THE ALGEBRAIC NUMBER REALMS
\[ \mathbb{A}(\sqrt{-2}), \mathbb{A}(\sqrt{3}), \mathbb{A}(\sqrt{-3}) \, . \]

by

Mary Jean Fisher

A Thesis submitted for the Degree of

MASTER OF ARTS

in the Department

of

MATHEMATICS

The University of British Columbia
January - 1931.
Table of Contents.

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>I</td>
</tr>
<tr>
<td>Part I</td>
<td>1</td>
</tr>
<tr>
<td>The Realm $\mathbb{A}(\sqrt{-2})$</td>
<td>1</td>
</tr>
<tr>
<td>Part II</td>
<td>14</td>
</tr>
<tr>
<td>The Realm $\mathbb{A}(\sqrt{5})$</td>
<td>14</td>
</tr>
<tr>
<td>Part III</td>
<td>26</td>
</tr>
<tr>
<td>The Realm $\mathbb{A}(\sqrt{-23})$</td>
<td>26</td>
</tr>
</tbody>
</table>
THE ALGEBRAIC NUMBER REALMS

\( \mathbb{A}(\sqrt{-2}), \mathbb{A}(\sqrt{5}) \) AND \( \mathbb{A}(\sqrt{-23}) \).

Introduction.

An algebraic number is a number which satisfies a rational equation, viz., an equation of the form

1) \[ x^n + a_1 x^{n-1} + \cdots + a_n = 0. \]

where \( a_1, a_2, \ldots, a_n \) are rational numbers.

An algebraic integer is an algebraic number which satisfies an equation of the form 1) in which \( a_1, a_2, \ldots, a_n \) are rational integers.

Hereafter, algebraic numbers and algebraic integers will usually be referred to as numbers and integers.

If equation 1) is the rational equation of lowest degree which a number \( \alpha \) satisfies, then 1) is irreducible, and \( \alpha \) is said to be a number of the \( n \)-degree. Equation 1) is then called the rank or minimum equation of \( \alpha \).

An algebraic number realm, or, more briefly, a realm, is a system of algebraic numbers such that the sum, difference, product and quotient of any two numbers of the system, excluding division by 0, are numbers of the system. Hence, if \( \alpha \) is an algebraic number, the system consisting of all rational functions of \( \alpha \), with rational coefficients, is a realm. Such a realm is denoted by \( \mathbb{A}(\alpha) \), and \( \alpha \) is said to define
the realm. If \( \alpha \) is a number of the second degree, then \( \mathcal{A}(\alpha) \) is said to be a realm of the second degree. In this case, the remaining root, \( \alpha' \), of the equation defining \( \alpha \), is called the conjugate of \( \alpha \), and \( \mathcal{A}(\alpha') \) is called the conjugate realm of \( \mathcal{A}(\alpha) \). If the realm \( \mathcal{A}(\alpha) \) is identical with \( \mathcal{A}(\alpha') \), it is called a Galois Realm.

The purpose of this paper is to develop and contrast the algebraic number theory for the particular Galois realms \( \mathcal{A}(\sqrt{-2}) \), \( \mathcal{A}(\sqrt{-5}) \) and \( \mathcal{A}(\sqrt{-23}) \). We find, for example, that the realms \( \mathcal{A}(\sqrt{-2}) \) and \( \mathcal{A}(\sqrt{-23}) \) have each only two units, viz., \( \pm 1 \), while the realm \( \mathcal{A}(\sqrt{-5}) \) has an infinite number of units; also, that the Unique Factorization Theorem holds for the realms \( \mathcal{A}(\sqrt{-2}) \) and \( \mathcal{A}(\sqrt{-5}) \), but does not hold for the realm \( \mathcal{A}(\sqrt{-23}) \). Unique Factorization may, however, be restored in the latter realm by the introduction of ideals. We show that in the realm \( \mathcal{A}(\sqrt{-2}) \), the norm of a prime is either 2, or a rational prime of the form \( 8n+1 \), or \( 8n+3 \). Likewise, in the realm \( \mathcal{A}(\sqrt{-5}) \) the norm of a prime is found to be \( \pm 5 \), or a rational prime of the form \( 6n \pm 1 \). In each of these realms the norm of the general integer appears as a binary quadratic form. With reference to these forms we derive theorems on representation. An application of these theorems is made in obtaining solutions of certain types of Diophantine Equations. Corresponding results are not obtained for the realm \( \mathcal{A}(\sqrt{-23}) \), in which factorization is not unique.
PART I

THE REALM \( k(\sqrt{-2}) \)

1. The Numbers of the Realm \( k(\sqrt{-2}) \).

The number \( \sqrt{-2} \) is defined by the equation

\[
x^2 + 2 = 0.
\]

Since \( (\sqrt{-2})^2 = -2 \), every number of \( k(\sqrt{-2}) \) is of the form

\[
\alpha = \frac{a + b\sqrt{-2}}{a + b\sqrt{-2}},
\]

where \( a, b, a_1, b_1 \) are rational numbers. Rationalizing the denominator we obtain

\[
\alpha = \frac{a_1a + b_1b}{a_1^2 + b_1^2} + \frac{a_1b - b_1a}{a_1^2 + b_1^2} \sqrt{-2}.
\]

Hence every number of \( k(\sqrt{-2}) \) is of the form

\[
\alpha = a + b\sqrt{-2},
\]

where \( a \) and \( b \) are rational numbers.

The other root of 1) defines the realm \( k(\sqrt{-2}) \) conjugate to \( k(\sqrt{-2}) \). But these realms are identical since \( k(\sqrt{-2}) \) contains all the numbers of \( k(-\sqrt{-2}) \) and \( k(\sqrt{-2}) \) contains all the numbers of \( k(\sqrt{-2}) \).

2. The Conjugate and Norm of a Number of \( k(\sqrt{-2}) \).

If \( \alpha = a + b\sqrt{-2} \) is a number of \( k(\sqrt{-2}) \), the number obtained from \( \alpha \) by replacing \( \sqrt{-2} \) by its conjugate \( -\sqrt{-2} \) is called the conjugate of \( \alpha \).

If \( \alpha = a + b\sqrt{-2} \) and \( \beta = a_2 + b_2\sqrt{-2} \) are the numbers of \( k(\sqrt{-2}) \)
then
\[(a\beta)'=(a_1a_2-2a_1+a_2)-(a_1a_2+4a_2)\sqrt{-2}=a'\beta',\]
and hence, the conjugate of a product of two or more numbers
of \(\mathcal{A}(\sqrt{-2})\) is equal to the product of the conjugates of its
factors.

The norm of a number of a realm of the second degree is
the product of the number by its conjugate.

The norm of \(\alpha=a+b\sqrt{-2}\) is, therefore,
\[n[\alpha]=(a+b\sqrt{-2})(a-b\sqrt{-2})=a^2+2b^2.\]
It follows that the norm of every number of \(\mathcal{A}(\sqrt{-2})\) is a posi-
tive rational number.

If \(\alpha\) and \(\beta\) are two numbers of \(\mathcal{A}(\sqrt{-2})\) and \(\alpha'\) and \(\beta'\) their
conjugates, then
\[n[\alpha\beta]=\alpha\beta\cdot\alpha'\beta'=\alpha\alpha'\beta\beta'=n[\alpha]\cdot n[\beta],\]
that is, the norm of a product of two or more numbers of
\(\mathcal{A}(\sqrt{-2})\) is equal to the product of the norms of its factors.

3. Primitive and Imprimitive Numbers of \(\mathcal{A}(\sqrt{-2})\).

If \(\alpha=a+b\sqrt{-2}\) is a number of \(\mathcal{A}(\sqrt{-2})\) then \(\alpha\) satisfies
the equation
\[x^2-2ax+a^2+2b^2=0,\]
whose other root is \(\alpha'=a-b\sqrt{-2}\). Thus every number of
\(\mathcal{A}(\sqrt{-2})\) satisfies an equation of the second degree. The num-
ber \(\alpha\) is said to be a primitive number of \(\mathcal{A}(\sqrt{-2})\), if equa-
tion 2) is irreducible, and to be imprimitive if the equation
is reducible. Equation 2) is reducible if, and only if, \(b=0\), and
so \(\alpha\) is a primitive number if, and only if, it is different
from its conjugate. The imprimitive numbers of \( \mathbb{A}(\sqrt{-2}) \) are therefore the rational numbers.

4. **Integers of \( \mathbb{A}(\sqrt{-2}) \).**

A rational number is an algebraic integer when, and only when, it is a rational integer. Hence, of the imprimitive numbers of \( \mathbb{A}(\sqrt{-2}) \) only the rational integers are integers of \( \mathbb{A}(\sqrt{-2}) \).

The necessary and sufficient condition that a primitive number of \( \mathbb{A}(\sqrt{-2}) \) be an algebraic integer of \( \mathbb{A}(\sqrt{-2}) \) is that the coefficients of the rank equation of the number shall be rational integers.

Let \( \alpha = a + b\sqrt{-2} \) be an integer of \( \mathbb{A}(\sqrt{-2}) \). Then \( \alpha \sqrt{-2} \) is also an integer of \( \mathbb{A}(\sqrt{-2}) \). The rank equations of \( \alpha \) and \( \alpha \sqrt{-2} \) are

\[
3) \quad x^2 - 2a, x + a^2 + 2b,^2 = 0,
\]

and

\[
4) \quad x^2 + 4b, x + 4b,^2 + 2a,^2 = 0,
\]

respectively. Therefore, from \( 3) \) and \( 4) \),

\[
2a, = m, \quad \text{a rational integer};
\]

and

\[
4b, = m, \quad \text{a rational integer}.
\]

Hence, we have

\[
5) \quad \begin{bmatrix} a, = \frac{m,}{2} \\ b, = \frac{m,}{2} \end{bmatrix}.
\]

Substituting \( 5) \) in \( 3) \),

\[
x^2 - m, x + \frac{m,^2}{4} + \frac{m,^2}{2} = 0.
\]
Therefore \( \frac{m^2 + n^2}{2} \) is a rational integer, and we have
\[
2m^2 + n^2 \equiv 0 \pmod{2^4} \\
\therefore n^2 \equiv 0 \pmod{2}, \text{ and } n \equiv 0 \pmod{2}.
\]

Let \( n = k_2 \),
then
\[
m^2 + 2k^2 \equiv 0 \pmod{2^4},
\]
and
\[
m \equiv k \equiv 0 \pmod{2}.
\]

But \( a = \frac{m}{2} \), and \( b = \frac{n}{2} = \frac{k}{2} \). Therefore, if \( \alpha \) is an integer of \( \mathbb{A}(\sqrt{-2}) \), \( \alpha \) has the form \( \alpha + \beta \sqrt{-2} \) where \( \alpha \) and \( \beta \) are rational integers.

5. Basis of \( \mathbb{A}(\sqrt{-2}) \).

Any two integers \( \omega_1 \) and \( \omega_2 \) of a realm are said to form a basis of the realm if every integer of the realm can be expressed in the form \( a_1 \omega_1 + a_2 \omega_2 \) where \( a_1 \) and \( a_2 \) are rational integers.

We have seen that every integer of \( \mathbb{A}(\sqrt{-2}) \) has the form \( \alpha + \beta \sqrt{-2} \) where \( \alpha \) and \( \beta \) are rational integers. Hence 1 and \( \sqrt{-2} \) are a basis of \( \mathbb{A}(\sqrt{-2}) \). The numbers \( 1 + \sqrt{-2} \) and \( 2 + 3 \sqrt{-2} \) may also be taken as a basis of \( \mathbb{A}(\sqrt{-2}) \). To prove this, let \( \alpha = a + \beta \sqrt{-2} \) be any integer of \( \mathbb{A}(\sqrt{-2}) \) and suppose
\[
\alpha = x (1 + \sqrt{-2}) + y (2 + 3 \sqrt{-2})
\]

Then
\[
x + 2y = a \\
x + 3y = \beta
\]
\[
\therefore y = \beta - a \text{ a rational integer}
\]
since \( \alpha \) and \( \beta \) are rational integers,
3a. — If a rational integer.

Hence \( 1 + \sqrt{-2} \) and \( 2 + \sqrt{-2} \) are a basis of \( \mathbb{K}(\sqrt{-2}) \).

**Theorem.** If \( \omega_1 \) and \( \omega_2 \) are a basis of \( \mathbb{K}(\sqrt{-2}) \) the necessary and sufficient condition that

\[
\omega_1^x = a_1 \omega_1 + a_2 \omega_2 \\
\omega_2^x = b_1 \omega_1 + b_2 \omega_2
\]

where \( a_1, a_2, b_1, b_2 \) are rational integers, shall be also a basis of \( \mathbb{K}(\sqrt{-2}) \) is

\[
\begin{vmatrix}
  a_1 & a_2 \\
  b_1 & b_2
\end{vmatrix} = \pm 1.
\]

The proof of the theorem for \( \mathbb{K}(\sqrt{-2}) \) is exactly the same as that given for the realm \( \mathbb{K}(i) \) in Reid, "The Elements of the Theory of Algebraic Numbers", and so will not be repeated here.

6. **The Discriminant of \( \mathbb{K}(\sqrt{-2}) \).**

The discriminant of a realm is the squared determinant formed from any pair of basis numbers and their conjugates.

The discriminant of \( \mathbb{K}(\sqrt{-2}) \) is therefore

\[
\Delta = \left| \begin{array}{cc}
  1 & \sqrt{-2} \\
  \sqrt{-2} & -1
\end{array} \right|^2 = -8.
\]

7. **Divisibility of Integers of \( \mathbb{K}(\sqrt{-2}) \).**

An integer \( \alpha \) of \( \mathbb{K}(\sqrt{-2}) \) is said to be divisible by an integer \( \beta \) of \( \mathbb{K}(\sqrt{-2}) \) if there exists an integer \( \gamma \) of \( \mathbb{K}(\sqrt{-2}) \) such that

\[
\alpha = \beta \gamma.
\]
Thus, $1+2\sqrt{-2}$ is divisible by $1-\sqrt{-2}$ since

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

8. **The Units of $\mathbb{A}(\sqrt{-2})$. Associated Integers.**

A unit of a realm is defined as an integer of the realm which divides every integer of the realm.

Let $\varepsilon = x + y\sqrt{-2}$ be a unit of $\mathbb{A}(\sqrt{-2})$. Then $\varepsilon$ must divide $1$ and conversely every divisor of $1$ is a unit. Hence $\alpha \varepsilon = 1$ where $\alpha$ is an integer of $\mathbb{A}(\sqrt{-2})$.

\begin{align*}
\therefore \ln[\alpha] \cdot \varepsilon = 1. \\
\therefore \ln[\varepsilon] = 1, \text{i.e. } x^2 + 2y^2 = 1. \\
\therefore x = \pm 1, y = 0.
\end{align*}

The units of $\mathbb{A}(\sqrt{-2})$ are therefore $\pm 1$.

Two integers, differing only in a unit factor, are said to be associated. The associates of any integer $\alpha$ of $\mathbb{A}(\sqrt{-2})$ are therefore $\pm \alpha$ and $-\alpha$.

9. **Prime Numbers of $\mathbb{A}(\sqrt{-2})$.**

An integer of $\mathbb{A}(\sqrt{-2})$ which is not a unit of $\mathbb{A}(\sqrt{-2})$ and which has no divisors other than its associates and the units, is called a prime number of $\mathbb{A}(\sqrt{-2})$.

To determine whether or not $3$ is a prime number of $\mathbb{A}(\sqrt{-2})$ we proceed as follows:

Let $3 = (a + b\sqrt{-2})(c + d\sqrt{-2})$, where $a, b, c, d$ are rational integers.

Then either

$$\begin{cases} 
\alpha^2 + 2 \beta^2 = 3 \\
c^2 + 2d^2 = 3
\end{cases}$$
If only 7) has solutions, \( 3 \) is a prime. But 6) has the solutions \( a = b = c = d = \pm 1 \).

\[ \cdot \cdot \cdot 3 = (1 + \sqrt{-2})(1 - \sqrt{-2}) \]

and is not a prime of \( \mathbb{A}(\sqrt{-2}) \).

Similarly it may be shown that \( \gamma \) and \( 3+\sqrt{-2} \) etc., are primes of \( \mathbb{A}(\sqrt{-2}) \).

10. The Unique Factorization Theorem for \( \mathbb{A}(\sqrt{-2}) \).

The proofs of the three theorems, A, B, C, (below) upon which the proof of the Unique Factorization Theorem for \( \mathbb{A}(\sqrt{-2}) \) depends, and the proof of the Unique Factorization Theorem itself, for \( \mathbb{A}(\sqrt{-2}) \) are identical with the proofs given for the corresponding theorems for the realm \( \mathbb{A}(i) \) in Reid, "The Elements of the Theory of Algebraic Numbers". Hence only the statement of the four theorems and their corollaries will be given.

Theorem A. If \( \alpha \) is an integer of \( \mathbb{A}(\sqrt{-2}) \) and \( \beta \) is any integer of \( \mathbb{A}(\sqrt{-2}) \) different from \( 0 \), there exists an integer \( \mu \) of \( \mathbb{A}(\sqrt{-2}) \) such that

\[ n[\alpha - \mu \beta] < n[\beta] \]

Theorem B. If \( \alpha \) and \( \beta \) are any two integers of \( \mathbb{A}(\sqrt{-2}) \) prime to each other, there exist two integers \( \xi \) and \( \eta \) of \( \mathbb{A}(\sqrt{-2}) \) such that

\[ \alpha \xi + \beta \eta = 1 \]
Cor. 1. If $\alpha$ and $\beta$ are any two integers of $\mathbb{N}(\sqrt{-2})$ there exists a common divisor $\delta$ of $\alpha$ and $\beta$ such that every common divisor of $\alpha$ and $\beta$ divides $\delta$, and there exist two integers $\gamma$ and $\eta$ of $\mathbb{N}(\sqrt{-2})$ such that

$$\alpha \gamma + \beta \eta = \delta.$$ 

Cor. 2. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are any $n$ integers of $\mathbb{N}(\sqrt{-2})$ there exists a common divisor $\delta$ of $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that every common divisor of $\alpha_1, \alpha_2, \ldots, \alpha_n$ divides $\delta$, and there exist $n$ integers $\gamma_1, \gamma_2, \ldots, \gamma_n$ such that

$$\alpha_1 \gamma_1 + \alpha_2 \gamma_2 + \ldots + \alpha_n \gamma_n = \delta.$$ 

Theorem C. If the product of two integers $\alpha$ and $\beta$ of $\mathbb{N}(\sqrt{-2})$ is divisible by a prime number $\pi$, at least one of the integers is divisible by $\pi$.

Cor. 1. If the product of any number of integers of $\mathbb{N}(\sqrt{-2})$ is divisible by a prime number $\pi$, at least one of the integers is divisible by $\pi$.

Cor. 2. If neither of two integers is divisible by a prime number $\pi$, their product is not divisible by $\pi$.

Cor. 3. If the product of two integers $\alpha$ and $\beta$ is divisible by an integer $\gamma$, and neither $\alpha$ nor $\beta$ is divisible by $\gamma$, then $\gamma$ is a composite number.

The Unique Factorization Theorem. Every integer of $\mathbb{N}(\sqrt{-2})$ can be represented in one, and only one, way as the product of prime numbers.

Cor. 1. If $\alpha$ and $\beta$ are prime to each other, and $\gamma$ is divisible by both $\alpha$ and $\beta$, then $\gamma$ is divisible by their
product.

Cor. 2. If $\alpha$ and $\beta$ are each prime to $\gamma$, then $\alpha\beta$ is prime to $\gamma$.

Cor. 3. If $\alpha$ is prime to $\gamma$, and if $\alpha\beta$ is divisible by $\gamma$, $\beta$ is divisible by $\gamma$.


Theorem. A rational integer which may be represented by the norm of an integer of the realm $A(\sqrt{-2})$, i.e., by the form $a^2 + 2b^2$, has its rational prime factors either (a) primes of the realm $A(\sqrt{-2})$, or (b) norms of primes of the realm. In case (a), these primes enter to even powers, and in case (b), the primes are themselves represented by the form $a^2 + 2b^2$.

Let $n$ be any integer of $A(\sqrt{-2})$, and write $n = n_1n_2\cdots$ where $n_1, n_2, \ldots$ are primes of the realm, not necessarily distinct. Then $n[n]$ is a rational integer, and one of the type specified in the Theorem.

Let

$$n[n] = p_1^{t_1}p_2^{t_2}\cdots$$

where $p_1, p_2, \ldots$ are distinct rational primes, and $t_1, t_2, \ldots$ positive rational integers. Then $n$ divides $n[n]$ and hence divides one of its rational prime factors, say $p_1$. It cannot divide two such factors, for then it would divide their rational greatest common divisor, and hence would be a unit. Let

$$p_1 = n, \lambda$$

where $\lambda$ is an integer of $A(\sqrt{-2})$. 
Therefore, since we cannot have $n[\pi] = 1$, we have either

$$n[\pi] = p,$$

or

$$n[\pi] = p^2.$$

From 9), $n, n' = p^2$, and it follows that $n' = \alpha$. Hence $p^2$ is the norm of a prime of $\mathcal{A}(\sqrt{-3})$.

From 10), it follows that $\alpha$ is a unit, and hence that $p$, is a prime of $\mathcal{A}(\sqrt{-3})$. Since

$$n[\pi] = n[\pi'] \cdot n[\pi''],$$

$p$, occurs to an even power in $n[\pi]$.

12. **Representation by the Binary Quadratic Form $a^2 + 3b^2$:**

**Lemma:** The norm of a prime of $\mathcal{A}(\sqrt{-3})$, not associated with a rational prime, is either 2, or a rational prime of the form $8n+1$ or $8n+3$. The norm of a prime of $\mathcal{A}(\sqrt{-3})$ which is associated with a rational prime is the square of the rational prime, and is of the form $8n+1$. Rational primes of the forms $8n-1$ and $8n-3$ are primes of $\mathcal{A}(\sqrt{-3})$. Every rational prime of the form $8n+1$ or $8n+3$ is factorable into two conjugate primes of $\mathcal{A}(\sqrt{-3})$ and so is the norm of a prime of $\mathcal{A}(\sqrt{-3})$.

We notice that $n[\sqrt{-3}] = 2$, and hence 2 can be factored into two conjugate primes of $\mathcal{A}(\sqrt{-3})$, and so is not a prime of
Let \( \pi = a + b\sqrt{-2} \) be a prime of \( \mathbb{A}(\sqrt{-2}) \), which is not associated with a rational prime, and consider \( \pi \neq \pm \sqrt{-2} \). Then

\[ \eta[\pi] = a^2 + 2b^2, \]

which is, by inspection, congruent to +1, or +3, \( \mod 8 \).

Let \( \pi \) be a prime of \( \mathbb{A}(\sqrt{-2}) \), which is associated with a rational prime, say \( p \). Then \( \pi = \pm p \), and \( \eta[\pi] = p^2 \), and we have \( \eta[\pi] \equiv 1 \mod 8 \).

Rational primes of the forms \( 8n-1 \) and \( 8n+3 \) are primes of \( \mathbb{A}(\sqrt{-2}) \), for a rational prime is factorable into conjugate primes of \( \mathbb{A}(\sqrt{-2}) \) only if it is 2, or of the form \( 8n+1 \) or \( 8n+3 \).

It remains to show that all primes of the forms \( 8n+1 \) and \( 8n+3 \) are factorable into two conjugate primes of \( \mathbb{A}(\sqrt{-2}) \). In proof, if \( p \equiv 1 \) or \( 3 \mod 8 \), then the congruence \( x^2 \equiv -2 \mod p \) has solutions, since \( -2 \) is a quadratic residue of all primes of the forms \( 8n+1 \) and \( 8n+3 \). Let \( a \) be a root. Then \( a^2 \equiv -2 \mod p \), and

\[ (a + \sqrt{-2})(a - \sqrt{-2}) \equiv 0 \mod p. \]

But \( a + \sqrt{-2} \) and \( a - \sqrt{-2} \) are integers of \( \mathbb{A}(\sqrt{-2}) \). Therefore, if \( p \) is a prime of \( \mathbb{A}(\sqrt{-2}) \), \( p \) must divide either \( a + \sqrt{-2} \) or \( a - \sqrt{-2} \). If

\[ a \pm \sqrt{-2} = p(c + d\sqrt{-2}) \]

where \( c + d\sqrt{-2} \) is an integer of \( \mathbb{A}(\sqrt{-2}) \), then

\[ pd = \pm 1 \]
which is impossible, since \( p \) and \( d \) are rational integers and \( p > 1 \). Hence \( p \) is not a prime of \( \mathbb{A}(\sqrt{-2}) \), but is factorable into two conjugate primes of \( \mathbb{A}(\sqrt{-2}) \), and so is the norm of a prime of \( \mathbb{A}(\sqrt{-2}) \).

As an immediate consequence of the lemma and the Theorem of Art. 11, we may state the following theorem on representation by the binary quadratic form \( a^2 + 2b^2 \).

**Theorem.** The binary quadratic form \( a^2 + 2b^2 \), represents \( 2 \) and all positive rational primes of the forms \( 8n + 1 \) and \( 8n + 3 \), and all positive rational integers which are products of primes of these forms, and even powers of primes of the forms \( 8n - 1 \) and \( 8n - 3 \). In the latter case, the primes divide both \( a \) and \( b \). The form \( a^2 + 2b^2 \) cannot represent positive rational primes of the form \( 8n - 1 \) or \( 8n - 3 \), or any positive rational integer which contains odd powers of primes of these forms.

13. **The Diophantine Equations: \( x^2 + 2y^2 = 1, x^2 + 2y^2 = p, x^2 + 2y^2 = m \).**

To find rational integral values of \( x \) and \( y \) which satisfy these equations, we have to find an integer \( \alpha \) of \( \mathbb{A}(\sqrt{-2}) \) whose norm is the right member of the equations. If \( \alpha = a + b\sqrt{-2} \) then \( x = \alpha a, y = \alpha b \) are the solutions.

Consider, first, the equation

1) \( x^2 + 2y^2 = 1 \).

The integer \( \alpha \) satisfies this equation if, and only if, \( \alpha \) is a unit of \( \mathbb{A}(\sqrt{-2}) \). Hence \( \alpha = \pm 1 \), and we have \( x = \pm 1, y = 0 \), as the only solutions of 1).
Consider, next, the equation
\[ x^2 + 2y^2 = p, \]
where \( p \) is a positive rational prime. By the Theorem of Art. 11, equation ii) has solutions if, and only if, \( p = 2 \) or \( p = 10r + 3 \mod 8 \). If \( x = a + b\sqrt{2} \) is an integer of \( \mathcal{A}(\sqrt{2}) \) whose norm is \( p \), then \( x = \pm a, y = \pm b \) are the solutions of \( \text{ii}) \).

Consider, finally, the equation
\[ x^2 + 2y^2 = m, \]
where \( m \) is a positive rational integer. By the Theorem of Art. 11, equation iii) has solutions if, and only if,
\[ m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \]
where \( p_1, p_2, \ldots, p_r \) are distinct primes of the forms \( 8n + 1 \) and \( 8n + 3 \) or \( 2 \); \( q_1, q_2, \ldots, q_s \) are distinct primes of the forms \( 8n - 1 \) and \( 8n - 3 \), and \( t_1, t_2, \ldots, t_s \) are positive rational integers. Then if
\[ p_1 = p_1', p_2 = p_2', \ldots, p_r = p_r', \]
we have
\[ m = (p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) (q_1^{e_1} q_2^{e_2} \cdots q_s^{e_s}) (t_1^{e_1} t_2^{e_2} \cdots t_s^{e_s}) = (a + b\sqrt{2}) (a - b\sqrt{2}) \]
Hence, \( x = \pm a, y = \pm b \), are solutions of iii). By interchanging one or more of the \( p_i \) with their conjugates in iii), we obtain all possible factorization of \( m \) into conjugate factors. Let \( m = (a + b\sqrt{2})(a - b\sqrt{2}) \) be the result of any such interchange. Then \( x = \pm a, y = \pm b \), are solutions of iii). Proceeding in this way, all the solutions of iii) may be obtained.
PART II

THE REALM $\mathbb{R}(\sqrt{3})$

1. The Numbers of the Realm $\mathbb{R}(\sqrt{3})$.

The number $\sqrt{3}$ is defined by the equation

$$x^2 - 3 = 0.$$ 

Since $(\sqrt{3})^2 = 3$, every number of $\mathbb{R}(\sqrt{3})$ is of the form

$$\beta = \frac{a + b\sqrt{3}}{a_2 + b_2\sqrt{3}},$$

where $a, b, a_2, b_2$ are rational numbers. Rationalizing the denominator, we see that every number of $\mathbb{R}(\sqrt{3})$ is of the form

$$\beta = a + b\sqrt{3},$$

where $a$ and $b$ are rational numbers.

The other root of 1) defines the realm $\mathbb{R}(-\sqrt{3})$, conjugate to $\mathbb{R}(\sqrt{3})$. As in $\mathbb{R}(\sqrt{2})$, the realms $\mathbb{R}(\sqrt{3})$ and $\mathbb{R}(-\sqrt{3})$ are identical.

2. The Conjugate and Norm of a Number of $\mathbb{R}(\sqrt{3})$.

If $\beta = a + b\sqrt{3}$ is a number of $\mathbb{R}(\sqrt{3})$, then $\beta = a - b\sqrt{3}$ is its conjugate.

The conjugate of a product of two or more numbers of $\mathbb{R}(\sqrt{3})$ is equal to the product of the conjugates of its factors.

The norm of $\beta = a + b\sqrt{3}$ is

$$\eta[\beta] = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 + 3b^2.$$ 

The norm of a product of two or more numbers of $\mathbb{R}(\sqrt{3})$
is equal to the product of the norms of its factors.

3. **Primitive and Imprimitive Numbers of \( \mathbb{A}(\sqrt{5}) \).**

Every number \( \beta = a + b\sqrt{5} \) of \( \mathbb{A}(\sqrt{5}) \) satisfies the equation

\[
x^2 - 2ax + a^2 - 5b^2 = 0.
\]

As in \( \mathbb{A}(\sqrt{3}) \), if equation 2) is irreducible, the number \( \beta \) is said to be a primitive number of \( \mathbb{A}(\sqrt{5}) \), and if 2) is reducible, \( \beta \) is said to be an imprimitive number of \( \mathbb{A}(\sqrt{5}) \).

The imprimitive numbers of \( \mathbb{A}(\sqrt{5}) \) are the rational numbers.

4. **Integers of \( \mathbb{A}(\sqrt{5}) \).**

Of the imprimitive numbers of \( \mathbb{A}(\sqrt{5}) \) only the rational integers are integers of \( \mathbb{A}(\sqrt{5}) \).

Let \( \beta = a + b\sqrt{5} \) be an integer of \( \mathbb{A}(\sqrt{5}) \). Then \( \beta \sqrt{5} \) is also an integer of \( \mathbb{A}(\sqrt{5}) \). The rank equations of \( \beta \), and \( \beta \sqrt{5} \) are

\[
x^2 - 2ax + a^2 - 5b^2 = 0,
\]

and

\[
x^2 - 10a_1x + 25b_1^2 - 5a_2^2 = 0,
\]

respectively. From 3) and 4),

\[
a_1 = m, \quad a_2 = n
\]

That is,

\[
\begin{bmatrix}
a_1 = \frac{m}{2} \\
b_1 = \frac{n}{10}
\end{bmatrix}
\]

Substituting in 3),
Therefore \( \frac{m^2 - n^2}{4} \) is a rational integer, and we have

\[
5 \frac{m^2 - n^2}{4} \equiv 0 \mod 5
\]

\[
\therefore n^2 \equiv 0 \mod 5 \text{ and } n \equiv 0 \mod 5.
\]

Let \( n = k^5 \). Then \( m^2 - 5k^2 \equiv 0, \mod 4 \); i.e., \( m^2 - k^2 \equiv 0 \mod 4 \)

since \( 5 \equiv 1 \mod 4 \). Therefore \( m = k \mod 2 \). Hence \( m \) and \( k \)

are both odd or both even. But \( n = 5k \), and \( a = \frac{n}{5} \), \( b = \frac{k}{5} = \frac{1}{2} \).

Hence every integer of \( \mathbb{Z} \sqrt{5} \) is of the form

\[
\beta = \frac{a + b \sqrt{5}}{2}
\]

where \( a \) and \( b \) are both odd or both even.

5. Basis of \( \mathbb{Z} \sqrt{5} \).

The integers of \( \mathbb{Z} \sqrt{5} \) are of the form \( \frac{a + b \sqrt{5}}{2} \) where \( a \)

and \( b \) are both odd or both even. Hence \( 1 \) and \( \sqrt{5} \) are not a

basis of \( \mathbb{Z} \sqrt{5} \), but we may prove that \( 1 \) and \( \frac{1 + \sqrt{5}}{2} \), which

are integers of \( \mathbb{Z} \sqrt{5} \), form a basis of \( \mathbb{Z} \sqrt{5} \). To do this,

let \( \alpha = \frac{a + b \sqrt{5}}{2} \) be an integer of \( \mathbb{Z} \sqrt{5} \) and suppose

\[
\alpha = x + \frac{1 + \sqrt{5}}{2}.
\]

Then

\[
x + \frac{\sqrt{5}}{2} = \frac{a}{2}
\]

and

\[
\frac{\sqrt{5}}{2} = \frac{b}{2}.
\]

Therefore \( y = b \), a rational integer; and \( x = \frac{a}{2} - \frac{b}{2} \), a rational-

al integer since \( a \) and \( b \) are both odd or both even.

Hence, every integer \( \alpha \) of \( \mathbb{Z} \sqrt{5} \) can be expressed in

the form

\[
\alpha = x + y \frac{1 + \sqrt{5}}{2}
\]

where \( x \) and \( y \) are rational integers. Therefore \( 1 \) and \( \frac{1 + \sqrt{5}}{2} \)
are a basis of \( \mathbf{k}(\sqrt{5}) \).

A theorem similar to that stated in Part I, Art. 5, for \( \mathbf{k}(\sqrt{2}) \) holds for \( \mathbf{k}(\sqrt{5}) \).

6. The Discriminant of \( \mathbf{k}(\sqrt{5}) \).

The discriminant of \( \mathbf{k}(\sqrt{5}) \) is

\[
d = \left| \begin{array}{cc} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{array} \right|^2 = 5.
\]

7. The Conjugate and Norm of the Integers of \( \mathbf{k}(\sqrt{5}) \).

Let \( \omega \) and \( \omega' \), where \( \omega = \frac{1+\sqrt{5}}{2} \), be a basis of \( \mathbf{k}(\sqrt{5}) \). Then \( \omega' = \frac{1-\sqrt{5}}{2} \), and \( \omega + \omega' = 1 \), \( \omega \omega' = -1 \). Hence \( \omega \) satisfies the equation \( x^2 - x - 1 = 0 \).

Let \( \beta = a + b \omega \) be an integer of \( \mathbf{k}(\sqrt{5}) \). Then

\[
\beta' = a + b \omega' = a + b(1 - \omega),
\]
and

\[
n[\beta] = (a + b \omega)(a + b(1 - \omega)) = a^2 + ab + b^2 \omega - b^2 \omega^2 = a^2 + ab + b^2 \omega - b^2 (1 + \omega).
\]

i.e., \( n[\beta] = a^2 + ab - b^2 \), a rational integer since \( a \) and \( b \) are rational integers.

8. Divisibility of Integers of \( \mathbf{k}(\sqrt{5}) \).

An integer \( \alpha \) of \( \mathbf{k}(\sqrt{5}) \) is said to be divisible by an integer \( \beta \) of \( \mathbf{k}(\sqrt{5}) \) if there exists an integer \( \gamma \) of \( \mathbf{k}(\sqrt{5}) \) such that

\[
\alpha = \beta \gamma.
\]

Thus \( 2 + 2\sqrt{5} \) is divisible by \( 3 - \sqrt{5} \) since...
9. The Units of $\mathbb{A}(\sqrt{5})$, Associated Integers.

The norm of every integer of $\mathbb{A}(\sqrt{5})$ which is a unit is $\pm 1$. Hence, every integer of the second degree which is a unit, satisfies an equation of the form

$$x^2 + ax \pm 1 = 0.$$  

To find the integers different from $\pm 1$ which are units of the realm, let $a$ take on the values $\pm 1, \pm 2, \pm 3, \ldots$.

If $a = \pm 1$, equation 6) becomes either

$$x^2 \pm x + 1 = 0$$

and has the solutions $x = \frac{-1 \pm \sqrt{3}}{2}$, which are not integers of $\mathbb{A}(\sqrt{5})$; or else

$$x^2 \pm x - 1 = 0,$$

and has the solutions $x = \frac{-1 \pm \sqrt{5}}{2}$, which are integers and units of $\mathbb{A}(\sqrt{5})$. When $a = \pm 2, \pm 3$, etc., other units of $\mathbb{A}(\sqrt{5})$ may be determined in a similar way.

Evidently $\frac{1 + \sqrt{5}}{2}$ is the smallest unit greater than 1. Theorem. All units of $\mathbb{A}(\sqrt{5})$ have the form $\pm \left(\frac{1 + \sqrt{5}}{2}\right)^n$, where $n$ is a positive or negative rational integer, or 0.

Let $\epsilon = \frac{1 + \sqrt{5}}{2}$. Then every number of the form $\epsilon^n$ where $n$ is a positive rational integer, is a unit of $\mathbb{A}(\sqrt{5})$, for $n \epsilon^n = n(\epsilon^n) = (-1)^n = 1 \epsilon^{m-1}$.

Also $\epsilon^{-n} = 1$, and hence $\epsilon^{-n}$ is a unit of $\mathbb{A}(\sqrt{5})$. If $p$ and $q$ are any two distinct positive or negative rational integers, then we have $\epsilon^p \neq \pm \epsilon^q$. For, suppose $p > q$, and $\epsilon^q = \pm \epsilon^q$. Then

$$\epsilon^{p-q} = \pm 1.$$
which is impossible since \( \varepsilon > 1 \).

Hence every number of the form \( \varepsilon^n \) where \( n \) is a positive or negative rational integer, is a unit of \( \mathbb{A}(\sqrt{\alpha}) \), and any two distinct values of \( n \) give distinct values of \( \varepsilon^n \); i.e., \( \mathbb{A}(\sqrt{\alpha}) \) has an infinite number of units.

We have now to show that if \( \eta \) is a unit of \( \mathbb{A}(\sqrt{\alpha}) \), then \( \eta = \pm \varepsilon^n \), where \( n \) is a positive or negative rational integer or 0.

Since, if \( \eta \) is a unit, \( \eta', -\eta, \eta' \) are units, we need consider only the case in which \( \eta \) is of the form \( a + b\sqrt{\alpha} \), where \( a > 0, b \geq 0 \).

Then \( \eta \geq 1 \) and either
\[
\eta = \varepsilon^n, \quad n \geq 0
\]
or
\[
\varepsilon^n \leq \eta \leq \varepsilon^{n+1}
\]
That is,
\[
\varepsilon^n \leq \eta \leq \varepsilon^{n+1}.
\]

Let \( \frac{\eta}{\varepsilon^n} = \zeta \), a unit, since \( \eta \) and \( \varepsilon^n \) are units. Then, from 7),
\[
1 \leq \zeta \leq \varepsilon.
\]

But the relation 8) cannot hold, since \( \varepsilon \) is the smallest unit \( > 1 \). Therefore \( \zeta = \varepsilon \), and \( \eta = \varepsilon^n \). Then \( -\eta = -\varepsilon^n \),
\[
\eta' = (\varepsilon^n)' = (\varepsilon')^n = (\pm 1)^n = \pm \varepsilon^{-n}, \quad \text{and} \quad -\eta' = \pm \varepsilon^{-n}.
\]

Hence if \( \eta \) is a unit of \( \mathbb{A}(\sqrt{\alpha}) \), \( \eta = \pm \varepsilon^n \), where \( \varepsilon = \frac{1 + \sqrt{\alpha}}{2} \), and is called the fundamental unit of the realm.
Two integers of \( \mathbb{A}(\sqrt{5}) \), differing only in a unit factor, are said to be associated. The associates of any integer \( \alpha \) of \( \mathbb{A}(\sqrt{5}) \), are therefore \( \pm \epsilon^n \delta \) where \( n \) is zero, or any positive or negative rational integer.

10. Prime Numbers of \( \mathbb{A}(\sqrt{5}) \).

The definition of a prime number of \( \mathbb{A}(\sqrt{5}) \), is identical with that given for \( \mathbb{A}(\sqrt{2}) \).

To determine whether or not \( \alpha \) is a prime number of \( \mathbb{A}(\sqrt{5}) \), we proceed as follows:

Let

\[
2 = (a + b\omega)(c + d\omega)
\]

where \( a, b, c, d \) are rational integers and \( \omega = \frac{1 + \sqrt{5}}{2} \).

Then

\[
\alpha = (a^2 + ab - b^2)(c^2 + cd - d^2)
\]

Therefore, either

9) \[
\begin{align*}
2 &= a^2 + ab - b^2 \\
2 &= c^2 + cd - d^2
\end{align*}
\]

or

10) \[
\begin{align*}
1 &= a^2 + ab - b^2 \\
4 &= c^2 + cd - d^2
\end{align*}
\]

Only 10) has solutions. Hence \( \alpha \) is a prime.

11. The Unique Factorization Theorem for \( \mathbb{A}(\sqrt{5}) \).

The Theorems stated in Part I, Art. 10, for \( \mathbb{A}(\sqrt{2}) \), hold for \( \mathbb{A}(\sqrt{5}) \) when we replace \( n[\alpha] \) by \( |n[\alpha]| \), where \( \alpha \) is any integer of \( \mathbb{A}(\sqrt{5}) \).
12. **Rational Prime Factors of Norms of Integers of \( \mathbb{A}(\sqrt{S}) \)**

**Theorem.** A rational integer which may be represented by the norm of an integer of the realm \( \mathbb{A}(\sqrt{S}) \), i.e., by the form 

\[ a^2 + a \theta - \theta^2, \]

has its rational prime factors either (a) primes of the realm \( \mathbb{A}(\sqrt{S}) \), or (b) norms of primes of the realm. In case (a), these primes enter to even powers, and in case (b), the primes are themselves represented by the form \( a^2 + a \theta - \theta^2 \).

The proof is identical with that given for the corresponding theorem for \( \mathbb{A}(\sqrt{-2}) \), in Part I, Art. 11.

13. **Representation by the Binary Quadratic Form** \( a^2 + a \theta - \theta^2 \)

**Lemma:** The norm of a prime of \( \mathbb{A}(\sqrt{S}) \), not associated with a rational prime, is either \( \pm S \), or a rational prime of the form \( S \pm 1 \). The norm of a prime of \( \mathbb{A}(\sqrt{S}) \) which is associated with a rational prime is the square of the rational prime, and is of the form \( S \pm 1 \). Rational primes of the forms \( S \pm 2 \) are primes of \( \mathbb{A}(\sqrt{S}) \). Every rational prime of the form \( S \pm 1 \) is factorable into two conjugate primes of \( \mathbb{A}(\sqrt{S}) \) and so is the norm of a prime of \( \mathbb{A}(\sqrt{S}) \).

We notice that 

\[ n \left[ \pm e \left( 2 + \frac{1 + \sqrt{S}}{2} \right) \right] = \pm S, \]

where \( e = \frac{1 + \sqrt{S}}{2} \), and \( n \) is any positive or negative rational integer or zero. Hence \( \pm S \) and \( -S \) can each be factorized into two conjugate primes of \( \mathbb{A}(\sqrt{S}) \), and so are not primes of \( \mathbb{A}(\sqrt{S}) \), but are the norms of primes of \( \mathbb{A}(\sqrt{S}) \).

Let \( \theta = a + \frac{1 + \sqrt{S}}{2} \) be a prime of \( \mathbb{A}(\sqrt{S}) \), which is not associated with a rational prime, and consider the case in
which \( n \neq \pm 5 \). Then

\[
\begin{align*}
\eta[n] &= a^2 + at - b^2 \\
\end{align*}
\]

where \( p \) is a unique rational prime, since every prime of \( \mathbb{A}(\sqrt{5}) \) divides one, and only one, rational prime. But \( p = \pm 5 \), and so we have \( p \equiv \pm 1 \), or \( \pm 2 \mod 5 \). Therefore

11) \( a^2 + at - b^2 \equiv 1 \mod 5 \), or

12) \( a^2 + at - b^2 \equiv 4 \mod 5 \), or

13) \( a^2 + at - b^2 \equiv 2 \mod 5 \), or

14) \( a^2 + at - b^2 \equiv 3 \mod 5 \).

The congruences 11) and 12) have solutions, but 13) and 14) have no solution. Hence \( \eta[n] \) is a rational prime of the form \( 5n \pm 1 \).

Let \( \pi \) be a prime of \( \mathbb{A}(\sqrt{5}) \), which is associated with a rational prime, \( \rho \), say. Then \( \pi = \pm \sqrt{5} \), where \( \epsilon = 1 + \frac{\sqrt{5}}{2} \) and \( n \) is any positive or negative rational integer or zero. Hence \( \eta[n] = \pm \pi^2 \), and we have \( \eta[n] \equiv \pm 1 \mod 5 \).

Rational primes of the form \( 5n \pm 2 \) are primes of \( \mathbb{A}(\sqrt{5}) \), for a rational prime is factorable into two conjugate primes of \( \mathbb{A}(\sqrt{5}) \) only if it is 5, or of the form \( 5n \pm 1 \).

It remains to show that all primes of the form \( 5n \pm 1 \) are factorable into two conjugate primes of \( \mathbb{A}(\sqrt{5}) \). In proof, if \( p \equiv \pm 1 \mod 5 \), then the congruence \( x^2 \equiv 5 \mod p \) has solutions, since 5 is a quadratic residue of all primes of the forms \( 5n \pm 1 \). Let \( a \) be a root. Then \( a^2 \equiv 5 \mod p \), and

\[
(a + \sqrt{5}x - a - \sqrt{5}) = 0 \mod p.
\]

But \( a + \sqrt{5} \) and \( a - \sqrt{5} \) are integers of \( \mathbb{A}(\sqrt{5}) \). Therefore, if \( p \) is a prime of \( \mathbb{A}(\sqrt{5}) \), \( p \) must divide either \( a + \sqrt{5} \) or \( a - \sqrt{5} \).
If

\[ a \pm b \sqrt{c} = \rho \left( \frac{\zeta \pm \mu \sqrt{c}}{\eta} \right) \]

where \[ \frac{\zeta \pm \mu \sqrt{c}}{\eta} \] is an integer of \[ \mathbb{R}(\sqrt{c}) \], then

\[ \pm 1 = \frac{p \rho}{\zeta \pm \mu \sqrt{c}}. \]

Hence \( d \equiv 0 \mod 2 \), since \( p \) and \( \alpha \) are rational integers, and therefore \( \rho \) is a divisor of \( \lambda \), which is impossible. Hence \( \rho \) is not a prime of \( \mathbb{R}(\sqrt{c}) \), but is factorable into two conjugate primes of \( \mathbb{R}(\sqrt{c}) \), and so is the norm of a prime of \( \mathbb{R}(\sqrt{c}) \).

The following Theorem on representation by the binary quadratic form \( a^2 + a \beta - \beta^2 \) is an immediate consequence of the Lemma and the Theorem of Art. 12.

**Theorem.** The binary quadratic form \( a^2 + a \beta - \beta^2 \) represents \( \pm 1 \), and all rational primes of the forms \( 6n \pm 1 \), and all rational integers which are products of primes of these forms and even powers of primes of the forms \( 6n \pm 2 \). In the latter case, the primes \( 6n \pm 2 \) divide both \( a \) and \( \beta \). The form \( a^2 + a \beta - \beta^2 \) cannot represent rational primes of the forms \( 6n \pm 2 \), or any rational integer which contains an odd power of a prime of one of these forms.

14. The Diophantine Equations: \[ x^2 + xy - y^2 = \pm 1, \]

\[ x^2 + xy - y^2 = \pm \rho. \]

To find rational integral values of \( x \) and \( y \) which satisfy the equation \( x^2 + xy - y^2 = \rho \), where \( \rho \) is a positive integer, we have to find an integer, \( \alpha \), of \( \mathbb{R}(\sqrt{c}) \), whose norm is \( \rho \). But \( n[\alpha] = n[\alpha \epsilon^{2d}] \), where \( \epsilon = \frac{1 + \sqrt{c}}{2} \), and \( \epsilon \) is any positive or negative rational integer, or zero. Let
Then \( x = \pm a, \ y = \pm \ell \), are solutions. Also, \( n[l^2] = n[l^4] \). Let \( \ell^2 \ell' = a_1 + b_1 \frac{1 + \sqrt{5}}{2} \). Then \( x = \pm a_2, \ y = \pm \ell' \), are solutions of the equation \( x^2 + xy - y^2 = -\ell \). All solutions of the equations \( x^2 + xy - y^2 = \pm \ell, \ \ell > 0 \), are obtained by letting \( \ell \) range over all positive and negative rational integers and \( 0 \). Since no two powers of \( \ell \) are equal, it follows that the number of solutions of each equation is infinite.

Consider, first, the equations

i) \[ x^2 + xy - y^2 = 1, \]

and

ii) \[ x^2 + xy - y^2 = -1. \]

The norm of an integer, \( \alpha \), of \( \mathbb{A} \) is \( \pm 1 \), if, and only if, \( \alpha \) is a unit. If \( n[\alpha] = +1 \), \( \alpha = \pm \sqrt{5} \). Let \( \alpha = a + \ell \frac{1 + \sqrt{5}}{2} \). Then \( x = \pm a, \ y = \pm \ell \), satisfy i). If \( n[\alpha] = -1 \), \( \alpha = \pm \sqrt{5} \). Let \( \alpha = a_2 + b_2 \frac{1 + \sqrt{5}}{2} \). Then \( x = \pm a_2, \ y = \pm \ell' \), satisfy ii).

By letting \( \ell \) range over all positive and negative rational integers and \( 0 \), all solutions of i) and ii) are obtained.

The equations

iii) \[ x^2 + xy - y^2 = p, \]

and

iv) \[ x^2 + xy - y^2 = -p, \]

where \( p \) is a positive rational prime, have solutions if, and only if, \( p = 5 \), or \( p \equiv \pm 1 \mod 5 \). (Theorem, Art. 13). Let \( \alpha \) be an integer of \( \mathbb{A} \) such that \( n[\alpha] = p \), and let \( \ell^2 \ell = a_2 + b_2 \frac{1 + \sqrt{5}}{2} \). Then \( x = \pm a, \ y = \pm \ell \), are solutions of iii). If \( \ell^2 \ell' = a_2 + b_2 \frac{1 + \sqrt{5}}{2} \), then \( x = \pm a_2, \ y = \pm \ell' \), are
solutions of iv). All solutions of iii) and iv) are obtained by letting $l$ range as before.

The equations

\[ x^2 + xy - y^2 = m \]

and

\[ x^2 + xy - y^2 = -m \]

where $m$ is a positive rational integer, have solutions if, and only if,

\[ m = p_1^{a_1} \cdots p_r^{a_r} \cdot \eta_1^{2\alpha_1} \cdots \eta_s^{2\alpha_s} \]

where $p_1, p_2, \cdots, p_r$ are distinct primes of the forms $5n \pm 1$ or $5$; $q_1, q_2, \cdots, q_s$ are distinct primes of the forms $5n \pm 2$, and $\eta_1, \cdots, \eta_s, \xi_1, \cdots, \xi_s$ are positive rational integers. (Theorem, Art. 13). Then if

\[ p_1 = \eta_1 \xi_1, \quad p_2 = \eta_2 \xi_2, \quad \cdots, \quad p_r = \eta_r \xi_r, \]

we have

\[ m = (\eta_1 \xi_1)^a \cdots (\eta_s \xi_s)^a \cdot \eta_1^{2\alpha_1} \cdots \eta_s^{2\alpha_s} \cdot \xi_1^{2\beta_1} \cdots \xi_s^{2\beta_s} \]

\[ = d, d', \text{ say.} \]

By interchanging one or more of the $\eta_i \xi_i$ with their conjugates in 15), we obtain all possible factorizations of $m$ into two conjugate factors. Let $m = d_1 d_2$ be the result of any such interchange, and let $a_j e^{2\theta_j} = a_1 + b_1 + \frac{cf_1}{a}$, and $d_2 e^{2\theta_2} = a_2 + b_2 + \frac{cf_2}{a}$. Then $x = \pm a_1, y = \pm b_1$, are solutions of v) and $x = \pm a_2, y = \pm b_2$ are solutions of vi). All solutions of v) and vi) are then obtained by letting $l = 0$, or any positive or negative rational integer.
1. **The Numbers of the Realm \( \mathbb{A}(\sqrt{-23}) \).**

   The number \( \sqrt{-23} \) is defined by the equation

   \[
   x^2 + 23 = 0.
   \]

   Since \( (\sqrt{-23})^2 = -23 \), every number of \( \mathbb{A}(\sqrt{-23}) \) is of the form

   \[
   \gamma = \frac{a_1 + b_1 \sqrt{-23}}{a_2 + b_2 \sqrt{-23}}.
   \]

   where \( a_1, b_1, a_2, b_2 \) are rational numbers. Rationalizing the denominator, we see that every number of \( \mathbb{A}(\sqrt{-23}) \) is of the form

   \[
   \gamma = a + b \sqrt{-23},
   \]

   where \( a \) and \( b \) are rational numbers.

   The other root of 1) defines the realm \( \mathbb{A}(-\sqrt{-23}) \), conjugate to \( \mathbb{A}(\sqrt{-23}) \), and identical with it.

2. **The Conjugate and Norm of a Number of \( \mathbb{A}(\sqrt{-23}) \).**

   If \( \gamma = a + b \sqrt{-23} \) is a number of \( \mathbb{A}(\sqrt{-23}) \), then

   \[
   \gamma' = a - b \sqrt{-23}
   \]

   is its conjugate.

   The conjugate of a product of two or more numbers of \( \mathbb{A}(\sqrt{-23}) \) is equal to the product of the conjugates of its factors.

   The norm of \( \gamma = a + b \sqrt{-23} \) is

   \[
   n[\gamma] = a^2 + 23b^2.
   \]

   The norm of a product of two or more numbers of \( \mathbb{A}(\sqrt{-23}) \)
is equal to the product of the norms of its factors. The norm of every number of \( A(\sqrt{23}) \) is evidently a positive rational number.

3. **Primitive and Imprimitive Numbers of \( A(\sqrt{23}) \).**

Every number \( \gamma = a + b\sqrt{23} \) of \( A(\sqrt{23}) \) satisfies the equation

\[ x^2 - 2ax + a^2 + 23b^2 = 0 \]

If equation 2) is irreducible, the number \( \gamma \) is said to be a primitive number of \( A(\sqrt{23}) \), and if equation 2) is reducible, \( \gamma \) is said to be an imprimitive number of \( A(\sqrt{23}) \). The imprimitive numbers of \( A(\sqrt{23}) \) are the rational numbers.

4. **Integers of the Realm \( A(\sqrt{23}) \).**

Of the imprimitive numbers of \( A(\sqrt{23}) \) only the rational integers are integers of the realm.

If \( \gamma \) is an integer of \( A(\sqrt{23}) \) it may be shown, as in \( A(\sqrt{3}) \), that \( \gamma \) is of the form

\[ \gamma = a + \frac{b\sqrt{23}}{2} \]

where \( a \) and \( b \) are both odd or both even.

5. **Basis of \( A(\sqrt{23}) \).**

By a method similar to that used in \( A(\sqrt{3}) \), it may be proven that \( 1, \frac{1 + \sqrt{23}}{2} \) are a basis of \( A(\sqrt{23}) \), since every integer of \( A(\sqrt{23}) \) can be put in the form \( a + \frac{b}{2} + \frac{\sqrt{23}}{2} \), where \( a \) and \( b \) are rational integers.

If \( \omega_1 \) and \( \omega_2 \) are a basis of \( A(\sqrt{23}) \), a theorem identical with that stated for \( A(\sqrt{3}) \) holds for \( A(\sqrt{23}) \).
6. The Discriminant of \( \mathbb{K}(\sqrt{-23}) \).

The discriminant of \( \mathbb{K}(\sqrt{-23}) \) is

\[
d = \left| \frac{1 + \sqrt{-23}}{2} \right|^2 = -23.
\]

7. The Conjugate and Norm of an Integer of \( \mathbb{K}(\sqrt{-23}) \).

Let \( \omega \) and \( \omega' \) where \( \omega = \frac{1 + \sqrt{-23}}{2} \) be a basis of \( \mathbb{K}(\sqrt{-23}) \).

Then \( \omega' = \frac{1 - \sqrt{-23}}{2} \), and \( \omega + \omega' = 1 \), \( \omega \omega' = 6 \). Therefore \( \omega \) satisfies the equation \( x^2 - x + 6 = 0 \).

If \( y = a + b\omega \) is an integer of \( \mathbb{K}(\sqrt{-23}) \), then

\[
y' = a + b\omega' = a + 4(1 - \omega),
\]

and

\[
n[y] = (a + b\omega)(a + b(1 - \omega)) = a^2 + a\omega + b^2\omega - 6\omega^2,
\]

\[
= a^2 + ab + b^2 - 6(\omega - 6),
\]

4) \( n[y] = a^2 + ab + b^2 \),

a rational integer, since \( a \) and \( b \) are rational integers.

8. Divisibility of Integers of \( \mathbb{K}(\sqrt{-23}) \).

An integer \( \alpha \) of \( \mathbb{K}(\sqrt{-23}) \) is said to be divisible by an integer \( \beta \) of \( \mathbb{K}(\sqrt{-23}) \) if there exists an integer \( \gamma \) of \( \mathbb{K}(\sqrt{-23}) \) such that \( \alpha = \beta \gamma \).

9. Units and Associated Integers.

To determine the units of \( \mathbb{K}(\sqrt{-23}) \), let \( e = \frac{a + \sqrt{-23}}{2} \) be a unit of \( \mathbb{K}(\sqrt{-23}) \). Then

\[
n[e] = a^2 + 23 - \frac{2}{4} = 1.
\]

Hence \( b = 0 \), \( a = \pm 2 \), and \( e = \pm 1 \).
The units of \( \mathbb{A}(\sqrt{23}) \) are therefore \( +1, -1 \).

Two integers of \( \mathbb{A}(\sqrt{23}) \) which differ only in a unit factor, are said to be associated. The associates of any integer \( y \) of \( \mathbb{A}(\sqrt{23}) \) are, therefore, \( +y \), and \( -y \).

10. **Prime Numbers of \( \mathbb{A}(\sqrt{23}) \).**

An integer of \( \mathbb{A}(\sqrt{23}) \), that is not a unit, and that has no divisors other than its associates and the units, is called a prime number of \( \mathbb{A}(\sqrt{23}) \).

In illustration, to determine whether or not \( \gamma \) is a prime of \( \mathbb{A}(\sqrt{23}) \), we proceed as follows:

Let \( \gamma = \frac{x+y\sqrt{23}}{2}, \frac{u+v\sqrt{23}}{2}, \)

where \( x \) and \( y \) are both odd or both even, and \( u \) and \( v \) are both odd or both even.

Then

\[
\mu \gamma = \frac{x^2+23y^2}{4}, \frac{u^2+23v^2}{4}
\]

We have therefore, either

\[
5) \quad \gamma = \frac{x^2+23y^2}{4}, \quad \gamma = \frac{u^2+23v^2}{4}
\]

or

\[
6) \quad \mu \gamma = \frac{x^2+23y^2}{4}, \quad l = \frac{u^2+23v^2}{4}
\]

From 5), \( 2\beta = x^2+23y^2 \) and \( 2\beta = u^2+23v^2 \). Neither of these equations have solutions, which are rational integers. From 6), \( 196 = x^2+23y^2 \) and \( l = u^2+23v^2 \). The solutions of these equations are \( y = 0, x = 14, v = 0, u = 2 \).

Hence \( \gamma \) is a prime number of \( \mathbb{A}(\sqrt{23}) \). Similarly, \( 2 + \sqrt{23} \) may be shown to be a prime number of \( \mathbb{A}(\sqrt{23}) \).
11. The Unique Factorization Theorem in \( \mathbb{A}(\sqrt{-23}) \).

The three theorems upon which the proof of the Unique Factorization Theorem depended in \( \mathbb{A}(\sqrt{-5}) \) and \( \mathbb{A}(\sqrt{5}) \), do not always hold in \( \mathbb{A}(\sqrt{-23}) \).

For \( \mathbb{A}(\sqrt{-23}) \), Theorem A of \( \mathbb{A}(\sqrt{-2}) \) and \( \mathbb{A}(\sqrt{5}) \) would be as follows:

If \( \alpha \) is an integer of \( \mathbb{A}(\sqrt{-23}) \) and \( \beta \) is any integer of \( \mathbb{A}(\sqrt{-23}) \) different from 0, there exists an integer \( \mu \) of \( \mathbb{A}(\sqrt{-23}) \) such that \( \eta [\alpha - \mu \beta] < \eta [\beta] \).

But if \( \alpha = 1 + \sqrt{-23} \) and \( \beta = 2 \),

\[
\frac{\alpha}{\beta} = \frac{1}{2} + \frac{1}{2} \sqrt{-23}.
\]

Let \( \mu = \frac{x + \sqrt{23}}{2} \) be the required integer of \( \mathbb{A}(\sqrt{-23}) \).

\[
\frac{\alpha}{\beta} - \mu = \left(\frac{1}{2} - \frac{\sqrt{23}}{2}\right) + \left(\frac{1}{2} - \frac{\sqrt{23}}{2}\right) \sqrt{-23}.
\]

\[
\eta \left[\frac{\alpha}{\beta} - \mu\right] = \left(\frac{1}{2} - \frac{\sqrt{23}}{2}\right)^2 + \left(\frac{1}{2} - \frac{\sqrt{23}}{2}\right)^2 \sqrt{-23}.
\]

For all integral values of \( x \), including 0, the term \( 23(\frac{1}{2} - \frac{\sqrt{23}}{2})^2 \) is itself > 1. Hence \( \eta \left[\frac{\alpha}{\beta} - \mu\right] > 1 \), and \( \eta [\alpha - \mu \beta] > \eta [\beta] \).

That is, we cannot find an integer \( \mu \) such that, for \( \alpha = 1 + \sqrt{-23} \), and \( \beta = 2, \eta [\alpha - \mu \beta] < \eta [\beta] \).

Theorem B for \( \mathbb{A}(\sqrt{-23}) \) would be:

If \( \alpha \) and \( \beta \) are any two integers of \( \mathbb{A}(\sqrt{-23}) \) prime to each other, there exist two integers \( \xi \) and \( \eta \) of \( \mathbb{A}(\sqrt{-23}) \) such that \( \alpha \xi + \beta \eta = 1 \).

Let \( \alpha = 3 \) and \( \beta = 2 + \sqrt{-23} \), and let \( \xi = \frac{x + \sqrt{23}}{2} \), and \( \eta = \frac{4 + \sqrt{23}}{2} \).

Suppose \( 3(x + \frac{\sqrt{23}}{2}) + (2 + \sqrt{23})(\frac{4 + \sqrt{23}}{2}) = 1 \).

Then

\[
3x + 2u - 23v = 2
\]

and

\[
y + u + 2v = 0.
\]
Multiplying equation 8) by 2, and subtracting the result from 7) we obtain

9) \[ 3x - 6y - 2\sqrt{23} z = 2. \]

The left member of 9) is divisible by 3 and the right member only by 2. Hence equation 9) has no solutions in rational integers. That is, we cannot find integers \( \xi \) and \( \eta \) of \( \mathcal{O}(\sqrt{-23}) \) such that, for \( x = \xi \), and \( y = 2 + \sqrt{-23}, \ \xi \xi + \eta \eta = 1 \).

Theorem 3 for \( \mathcal{O}(\sqrt{-23}) \) would be:

If the product of two integers, \( \xi \) and \( \eta \) of \( \mathcal{O}(\sqrt{-23}) \) is divisible by a prime number \( \pi \), at least one of the integers is divisible by \( \pi \).

But \( 2\eta = 3 = (2 + \sqrt{-23})(2 - \sqrt{-23}) \), and it may be shown that \( 3, 2 + \sqrt{-23}, 2 - \sqrt{-23} \) are all primes of \( \mathcal{O}(\sqrt{-23}) \). Also the factors of one product are not associated with the factors of the other. Thus, \( 2\eta \) can be represented in two ways as the product of prime factors, and we see that the Unique Factorization Theorem does not hold for \( \mathcal{O}(\sqrt{-23}) \).

By the introduction of ideal numbers into \( \mathcal{O}(\sqrt{-23}) \), the Unique Factorization Theorem may be restored for the realm \( \mathcal{O}(\sqrt{-23}) \), when factorization is expressed in terms of prime ideal factors.

12. **Ideals of \( \mathcal{O}(\sqrt{-23}) \).**

Let \( \alpha, \alpha, \ldots, \alpha \) be integers of \( \mathcal{O}(\sqrt{-23}) \). Then the infinite system of integers of the form \( \sum_{i=1}^{\infty} \eta_i \alpha_i \), where each \( \eta_i \) is an integer of \( \mathcal{O}(\sqrt{-23}) \) is called an ideal \( \mathfrak{a} \) of \( \mathcal{O}(\sqrt{-23}) \) and we write \( \mathfrak{a} = (\alpha, \alpha, \ldots, \alpha) \).
The integers \( a_1, a_2, \ldots, a_n \) are said to define the ideal \( \mathfrak{a} \), and \((a_1, a_2, \ldots, a_n)\) is called the symbol of the ideal \( \mathfrak{a} \).

The numbers of the infinite system of integers \( \sum \eta \cdot a_i \) which constitutes the ideal \( \mathfrak{a} \) are called the numbers of the ideal.

Any integer of \( \mathbb{A}(\sqrt{-23}) \) which is a linear combination of the numbers in the symbol of \( \mathfrak{a} \), may be introduced into the symbol of \( \mathfrak{a} \), and any number in the symbol which is a linear combination of the remaining numbers in the symbol, may be omitted from the symbol.

If \( n = 1, \mathfrak{a} = (a) \), and is called a principal ideal. All numbers of \( \mathfrak{a} \) are then of the form \( \eta a \), where \( \eta \) is an integer of \( \mathbb{A}(\sqrt{-23}) \).

If \( \mathfrak{a} = (a_1, a_2, \ldots, a_n) \) is an ideal of \( \mathbb{A}(\sqrt{-23}) \), the ideal \( \mathfrak{a}' = (a'_1, a'_2, \ldots, a'_n) \) whose numbers are the conjugates of the numbers of \( \mathfrak{a} \), is called the conjugate of \( \mathfrak{a} \).

13. Equality, Multiplication and Division of Ideals of \( \mathbb{A}(\sqrt{-23}) \)

Two ideals, \( \mathfrak{a} = (a_1, a_2, \ldots, a_n) \), \( \mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_g) \), of \( \mathbb{A}(\sqrt{-23}) \) are said to be equal, and we write \( \mathfrak{a} = \mathfrak{b} \), if every number of \( \mathfrak{a} \) is a number of \( \mathfrak{b} \), and every number of \( \mathfrak{b} \) is a number of \( \mathfrak{a} \); i.e., if

\[
a_i = \sum_{j=1}^{g} \eta_{ij} \beta_j \quad i = 1, \ldots, n,
\]

and

\[
\beta_j = \sum_{i=1}^{n} \eta_{ij} a_i \quad j = 1, \ldots, g,
\]

where \( \eta_{ij} \) and \( \eta_{ji} \) are integers of \( \mathbb{A}(\sqrt{-23}) \).
If \( A = (a_1, a_2, \ldots, a_n) \) and \( B = (\beta_1, \beta_2, \ldots, \beta_q) \) are two ideals of \( \mathbb{Z}/23\mathbb{Z} \), the ideal defined by all possible products of a number of \( A \) by a number of \( B \) is called the product of \( A \) and \( B \). That is,
\[
A B = (a_1 \beta_1, a_2 \beta_2, \ldots, a_n \beta_q, a_1 \beta_2, \ldots, a_n \beta_q).
\]

An ideal \( A \) of \( \mathbb{Z}/23\mathbb{Z} \) is said to be divisible by an ideal \( B \) of \( \mathbb{Z}/23\mathbb{Z} \) if there exists an ideal \( C \) of \( \mathbb{Z}/23\mathbb{Z} \) such that \( A = B C \).

**Theorem.** If an ideal \( A = (a_1, a_2, \ldots, a_n) \) of \( \mathbb{Z}/23\mathbb{Z} \) is divisible by an ideal \( B = (\beta_1, \beta_2, \ldots, \beta_q) \) of \( \mathbb{Z}/23\mathbb{Z} \) then all numbers of \( A \) belong to \( B \).

Let \( A = B C \), where \( C = (\gamma, \gamma_2, \ldots, \gamma_p) \) is an ideal of \( \mathbb{Z}/23\mathbb{Z} \). Then
\[
A = (\beta_1 \gamma, \beta_2, \ldots, \beta_q \gamma_1, \ldots, \beta_q \gamma_p).
\]
But the numbers \( \beta, \gamma, \beta, \gamma_2, \ldots, \beta_q \gamma_p \) defining \( A \) are numbers of \( B \). Hence all numbers of \( A \) are numbers of \( B \).

14. **The Unit Ideal.** **Prime Ideals.**

Let \( A = (a_1, a_2, \ldots, a_n) \). Then \( (1)A = A(1) = (a_1, \ldots, a_n) = A \).

Hence every ideal \( A \) is divisible by the ideal \( (1) \).

Let \( d = (d_1, d_2, \ldots, d_p) \) be an ideal of \( \mathbb{Z}/23\mathbb{Z} \) which divides every ideal of \( \mathbb{Z}/23\mathbb{Z} \). Then \( d \) divides \( (1) \).

Let \( l = d m \) where \( m = (\mu, \mu_2, \ldots, \mu_p) \).

Then
\[
(1) = (d_1, \ldots, d_p)(\mu, \ldots, \mu_p)
\]
\[
\therefore l = \frac{d_1}{\mu_1} \ldots \frac{d_p}{\mu_p} f_1 \ldots f_p
\]
where \( f_{ij} \) is an integer of \( \mathbb{Z}/23\mathbb{Z} \).
where \( \eta_i \) is an integer of \( \mathcal{A}(\sqrt{-23}) \). Hence \( \phi \) is a number of \( \phi \). Therefore \( \phi = (\eta_1, \eta_2, \ldots, \eta_n) = (1) \).

Hence the ideal \( (1) \) is the only ideal which divides every ideal of \( \mathcal{A}(\sqrt{-23}) \). The ideal \( (1) \) is therefore called the unit ideal of \( \mathcal{A}(\sqrt{-23}) \). It contains every integer of \( \mathcal{A}(\sqrt{-23}) \).

An ideal of \( \mathcal{A}(\sqrt{-23}) \), not the unit ideal, and divisible only by itself and the unit ideal, is called a prime ideal of \( \mathcal{A}(\sqrt{-23}) \).

Two ideals of \( \mathcal{A}(\sqrt{-23}) \) are said to be prime to each other, or relatively prime, if they have no common divisor except \( (1) \). Two integers \( \alpha \) and \( \beta \) of \( \mathcal{A}(\sqrt{-23}) \) are said to be prime to each other if the principal ideals \( (\alpha) \) and \( (\beta) \) are prime to each other.

15. **The Unique Factorization Theorem for** \( \mathcal{A}(\sqrt{-23}) \)** in Terms of **Ideal Factors.**

The proof of the Unique Factorization Theorem for the ideals of the realm \( \mathcal{A}(\sqrt{-23}) \) depends upon several other theorems relating to the ideals of the realm. The proofs of these theorems and of the Unique Factorization Theorem itself, for the general quadratic realm, are given in Reid, "The Elements of the Theory of Algebraic Numbers". Hence only a statement of the theorems will be given.

**Theorem 1.** There exist in every ideal \( \mathfrak{a} \) of a quadratic realm, two numbers, \( \eta_1, \ldots, \eta_n \), such that every number of the ideal can be expressed in the form

\[
\mathfrak{a} = \eta_1 \mathfrak{a} + \ldots + \eta_n \mathfrak{a}.
\]
where \( l \) and \( l_2 \) are rational integers.

**Theorem 2.** An ideal \( \mathfrak{a} \) is divisible by only a finite number of distinct ideals.

**Theorem 3.** If the coefficients \( a_1, a_2, \beta_1, \beta_2 \) of the two rational integral functions of \( x \),

\[
\phi(x) = a_1 x + a_2 \quad \text{and} \quad \psi(x) = \beta_1 x + \beta_2
\]

are integers of \( \mathbb{R}(\sqrt{-m}) \) and \( \omega \), an integer of \( \mathbb{R}(\sqrt{-m}) \), divides each of the coefficients \( \gamma_1, \gamma_2, \gamma_3 \) of the product of the two functions,

\[
F(x) = \phi(x) \cdot \psi(x) = (a_1 \beta_1 + a_2 \beta_2) x^2 + (a_1 \beta_2 + a_2 \beta_1) x + a_1 a_2
\]

then each of the numbers \( \alpha, \beta_1, \alpha \beta_1, \alpha \beta_2, \alpha \beta_3 \) is divisible by \( \omega \).

**Theorem 4.** For every ideal \( \mathfrak{a} \) of a quadratic realm there exists an ideal \( \mathfrak{b} \) of the realm such that the product \( \mathfrak{a} \mathfrak{b} \) is a principal ideal.

**Theorem 5.** If \( \mathfrak{a}, \mathfrak{b} \) and \( \mathfrak{c} \) are ideals and \( \mathfrak{a} \mathfrak{b} = \mathfrak{b} \mathfrak{c} \), then \( \mathfrak{a} = \mathfrak{b} \).

**Theorem 6.** If all numbers of an ideal \( \mathfrak{a} \) belong to an ideal \( \mathfrak{c} \), \( \mathfrak{a} \mathfrak{c} \) is divisible by \( \mathfrak{c} \).

**Theorem 7.** If \( \mathfrak{a} \) and \( \mathfrak{b} \) are any two ideals prime to each other, there exists a number \( \alpha \) of \( \mathfrak{a} \) and a number \( \beta \) of \( \mathfrak{b} \) such that \( \alpha + \beta = 1 \).

**Theorem 8.** If the product of two ideals, \( \mathfrak{a} \) and \( \mathfrak{b} \), is divisible by a prime ideal \( \mathfrak{p} \), at least one of the ideals is divisible by \( \mathfrak{p} \).
Cor. 1. If the product of any number of ideals is divisible by a prime ideal \( \mathfrak{p} \), at least one of the ideals is divisible by \( \mathfrak{p} \).

Cor. 2. If neither of two ideals is divisible by a prime ideal \( \mathfrak{p} \), their product is not divisible by \( \mathfrak{p} \).

Cor. 3. If the product of two ideals \( \mathfrak{a} \) and \( \mathfrak{b} \), is divisible by an ideal \( \mathfrak{j} \), and neither \( \mathfrak{a} \) nor \( \mathfrak{b} \) is divisible by \( \mathfrak{j} \), then \( \mathfrak{j} \) is a composite ideal.

The Unique Factorization Theorem for Ideals is proven by use of the above theorems. This fundamental theorem reads: Every ideal can be represented in one, and only one, way as the product of prime ideals.

The Unique Factorization Theorem enables us to develop the arithmetic of ideals in a manner analogous to the development of the arithmetic of integers in realms in which factorization is unique. A body of theorems is readily derived, but as these are given in Reid for the general quadratic realm, they will not be repeated here.

We recall that on page 31 we indicated the possibility of more than one factorization into primes of the integer 27 in the realm \( \mathbb{A}(\sqrt{-23}) \). We close the paper by showing that the principal ideal \( (27) \) admits one, and only one, factorization into prime ideals.

We have

\[(27) = (3)^2 = (2 + \sqrt{-23})(2 - \sqrt{-23})\]

But

\[(3) = (3, \frac{1 + \sqrt{-23}}{2})(3, \frac{1 - \sqrt{-23}}{2})\]
where \((3, \frac{1 + \sqrt{-23}}{2})\) and \((3, \frac{1 - \sqrt{-23}}{2})\) are prime ideals of \(\mathbb{A}(\sqrt{-23})\).

\[ (3)^3 = (3, \frac{1 + \sqrt{-23}}{2})(3, \frac{1 - \sqrt{-23}}{2})^3. \]

Also

\[ (2 + \sqrt{-23}) = (3, \frac{1 - \sqrt{-23}}{2})^3 \]

and

\[ (2 - \sqrt{-23}) = (3, \frac{1 + \sqrt{-23}}{2})^3 \]

and

\[ (2 \gamma) = (2 + \sqrt{-23})(2 - \sqrt{-23}) = (3, \frac{1 + \sqrt{-23}}{2})(3, \frac{1 - \sqrt{-23}}{2})^3. \]

That is, \((2 \gamma)\) can be factored in one, and only one, way in \(\mathbb{A}(\sqrt{-23})\) into prime ideal factors.