NOTE ON FACTORIZATION IN A QUADRATIC FIELD

GORDON PALL

1. **Introduction.** In this note we shall prove certain theorems relating to the "existence" and "uniqueness" of factorization in a quadratic field (cf. §§2 and 3); and shall maintain that the introduction of ideals should be regarded as restoring *existence* rather than *uniqueness* of factorization into primes.

To illustrate this, let us consider first the case of quaternions. Let $x=x_0+i_1x_1+i_2x_2+i_3x_3$ be a *primitive* quaternion, that is, let the coordinates $x_0, \cdots, x_3$ be relative-prime rational integers. Let the norm $Nx=\sum x_i^2$ be factored into a product of rational primes $p_1 \cdots p_s$. Then, by a theorem of Lipschitz,[1] there exist prime quaternions $t', t'', \cdots, t^{(s)}$, of respective norms $p_1, \cdots, p_s$ such that $x=t't'' \cdots t^{(s)}$. This factorization is unique, for any given ordering of the primes $p_1, \cdots, p_s$, except that we can insert unit factors in the trivial way illustrated by the example $t't''t'''=(t'i_1)(i_1t''i_3)(i_3t''')$ $=(-t')(t''i_2)(i_2t''')=\cdots$.

It is proved elsewhere that a similar uniqueness of factorization holds in every system of "generalized quaternions," but that the existence of such a factorization will fail if certain rational primes p_i are not norms.

As is well known there exists a very satisfactory arithmetic of ordinary quaternions, without the necessity of introducing ideals. Nevertheless, factorization of imprimitive quaternions is not unique. For example,

$$\begin{aligned} 6 &= (1-i_1-i_2)(1-i_1)(1+i_1)(1+i_1+i_2) \\ &= (1-i_1-i_3)(1-i_1)(1+i_1)(1+i_1+i_3), \end{aligned}$$

where the primes $1-i_1-i_2$ and $1-i_1-i_3$ do not differ only by unit factors.

Similarly, in the quadratic field $R(\rho)$, where $\rho^2=-5$, we have

$$6 = (1+\rho)(1-\rho) = 2\cdot 3,$$

where the factors are essentially different prime integers of the field, and hence factorization is not unique. Yet a uniqueness theorem analogous to that for ordinary quaternions holds for the factoriza-

Presented to the Society, August 14, 1944; received by the editors June 5, 1944, and, in revised form, July 18, 1945.

[1] Lipschitz, Journal de Mathématiques (4) vol. 2 (1886) pp. 373–439; Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*, 1919.

tion of *primitive* integers in every quadratic field.

Indeed, let Δ be a non-square integer, $\Delta \equiv \epsilon \pmod 4$, $\epsilon = 0$ or 1, $\Delta/(2-\epsilon)^2$ be squarefree. Set $\rho = (-\epsilon + \Delta^{1/2})/2$. Then the integers of the field $R(\rho)$ have the form $x = x_0 + x_1\rho$, where x_0 and x_1 are rational integers. The norm of x is $Nx = x_0^2 - \epsilon x_0 x_1 + (\epsilon^2 - \Delta)x_1^2/4$. Suppose that x is primitive, that is, $(x_0, x_1) = 1$, and factor $Nx = p_1 \cdots p_s$ as a product of ordinary primes p_i. Then (as a corollary of Theorem 1) the factorizations $x = t't'' \cdots t^{(s)}$ with $N(t^{(i)}) = p_i$ are unique apart from unit factors. However, the prime factors p_i of Nx need not be norms, and so such factorizations need not exist.

When ideals are introduced into the quadratic field, there are ideals of every prime norm which can divide the norm of a primitive integer. For, if $(\Delta \mid p) = -1$, then $p \mid Nx$ implies that $p \mid x$. Hence the principal service performed by the introduction of ideals is to restore existence rather than uniqueness of factorization into "primes." It is the fact that every prime is a sum of four squares that makes the arithmetic of quaternions satisfactory; and the fact that every prime p such that $(\Delta \mid p) \neq -1$ is a norm (in essentially only one way) that makes the fundamental theorem of arithmetic hold in those quadratic fields in which there is only one class of forms of discriminant Δ.

2. **Quadratic integers; unique factorization.** Let Δ be a non-square integer, $\Delta \equiv \epsilon \pmod 4$, where $\epsilon = 0$ or 1. Set $\rho = (-\epsilon + \Delta^{1/2})/2$. We shall consider factorization in the ring of quadratic integers $x = x_0 + x_1\rho$, where x_0 and x_1 are rational integers. The letters $t, \cdots, z$ (without subscripts) will be reserved for such integers. We do not restrict attention to the case where $\Delta/(2-\epsilon)^2$ is squarefree. This restriction is commonly made in books on quadratic fields, and does in fact make the arithmetical theory simpler than it would otherwise be, since it excludes from consideration certain complicated cases. But, arithmetically, we are as much interested in the complicated cases (such as, say $x_0 + x_1(13)^{1/2}$) as in the others, and with very little effort can remove the restriction. It is to be noted that if $\Delta/(2-\epsilon)^2$ is squarefree, our set of integers is the same as that in the classical theory.

It will be observed that x (along with its conjugate $\bar{x} = x_0 + x_1\bar{\rho}$, where $\bar{\rho} = (-\epsilon - \Delta^{1/2})/2$) satisfies the equation

$$x^2 - (2x_0 - \epsilon x_1)x + (x_0^2 - \epsilon x_0 x_1 + (\epsilon^2 - \Delta)x_1^2/4) = 0.$$

The rational integers $x + \bar{x} = 2x_0 - \epsilon x_1$ and $x\bar{x} = x_0^2 - \epsilon x_0 x_1 + (\epsilon^2 - \Delta)x_1^2/4$ are called the trace and norm of x, respectively, the latter denoted by Nx.

If $x = yz$, evidently $\bar{x} = \bar{y}\bar{z}$, whence $Nx = Ny \cdot Nz$. Hence if t is a di-

visor of x, $Nt \mid Nx$. If θ denotes any unit, that is if $N\theta = 1$, the associates θt are (with t) factors of x, all with the same norm.

THEOREM 1. *If x is primitive (that is, x_0, x_1 coprime), and*

$$x = ut = vt', \qquad Nt = Nt',$$

then t and t' are associates, except possibly when Nt is divisible by a prime p for which Δ/p^2 is an integer congruent to 0 or 1 mod 4.[2]

The proof is made up of three lemmas:

LEMMA 1. *If $x \equiv y \pmod{m}$, then x and y have the same factors of norm m.*

PROOF. If $x = ut$ and $Nt = m$, then $x + zm = (u + z\bar{t})t$.

LEMMA 2. *If $ut = vt'$, $Nt = Nt' = m$, and Nv is prime to m, then t and t' are associates.*

PROOF. Let $k \cdot Nv \equiv 1 \pmod{m}$. Then $k\bar{v}ut = k \cdot Nv \cdot t'$. By Lemma 1, t' has t for a factor, $t' = wt$, $Nt' = Nw \cdot Nt$, $Nw = 1$.

LEMMA 3. *If x is primitive, and $x = ut$ where $Nt = m$, then we can find an integral z such that $\{N(x+zm)\}/m$ is prime to m, except possibly when m is not semiprime to Δ.*

PROOF. Set $x\bar{x} = km$, that is, $(2x_0 - \epsilon x_1)^2 - \Delta x^2 = 4km$. We have

$$\begin{aligned} N(x + zm) &= (x + zm)(\bar{x} + \bar{z}m) = x\bar{x} + (x\bar{z} + z\bar{x})m + z\bar{z}m^2 \\ &= m\{k + (2x_0 - \epsilon x_1)z_0 \\ &\quad + (-\epsilon x_0 + (\epsilon^2 - \Delta)x_1/2)z_1 + mNz\}. \end{aligned}$$

We can evidently choose z_0 and z_1 to make $\{N(x+zm)\}/m$ prime to m, except when for some prime p dividing m and k,

$$2x_0 - \epsilon x_1 \equiv 0 \equiv -\epsilon x_0 + (\epsilon^2 - \Delta)x_1/2 \pmod{p}. \tag{1}$$

Since $(x_0, x_1) = 1$ this requires that $p^2 \mid \Delta$ if $p > 2$. If $p = 2$ and $\epsilon = 1$, (1) implies $2 \mid x_0$ and $2 \mid x_1$, a contradiction. If $p = 2$ and $\epsilon = 0$, then $4 \mid x_0^2 - \Delta x_1^2/4$, implying x_0 and x_1 even, if $\Delta/4 \equiv 2$ or $3 \pmod 4$.

3. **Conditions for the existence of factors of given norm.** For a given x, and a given rational integer m which satisfies the obviously necessary conditions

---

[2] Hence there is no exception if $\Delta/(2-\epsilon)^2$ is squarefree. We shall say that m is semiprime to Δ if m is divisible by no prime p such that $p^2 \mid \Delta$ $(p > 2)$, nor by the prime 2 if $\Delta/4 \equiv 0$ or $1 \pmod 4$. All integers are semiprime to Δ if $\Delta/(2-\epsilon)^2$ is squarefree.

(2) $$m \text{ is a norm}, \qquad m \mid Nx,$$

we investigate the set of divisors t of x having norm m. Consider then

(3) $$x = ut, \qquad Nt = m.$$

These conditions on t are equivalent to the following:

(4) $$x\bar{t} \equiv 0 \pmod{m}, \qquad Nt = m.$$

The condition $x\bar{t} \equiv 0$ expands into the following:

(5) $$x_1 t_0 - x_0 t_1 \equiv 0 \pmod{m},$$

(6) $$x_0 t_0 - (\epsilon x_0 - (\epsilon^2 - \Delta)x_1/4)t_1 \equiv 0 \pmod{m}.$$

Hereafter we assume, for simplicity, that:

(7) $$x \text{ is primitive, and } m \text{ is semiprime to } \Delta.$$

Since $m \mid x_0^2 - \epsilon x_0 x_1 + (\epsilon^2 - \Delta)x_1^2/4$, $(m, x_1) = 1$. Hence (5) can be written $t_0 \equiv \lambda t_1 \pmod{m}$, where $\lambda \equiv x_0/x_1$. If this is put into (6), (6) reduces to $(t_1/x_1)Nx \equiv 0 \pmod{m}$, a consequence of (2_2).

Hence, under assumptions (2) and (7_1), (3) holds if and only if

(8) $$Nt = m, \qquad t_0 \equiv \lambda t_1 \pmod{m}.$$

Putting $t_0 = my_0 + \lambda y_1$, $t_1 = y_1$, into (8_1), we get

(9) $$my_0^2 + (2\lambda - \epsilon)y_0 y_1 + ky_1^2 = 1,$$

where k is the integer defined by

$$km = \lambda^2 - \epsilon\lambda + (\epsilon^2 - \Delta)/4.$$

The binary form $\phi = my_0^2 + (2\lambda - \epsilon)y_0 y_1 + ky_1^2$ has discriminant Δ.

Now it is well known that only one class of binary quadratic forms of discriminant Δ can represent 1, namely the principal class, containing the form $\phi_0 = x_0^2 - \epsilon x_0 x_1 + (\epsilon^2 - \Delta)x_1^2/4$.

There are certain cases in which we can be sure that ϕ belongs to the principal class. An integer m semiprime to Δ is represented by forms in at most one genus of discriminant Δ. Hence if ϕ_0 is in a genus of one class, ϕ, which represents m, must be equivalent to ϕ_0. In particular the form $x_0^2 + 5x_1^2$ is included in this case.

Secondly, a prime is represented in at most one class and its reciprocal. Hence $\phi \sim \phi_0$ if $\pm m$ is a prime.

Finally we shall state without proof necessary and sufficient conditions that an integer m which is semiprime to Δ be isolated, that is, be represented by at most one class and its reciprocal class under composition. First suppose that the primes $p_1, \cdots, p_r$ are repre-

sented in non-ambiguous classes $G_1, \cdots, G_r$, and that $a_1, \cdots, a_r$ are positive integers. Then $n_1 = p_1^{a_1} \cdots p_r^{a_r}$ is isolated if and only if either $r = 0$, or $r = 1 = a_1$, or

$$a_1 + a_2 + \cdots + a_r \text{ is odd}, G_1^2 = \cdots = G_r^2, G_1^4 = \cdots = G_r^4 = 1.$$

Next, if n_1 contains only primes represented in non-ambiguous classes, and n_2 only primes represented only in ambiguous classes (these include primes dividing the discriminant but semiprime to it), then $n_1 n_2$ is isolated if and only if n_1 is isolated. Finally, the only other primes which may divide an integer m which is semiprime to Δ are primes such that $(\Delta \mid p) = -1$; such primes must appear in m to an even power, if m is represented at all, and can be cancelled out of m and its representations.

It is only when there is but one class of forms of discriminant Δ that every prime p such that $(\Delta \mid p) \neq -1$, and p is semiprime to Δ, is a norm. Further, every such prime is a norm in only one way, so that its factors are unique. Hence in this case we can easily deduce from the preceding theory that every quadratic integer whose norm is semiprime to Δ has a unique expression into factors, which are either of prime norm or are themselves rational primes such that $(\Delta \mid p) = -1$.

McGill University