QUADRATIC FIELDS IN WHICH FACTORIZATION IS ALWAYS UNIQUE*

BY L. E. DICKSON

1. *Definitions.* Let m be an integer, other than 0 and 1, such that m is not divisible by a perfect square exceeding unity. All numbers $r+s\sqrt{m}$ in which r and s are rational constitute a *field* $R(\sqrt{m})$. Its *algebraic integers* are known to be $x+y\theta$, where x and y are rational integers, and

(1) $\theta=\sqrt{m}$ if $m\equiv 2$ or $m\equiv 3 \pmod 4$,

(2) $\theta=\frac{1}{2}(1+\sqrt{m})$, $\theta^2=\theta-k$, if $m\equiv 1 \pmod 4$,

where $k=\frac{1}{4}(1-m)$. The *conjugate* of $\xi=x+y\theta$ is defined to be $\xi'=x+y\theta'$, where $\theta'=-\theta$ in case (1), and $\theta'=\frac{1}{2}(1-\sqrt{m})$ in case (2). The product $\xi\xi'$ is called the *norm* of ξ, and is denoted by $N(\xi)$. According as the case is (1) or (2), we have

(3) $N(x+y\theta)=x^2-my^2$ or $x^2+xy+ky^2$.

If ξ is an algebraic integer such that $N(\xi)=\pm 1$, then ξ is called a *unit*. The only units in $R(i)$ are ± 1 and $\pm i$.

2. *Object of the Paper.* It is known† that -1, -2, -3, -7 and -11 are the only negative values of m for which the greatest common divisor process yielding numerically decreasing norms is always applicable in $R(\sqrt{m})$, so that if a and b are any algebraic integers $(b\neq 0)$ there exist algebraic integers q and r of the field such that

$$a=bq+r, \quad |\text{norm } r|<|\text{norm } b|.$$

* Presented to the Society, December 29, 1923. See also This BULLETIN, p. 90, Jan.–Feb., 1924, and footnote, p. 247, May–June, 1924.

† For a geometric proof, see Birkhoff, AMERICAN MATHEMATICAL MONTHLY, vol. 13 (1906), pp. 156–159.

For a few positive values of m, as 2, 3, 5, 11, such a process exists. But there are many values of m for which this process is not applicable, although there exists a greatest common divisor as shown by the theory of ideals when the number of classes of ideals is unity.

Avoiding the theory of ideals, we shall give an elementary proof of the following result.

THEOREM 1. *Let m be any integer for which there is a single* class of properly primitive binary quadratic forms capable of representing positive integers and having the discriminant $4m$ or m according as the case is* (1) *or* (2). *Then the algebraic integers of $R(\sqrt{m})$ admit unique factorization into primes apart from the association of unit factors.*†

This proof places at the disposal of students of elementary theory of numbers an effective tool utilized by Gauss and Dirichlet in the case $m = -1$. Moreover, the proof furnishes a model for the investigation‡ of the arithmetics of linear algebras for which no theory of ideals is available.

3. LEMMA 1. *If a and b are relatively prime and*

$$(4) \qquad a^2 - mb^2 = pq \quad or \quad a^2 + ab + kb^2 = pq, \quad p > 0,$$

there exist integers z and w such that

$$(5) \qquad p = z^2 - mw^2 \quad or \quad p = z^2 + zw + kw^2,$$

according as case (1) *or* (2) *holds.*

For, b and q are relatively prime since otherwise a common prime divisor of them would divide a^2 and hence a. Hence

* In this BULLETIN, vol. 17 (1910–11), pp. 534–37, the writer proved that there is a single class of positive primitive quadratic forms of negative discriminant $-P$ with $P < 1{,}500{,}000$ only when $P = 3, 4, 7, 8, 11, 12, 16, 19, 27, 28, 43, 67, 163$. But the cases in which the discriminant is positive are very numerous.

† Theorem 1 holds also if there are only two classes and these are *opposite* classes of properly primitive forms of discriminant $4m$ or m. In the first case, every such form is equivalent to $x^2 - my^2$ or $mx^2 - y^2$. The proof differs from that in the text only by the occasional insertion of the double sign $\pm$.

‡ See L. E. DICKSON, AMERICAN JOURNAL, 1924.

there exist integers s and t such that $a = sb + tq$. Inserting this in (4), we get

$$pq = Ab^2 + Bbqt + q^2t^2,$$

where $A = s^2 - m$, $B = 2s$ in case (1); while $A = s^2 + s + k$, $B = 2s + 1$ in case (2). Hence A must be divisible by q. Write $A = qe$. Then

$$p = eb^2 + Bbt + qt^2. \tag{6}$$

The discriminant of this form is $B^2 - 4eq = 4m$ or m according as the case is (1) or (2). If any odd prime divides e, B and q, its square divides $B^2 - 4eq$, whereas m has no square factor. If, in case (1), 2 divides both e and q, then $m = s^2 - eq \equiv s^2 \equiv 0$ or $1 \pmod 4$, contrary to (1). Hence in every case (6) is a properly primitive form representing the positive integer p and therefore, by our hypothesis of a single class, is equivalent to the respective form (5) of discriminant $4m$ or m.

4. LEMMA 2.* *If a and b are relatively prime integers and if $N(a + b\theta)$ is divisible by the rational prime p, then p decomposes and one of its integral algebraic factors divides $a + b\theta$.*

By hypothesis, we have (4) and hence (5).

(i) Let the first equations (4) and (5) hold. Then

$$mb^2 \equiv a^2, \quad z^2 \equiv mw^2 \pmod p.$$

By multiplication we get $bz \equiv \pm aw \pmod p$ if m is not divisible by p, and we may choose the upper sign after changing the sign of w if necessary. If m is divisible by p, we have $z \equiv 0$, $a \equiv 0 \pmod p$. Hence $bz \equiv aw \pmod p$ in all cases. Define rational numbers x and y by means of

$$p(x + y\theta) = (a + b\theta)(z - w\theta), \tag{7}$$

* Another proof follows from the writer's theorem in this BULLETIN, vol. 29 (1923), pp. 464–467, that all solutions of $N(a + b\theta) = pq$ are products of the same integer ρ by the numbers obtained from (8) and $p = N(z + w\theta)$, $q = N(x + y\theta)$. Here $\rho = \pm 1$ since a and b are relatively prime. But if we omit §§ 3–4, we must replace § 5 by one of the standard proofs of unique representation of a prime as a norm.

whence

$$x = \frac{az - mbw}{p}, \quad y = \frac{bz - aw}{p},$$

so that y is an integer. Since $p = (z + w\theta)(z - w\theta)$, we may cancel $z - w\theta$ from (7) and get

$$(z + w\theta)(x + y\theta) = a + b\theta. \tag{8}$$

Taking norms, we have $p(x^2 - my^2) = pq$, whence x^2 is the integer $my^2 + q$. Hence both x and y are integers in (8), which is the desired result.

(ii) Let the second equations (4) and (5) hold. Then

$$(2a + b)^2 - mb^2 = 4pq, \quad 4p = (2z + w)^2 - mw^2,$$

$$mb^2(2z + w)^2 \equiv (2a + b)^2 mw^2 \pmod{p}.$$

If m is not divisible by p, we get

$$b(2z + w) \equiv \pm(2a + b)w \pmod{p}. \tag{9}$$

First, let the upper sign hold in (9). Then, if $p \neq 2$, $bz \equiv aw \pmod{p}$. This follows also if m is divisible by p, whence $2a + b \equiv 0$, $2z + w \equiv 0$. Define rational numbers x and y by means of

$$p(x + y\theta) = (a + b\theta)(z + w\theta'), \tag{10}$$

whence

$$x = \frac{a(z + w) + kbw}{p}, \quad y = \frac{bz - aw}{p},$$

so that y is an integer. Since $p = (z + w\theta)(z + w\theta')$, we may cancel $z + w\theta'$ from (10) and get (8). By the norm of (8), $p(x^2 + xy + ky^2) = pq$. Thus x is a rational root of an equation with integral coefficients and leading coefficient unity; hence x is an integer.

Second, let the lower sign hold in (9). Then if $p \neq 2$, $b(z + w) \equiv -aw \pmod{p}$. Introduce the integers $Z = z + w$, $W = -w$. Then $bZ \equiv aW$ and

$$Z^2 + ZW + kW^2 = z^2 + zw + kw^2 = p, \tag{11}$$

and we are led to our first case with Z and W in place of z and w. Hence $a + b\theta$ has the factor $Z + W\theta = z + w\theta'$.

Finally, let $p = 2$. If b is even, so that a is odd, $a^2 + ab$

$+kb^2$ is odd, whereas it is divisible by $p=2$ by (4). If w is even, z is even in $2=z^2+zw+kw^2$, which is then divisible by 4. Hence b and w are both odd. By (11) we may add w to z and hence make z even or odd at pleasure and hence make $z\equiv a \pmod 2$. Then $bz\equiv aw \pmod 2$. We proceed as in the first case.

5. LEMMA 3. *If a rational prime p is expressible as a norm, it is the product of two algebraic integers, neither a unit, in one and only one way apart from unit factors and apart from the arrangement of the two integers.*

We have $p=(z+w\theta)(z+w\theta')$. Let also $p=\pi\varrho$, where $\pi=a+b\theta$ and ϱ are algebraic integers neither a unit. Then $p^2=N(\pi)N(\varrho)$, whence $N(\pi)=N(\varrho)=\pm p$. If a and b had a common prime factor, its square would divide $N(\pi)=\pm p$. Hence we may apply the proof of Lemma 2 with $q=\pm 1$ and obtain (8) or the similar equation with $z+w\theta$ replaced by $z+w\theta'$. Then $x+y\theta$ is a unit since its norm is $q=\pm 1$. Hence every factorization $p=\pi\varrho$ differs from the given one only by the insertion of unit factors or by the interchange of the given factors.

6. *Algebraic Primes.* An algebraic integer not a unit of $R(\theta)$ is called an *algebraic prime* if it is not a product of two algebraic integers neither a unit of $R(\theta)$.

If a rational prime p is a norm, so that $p=\pi\pi'$, then π and π' are algebraic primes. For, if $\pi=\alpha\beta$, where neither α nor β is a unit, then $p=N(\alpha)N(\beta)$, and one of the norms is ± 1, so that α or β is a unit.

7. LEMMA 4. *If $N(c+d\theta)$ is divisible by a rational prime p, then either $c+d\theta$ is divisible by p or else p decomposes and $c+d\theta$ is divisible by one of the algebraic prime factors of p.*

Let g be the greatest common divisor of $c=ga$, $d=gb$. Then

$$c+d\theta=g(a+b\theta) \tag{12}$$

is divisible by p if g is. Next, let g be not divisible by p. Since $N(c+d\theta) = q^2N(a+b\theta)$ is divisible by p, $N(a+b\theta)$ is divisible by p and Lemma 2 shows that p decomposes and that $a+b\theta$ is divisible by one of the algebraic prime factors of p. Hence (12) is divisible by that factor.

8. THEOREM 2. *If an algebraic prime divides a product AB, it divides A or B.*

(i) Suppose the algebraic prime is a rational prime p. We may write $A = q\alpha$, where q is a rational integer and α has relatively prime coordinates. Then p divides qP, where $P = \alpha B = r+s\theta$. Then p divides qr and qs. If p divides q, it divides A. In the contrary case, p divides r, s and hence also αB. Write $B = t\beta$, where β has relatively prime coordinates. As before, either p divides t and hence B, or else p divides $\alpha\beta$, so that p^2 divides $N(\alpha)N(\beta)$. We may then assume that p divides $N(\alpha)$ for example, whence, by Lemma 2, p decomposes, whereas it is an algebraic prime.

(ii) Let π be an algebraic prime not the product of an integer by a unit. Hence the coordinates of π are relatively prime. The integer $N(\pi)$ is divisible by a rational prime p. Hence, by Lemma 2, $p = \varrho\varrho'$ and ϱ is a divisor of π. Thus the prime π is the product of ϱ by a unit, whence $N(\pi) = \pm N(\varrho) = \pm p$. Suppose that π divides AB, but divides neither A nor B. Then $\pm p = N(\pi)$ divides $N(A)N(B)$. Let therefore p divide $N(A)$ for example. By Lemmas 3 and 4, A is divisible by π or π'. Hence A is divisible by π'. Write $A = \pi'\alpha$, $P = \alpha B$. Then π divides $AB = \pi'P$, so that $p = \pm\pi\pi'$ divides π'^2P. We shall prove that p divides $\pi'P$. Write

$$\pi' = a+b\theta,\ P = c+d\theta,\ \pi'^2P = r+s\theta,$$
$$r \equiv s \equiv 0 \pmod{p}.$$

First, let $\theta = \sqrt{m}$. Then $\pm p = a^2 - mb^2$ and

$$r = a^2c+2mabd+mb^2c, \quad s = a^2d+2abc+mb^2d.$$

Elimination of a^2 by means of $a^2 \equiv mb^2 \pmod{p}$ gives

$$r \equiv 2mb(ad+bc) \equiv 0, \quad s \equiv 2b(ac+mbd) \equiv 0 \pmod{p}.$$

If $2mb$ is not divisible by p, the numbers in parenthesis, which are the coordinates of $\pi' P$, are divisible by p. Hence P is divisible by π. Thus π divides αB, but divides neither α nor B. A repetition of the argument leads evidently to a contradiction. Next, if b were divisible by p, a would be also in view of $\pm p = a^2 - mb^2$, which would then be divisible by p^2. If m were divisible by p, a would be also, whence π'^2 is divisible by p, and hence π' by π, so that π' is the product of π by a unit. Since A is divisible by π', it is divisible by π. If $p = 2$, $\pi'^2 \equiv a^2 + b^2 m \equiv 0 \pmod{p}$.

Second, consider case (2). Then $\pm p = a^2 + ab + kb^2$, so that b is not divisible by p. In

$$r = a^2c - 2kabd - kb^2c - kb^2d,$$
$$s = a^2d + b^2c + 2abc + 2abd + (1-k)b^2d$$

we replace a^2 by $-ab - kb^2 \pmod{p}$, cancel factors b, and get

$$\begin{aligned} 2kad + ac + 2kbc + kbd &\equiv 0, \\ bc + 2ac + ad + (1-2k)bd &\equiv 0 \end{aligned} \qquad (\text{mod } p). \tag{13}$$

Elimination of ac gives $(4k-1)E \equiv 0$, where $E = ad + bc + bd$. But if $4k - 1 = -m$ were divisible by p, $\pm 4p = (2a+b)^2 - mb^2$ shows that $2a + b \equiv 0$, whence

$$\pi'^2 = a^2 - kb^2 + b(b+2a)\theta \equiv a^2(1-4k) = ma^2 \equiv 0 \pmod{p},$$

so that A is divisible by π as in the first case. In view of this contradiction, we have $E \equiv 0$. Adding $-2kE$ to the first equation (13), we get $F \equiv ac - kbd \equiv 0$. Hence

$$\pi' P = F + E\theta \equiv 0 \pmod{p}.$$

THE UNIVERSITY OF CHICAGO