Read 12 October 1960

# On the sum of two integral squares in certain quadratic fields

By Trygve Nagell

## § 1. Introduction

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

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

where $\xi$ and $\eta$ are integers in $\mathbf{\Omega}$, is a *primitive representation* if the ideal $(\xi, \eta)$ is the unit ideal, and otherwise an *imprimitive representation.*

In a previous paper [1] I have determined the A-numbers in the quadratic fields $\mathbf{K}(\sqrt{D})$, where $D = -1, \pm 2, \pm 3, \pm 7, \pm 11, \pm 19, \pm 43, \pm 67$ and $\pm 163$. In the present paper we shall continue the investigations and treat the cases $D = \pm 5$ and $D = \pm 13$. The following developments are in general based on the results obtained in [1].

It is well known that the number of ideal classes is $=1$ in the fields $\mathbf{K}(\sqrt{5})$, $\mathbf{K}(\sqrt{13})$ and $\mathbf{K}(\sqrt{37})$ and $=2$ in the fields $\mathbf{K}(\sqrt{-5})$, $\mathbf{K}(\sqrt{-13})$ and $\mathbf{K}(\sqrt{-37})$; see [2].

From a general theorem due to Dirichlet [3] we get

**Lemma 1.** *The number of ideal classes in the Dirichlet field* $\mathbf{K}(\sqrt{D}, \sqrt{-D})$ *of the fourth degree is* $=1$, *when* $D = 5$, 13 *and* 37.

**2.** We also need the following lemmata:

**Lemma 2.** *Let $D$ be a square-free rational integer which is $\equiv 2$ or $\equiv 3$ (mod 4). If $x$ and $y$ are rational integers, and if $x + y\sqrt{D}$ is an A-number in the field $\mathbf{K}(\sqrt{D})$, then $y$ is even.*

**Lemma 3.** *If $\alpha$ is an integer in the Dirichlet field $\mathbf{K}(\sqrt{D}, \sqrt{-D})$ with square-free $D$, the number $2\alpha$ belongs to the ring $\mathbf{R}(1, \sqrt{-1}, \sqrt{D}, \sqrt{-D})$.*

For the proofs see [1], p. 8–9. In [1] we also established the following results:

**Lemma 4.** *Let $\alpha$ and $\pi$ be A-numbers in the field $\mathbf{\Omega}$. If $(\pi)$ is a prime ideal divisor of $(\alpha)$. the quotient $\alpha/\pi$ is also an A-number in $\mathbf{\Omega}$. This result also holds if $\pi$ is a unit* (Theorem 4 in [1]).

**Lemma 5.** *Let $\alpha$, $\pi$, $\pi_1$ and $\eta$ be integers $\neq 0$ in the field $\mathbf{\Omega}$ with the following properties. The number $\alpha/(\pi\pi_1)$ is an integer; the principal ideals $(\pi)$ and $(\pi_1)$ are prime ideal divisors of $(\alpha)$; $\pi$ and $\eta$ are relatively prime. The integers $\alpha$, $\pi\pi_1$, $\pi\eta$ and $\pi_1\eta$ are A-numbers in $\mathbf{\Omega}$, such that*

$$\pi\eta = f^2 + g^2,$$

$$\pi_1\eta = f_1^2 + g_1^2,$$

*and*

$$\pi\pi_1 = \left(\frac{ff_1 + gg_1}{\eta}\right)^2 + \left(\frac{fg_1 - gf_1}{\eta}\right)^2,$$

*where $f$, $g$, $f_1$, $g_1$, $(ff_1+gg_1)/\eta$ and $(fg_1-gf_1)/\eta$ are integers in $\mathbf{\Omega}$. Then the quotient $\alpha/(\pi\pi_1)$ is also an A-number in $\mathbf{\Omega}$.*

*This result also holds when one of the numbers $\pi$ and $\pi_1$ is a unit or when both of them are units* (Theorem 5 in [1]).

## § 2. The imaginary field $K(\sqrt{-q})$ where $q$ is either $=5$ or $=13$

**3.** *Units and divisors of the rational primes* 2 *and* $q$. The number $-1$ is an A-number in these fields since

$$-1 = 2^2 + (\sqrt{-5})^2$$

and

$$-1 = 18^2 + (5\sqrt{-13})^2.$$

Thus the numbers $\alpha$ and $-\alpha$ are simultaneously A-numbers or not.

It follows from Lemma 2 that the prime $\sqrt{-q}$ is not an A-number. Clearly, no irrational power of $\sqrt{-q}$ can be an A-number. The number $-1$ is a quadratic residue modulo $\sqrt{-q}$. The number $u+v\sqrt{-q}$, where $u$ and $v$ are rational integers, is never an A-number when $v$ is odd.

In virtue of the relations

$$2\sqrt{-5} = 2^2 + (1+\sqrt{-5})^2$$

and

$$2\sqrt{-13} = (4 + 2\sqrt{-13})^2 + (7-\sqrt{-13})^2$$

we may state: *the number $2\sqrt{-q}$ is always an A-number.* We have

$$(2) = \mathfrak{q}^2 = (1^2 + 1^2),$$

where the prime ideal $\mathfrak{q}$ is not principal. The number $-1$ is a quadratic residue modulo $\mathfrak{q}$.

**4.** *The rational primes for which $-q$ is a quadratic non-residue.* Let $p$ be an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = +1 \text{ and } \left(\frac{-q}{p}\right) = -1.$$

Then $(p)$ is a prime ideal in the field and since

$$p = u^2 + v^2,$$

where $u$ and $v$ are rational integers, $p$ is an A-prime.

Suppose next that $p$ is an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = -1 \text{ and } \left(\frac{-q}{p}\right) = -1.$$

Then $(p)$ is a prime ideal in $\mathbf{K}(\sqrt{-q})$. Since $\left(\frac{q}{p}\right) = +1$, and since the field $\mathbf{K}(\sqrt{q})$ is simple, the equation

$$4p = x^2 - qy^2$$

is solvable in rational integers $x$ and $y$. If $x$ and $y$ are both even, we get

$$p = x_1^2 + (\sqrt{-q}\, y_1)^2,$$

where $x_1 = \frac{1}{2}x$ and $y_1 = \frac{1}{2}y_1$. Hence $p$ is an A-prime.

If $x$ and $y$ are both odd, we get, in the case $q = 5$,

$$\tfrac{1}{2}(x + \sqrt{5}\, y) \cdot \tfrac{1}{2}(\sqrt{5} \pm 1) = \tfrac{1}{4}(5y \pm x) + \tfrac{1}{4}\sqrt{5}\,(x \pm y).$$

Here it is possible to choose the sign such that the numbers

$$u = \tfrac{1}{4}(5y \pm x) \text{ and } v = \tfrac{1}{4}(y \pm y)$$

are both integers.

In the case $q = 13$ we get, if $x$ and $y$ are both odd,

$$\tfrac{1}{2}(x + \sqrt{13}\, y) \cdot \tfrac{1}{2}(\sqrt{13} \pm 3) = \tfrac{1}{4}(13y \pm 3x) + \tfrac{1}{4}\sqrt{13}\,(x \pm 3y).$$

Just as in the proceeding case, we may choose the sign such that the numbers

$$u = \tfrac{1}{4}(13y \pm 3x) \text{ and } v = \tfrac{1}{4}(x \pm 3y)$$

are both integers. Thus we have in both cases

$$-p = u^2 + (v\sqrt{-q})^2.$$

Hence $p$ is an A-prime. Thus the number $-1$ is a quadratic residue modulo $p$ in the field $\mathbf{K}(\sqrt{-q})$.

**5.** *The rational primes $p \equiv -1$ (mod 4) for which $-q$ is a quadratic residue.* Let $p$ be an odd prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = -1 \text{ and } \left(\frac{-q}{p}\right) = +1.$$

Then we have
$$(p) = \mathfrak{p}\,\mathfrak{p}',$$

where $\mathfrak{p}$ and $\mathfrak{p}'$ are different prime ideals in the field $\mathbf{K}(\sqrt{-q})$. In this field we further have

$$\left(\frac{-1}{\mathfrak{p}}\right) = (-1)^{\frac{1}{2}(N\mathfrak{p}-1)} = -1. \tag{1}$$

*The ideal $\mathfrak{p}$ can never be principal.* In fact, if we had $\mathfrak{p} = (x + y\sqrt{-q})$, with rational integers $x$ and $y$, we should have

$$p = x^2 + q y^2.$$

But this equation clearly implies $p \equiv +1$ (mod 4).

**Lemma 6.** *Let $\alpha$ and $\beta$ be integers in $\mathbf{K}(\sqrt{-q})$, not both equal to zero. Further, let $\mathfrak{p}$ be a prime ideal in the field satisfying relation* (1). *If the sum $\alpha^2 + \beta^2$ is divisible by the power $\mathfrak{p}^m$, we must have*

$$\alpha \equiv \beta \equiv 0 \pmod{\mathfrak{p}^\nu},$$

*where $\nu = [\frac{1}{2}(m+1)]$.*

*Proof.* We prove it by induction. In virtue of (1) the lemma is true for $m = 1$. Hence we may suppose $m \geqslant 2$. Suppose it is true for all exponents $\leqslant m$. Let $\xi$ and $\eta$ be integers in the field such that $\xi^2 + \eta^2$ is divisible by $\mathfrak{p}^{m+1}$. In virtue of (1) the numbers $\xi$ and $\eta$ are divisible by $\mathfrak{p}$. When $\mathfrak{q}$ is the prime ideal which divides 2, we put

$$\mathfrak{q}(\xi) = \mathfrak{p}(\alpha) \text{ and } \mathfrak{q}(\eta) = \mathfrak{p}(\beta),$$

where $\alpha$ and $\beta$ are integers in the field. Then we get

$$\mathfrak{q}^2(\xi^2 + \eta^2) = 2(\xi^2 + \eta^2) = \mathfrak{p}^2(\alpha^2 + \beta^2).$$

Hence $\alpha^2 + \beta^2$ is divisible by $\mathfrak{p}^{m-1}$, and, by hypothesis, we have

$$\alpha \equiv \beta \equiv 0 \pmod{\mathfrak{p}^\lambda},$$

where $\lambda = [\frac{1}{2}m]$. From this relation follows

$$\xi \equiv \eta \equiv 0 \pmod{\mathfrak{p}^{\lambda+1}}.$$

This proves the lemma.

**Lemma 7.** *Let* $\mathfrak{p}$ *be a prime ideal satisfying relation* (1). *Then* $\mathfrak{p}^2$ *is a principal ideal* $=(u+v\sqrt{-q})$, $u$ *and* $v$ *rational integers, where* $u$ *is even and* $v$ *odd.*

*Proof.* Suppose that $N\mathfrak{p}=p$. Then we have

$$p^2=u^2+qv^2.$$

If $v$ were even, we should have

$$p\pm u=2u_1^2, \quad p\mp u=2qv_1^2,$$

where $u_1$ and $v_1$ are rational integers. Hence

$$p=u_1^2+qv_1^2,$$

which is impossible, since $p\equiv -1 \pmod 4$. Thus $u$ is even and $v$ odd.

**Lemma 8.** *Let* $\mathfrak{p}$ *and* $\mathfrak{p}_1$ *be different prime ideals such that*

$$\left(\frac{-1}{\mathfrak{p}}\right)=\left(\frac{-1}{\mathfrak{p}_1}\right)=-1.$$

*Then* $\mathfrak{p}\mathfrak{p}_1$ *is a principal ideal* $=(\alpha)$, *where the integer* $\alpha$ *is not an A-number. The square* $\mathfrak{p}^2\mathfrak{p}_1^2$ *is a principal ideal* $=(\omega)$, *where the integer* $\omega$ *is an A-number.*

*Proof.* If we had $\alpha=\xi^2+\eta^2$, according to Lemma 6, the integers $\xi$ and $\eta$ should be divisible by $\mathfrak{p}$, which is impossible since $\mathfrak{p}\neq\mathfrak{p}_1$. Putting $\alpha=u+v\sqrt{-q}$, $u$ and $v$ rational integers, we get

$$(\mathfrak{p}\mathfrak{p}_1)^2=(\omega)=(u+v\sqrt{-q})^2+0^2.$$

This proves the lemma.

As a consequence of Lemmata 7–8 we may state: Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m$ be $m$ prime ideals (different or not) such that $\left(\frac{-1}{\mathfrak{p}_i}\right)=-1$, and put

$$(\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m)^2=(\omega),$$

where $\omega$ is an integer. Then $\omega$ is an A-number if and only if $m$ is even.

**Lemma 9.** *Let* $\mathfrak{p}$ *be a prime ideal satisfying* (1) *and let* $\mathfrak{p}^2=(\omega)$, *then* $2\omega$ *is an A-number.*

*Proof.* If $(2)=\mathfrak{q}^2$ we have $\mathfrak{q}\mathfrak{p}=(u+v\sqrt{-q})$, where $u$ and $v$ are *odd* rational integers. Hence

$$2\omega=(u+v\sqrt{-q})^2+0^2.$$

**Lemma 10.** *Let* $\mathfrak{p}$ *be a prime ideal satisfying* (1) *and let* $\mathfrak{p}^2=(\omega)$, *then* $\sqrt{-q}\,\omega$ *is an A-number.*

*Proof.* From the preceding proof we get

$$\sqrt{-q}\,\omega = \tfrac{1}{2}\sqrt{-q}\,(u + v\sqrt{-q})^2,$$

where $u$ and $v$ are odd rational integers. For $q=5$ we obtain

$$\begin{aligned}\sqrt{-5}\,\omega &= \tfrac{1}{4}[u + v\sqrt{-5}]^2 \cdot [2^2 + (1+\sqrt{-5})^2] \\ &= [u + v\sqrt{-5}]^2 + [\tfrac{1}{2}(u-5v) + \tfrac{1}{2}(u+v)\sqrt{-5}]^2.\end{aligned}$$

For $q=13$ we have

$$\begin{aligned}\sqrt{-13}\,\omega &= \tfrac{1}{4}[u + v\sqrt{-13}]^2 \cdot [(4+2\sqrt{-13})^2 + (7-\sqrt{-13})^2] \\ &= [2u - 13v + (u+2v)\sqrt{-13}]^2 + [\tfrac{1}{2}(7u+13v) + \tfrac{1}{2}(7v-u)\sqrt{-13}]^2.\end{aligned}$$

Since the numbers $\frac{1}{2}(u-5v)$, $\frac{1}{2}(u+v)$, $\frac{1}{2}(7u+13v)$ and $\frac{1}{2}(7v-u)$ are integers, the lemma is proved.

**6.** *The rational primes* $p \equiv +1 \pmod 4$ *for which* $-q$ *is a quadratic residue.* Consider finally the cases

$$\left(\frac{-1}{p}\right) = +1 \text{ and } \left(\frac{-q}{p}\right) = +1,$$

where $p$ is an odd rational prime. Here we have

$$(p) = \mathfrak{p}\,\mathfrak{p}',$$

where $\mathfrak{p}$ and $\mathfrak{p}'$ are different prime ideals in the field. We shall show that these ideals are always principal.

In fact, suppose that $\mathfrak{p}$ were not principal. We have $(2) = \mathfrak{q}^2$, where $\mathfrak{q}$ is not principal. Then the product $\mathfrak{q}\,\mathfrak{p}$ is principal, since the number of ideal classes is $=2$. Hence the equation

$$N(\mathfrak{q}\,\mathfrak{p}) = 2p = a^2 + qb^2$$

would be solvable in rational odd integers $a$ and $b$. But this is impossible since $a^2 + qb^2 \equiv 1 + q \equiv 6 \pmod 8$ and $2p \equiv 2 \pmod 8$. Hence $\mathfrak{p}$ is a principal ideal, and we have

$$p = u^2 + qv^2,$$

where $u$ and $v$ are rational integers. Then the numbers

$$\omega = u + v\sqrt{-q} \text{ and } \omega' = u - v\sqrt{-q}$$

are conjugate prime factors of $p$ in $\mathbf{K}(\sqrt{-q})$. Since by Lemma **1** the field

$\mathbf{K}(\sqrt{-q}, \sqrt{q})$ is simple, we have

$$\omega = \pi_1 \pi_2,$$

where $\pi_1$ and $\pi_2$ are primes in that field. According to Lemma 3 we may suppose that

$$\pi_1 = \tfrac{1}{2}(a + c\sqrt{-q}) + i\tfrac{1}{2}(b + d\sqrt{-q})$$

and

$$\pi_2 = \tfrac{1}{2}(a + c\sqrt{-q}) - i\tfrac{1}{2}(b + d\sqrt{-q}),$$

where $a$, $b$, $c$ and $d$ are rational integers. Hence

$$\omega = \tfrac{1}{4}(a + c\sqrt{-q})^2 + \tfrac{1}{4}(b + d\sqrt{-q})^2, \tag{2}$$

which involves the equations

$$4u = a^2 + b^2 - qc^2 - qd^2 \tag{3}$$

and

$$2v = ac + bd.$$

It follows from the latter of these relations that, if $a$ is even, either $b$ or $d$ must be even. Suppose that $a$ and $b$ are even and $c$ and $d$ odd. Then we obtain from (3) modulo 4:

$$0 \equiv -q - q \equiv 2 \pmod 4,$$

which is impossible. Supposing that $a$ and $b$ are odd and $c$ and $d$ even, we get from (3):

$$0 \equiv 1 + 1 \pmod 4,$$

which is also impossible. Hence, the remaining possibilities are: (i) all the numbers $a$, $b$, $c$ and $d$ are even; (ii) all the numbers $a$, $b$, $c$ and $d$ are odd; (iii) $a$ and $d$ are even and $b$ and $c$ are odd. It is, of course, unnecessary to treat the case with $b$ and $c$ even and $a$ and $d$ odd.

If all the numbers $a$, $b$, $c$ and $d$ are even, $\omega$ is clearly an A-number since the numbers

$$\tfrac{1}{2}(a + c\sqrt{-q}) \text{ and } \tfrac{1}{2}(b + d\sqrt{-q})$$

are integers. If the numbers $a$, $b$, $c$ and $d$ are all odd, we get from (3)

$$4u \equiv 1 + 1 - q - q \equiv 0 \pmod 8.$$

Hence $u$ is even. But according to Lemma 2, $u$ is odd when $\omega$ is an A-number.

Suppose finally that $a$ and $d$ are even and $b$ and $c$ are odd. Then we get from (3)

$$4\,u \equiv a^2 + 1 - q - q\,d^2 \pmod 8,$$

whence
$$4\,(u+1) \equiv a^2 + d^2 \pmod 8. \tag{4}$$

When $u$ is even, it follows from this relation that one of the numbers $a/2$ and $d/2$ is even and the other one odd. In this case $\omega$ is not an A-number.

When $u$ is odd, it follows from (4) that the numbers $a/2$ and $d/2$ are either both odd or both even. We shall show that, in this case, $\omega$ is an A-number. If $q=5$ we multiply the integer

$$\pi_1 = \tfrac{1}{2}\left(a + c\sqrt{-5}\right) + i\,\tfrac{1}{2}\left(b + d\sqrt{-5}\right)$$

by the unit $E = \frac{1}{2}(\sqrt{5} \pm 1)$. The product is equal to

$$\tfrac{1}{4}\,(a \mp d)\sqrt{5} + \tfrac{1}{4}\,(5\,c \pm b)\,i + \tfrac{1}{4}\,(b \pm c)\sqrt{5} + \tfrac{1}{4}\,(\pm a - 5\,d).$$

Here the numbers

$$\tfrac{1}{4}\,(a \mp d) \text{ and } \tfrac{1}{4}\,(\pm a - 5\,d)$$

are always integers since $a/2$ and $d/2$ are of the same parity. Further, by an appropriate choice of the sign in the unit $E$, we may obtain that the number $b \pm c$ be divisible by 4. Then the number $5\,c \pm b$ is also divisible by 4. Hence the product $\pi_1 E$ belongs to the ring $\mathbf{R}\left(1, i, \sqrt{5}, \sqrt{-5}\right)$, and thus it is permitted to suppose that, in $\pi_1$, the numbers $a$, $b$, $c$ and $d$ are all even. Then we have

$$\omega = \left(a_1 + c_1\sqrt{-5}\right)^2 + \left(b_1 + d_1\sqrt{-5}\right)^2,$$

where $a_1$, $b_1$, $c_1$ and $d_1$ are rational integers. Hence $\omega$ and $\omega'$ are A-numbers.

Consider next the case $q=13$. Multiplying the integer

$$\pi_1 = \tfrac{1}{2}\left(a + c\sqrt{-13}\right) + i\,\tfrac{1}{2}\left(b + d\sqrt{-13}\right)$$

by the unit $E = \frac{1}{2}(\sqrt{13} \pm 3)$ we get the product

$$\tfrac{1}{4}(a \mp 3\,d)\sqrt{13} + \tfrac{1}{4}\,(\pm 3\,b + 13\,c)\,i + \tfrac{1}{4}\,(\pm 3\,c + b)\sqrt{-13} + \tfrac{1}{4}\,(\pm 3\,a - 13\,d).$$

Here the numbers

$$\tfrac{1}{4}\,(a \mp 3\,d) \text{ and } \tfrac{1}{4}\,(\pm 3\,a - 13\,d)$$

are always integers since $a/2$ and $d/2$ are of the same parity. Further, by an appropriate choice of the sign in the unit $E$, we may obtain that the number $\pm 3\,c + b$ be divisible by 4. Then the number $\pm 3\,b + 13\,c$ is also divisible by 4. Hence the product $\pi_1 E$ belongs to the ring $\mathbf{R}\left(1, i, \sqrt{13}, \sqrt{-13}\right)$, and thus it is permitted to suppose that, in $\pi_1$, the numbers $a$, $b$, $c$ and $d$ are all even. Then we have

$$\omega = (a_1 + c_1 \sqrt{-13})^2 + (b_1 + d_1 \sqrt{-13})^2,$$

where $a_1$, $b_1$, $c_1$ and $d_1$ are rational integers. Hence $\omega$ and $\omega'$ are A-numbers.

7. *Definition of C-primes. Further lemmata.* Let $\omega$ be a prime in $\mathbf{K}(\sqrt{-q})$ of the form $\omega = u + v\sqrt{-q}$ where $u$ and $v$ are rational integers. According to the preceding section, $\omega$ is an A-number in the field, if $u$ is odd and $v$ even. If $u$ is even and $v$ odd, $\omega$ is never an A-number and in this case we call $\omega$ a *C-prime*.

If $\omega$ is a $C$-prime is follows from relation (2) in Section 6 that $4\omega$ is an A-number. But we can furthermore prove the following lemma.

**Lemma 11.** *If $\omega$ is a C-prime, the number $2\omega$ is an A-number.*

*Proof.* We put $\omega = u + v\sqrt{-q}$, where $u$ and $v$ are rational integers; $u$ is even and $v$ odd. Then we have

$$\omega = \tfrac{1}{4}\alpha^2 + \tfrac{1}{4}\beta^2,$$

where $\alpha$ and $\beta$ are integers in $\mathbf{K}(\sqrt{-q})$. Multiplying by 2 we get

$$2\omega = \left(\frac{a + c\sqrt{-q}}{2}\right)^2 + \left(\frac{b + d\sqrt{-q}}{2}\right)^2,$$

where $a$, $b$, $c$ and $d$ are rational integers. Hence

$$8u = a^2 + b^2 - qc^2 - qd^2, \tag{5}$$

$$4v = ac + bd. \tag{6}$$

If $a$, $b$, $c$ and $d$ are all even, the number $2\omega$ is an A-number. Suppose next that $a$ and $b$ are even and $c$ and $d$ odd. Then we get from (5) $a^2 + b^2 \equiv 2 \pmod 8$ which is impossible. Consider next the case when $a$ and $d$ are even and $b$ and $c$ odd. Then it follows from (5)

$$(a/2)^2 - 5(d/2)^2 \equiv 1 \pmod 2.$$

Hence one of the numbers $a/2$ and $d/2$ is odd and the other one is even. But this is impossible because of the relation (6).

Finally we consider the remaining case when $a$, $b$, $c$ and $d$ are all odd. When $q = 5$ we multiply $2\omega$ by the number $-1 = \frac{1}{4}(1^2 + (\sqrt{-5}))^2$. The product $-2\omega$ is equal to (in virtue of Lemma 1 in [1])

$$\tfrac{1}{16}[a + c\sqrt{-5} \pm (b\sqrt{-5} - 5d)]^2 + \tfrac{1}{16}[a\sqrt{-5} - 5c \mp (b + d\sqrt{-5})]^2$$
$$= \tfrac{1}{16}[(a \mp 5d) + (c \pm b)\sqrt{-5}]^2 + \tfrac{1}{16}[(-5c \mp b) + (a \mp d)\sqrt{-5}]^2.$$

By choosing the sign in an appropriate way the number $\frac{1}{4}(a \mp d)$ will be an integer and so will $\frac{1}{4}(a \mp 5d)$. Then it follows from relation (6) that

$$ac + bd \equiv ac \pm ab \equiv 0 \pmod 4.$$

Hence
$$c \pm b \equiv 0 \pmod 4,$$

and thus the numbers
$$\tfrac{1}{4}(c \pm b) \text{ and } \tfrac{1}{4}(-5c \mp b)$$

are both integers. Consequently $-2\omega$ is an A-number. This proves Lemma 11 when $q = 5$.

When $q = 13$, we multiply $2\omega$ by the number $-1 = \frac{1}{4}(3^2 + (\sqrt{-13})^2)$. The product will be

$$\tfrac{1}{16}[(3a \mp 13d) + (3c \pm b)\sqrt{-13}]^2 + \tfrac{1}{16}[(-13c \mp 3b) + (a \mp 3d)\sqrt{-13}]^2.$$

Here we may choose the sign in a way such that the numbers

$$3a \mp 13d,\ 3c \pm b,\ -13c \mp 3b,\ a \mp 3d$$

are all divisible by 4. Hence $-2\omega$ is an A-number, and the proof of Lemma 11 is complete.

We next prove

**Lemma 12.** *The product of two C-primes is an A-number.*

*Proof.* Let $\omega$ and $\omega_1$ be two $C$-primes

$$\omega = u + r\sqrt{-q}, \quad \omega_1 = u_1 + v_1\sqrt{-q},$$

where $u$, $v$, $u_1$ and $v_1$ are rational integers, $u$ and $u_1$ even, $v$ and $v_1$ odd. We put

$$\omega\omega_1 = U + V\sqrt{-q},$$

where $U$ and $V$ are rational integers; $U$ is clearly odd and $V$ even. According to Lemma 11, we have

$$4\omega\omega_1 = (a + c\sqrt{-q})^2 + (b + d\sqrt{-q})^2,$$

where $a$, $b$, $c$ and $d$ are rational integers. We get

$$4U = a^2 + b^2 - qc^2 - qd^2, \tag{7}$$

$$2V = ac + bd. \tag{8}$$

If the numbers $a$, $b$, $c$ and $d$ are all odd, we get from (7)

$$4U \equiv 1 + 1 - q - q \equiv 0 \pmod 8),$$

which is impossible since $U$ is odd. If all the numbers $a$, $b$, $c$ and $d$ are even, Lemma **12** is proved.

Suppose next that $a$ and $b$ are even and $c$ and $d$ odd. Then we get from (7)

$$2q+4 \equiv a^2+b^2 \equiv 6 \pmod 8,$$

which is clearly impossible.

Consider finally the case that $a$ and $d$ are even and $b$ and $c$ are odd. Then it follows from (7) that

$$a^2 \equiv q d^2 \pmod 8.$$

Hence we conclude that $a \equiv d \pmod 4$.

When $q=5$, we multiply the number $4\omega\omega_1$ by $-4=1^2+(\sqrt{-5})^2$. The product is equal to

$$-16\,\omega\,\omega_1=\left[(a\mp 5d)+(c\pm b)\sqrt{-5}\right]^2+\left[(-5c\mp b)+(a\mp d)\sqrt{-5}\right]^2.$$

Here we may choose the sign such that the numbers

$$c\pm b \quad \text{and} \quad -5c\mp b$$

will both be divisible by 4. Since the numbers

$$a\mp 5d \quad \text{and} \quad a\mp d$$

are also divisible by 4, we see that the number $-\omega\omega_1$ is an $A$-number.

When $q=13$, we multiply the number $4\omega\omega_1$ by $-4=3^2+(\sqrt{-13})^2$, and the proof of Lemma **12** proceeds in an analogous manner.

**Lemma 13.** *If $\omega$ is a $C$-prime, the number $\sqrt{-q}\,\omega$ is an $A$-number.*

*Proof.* According to Lemma **11**, the number $2\omega$ is an $A$-number. Hence

$$2\omega=2u+2v\sqrt{-q}=(a+c\sqrt{-q})^2+(b+d\sqrt{-q})^2,$$

where $u, v, a, b, c$ and $d$ are rational integers; $u$ is even, $v$ odd. Then we get

$$2u=a^2+b^2-qc^2-qd^2, \quad v=ac+bd.$$

Hence we may suppose that $ac$ is even. This implies that $b$ and $d$ are odd and that $a$ and $c$ are both even. Suppose first $q=5$. Using the identity

$$2\sqrt{-5}=2^2+(1+\sqrt{-5})^2$$

we get

$$2\omega\cdot 2\sqrt{-5}=[2a+b-5d+\sqrt{-5}(d+b+2c)]^2+[-a+5c-2b+\sqrt{-5}\,(-a-c-2d)]^2.$$

Here the numbers $2a+b-5d$, $d+b+2c$, $a-5c-2b$ and $a+c-2d$ are all even. Hence $\omega\sqrt{-5}$ is an $A$-number.

Suppose next $q=13$. Using the identity

$$2\sqrt{-13}=(4+2\sqrt{-13})^2+(7-\sqrt{-13})^2.$$

we get

$$2\omega\cdot 2\sqrt{-13}=[4a-26c+7b-13d+\sqrt{-13}\,(4c+2a+7d-b)]^2$$
$$+[7a+13c-4b+26d+\sqrt{-13}\,(7c-a-4d-2b)]^2.$$

As in the preceding case we see then that $\omega\sqrt{-13}$ is an $A$-number.

**Lemma 14.** *Let $\mathfrak{p}$ be a prime ideal satisfying* (1) *and $\mathfrak{p}^2=(\gamma)$, and let $\omega$ be a C-prime. Then the product $\omega\gamma$ is an A-number.*

*Proof.* We have

$$2\omega=(a+c\sqrt{-q})^2+(b+d\sqrt{-q})^2,$$

where, according to the proof of Lemma **13**, we may suppose that $a$ and $c$ are even and that $b$ and $d$ are odd. According to Lemma **9**, we have

$$2\gamma=(a_1+c_1\sqrt{-q})^2,$$

where $a_1$ and $c_1$ clearly are odd. Hence we get

$$4\omega\gamma=[a a_1-q c c_1+\sqrt{-q}\,(a c_1+a_1 c)]^2$$
$$+[a_1 b-q c_1 d+\sqrt{-q}\,(a_1 d+b c_1)]^2.$$

Since the numbers $aa_1-qcc_1$, $ac_1+a_1c$, $a_1b-qc_1d$ and $a_1d+bc_1$ are all even, the lemma is proved.

**8.** *Summary and proof of the main result.* As a consequence of the discussions in Sections 3–6, we may state the following results.

**Theorem 1.** *All the prime ideals in* $\mathbf{K}(\sqrt{-q})$ *are principal except the prime ideal divisors of* 2 *and of the odd rational primes $p$ satisfying the relations, in* $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right)=-1,\ \left(\frac{-q}{p}\right)=+1.$$

**Theorem 2.** *The prime $\omega$ in* $\mathbf{K}(\sqrt{-q})$ *is an A-number only in the following cases:*

(i) *$\omega=\pm p$ where $p$ is an odd rational prime such that, in* $\mathbf{K}(1)$,

$$\left(\frac{-q}{p}\right)=-1.$$

(ii) *$\omega$ is of the form $u+v\sqrt{-q}$, where $u$ and $v$ are rational integers, $u$ odd, $v$ even, such that $u^2+qv^2$ is a rational prime.*

*The prime* $\omega$ *in the field is a C-prime only when* $\omega = u + v\sqrt{-q}$, *where* $u$ *and* $v$ *are rational integers,* $u$ *even,* $v$ *odd, such that* $u^2 + qv^2$ *is a rational prime.*

We further need the result:

**Lemma 15.** *Let* $\mathfrak{q}$ *be the prime ideal which divides* 2, *and let* $\xi$ *be an A-number which is divisible by* $\mathfrak{q}^m$ *and not by* $\mathfrak{q}^{m+1}$. *Then* $m$ *is even.*

*Proof.* Suppose that $\xi = \alpha^2 + \beta^2$, where $\alpha$ and $\beta$ are integers. If $m$ were odd, it is evident that $\xi$ should be divisible by the power $\mathfrak{p}^\nu$ of a non-principal prime ideal $\mathfrak{p} \neq \mathfrak{q}$ with an odd exponent $\nu$. But, according to Theorem **1** and Lemma **6**, the exponent $\nu$ must be even.

We are now in position to establish our main result.

**Theorem 3.** *The integer* $\alpha$ *in the field* $\mathbf{K}(\sqrt{-q})$ *is an A-number if and only if*

$$\alpha = \beta\gamma\delta(\sqrt{-5})^n \cdot 2^k,$$

*where* $\beta$, $\gamma$ *and* $\delta$ *are integers in the field with the following properties:* $\beta$ *is either* $= \pm 1$ *or* $=$ *a product of A-primes, different or not;* $\gamma$ *is either* $= \pm 1$ *or* $=$ *a product of* $\nu$ *C-primes, different or not;* $\delta$ *is either* $= \pm 1$ *or* $=$ *a product of* $m$ *numbers* $\omega_i$, *different or not, defined by the equations* $(\omega_i) = \mathfrak{p}_i^2$, $\mathfrak{p}_i$ *being a non-principal prime ideal not dividing* 2.

*The numbers* $\nu$, $m$, $n$ *and* $k$ *are rational integers* $\geq 0$ *satisfying one of the following conditions:*

$$\begin{aligned}
&\nu \text{ even } \geq 0,\ m \text{ even } \geq 0,\ n \text{ even } \geq 0,\ k \geq 0;\\
&\nu \text{ even } \geq 0,\ m \text{ even } \geq 0,\ n \text{ odd},\ k \geq 1;\\
&\nu \text{ even } \geq 0,\ m \text{ odd},\ n \text{ even } \geq 0,\ k \geq 1;\\
&\nu \text{ even } \geq 0,\ m \text{ odd},\ n \text{ odd},\ k \geq 0;\\
&\nu \text{ odd},\ m \text{ even } \geq 0,\ n \text{ odd},\ k \geq 0;\\
&\nu \text{ odd},\ m \text{ even } \geq 0,\ n \text{ even } \geq 0,\ k \geq 1,\\
&\nu \text{ odd},\ m \text{ odd},\ n \text{ even } \geq 0,\ k \geq 0;\\
&\nu \text{ odd},\ m \text{ odd},\ n \text{ odd},\ k \geq 1.
\end{aligned}$$

*Proof.* It is evident that the conditions in this theorem are sufficient. If $\alpha$ is an $A$-number we may, in virtue of Lemma **4**, neglect the $A$-prime divisors. In virtue of Lemmata **5** and **12** we may suppose that $\nu$ is either $= 0$ or $= 1$. Suppose that $\alpha$ is divisible by $\mathfrak{p}^h$, where $\mathfrak{p}$ is a non-principal prime ideal not dividing 2. Then, according to Lemma **6**, it is sufficient to suppose $h = 2$. For the rest of the proof we only have to apply Lemmata **7**, **8**, **9**, **10**, **11**, **13**, **14**, **15** and to observe the following fact. Let $u$, $v$, $u_1$ and $v_1$ be rational integers, $u_1$ and $v$ odd. Then the product of the two numbers $2u + v\sqrt{-q}$ and $u_1 + 2v_1\sqrt{-q}$ is of the form $2u_2 + v_2\sqrt{-q}$. where $v_2$ is odd, and thus it cannot be an $A$-number. Then it is easily seen that the eight cases indicated in the theorem are the only possible ones.

**9.** *On the primitivity of the representations as a sum of two integral squares.* Finally we shall determine the $A$-numbers in the quadratic fields $K(\sqrt{-5})$ and $K(\sqrt{-13})$ which have at least one *primitive* representation. By Theorems 29–31 in [1] it suffices to examine the numbers which are products of prime ideal factors of 2. In the actual case we have only to examine the powers of 2. Consider the equation

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

where $a$, $b$, $c$ and $d$ are rational integers. For $h = 1$ and $h = 2$ we have the primitive representations

$$2 = 1^2 + 1^2,$$

$$2^2 = 3^2 + (\sqrt{-5})^2,$$

$$2^2 = 11^2 + 3(\sqrt{-13})^2.$$

We shall show that there are no primitive representations for $h \geqslant 3$. If the representation (9) is primitive it is clear that the numbers $a$, $b$, $c$, $d$ cannot be all odd. From (9) we obtain

$$2^h = a^2 + b^2 - q(c^2 + d^2), \tag{10}$$

and

$$ac = -bd. \tag{11}$$

From (10) it follows that two of the numbers $a$, $b$, $c$, $d$ are odd and two of them are even. If $d = 0$ we must have either $a = 0$ or $c = 0$. When $a = 0$ we get from (10)

$$2^h = b^2 - qc^2,$$

where $b$ and $c$ are odd. But this is impossible when $h \geqslant 3$. When $c = 0$ we get from (10)

$$2^h = a^2 + b^2,$$

where $a$ and $b$ are odd. Since $h \geqslant 3$ this equation is impossible too. Hence we may suppose $cd \neq 0$. By elimination of $b$ we obtain from (10) and (11)

$$2^h d^2 = (a^2 - qd^2)(c^2 + d^2).$$

Put $c = g_1 c_1$, $d = g_1 d_1$, where $(c_1, d_1) = 1$. Then we get

$$2^h d_1^2 = (a^2 - q g_1^2 d_1^2)(c_1^2 + d_1^2).$$

It follows from this equation that $a$ is divisible by $d_1$. Putting $a = d_1 f_1$ we obtain

$$2^h = (f_1^2 - q g_1^2)(c_1^2 + d_1^2).$$

Since $(c_1, d) = 1$ and since $c_1^2 + d_1^2$ is a power of 2, we must have $c_1^2 = d_1^2 = 1$. Hence

$$2^{h-1} = f_1^2 - q g_1^2.$$

Since $q \equiv 5 \pmod 8$, $h-1$ is even and $=2n+2$ with $n \geqslant 0$. Then $f_1$ and $g_1$ are divisible by $2^n$. Hence the representation (9) must have the form

$$2^h = 2^{2n+3} = (f_1 + g_1\sqrt{-q})^2 + (f_1 - g_1\sqrt{-q})^2.$$

But this representation is always imprimitive, since $f_1$ and $g_1$ are of the same parity.

## § 3. The real field $K(\sqrt{q})$ where $q$ is either $=5$ or $=13$

**10.** *Units and divisors of the rational primes* 2 *and* $q$. Every $A$-number in this field must be positive and have a positive norm. The fundamental unit $\varepsilon$ in $\mathbf{K}(\sqrt{q})$ is $\frac{1}{2}(\sqrt{5}+1)$ or $\frac{1}{2}(\sqrt{13}+3)$ according as $q=5$ or 13. Since $N(\varepsilon)=-1$ in this field, $\varepsilon$ is never an $A$-number. The $n$th power of $\varepsilon$ is an $A$-number if and only if $n$ is even. The number 2 is a prime in the field and, of course, an $A$-number.

Since the prime $\sqrt{q}$ has the negative norm $-q$ it cannot be an $A$-number. The number $-1$ is a quadratic residue modulo $\sqrt{q}$. From the relations

$$\tfrac{1}{2}(\sqrt{5}+1)\sqrt{5} = 1^2 + \tfrac{1}{4}(\sqrt{5}+1)^2,$$

and

$$\tfrac{1}{2}(\sqrt{13}+3)\sqrt{13} = 1^2 + \tfrac{1}{4}(\sqrt{13}+1)^2,$$

it follows that *the product* $\varepsilon\sqrt{q}$ *is always an* $A$*-number*. Then it is evident that the number

$$\varepsilon^m (\sqrt{q})^n,$$

where $m$ and $n$ are rational integers. $n \geqslant 0$, is an $A$-number if and only if $m+n$ is even.

**11.** *The rational primes for which* $q$ *is a quadratic non-residue*. Let $p$ be an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = +1 \quad \text{and} \quad \left(\frac{q}{p}\right) = -1.$$

Then $p$ is a prime in the field and since

$$p = u^2 + v^2,$$

where $u$ and $v$ are rational integers, $p$ is an $A$-prime.

Suppose next that $p$ is an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = -1 \quad \text{and} \quad \left(\frac{q}{p}\right) = -1.$$

Then $p$ is a prime in $\mathbf{K}(\sqrt{q})$. Since $\left(\frac{-q}{p}\right) = +1$ we have in $\mathbf{K}(\sqrt{-q})$

$$(p) = \mathfrak{p}\,\mathfrak{p}',$$

where $\mathfrak{p}$ and $\mathfrak{p}'$ are different prime ideals. We showed in Section **5** that these prime ideals are not principal when $q=5$ or $=13$. If $\mathfrak{q}$ is the prime ideal divisor of 2 in $\mathbf{K}(\sqrt{-q})$, the product $\mathfrak{p}\mathfrak{q}$ is a principal ideal. Hence

$$2p = x^2 + qy^2,$$

where $x$ and $y$ are rational odd integers. Since this relation may be written

$$p = \tfrac{1}{4}(x + y\sqrt{q})^2 + \tfrac{1}{4}(x - y\sqrt{q})^2,$$

the number $p$ is an $A$-prime in $\mathbf{K}(\sqrt{q})$. Hence in this field the number $-1$ is a quadratic residue modulo $p$.

**12.** *The rational primes for which $q$ is a quadratic residue.* Let $p$ an odd rational prime such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = -1 \quad \text{and} \quad \left(\frac{q}{p}\right) = +1.$$

In this case we have $$p = \omega\omega',$$

where $\omega$ and $\omega'$ are different primes. Since

$$\left(\frac{-1}{\omega}\right) = (-1)^{\frac{1}{2}(|N\omega|-1)} = -1,$$

the prime $\omega$ is not an $A$-number.

Finally, we consider an odd rational prime $p$ such that, in $\mathbf{K}(1)$,

$$\left(\frac{-1}{p}\right) = +1 \quad \text{and} \quad \left(\frac{q}{p}\right) = +1.$$

Since the field is simple, and since the norm of the fundamental unit $\varepsilon$ is $= -1$, we have always

$$4p = u^2 - qv^2,$$

where $u$ and $v$ are rational integers. If $u$ and $v$ are even, $p$ may be written in the form

$$p = (u/2)^2 - q(v/2)^2.$$

Suppose next that $u$ and $v$ are both odd. The number $\varepsilon^2$ is of the form $\frac{1}{2}(a + b\sqrt{q})$, where $a$ and $b$ are odd integers; when $q=5$, we have $a=3$, $b=1$; when $q=13$, we have $a=11$, $b=3$. Consider the product

$$\tfrac{1}{2}(a \pm b\sqrt{q}) \cdot \tfrac{1}{2}(u + v\sqrt{q}) = \tfrac{1}{4}(au \pm qbv) + \tfrac{1}{4}(av \pm bu)\sqrt{q}.$$

Here we may choose the sign such that the number $au \pm qbv$ be divisible by 4. Then the number $av \pm bu$ is also divisible by 4, since $q \equiv 1 \pmod 4$. Hence, we conclude: the prime $p$ may always be written in the form

$$p = u^2 - qv^2,$$

where $u$ and $v$ are rational integers. Then the numbers

$$\omega = u + v\sqrt{q} \quad \text{and} \quad \omega' = u - v\sqrt{q}$$

are conjugate prime factors of $p$ in the field. If we suppose $u > 0$, the numbers $\omega$ and $\omega'$ are positive. Since by Lemma 1 the field $\mathbf{K}(\sqrt{q}, \sqrt{-1})$ is simple, we have

$$\omega = \pi_1 \pi_2 \eta,$$

where $\eta$ is a unit and $\pi_1$ and $\pi_2$ are primes in that field. According to Lemma **3**, we may suppose that

$$\pi_1 = \tfrac{1}{2}\left(a + c\sqrt{q}\right) + \tfrac{1}{2} i \left(b + d\sqrt{q}\right)$$

and

$$\pi_2 = \tfrac{1}{2}\left(a + c\sqrt{q}\right) - \tfrac{1}{2} i \left(b + d\sqrt{q}\right),$$

$a$, $b$, $c$ and $d$ being rational integers. The unit $\eta$ belongs to the field $\mathbf{K}(\sqrt{q})$, since the product $\pi_1 \pi_2$ belongs to this field. Since $\omega$ is positive, $\eta$ is so. The norm of $\omega$ is positive and the norm of $\pi_1 \pi_2$ is also positive. Hence the norm of $\eta$ is positive. Thus we have

$$\eta = \varepsilon^{2m}.$$

Putting

$$\psi_1 = \pi_1 \varepsilon^m \quad \text{and} \quad \psi_2 = \pi_2 \varepsilon^m,$$

we get

$$\omega = \psi_1 \psi_2,$$

where $\psi_1$ and $\psi_2$ are primes in $\mathbf{K}(\sqrt{q}, \sqrt{-q})$ such that $\psi_1$ is transformed into $\psi_2$ when $i$ is substituted by $-i$ and vice versa. Consequently we may suppose that $\eta = 1$. Hence

$$\omega = \tfrac{1}{4}\left(a + c\sqrt{q}\right)^2 + \tfrac{1}{4}\left(b + d\sqrt{q}\right)^2, \tag{12}$$

which involves the relations

$$4u = a^2 + b^2 + q(c^2 + d^2) \tag{13}$$

and

$$2v = ac + bd. \tag{14}$$

If the integers $a$, $b$, $c$ and $d$ are all odd or all even, it is evident that $\omega$ is an $A$-number. If the number $\tfrac{1}{2}\left(a + c\sqrt{q}\right)$ is an integer, it follows from (12) that the number $\tfrac{1}{2}\left(b + d\sqrt{q}\right)$ is also an integer: hence $\omega$ is an $A$-number. Then it remains to consider the following cases: (i) $a$ is even, $c$ is odd; (ii) a is odd, $c$ is even. In both cases $bd$ is even in virtue of (14); thus one of the numbers $b$ and $d$ is even and the other one is odd. In the first case we get from (13) modulo 4:

$$b^2 + 1 + d^2 \equiv 0 \pmod{4}.$$

But this congruence is clearly impossible. In the second case we get from (13) the same congruence modulo 4. Hence $\omega$ and $\omega'$ are always $A$-numbers.

**13.** *Summary and proof of the main result.* As a consequence of the discussions in Sections **10–12** we may state the following result.

**Theorem 4.** *The prime $\omega$ in $\mathbf{K}(\sqrt{q})$ is an A-number only in the following cases:* (i) $\omega = 2\varepsilon^{2m}$; (ii) $\omega = \sqrt{q}\cdot\varepsilon^{2m+1}$; (iii) $\omega = p\,\varepsilon^{2m}$, *where $p$ is an odd rational prime such that* $\left(\frac{q}{p}\right) = -1$; (iv) *$\omega$ is of the form $\frac{1}{2}(u + v\sqrt{q})$, where $u$ and $v$ are rational integers such that $\frac{1}{4}(u^2 - qv^2)$ is a rational prime* $\equiv 1 \pmod 4$.

We are now in position to establish our main result.

**Theorem 5.** *The integer $\alpha$ in the field $\mathbf{K}(\sqrt{q})$ is an A-number if and only if*

$$\alpha = \beta\gamma^2(\sqrt{q})^m \cdot \varepsilon^n,$$

*where $\beta$ and $\gamma$ are integers in the field with the following properties: $\beta$ and $\gamma$ are prime to $\sqrt{q}$; $\beta$ is either $=1$ or $=$ a product of A-primes, different or not; $\gamma$ is either a unit or $=$ a product of primes $\pi$ such that in $\mathbf{K}(\sqrt{q})$*

$$\left(\frac{-1}{\pi}\right) = -1.$$

*$m$ and $n$ are rational integers, $m \geqslant 0$, such that $m+n$ is even. $\varepsilon$ is the fundamental unit, chosen $>1$.*

*Proof.* It is evident that the conditions are sufficient. Suppose that $\alpha$ is an $A$-number and that

$$\alpha = \xi\eta(\sqrt{q})^m,$$

where $\xi$ and $\eta$ are integers in the field with the following properties: they are prime to $\sqrt{q}$; $\xi$ is either $=1$ or $=$ product of primes $\pi$ such that, in $\mathbf{K}(\sqrt{q})$,

$$\left(\frac{-1}{\pi}\right) = -1;$$

$m$ is a rational integer $\geqslant 0$. Then we must have $\eta = \varrho\gamma^2$, where $\gamma$ is an integer in the field and $\varrho$ a unit; thus the number $\alpha/\gamma^2$ is an $A$-number. Now applying Lemma **4** a certain number of times to the prime factors $\pi$ of $\xi$, we find that the number

$$\frac{\alpha}{\gamma^2\xi} = \varrho(\sqrt{q})^m$$

must be an $A$-number. Finally, applying a result in Section **10** we achieve the proof.

*Note.* The fields $\mathbf{K}(\sqrt{\pm 37})$ have in the main the same properties as the fields $\mathbf{K}(\sqrt{\pm 5})$ and $\mathbf{K}(\sqrt{\pm 13})$. There is, however, an essential difference: The fundamental unit has the form $6 + \sqrt{37}$. Thus the equations $x^2 - 37y^2 = \pm 4$ have no solutions in odd (rational) integers. This fact necessitates a modification of the methods used in this paper. We shall treat the fields $\mathbf{K}(\sqrt{\pm 37})$ in a following paper.

**14.** *Numerical examples.* The number $3+2\sqrt{-5}$ is an $A$-prime in $\mathbf{K}(\sqrt{-5})$ since

$$3+2\sqrt{-5}=(3+\sqrt{-5})^2+(2-\sqrt{-5})^2$$

and since
$$N(3+2\sqrt{-5})=29.$$

The number $3+2\sqrt{-13}$ is an $A$-prime in $\mathbf{K}(\sqrt{-13})$ since

$$3+2\sqrt{-13}=(11+5\sqrt{-13})^2+(18-3\sqrt{-13})^2$$

and since
$$N(3+2\sqrt{-13})=61.$$

The number $6+\sqrt{-5}$ is a $C$-prime in $\mathbf{K}(\sqrt{-5})$ since

$$N(6+\sqrt{-5})=41\equiv 1 \pmod 4.$$

The number $3+\sqrt{-13}$ is a $C$-prime in $\mathbf{K}(\sqrt{-13})$ since

$$N(2+\sqrt{-13})=17\equiv 1 \pmod 4.$$

We have
$$(2+\sqrt{-5})=\mathfrak{p}^2,$$

where $\mathfrak{p}$ is a prime ideal dividing 3 in $\mathbf{K}(\sqrt{-5})$. We have

$$(6+\sqrt{-13})=\mathfrak{p}^2,$$

where $\mathfrak{p}$ is a prime ideal dividing 7 in $\mathbf{K}(\sqrt{-13})$. The number 7 is an $A$-prime in $\mathbf{K}(\sqrt{5})$ since

$$7=\tfrac{1}{4}(3+\sqrt{5})^2+\tfrac{1}{4}(3-\sqrt{5})^2.$$

The number 7 is an $A$-prime in $\mathbf{K}(\sqrt{13})$ since

$$7=\tfrac{1}{4}(1+\sqrt{13})^2+\tfrac{1}{4}(1-\sqrt{13})^2.$$

The number $7+2\sqrt{5}$ is an $A$-prime in $\mathbf{K}(\sqrt{5})$ since

$$7+2\sqrt{5}=1^2+(1+\sqrt{5})^2$$

and since
$$N(7+2\sqrt{5})=29.$$

The number $15+2\sqrt{13}$ is an $A$-prime in $\mathbf{K}(\sqrt{13})$ since

$$15 + 2\sqrt{13} = 1^2 + (1 + \sqrt{13})^2$$

and since
$$N(15 + 2\sqrt{13}) = 173$$

is a prime.

**15.** *Addition to paper* [1]. The proof of the last part of Theorem **17** in [1], p. 54, is not in order and may be replaced by the following correct proof:

Let $\omega$ be an $A$-number with the representation

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

$\alpha$ and $\beta$ being integers in $\mathbf{\Omega}$. Suppose that equation (30) has an infinity of solutions $x = \xi_n$ and $y = \eta_n$ given by (18) and (29). 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
$$(\alpha_n + \beta_n i)(\alpha_n - \beta_n i) = (\xi_n^2 + \eta_n^2)(\alpha^2 + \beta^2).$$

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

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

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

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

But, in the proof of Theorem 15 we showed that this relation is possible only for $m = n$.

## 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. SOMMER, J., Vorlesungen über Zahlentheorie, S. 346–354. Leipzig 1907.
3. DIRICHLET, L., Recherches sur les formes quadratiques à coefficients et à indétermininées complexes. Werke I, p. 578–588.

Tryckt den 22 februari 1961

Uppsala 1961. Almqvist & Wiksells Boktryckeri AB