alpha_2^2-\alpha_1^3+3\alpha_1\alpha_2^2+\alpha_2^3$$

represents 1, 3, *all primes of the form* $9m\pm 1$ *and all products whose prime factors are* 3 *and primes* $9m\pm 1$. *The form represents no prime other than these. Other primes are divisors of the form only when they divide each of* α_0, α_1, *and* α_2, *and then they appear in powers which are multiples of* 3.

6. *Relation to Eisenstein's Canonical Form.*[*] Eisenstein's canonical form for $p=7$, reduces to

$$u^3-21uv^2+21uvw-21uw^2+7v^3-105v^2w+84vw^2+7w^3.$$

This transforms into F_1 on the substitution

$$\begin{array}{ll} u= & \alpha_0-\dfrac{1}{3}\alpha_1+\dfrac{5}{3}\alpha_2\ , \\ v= & \qquad\qquad\quad\ \dfrac{1}{3}\alpha_2 \\ w= & \qquad\ \dfrac{1}{3}\alpha_1\ , \end{array}$$

with determinant equal to $-\frac{1}{9}$.

Thus the form F_1 and Theorem 2 might have been deduced from Eisenstein's results. The form F_2 is, however, not obtainable from Eisenstein's canonical form, since his form has relation to the division of the circle into p parts, where p is a prime of the form $3m+1$, whereas, the form F_2 has relation to the division of the circle into nine parts.

THE UNIVERSITY OF MANITOBA

[*] JOURNAL FÜR MATHEMATIK, vol. 28, p. 303.