ARKIV FÖR MATEMATIK Band 4 nr 37

Read 8 November 1961

On the number of representations of an A-number in an algebraic field

By Trygve Nagell

§ 1. Introduction

1. Let α be an integer $\neq 0$ in the algebraic field $\mathbf{\Omega}$. If α is representable as the sum of two integral squares in $\mathbf{\Omega}$, we say, for the sake of brevity, that α is an *A-number in* $\mathbf{\Omega}$. We say that

$$\alpha = \xi^2 + \eta^2,$$

where ξ and η are integers in $\mathbf{\Omega}$, is a *primitive representation* if the ideal (ξ, η) is the unit ideal, and otherwise an *imprimitive representation*. In the following we shall use the terms *A-prime* and *A-unit*. The representations $\alpha = x^2 + y^2$ with $x = \pm\xi$, $y = \pm\eta$ and $x = \pm\eta$, $y = \pm\xi$ are considered to be one and the same. When the degree of $\mathbf{\Omega}$ is $\geqslant 2$ the integer π is said to be a prime when (π) is a prime ideal. The relation $1 = 1^2 + 0^2$ is called the trivial representation of the number 1.

Design by $\mathbf{G}$ an infinite (abelian) group of units belonging to $\mathbf{\Omega}$ (composition = multiplication). By the *rank* of $\mathbf{G}$ we understand the maximal number of independent units (of infinite order) in $\mathbf{G}$. The rank of the group consisting of all the units in $\mathbf{\Omega}$ is $r = r_1 + r_2 - 1$, where r_1 is the number of real conjugated fields and $2r_2$ the number of imaginary conjugated fields.

Design by $\mathbf{R}$ a ring of integers contained in $\mathbf{\Omega}$ but not in any sub-field of $\mathbf{\Omega}$. If $\mathbf{R}$ contains the number 1, it contains an infinity of units and it is well-known that the unit-group of $\mathbf{R}$ has the rank r.

§ 2. The representations of A-units and A-primes

2. We first prove

Theorem 1. *When there are more representations of the number 1 than the trivial one, then there are infinitely many representations.*

Proof. Suppose that

$$1 = \xi^2 + \eta^2,$$

where ξ and η are integers in $\mathbf{\Omega}$ and $\xi\eta \neq 0$. Put for $n = 1, 2, 3, \ldots$,

$$\xi_n + \eta_n i = (\xi + \eta i)^n,$$

where

$$\xi_n = \xi^n - \binom{n}{2} \xi^{n-2} \eta^2 + \binom{n}{4} \xi^{n-4} \eta^4 - + \dots \tag{1}$$

and

$$\eta_n = \binom{n}{1} \xi^{n-1} \eta - \binom{n}{3} \xi^{n-3} \eta^3 + - \dots . \tag{2}$$

Then we clearly have

$$\xi_n - \eta_n i = (\xi - \eta i)^n$$

and

$$(\xi_n + \eta_n i)(\xi_n - \eta_n i) = (\xi + \eta i)^n (\xi - \eta i)^n = (\xi^2 + \eta^2)^n.$$

Hence

$$\xi_n^2 + \eta_n^2 = 1.$$

Thus the Diophantine equation

$$x^2 + y^2 = 1 \tag{3}$$

has the integral solutions

$$x = \xi_n, \ y = \eta_n.$$

It is easy to prove that these solutions are all different.

In fact, if we have (for $n \neq m$),

$$\xi_n = \xi_m, \ \eta_n = \eta_m,$$

we get

$$(\xi + i\eta)^m = (\xi + i\eta)^n,$$

Hence $\xi + i\eta$ is a root of unity. Suppose that

$$\xi + i\eta = \varrho$$

is a primitive Nth root of unity. Since

$$\xi - i\eta = \varrho^{-1},$$

we get

$$\xi = \frac{1}{2}(\varrho + \varrho^{-1}), \quad \eta = \frac{1}{2i}(\varrho - \varrho^{-1}).$$

It is easy to show that these numbers are not integers if $N \neq 4$, $\neq 2$ and $\neq 1$.

Suppose first that N is a powder of 2 and $\geqq 8$. If $\frac{1}{2}(\varrho^2 - 1)$ were an integer, the number

$$\tfrac{1}{2}(\varrho^{\frac{N}{4}} - 1) = \tfrac{1}{2}(\pm i - 1)$$

should also be an integer. But this is not the case.

Suppose next that N is divisible by the odd prime p. If $\frac{1}{2}(\varrho^2-1)$ were an integer, the number

$$\tfrac{1}{2}(\varrho^{\frac{2N}{p}}-1)$$

should also be an integer. Hence, if x is an arbitrary primitive pth root of unity, the number $y=\frac{1}{2}(x-1)$ should be an integer. But the numbers y clearly are the roots of the irreducible algebraic equation

$$\frac{1}{2y}[(2y+1)^p-1]=2^{p-1}y^{p-1}+\dots+p(p-1)y+p=0$$

with integral coefficients. Hence they are not integers.

Since the values $N=4$, 2 or 1 imply either $\xi=0$ or $\eta=0$, theorem 1 is proved.

3. We next prove

Theorem 2. *There is exactly one representation of every A-prime, if the number 1 has only the trivial representation. Otherwise there is an infinity of representations. This result also holds for every A-unit.*

Proof. Suppose that the number 1 has only the trivial representation. Let π be an A-prime with the two representations

$$\pi=\alpha^2+\beta^2$$

and

$$\pi=\alpha_1^2+\beta_1^2,$$

where α, β, α_1 and β_1 are integers in the field. From these representations we get

$$\pi(\beta^2-\beta_1^2)=\alpha_1^2\beta^2-\alpha^2\beta_1^2.$$

Since π is a prime, either of the numbers $\alpha_1\beta+\alpha\beta_1$ and $\alpha_1\beta-\alpha\beta_1$ must be divisible by π. We may choose the sign of β_1 such that we obtain

$$\alpha_1\beta\equiv\alpha\beta_1 \pmod{\pi}.$$

Multiplying together the two representations of π, we get

$$\pi^2=(\alpha\alpha_1+\beta\beta_1)^2+(\alpha_1\beta-\alpha\beta_1)^2.$$

Since $\alpha_1\beta-\alpha\beta_1$ is divisible by π, the number $\alpha\alpha_1+\beta\beta_1$ is so. If we put

$$\alpha\alpha_1+\beta\beta_1=\pi\eta \quad \text{and} \quad \alpha_1\beta-\alpha\beta_1=\pi\eta_1,$$

where η and η_1 are integers, we get

$$1=\eta^2+\eta_1^2.$$

By hypothesis this equation is possible only for $\eta = 0$ or $\eta_1 = 0$. For $\eta = 0$ and $\eta_1 = \pm 1$ we get

$$\alpha\alpha_1 = -\beta\beta_1 \quad \text{and} \quad \alpha_1\beta - \alpha\beta_1 = \pm\pi,$$

whence by elimination of β_1,

$$\alpha_1\beta + \frac{\alpha^2\alpha_1}{\beta} = \frac{\alpha_1}{\beta}(\alpha^2+\beta^2) = \frac{\alpha_1}{\beta}\pi = \pm\pi.$$

Hence $\alpha_1 = \pm\beta$ and $\beta_1 = \pm\alpha$.

For $\eta_1 = 0$ and $\eta = \pm 1$ we get

$$\alpha_1\beta = \alpha\beta_1 \quad \text{and} \quad \alpha\alpha_1 + \beta\beta_1 = \pm\pi,$$

whence by elimination of β_1

$$\alpha\alpha_1 + \frac{\beta^2\alpha_1}{\alpha} = \frac{\alpha_1}{\alpha}(\alpha^2+\beta^2) = \frac{\alpha_1}{\alpha}\pi = \pm\pi.$$

Hence $\alpha_1 = \pm\alpha$ and $\beta_1 = \pm\beta$. Thus there is only a single representation of the prime. The proof also holds when π is a unit.

Suppose next that the equation (3) has an infinity of solutions $x = \xi_n$, $y = \eta_n$ given by (1) and (2). Let ω be an A-number with the representation

$$\omega = \alpha^2 + \beta^2,$$

α and β being integers in $\mathbf{\Omega}$. Put for $n = 1, 2, 3, \ldots$,

$$\alpha_n + \beta_n i = (\xi_n + \eta_n i)(\alpha + \beta i),$$

where

$$\alpha_n = \alpha\xi_n - \beta\eta_n \quad \text{and} \quad \beta_n = \alpha\eta_n + \beta\xi_n.$$

Then we have

$$\alpha_n - \beta_n i = (\xi_n - \eta_n i)(\alpha - \beta i)$$

and

$$(\alpha_n + \beta_n i)(\alpha_n - \beta_n i) = (\xi_n^2 + \eta_n^2)\cdot(\alpha^2+\beta^2) = \omega.$$

Hence

$$\omega = \alpha_n^2 + \beta_n^2.$$

It is easy to see that, in this way, we get an infinity of representations of ω. In fact, supposing

$$\alpha_m = \alpha_n,\ \beta_m = \beta_n,$$

we get

$$\xi_n + \eta_n i = \xi_m + \eta_m i.$$

But in the proof of theorem 1 we showed that this relation is possible only for $m = n$. Thus we have proved theorem 2. Moreover we have proved the more general result: If the number 1 has an infinity of representations, there is an infinity of representations of every A-number.

§ 3. The representations of an arbitrary A-number

4. Owing to the above proof we have already established the result expressed in the second part of

Theorem 3. *If the number 1 has only the trivial representation, the number of representations of every A-number is finite. Otherwise there is an infinity of representations.*

Proof. Suppose that the number 1 has only the trivial representation. Let ω be an A-number having an infinity of different representations

$$\omega = \alpha_n^2 + \beta_n^2, \quad (n = 1, 2, 3, \dots)$$

α_n and β_n being integers, with $\alpha_n\beta_n \neq 0$. Then we have for all indices m and n $(m \neq n)$: $\alpha_n \neq \pm\alpha_m$, $\beta_n \neq \pm\beta_m$, $\alpha_n \neq \pm\beta_m$ and $\beta_n \neq \pm\alpha_m$.

Among these representations of ω there must exist at least two different representations

$$\alpha_m^2 + \beta_m^2 \quad \text{and} \quad \alpha_n^2 + \beta_n^2, \tag{4}$$

which satisfy the congruence conditions

$$\alpha_m \equiv \alpha_n \pmod{\omega} \quad \text{and} \quad \beta_m \equiv \beta_n \pmod{\omega}. \tag{5}$$

In fact, the number of residue classes modulo ω is $|N\omega|$, and thus the remainders of the four numbers α_m, β_m, α_n and β_n may be combined in at most $|N\omega|^4$ ways. Multiplying the two representations

$$\omega = \alpha_m^2 + \beta_m^2 \quad \text{and} \quad \omega = \alpha_n^2 + \beta_n^2,$$

we get

$$\omega^2 = (\alpha_m\beta_n - \beta_m\alpha_n)^2 + \alpha_m\alpha_n + \beta_m\beta_n)^2.$$

It follows from (5) that the two numbers

$$\alpha_m\beta_n - \beta_m\alpha_n \quad \text{and} \quad \alpha_m\alpha_n + \beta_m\beta_n$$

are divisible by ω. Hence we may put

$$\alpha_m\beta_n - \beta_m\alpha_n = \omega\eta \quad \text{and} \quad \alpha_m\alpha_n + \beta_m\beta_n = \omega\eta_1, \tag{6}$$

where η and η_1 are integers. Then we get

$$1 = \eta^2 + \eta_1^2.$$

Thus by our hypothesis we must have either $\eta = 0$ or $\eta_1 = 0$. If $\eta = 0$, it follows from (6)

$$\alpha_m\beta_n = \beta_m\alpha_n \quad \text{and} \quad \alpha_m\alpha_n + \beta_m\beta_n = \pm\omega,$$

whence by elimination of β_n,

$$\alpha_m\alpha_n + \frac{\beta_m^2\alpha_n}{\alpha_m} = \frac{\alpha_n}{\alpha_m}(\alpha_m^2 + \beta_m^2) = \frac{\alpha_n}{\alpha_m}\omega = \pm\omega.$$

Hence $\alpha_n = \pm\alpha_m$ and $\beta_n = \pm\beta_m$. For $\eta_1 = \pm 1$ we get from (6):

$$\alpha_m\alpha_n = -\beta_m\beta_n \quad \text{and} \quad \alpha_m\beta_n - \beta_m\alpha_n = \pm\omega,$$

whence by elimination of β_m:

$$\alpha_m\beta_n + \frac{\alpha_n^2\alpha_m}{\beta_n} = \frac{\alpha_m}{\beta_n}(\beta_n^2 + \alpha_n^2) = \frac{\alpha_m}{\beta_n}\omega = \pm\omega.$$

Hence $\alpha_m = \pm\beta_n$ and $\beta_m = \pm\alpha_n$.

From this we conclude that the representations (4) cannot be different. Consequently, the number of representations must be finite.

§ 4. The totally real fields and the imaginary quadratic fields

5. We next prove

Theorem 4. *In the totally real field* $\boldsymbol{\Omega}$ *there is only a finite number of representations of a given A-number. There is exactly on representation of the number 1 and likewise of every A-prime and of every A-unit. A unit is an A-number only when it is a square.*

Proof. A real field is called totally real when all the conjugate fields are real. Let ξ be an A-number in $\boldsymbol{\Omega}$ with the representation

$$\xi = \alpha^2 + \beta^2,$$

where α and β are integers in $\boldsymbol{\Omega}$. Then the conjugate equations

$$\xi^{(k)} = (\alpha^{(k)})^2 + (\beta^{(k)})^2$$

also hold. Since the conjugates are all real, we get

$$|\alpha^{(k)}| \leq |\sqrt{\xi^{(k)}}|$$

for every value of k. Hence there is only a finite number of possibilities for α when ξ is given.

Consider in particular the case $\xi = 1$. If we suppose $\beta = 0$, we get $|\alpha^{(k)}| < 1$, hence $\alpha = 0$.

When ξ is a prime or a unit, we may apply theorem 2.

Finally, suppose that ε is a unit with the representation

$$\varepsilon = \alpha^2 + \beta^2,$$

α and β being integers in $\boldsymbol{\Omega}$. Then we get by squaring

$$\varepsilon^2 = (\alpha^2 - \beta^2)^2 + (2\alpha\beta)^2,$$

whence

$$1 = \left(\frac{\alpha^2 - \beta^2}{\varepsilon}\right)^2 + \left(\frac{2\alpha\beta}{\varepsilon}\right)^2.$$

Since the number 1 has only the trivial representation, this implies either $\alpha^2 - \beta^2 = 0$ or $\alpha\beta = 0$; but it is clear that $\alpha^2 - \beta^2 = 0$ is impossible when ε is a unit.

6. We add the following result:

Theorem 5. *In the field* $\mathbf{K}(\sqrt{-1})$ *there is only a finite number of representations of a given A-number. There is exactly one representation of the number 1 and likewise of every A-prime.*

Proof. By theorems 2 and 3 it is sufficient to show that the number 1 has only the trivial representation. The equation

$$1 = \alpha^2 + \beta^2,$$

where α and β are integers in $\mathbf{K}(\sqrt{-1})$ leads to either of the following systems:

$$\alpha + \beta i = 1, \ \alpha - \beta i = 1$$

or

$$\alpha + \beta i = i, \ \alpha - \beta i = -i.$$

But the first system implies that $\beta = 0$ and the second that $\alpha = 0$. This proves theorem 5.

It is easy to prove

Theorem 6. *In the imaginary quadratic field* $\mathbf{K}(\sqrt{-D})$ *there is an infinity of representations of every A-number, except when the field is* $\mathbf{K}(\sqrt{-1})$.

Proof. According to theorem 3 it suffices to show that the number 1 has a non trivial representation, In fact, since the equation

$$x^2 - Dy^2 = 1$$

has solutions in rational integers x and y, $y \neq 0$, the number 1 has the non trivial representation

$$1 = x^2 + (y\sqrt{-D})^2.$$

§ 5. The main result on the representations

7. Theorems 4, 5, and 6 are contained in the following general result:

Theorem 7. *There is an infinity of representations of every A-number in any algebraic field* $\mathbf{\Omega}$ *except in the following cases:*

1° Ω *is the Gaussian field* $K(\sqrt{-1})$.
2° Ω *is totally real.*

Proof. In virtue of theorem 3 it is sufficient to prove that there is an infinity of representations of the number 1, provided that Ω is not one of the exceptional fields in theorem 7. By theorem 1 it suffices to show that there is a non-trivial representation of the number 1.

Denote by n the degree of the field Ω; by r_1 the number of real conjugate fields $\Omega^{(h)}$, by r_2 the number of pairs of imaginary conjugate fields and by $r = r_1 + r_2 - 1$ the number of units in a fundamental system of units in the field Ω.

We first consider the case that Ω contains the number $\sqrt{-1}$. In this case we have $n \geqslant 4$. Since $r \geqslant 1$, there exists in Ω a unit E which is not a root of unity.

Then the equation

$$1 = \alpha^2 + \beta^2$$

is satisfied by the following numbers:

$$\alpha = \tfrac{1}{2}(E^m + E^{-m})$$

and

$$\beta = \frac{1}{2i}(E^m - E^{-m}),$$

where m is an arbitrary rational integer. Let us choose the number m as a multiple of $\varphi(2)$, where $\varphi(2)$ denotes the number of residue classes modulo 2 in Ω which are prime to 2. Then we have for any integer γ in Ω which is prime to 2,

$$\gamma^m \equiv 1 \pmod{2}.$$

Hence the numbers α and β are integers in Ω; for $m \neq 0$ we have $\alpha\beta \neq 0$.

Consider next the case that Ω does not contain the number $\sqrt{-1}$. Adjoining this number to Ω we get the field $\Omega(\sqrt{-1}) = \Omega_1$. This field has the degree $2n$. Denote by R_1 the number of real conjugate fields $\Omega_1^{(k)}$, by R_2 the number of pairs of imaginary conjugate fields and by $R = R_1 + R_2 - 1$ the number of units in a fundamental system of units in the field Ω_1.

If ξ is a generating number of Ω, one may find a rational u such that the $2n$ conjugate fields $\Omega_1^{(k)}$ $(k = 1, 2, 3, \ldots, 2n)$ are generated by the $2n$ numbers

$$\omega = \xi^{(h)} \pm u\sqrt{-1},$$

where $\xi^{(h)}$ runs through the system of n numbers conjugate to ξ (see f. ex. Hecke [4], p. 67). If $\xi^{(h)}$ is real, it is evident that ω is imaginary, since $u \neq 0$. If $\xi^{(h)}$ is imaginary, it is evident that ω may be real for at most two special values of u, for all other values of u the number ω is imaginary. Hence, all the $2n$ conjugate fields $\Omega_1^{(k)}$ are imaginary. Thus we have $R_1 = 0$, $R_2 = r_1 + 2r_2$ and

$$R = R_1 + R_2 - 1 = r_1 + 2r_2 - 1 = r + r_2.$$

Since Ω is not totally real, we have $r_2 \geqslant 1$ and thus

$$R > r.$$

R is the rank of the group of all the units in Ω_1, and r is the rank of the group of all the units Ω. Let us consider the ring consisting of the numbers in Ω_1 having the form $c + di$, where c and d are *integers* in Ω. The unit-group $\mathfrak{G}$ of this ring has the rank R. The sub-group $\mathfrak{G}_1$ consisting of the squares of the units in $\mathfrak{G}$ clearly has the same rank R. The units in $\mathfrak{G}_1$ cannot all be equal to the product of a unit in Ω and a root of unity since $r < R$. Hence we conclude that there exists a unit $E = a + bi$ in the ring, a and b integers in Ω, such that $ab \neq 0$, and such that E^2 is not equal to the product of a unit in Ω and a root of unity. Then the number $E_1 = a - bi$ is also a unit in Ω_1. Hence $a^2 + b^2$ is a unit in Ω. Then the equation

$$1 = \alpha^2 + \beta^2$$

is satisfied by the following numbers:

$$\alpha = \frac{E^{2m} + E_1^{2m}}{2\,(a^2 + b^2)^m}$$

and

$$\beta = \frac{E^{2m} - E_1^{2m}}{2i\,(a^2 + b^2)^m},$$

where m is a natural number. It is evident that α and β are integers in Ω, since a and b are so. The hypothesis $\alpha\beta = 0$ leads to

$$E^{4m} = E_1^{4m}.$$

Hence EE_1^{-1} should be a root of unity $= E_2$, and we should have

$$E^2 = (a^2 + b^2)\,E_2.$$

But this is contrary to our assumption on E. Thus, for $m \neq 0$, we have $\alpha\beta \neq 0$, and the proof of theorem 7 is complete.

Remarks on previous papers on A-numbers.

In two previous papers, [1] and [2], we have already established a number of theorems on A-numbers. The proof of theorem 21 in paper [1] was not complete as we did not show that m may be chosen such that $\alpha\beta \neq 0$. This lacuna was repaired in the above proof of theorem 7. Theorems 2 and 3 in this paper correspond to theorems 16 and 17 in paper [1] with a certain correction in the proof.

In theorem 2 in [1] it is necessary to add the following condition: The ideal (α, β) is either the unit ideal or the power of a prime ideal $\mathfrak{p}$ which does not divide 2. Thus the theorem ought to be pronounced as follows:

Let α and β be A-numbers in the field Ω with the primitive representations in Ω

$$\alpha = a^2 + b^2$$

and

$$\beta = c^2 + d^2.$$

If $(\alpha, \beta) = \mathfrak{p}^m$, $m \geqslant 0$, *where the prime ideal* $\mathfrak{p}$ *is prime to* (2), *then the product* $\alpha\beta$ *has a primitive representation of the form*

$$\alpha\beta = (ac \pm bd)^2 + (ad \mp bc)^2,$$

either for the upper or for the lower sign.

This restriction in the theorem does not make necessary any alterations in the proofs of theorems 29–31 in [1].

The following misprints in paper [1] ought to be noticed: Page 24, in line 14 replace ε by π_1 in the right-hand side of the equation. Page 33, in line 7 the first equation shall be $\left(\frac{-1}{p}\right) = +1$. Page 41, in line 11 from below add, after the word even, $\geqslant 2$. Page 46, in the last line replace db_1 by cb_1. Page 50, in line 5 from below replace ξ by β. Page 58, in line 11 from below add, after E, the square of which. Page 68, in line 9 the first factor shall be $(\sqrt{2}+1)$.

The last 11 lines on page 34 in [1] ought to be replaced by: This congruence is possible only when one of the numbers b and c is divisible by 4 and the other one is $\equiv 2 \pmod 4$. Since $2v = ac + bd$, where v is even, we get $ac \equiv -bd \pmod 4$. Thus, a and d being odd, both b and c should be divisible by 4. Since this is impossible we conclude that the numbers a, b, c and d are all even.

In paper [2] on pape 279, line 12, read q instead of 5.

§ 6. The complete solution of $\xi^2 + \eta^2 = 1$ in a quadratic field

8. According to theorems 4 and 5 it suffices to consider the imaginary quadratic fields $\mathbf{K}(\sqrt{-D})$, where D is a square-free natural number > 1.

First case. $-D \equiv 2$ or $\equiv 3 \pmod 4$.

The equation in question is

$$(a + c\sqrt{-D})^2 + (b + d\sqrt{-D})^2 = 1, \tag{7}$$

where a, b, c and d are rational integers. Hence we get the system

$$a^2 + b^2 - D(c^2 + d^2) = 1, \; ac = -bd.$$

If $c = 0$ we must have $b = 0$ ($d = 0$ gives the trivial solution). Hence

$$a^2 - Dd^2 = 1. \tag{8}$$

Suppose next $cd \neq 0$. By elimination of a we obtain

$$1 = b^2d^2c^{-2} + b^2 - D(c^2 + d^2).$$

Then we get

$$c^2 = (c^2 + d^2)(b^2 - Dc^2),$$

which is impossible since $d \neq 0$.

Conclusion: We obtain all the solutions of (7) when $b = c = 0$ and a and d satisfy equation (8).

Second case. $-D \equiv 1 \pmod 4$.

Then the equation is

$$(a + c\sqrt{-D})^2 + (b + d\sqrt{-D})^2 = 4, \tag{9}$$

where a, b, c and d are rational integers. a and c are of the same parity, and so are b and d. Hence we get the system

$$a^2 + b^2 - D(c^2 + d^2) = 4, \; ac = -bd.$$

If $c = 0$ we must have $b = 0$. Thus we get

$$a^2 - Dd^2 = 4. \tag{10}$$

Suppose next $cd \neq 0$. By elimination of a we obtain

$$4c^2 = (c^2 + d^2)(b^2 - Dc^2). \tag{11}$$

Put $(c, d) = g$, $c = gc_1$, $d = gd_1$ and $(c_1, d_1) = 1$, where g, c_1 and d_1 are rational integers. Then we get from (11)

$$4c_1^2 = (c_1^2 + d_1^2)(b^2 - Dg^2c_1^2).$$

Hence b is divisible by c_1. Putting $b = c_1 f$ we get

$$4 = (c_1^2 + d_1^2)(f^2 - Dg^2).$$

This is possible only for $c_1^2 = d_1^2 = 1$. Hence

$$f^2 - Dg^2 = 2. \tag{12}$$

In this relation f and g are clearly odd numbers. Hence we must have $D \equiv -1 \pmod 8$.

Conclusion: We obtain all the solutions of (9) from the formula

$$a^2 + (d\sqrt{-D})^2 = 4,$$

and, if equation (12) is solvable, from the formula

$$(f + g\sqrt{-D})^2 + (f - g\sqrt{-D})^2 = 4.$$

Equation (12) is not always solvable for $D \equiv -1 \pmod 8$. Thus it is solvable for $D = 7$ but not for $D = 15$.

Our results in this section may be interpreted in the Dirichlet-field $\mathbf{K}(i, \sqrt{-D})$ in the following manner. Design by ε the fundamental unit in $\mathbf{K}(\sqrt{D})$, $\varepsilon > 1$, and by E the fundamental unit in $\mathbf{K}(i, \sqrt{-D})$, $|E| > 1$ and $E > 1$, if E is real. Then we have, for $D > 3$, either $E = \varepsilon$ or $E = \sqrt{\varepsilon i}$. The necessary and sufficient condition for the latter case is that the ideal (2) is the square of a *principal* ideal in $\mathbf{K}(\sqrt{D})$. For the proof see [3], p. 11–15. Hence we may conclude: The solutions of $\xi^2 + \eta^2 = 1$ are given by $\pm \varepsilon^M$ or by $\pm \varepsilon^{2M}$ according as $N(\varepsilon)$ is $= +1$ or $= -1$. In this way we get all the solutions except when $D \equiv -1 \pmod 8$ and the ideal (2) is the square of a principal ideal in $\mathbf{K}(\sqrt{D})$ in which case we have the further solutions $\pm E\varepsilon^M$. The exponent M is an arbitrary rational integer.

REFERENCES

1. NAGELL, T., On the representations of integers as the sum of two integral squares in algebraic, mainly quadratic fields. Nova Acta Soc. Sci. upsal., Ser. IV, Vol. *15*, No. 11. Uppsala 1953.
2. NAGELL, T., On the sum of two integral squares in certain quadratic fields. Arkiv för matem., Bd. *4*, nr. 20. Uppsala 1961.
3. NAGELL, T., Sur quelques questions dans la théorie des corps biquadratiques. Arkiv för matem., Bd. *4*, nr 26. Uppsala 1961.
4. HECKE, E., Theorie der algebraischen Zahlen, Leipzig 1923.

Tryckt den 29 januari 1962

Uppsala 1962. Almqvist & Wiksells Boktryckeri AB