We find thus Baire's well known theorem to the effect that the limit of a sequence of continuous functions is at most point-wise discontinuous.

In connection with convergent sequences of continuous functions, the saltus function here considered can be related with the *measure of non-uniform convergence* introduced by Hobson and Osgood.* These two functions vanish at the same points, which fact shows, of course, that the above proof of Baire's theorem is not fundamentally distinct from that based on the measure of non-uniform convergence. There is no other relation of equality between the two functions.

COLUMBIA UNIVERSITY.

A NEW METHOD IN DIOPHANTINE ANALYSIS.

BY PROFESSOR L. E. DICKSON.

(Read before the American Mathematical Society March 26, 1921.)

1. *Introduction and Summary.* In the preceding number of this BULLETIN (p. 312) I gave reasons why due caution should be observed toward the literature on the solution of homogeneous equations in integers. The valid knowledge concerning this subject is much less than has been usually admitted. The lack of general methods is even greater than in the subject of non-homogeneous equations. The chief aim of the present paper is to suggest such a method, based on the theory of ideals. The method is applicable in simple cases (§§ 2–4) without introducing ideals.

For the sake of brevity we shall restrict attention to the problem of finding all integral solutions of the equation

$$x_1^2 + ax_2^2 + bx_3^2 = x_4^2,$$

an equation admitted† to be difficult of treatment by any known methods, and previously solved completely in integers only in the single case $a = b = 1$.

Let us write

$$x_4 - x_1 = z, \quad x_4 + x_1 = w.$$

Then from the integral solutions of $ax^2 + by^2 = zw$ we must

* Hobson, loc. cit., p. 484.

† Carmichael, *Diophantine Analysis*, 1915, p. 38.

select those for which $z \equiv w \pmod 2$. The trouble in making such a (simple) selection is avoided when $a = 1$, $b = 4k - 1$, by a reduction* to

$$x^2 + xy + ky^2 = zw.$$

Further, any solution of

$$ax^2 + by^2 = zw$$

yields a solution $X = ax$, $Y = y$, $Z = az$, $W = w$, of $X^2 + abY^2 = ZW$ in which X and Z are divisible by a, and conversely. Hence our problem leads to the canonical equation $N = zw$, where N is $x^2 - my^2$ or $x^2 + xy + ky^2$. We shall see that the theory of algebraic numbers is admirably adapted to the complete solution of $N = zw$ in integers.

2. *Definition of Integral Algebraic Numbers.* Let m be an integer other than 0 and 1, and such that m is not divisible by a perfect square. The numbers $\tau = r + s\sqrt{m}$, where r and s are rational, form a domain of rationality (or field) $R(\sqrt{m})$. Evidently τ and its *conjugate* $\tau' = r - s\sqrt{m}$ are the roots of the equation

$$x^2 - 2rx + r^2 - ms^2 = 0.$$

If the coefficients of this quadratic are all integers, τ and τ' are called *integral algebraic numbers* of $R(\sqrt{m})$. A simple discussion† leads to the following theorem.

THEOREM 1. *The integral algebraic numbers of* $R(\sqrt{m})$ *are* $x + y\theta$, *where* x *and* y *are integers, and where*

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

(1′) $\quad \theta = \frac{1}{2}(1 + \sqrt{m})$, $\theta^2 - \theta + \frac{1}{4}(1 - m) = 0$, *if* $m \equiv 1 \pmod 4$.

The conjugate to $\xi = x + y\theta$ is $\xi' = x + y\theta'$, where $\theta' = -\sqrt{m}$ in case (1), and $\theta' = \frac{1}{2}(1 - \sqrt{m})$ in case (1′). The product $\xi\xi'$ is called the *norm* of ξ and denoted by $N(\xi)$. Hence, in the respective cases,

* Details are given in the writer's address before the International Mathematical Congress at Strasbourg, in which he described the present method for the simplest cases, including the solution, by use of the arithmetic of quaternions (see PROCEEDINGS LONDON MATH. SOC., 1921), of $x^2 + y^2 + \xi^2 + \eta^2 = zw$ and hence of $x_1^2 + \cdots + x_5^2 = x_6^2$.

† See this BULLETIN, vol. 13 (1906–7), p. 350, or any text on algebraic numbers.

(2) or (2′) $N(x+y\theta) = x^2 - my^2$ or $x^2 + xy + \frac{1}{4}(1-m)y^2$.

3. *All Rational Solutions of* $N(x+y\theta) = zw$. If $z \neq 0$, we may write

$$\frac{x}{z} = \frac{a}{c}, \qquad \frac{y}{z} = \frac{b}{c},$$

where a, b, and c are integers without a common factor greater than 1. Then we have

$$\frac{w}{z} = \frac{N(x+y\theta)}{z^2} = N\left(\frac{x}{z} + \frac{y\theta}{z}\right) = N\left(\frac{a+b\theta}{c}\right) = \frac{N(a+b\theta)}{c^2}.$$

If we take $\rho = z/c^2$, where ρ is rational, we obtain

(3) $x = \rho ac, \qquad y = \rho bc, \qquad z = \rho c^2, \qquad w = \rho N(a+b\theta).$

But if $z = 0$, then $N(x+y\theta) = 0$ and $x = y = 0$, and this solution is the case $c = 0$ of (3).

THEOREM 2. *All rational solutions of* $N(x+y\theta) = zw$ *are given by* (3), *where* a, b, c *are integers without a common factor and* ρ *is rational.*

4. *Integral Solutions without the Use of Ideals.* Not all integral solutions of $N(x+y\theta) = zw$ are obtained from (3) by restricting ρ to integral values, as was shown in § 4 of my preceding paper. To obtain further solutions, note that the norm of the product

(4) $$x + y\theta = (a+b\theta)(c+d\theta)$$

of two numbers of our field $R(\theta)$ equals the product of their norms. Hence $N(x+y\theta) = zw$ has the solution

(5) $z = N(c+d\theta), \qquad w = N(a+b\theta), \qquad x, y$ by (4);

or explicitly,

(5$_1$) $x = ac + mbd, \qquad y = ad + bc, \qquad z = c^2 - md^2,$
$w = a^2 - mb^2, \qquad m \equiv 2 \text{ or } 3 \pmod 4;$

(5$_2$) $x = ac + \frac{(m-1)}{4}bd, \qquad y = ad + bc + bd,$

$z = c^2 + cd + \frac{1}{4}(1-m)d^2, \qquad w = a^2 + ab + \frac{1}{4}(1-m)b^2,$

where $m \equiv 1 \pmod 4$.

We shall restrict attention to integral values of a, b, c, and d

without a common factor. The products of the resulting numbers (5) by an arbitrary rational number ρ give all rational solutions of $N(x + y\theta) = zw$, since those products reduce to (3) when $d = 0$.

When the field $R(\theta)$ is such that its integral algebraic numbers $x + y\theta$ obey the laws of divisibility of arithmetic, we shall prove that all integral solutions of $N(x + y\theta) = zw$ are given by the products of the numbers (5) by an arbitrary integer ρ, where a, b, c, and d are integers without a common factor. We have merely to show that when the products of the numbers (5) by an irreducible fraction n/p are integers, so that the numbers (5) are divisible by p, then the quotients are expressible in the same form (5) with new integral parameters in place of a, b, c, and d. It suffices to prove this for the prime factors (equal or distinct) of p, since after each of them has been divided out in turn, p itself has been divided out.

Let therefore p be a prime which divides the four numbers (5). If p divided both d and b, it would divide also c and a, in view of z and w, contrary to the hypothesis that a, b, c, and d have no common factor. By the interchange of a with c and b with d, x and y remain unaltered, while z and w are interchanged. Hence we shall be treating one of two entirely similar cases if we assume that d is not divisible by p.

The prime p divides the product z of $c + d\theta$ and $c + d\theta'$, without dividing either factor. For, if $c + d\theta$ or $c + d\theta' = c + d(\alpha - \theta)$, where $\alpha = 0$ or 1 in the respective cases (1) or (1'), were the product of p by $k + l\theta$, where k and l are integers, then $\pm d = pl$, whereas d is not divisible by p. Since the laws of divisibility of arithmetic were assumed to hold for the integral numbers of $R(\theta)$, it follows that p is not an algebraic prime, but decomposes into $p = \pi\pi'$, where π and π' are conjugate primes.* By choice of the notation between π and π', we may assume that π is the one of the two prime factors π and π' of p which divides $c + d\theta$, and we may write

$$(6) \qquad c + d\theta = \pi(C + D\theta), \qquad z = pN(C + D\theta),$$

where C and D are integers. Since x and y are divisible by p,

* Otherwise, p would be a product of three integral algebraic numbers, no one a unit, and its norm p^2 would be a product of three integers no one of which is ± 1. A unit u is an integral algebraic number which divides unity, whence $N(u) = \pm 1$ ($+1$ if m is negative).

and $c + d\theta$ is divisible by π, but not by the product $p = \pi\pi'$, it follows from (4) that $a + b\theta$ is divisible by π', i.e.

$$(7) \qquad a + b\theta = \pi'(A + B\theta), \qquad w = pN(A + B\theta),$$

where A and B are integers.

Comparing the product of (6) and (7) with (4), we have

$$x + y\theta = p(\xi + \eta\theta), \qquad \xi + \eta\theta \equiv (A + B\theta)(C + D\theta).$$

Hence the integral quotients $\xi = x/p$, $\eta = y/p$, z/p, w/p are of the form (5) with a, b, c, and d replaced by the integers A, B, C, and D. This proves the following theorem.

THEOREM 3. *All integral solutions of $N(x + y\theta) = zw$ are obtained by multiplying an arbitrary integer by the numbers* (5) *in which a, b, c, and d are integers without a common factor (in brief by the formula which expresses the fact that the norm of the product of two numbers $a + b\theta$ and $c + d\theta$ of the field $R(\theta)$ equals the product of their norms), provided the integral algebraic numbers of the field $R(\theta)$ obey the laws of divisibility of arithmetic, and this condition is satisfied only for the following* 45 *values* of m numerically $\leqq 100$, m having no square factor:*

$m = -1, -2, -3, -7, -11, -19, -43, -67, 2, 3, 5,$

$6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 33, 37, 38, 41, 43, 46, 47,$

$53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97.$

5. *Definition of Ideals. Known Theorems.* When the laws of divisibility fail for the integral algebraic numbers of a field, we may restore those laws by the introduction of ideals, as was first done by Kummer for a field defined by a root of unity, and by Dedekind for any algebraic field. By an *ideal* of a field $R(\theta)$ is meant any set S of integral algebraic numbers of $R(\theta)$, not composed of zero only, such that the sum and difference of any two (equal or distinct) numbers of the set S are themselves numbers of this set, while every product of a number of the set S and an integral algebraic number of the field $R(\theta)$ is a number of the set S.

* The cases in which all ideals of the field are principal ideals, J. Sommer, *Zahlentheorie*, 1907, tables, pp. 346–358. Dickson, this BULLETIN, vol. 17 (1910–11), pp. 534–7, proved that if $m = -P$ is negative, 163 is the only value of P between 67 and 1,500,000.

If s ranges over the numbers of an ideal S, and s_1 ranges over the numbers of an ideal S_1, where S and S_1 are ideals of the same field $R(\theta)$, then the products ss_1 and their linear combinations with rational integral coefficients form an ideal of $R(\theta)$, called the *product* of the factors S and S_1, and denoted by SS_1 or by S_1S.

For quadratic fields, the case in which we are here interested, the theory of ideals has been developed quite simply.* Two notations are needed. First, $[k, l]$ denotes the totality of linear homogeneous functions of k and l with rational integral coefficients. Second, $\{k\}$ denotes a *principal ideal,* defined as the totality of the products of k by integral algebraic numbers $x + y\theta$ of our field $R(\theta)$, where x and y are rational integers. Hence we have

$$\{k\} = [k, k\theta].$$

THEOREM 4. *In a quadratic field $R(\theta)$, where θ is defined by* (1) *or* (1′), *all ideals are given by $[ne, n(f + \theta)]$, where n, e, f are rational integers such that*

$$(8) \text{ or } (8') \quad f^2 \equiv m \pmod{e}, \quad f^2 + f + \tfrac{1}{4}(1 - m) \equiv 0 \pmod{e},$$

in the respective cases (1) *or* (1′).

THEOREM 5. *In a quadratic field $R(\theta)$, the product of the ideal $[ne, n(f + \theta)]$ by its conjugate $[ne, n(f + \theta')]$ equals the principal ideal $\{n^2e\}$.*

The positive integer $n^2|e|$ is called the *norm* of $[ne, n(f + \theta)]$. The norm of any principal ideal $\{k\}$ is $|N(k)|$.

An ideal S is said to be *divisible* by an ideal T when there exists an ideal Q of the same field such that $S = TQ$. An ideal, which is different from the principal ideal $\{1\}$ and is divisible by no ideal other than itself and $\{1\}$, is called a *prime ideal.*

THEOREM 6. *If a prime ideal divides AB, it divides A or B. Every ideal which is neither $\{1\}$ nor a prime can be expressed in one and but one way as a product of a finite number of prime ideals. Hence ideals obey the laws of divisibility of arithmetic.*

Two ideals A and B are called *equivalent* if there exist principal ideals $\{\alpha\}$ and $\{\beta\}$ such that $\{\alpha\}A = \{\beta\}B$; we write $A \sim B$. If A is equivalent also to C, with $\{\delta\}A = \{\gamma\}C$,

* Dickson, this BULLETIN, vol. 13 (1906–7), pp. 353–6; and, for a very detailed treatment of the case $m = -5$, ANNALS OF MATH., (2), vol. 18 (1917), pp. 169–178.

then $\{\beta\delta\}B = \{\alpha\gamma\}C$ and B is equivalent to C. Hence all the ideals of a field which are equivalent to a given one are equivalent to each other, and are said to form a *class of ideals*. The *principal class* contains all the principal ideals and no others. For, if $A \sim \{1\}$, $\{\alpha\}A = \{\beta\}$, so that the number β of the product is in $\{\alpha\}$, whence β is divisible by α, and $A = \{\beta/\alpha\}$.

6. *Application of Ideals to our Problem.* We now dispense with the assumption made in § 4 that the integral algebraic numbers of our quadratic field $R(\theta)$ obey the laws of divisibility of arithmetic. We shall examine by means of the theory of ideals our assumption that the solutions (5) of

$$N(x + y\theta) = zw \tag{9}$$

are all divisible by the prime p. The prime ideal $\{p\}$ therefore divides the product $\{z\}$ of the principal ideals $\{c + d\theta\}$ and $\{c + d\theta'\}$, without dividing either of the latter. Hence $\{p\}$ is not a prime ideal (§ 5). Thus $\{p\} = PP'$, where P and P' are conjugate prime ideals (which may coincide). By choice of the notation between P and P', we may assume that P is the one dividing $\{c + d\theta\}$, i.e.

$$\{c + d\theta\} = PL, \tag{10}$$

where L is an ideal of our field $R(\theta)$. By hypothesis, p divides x and y, whence, by (4), $\{p\} = PP'$ divides the product of the principal ideals $\{c + d\theta\}$ and $\{a + b\theta\}$. Since $\{c + d\theta\}$ is divisible by P, but not by $PP' = \{p\}$, it follows that $\{a + b\theta\}$ is divisible by P':

$$\{a + b\theta\} = P'T, \tag{11}$$

where T is an ideal of our field $R(\theta)$.

(a) First, let L be a principal ideal. Then, by (10), P is equivalent to the principal ideal $\{1\}$ and hence P is a principal ideal. Evidently its conjugate P' is a principal ideal. Then, by (11), T is equivalent to, and hence equal to, a principal ideal. Hence equations (10) and (11) between principal ideals yield* equations (6) and (7) between numbers of our field, from which we conclude as in § 4 that the quotients of

* After inserting or removing unit factors, since $\{\pi\} = \{\lambda\}$ implies that λ is the product of π by a unit and conversely.

x, y, z, and w by p are the form (5) with a, b, c, and d replaced by new integers A, B, C, and D.*

(b) Second, let L be equivalent to an ideal S which is not a principal ideal. If S' is the conjugate to S, $SS' = \{e\}$, where e is a rational integer (Theorem 5). Then we shall have $LS' \sim SS' = \{e\}$, so that LS' is a principal ideal $\{\delta\}$. Multiplying (10) by S', we get

$$S'\{c + d\theta\} = P\{\delta\}. \tag{12}$$

Multiplying (12) by S, and using $SS' = \{e\}$, we see that $SP\{\delta\}$ is a principal ideal, so that $SP \sim \{1\}$, whence SP is a principal ideal. Its conjugate $S'P'$ is a principal ideal. But the product of (11) by $SS' = \{e\}$ shows that $S'P' \cdot ST$ is a principal ideal. Thus $ST \sim \{1\}$ and ST is a principal ideal $\{\epsilon\}$. Hence, by (11),

$$S\{a + b\theta\} = P'\{\epsilon\}. \tag{13}$$

By the norms of the members of (12) and (13), in connection with (5), we get

$$|ez| = |eN(c + d\theta)| = p|N(\delta)|,$$
$$|ew| = |eN(a + b\theta)| = p|N(\epsilon)|.$$

By hypothesis, x, y, z, and w are divisible by p. Hence $N(\delta)$ and $N(\epsilon)$ are divisible by e. By comparing the product of (12) and (13) with (4), we get

$$\{e\}\{x + y\theta\} = \{p\}\{\delta\epsilon\}.$$

Hence $e(x + y\theta)/p = \delta\epsilon u$, where u is a unit. Replacing ϵu by ϵ, we conclude that the quotients of x, y, z, and w by p are integers X, Y, Z, and W, such that

$$X + Y\theta = \frac{\delta\epsilon}{e}, \qquad Z = \pm\frac{N(\delta)}{e}, \qquad W = \pm\frac{N(\epsilon)}{e}. \tag{14}$$

The requirement that $\delta\epsilon$, $N(\delta)$, $N(\epsilon)$ be divisible by e may be expressed by congruential conditions modulo e upon the four coordinates of δ and ϵ (cf. § 7). In the future we shall retain only the upper sign in (14) and understand that the

* If we attend only to the numbers z of our solutions, we see that our discussion, with omission of the details leading to (11) and (13), leads to the quadratic forms of all divisors of the numbers represented by the quadratic form N.

simultaneous change of signs of Z and W in any solution leads to a companion solution which will not be listed. Our initial solution (5) is the case $e = 1$ of (14). The removal from (5) of a prime factor led us to the solutions (14). Bearing in mind that we must remove from (5) in succession the various prime factors of the common factor of the numbers (5), we may state the following lemma.

LEMMA. *From each class of ideals of the field $R(\theta)$, where θ is defined in terms of m by* (1) *or* (1′), *select a representative ideal and call its norm e. For each e impose on the coordinates of δ and ϵ the conditions that the divisions indicated in* (14) *are possible and derive the resulting solution* (14) *in integers. Similarly, examine the conditions that the four numbers in any such formula* (14) *shall be divisible by an arbitrary one of the numbers e and derive the resulting solution in integers. Delete one of two such solutions if they are equivalent,* i.e. *if they differ only by a change of integral parameters. Repeat the process until closure results, so that the final sets of solutions $S_1, \cdots, S_k$ are such that, when the numbers of any S_i are divisible by any e, the resulting solution is equivalent to one of $S_1, \cdots, S_k$. Then all integral solutions of $N(x + y\theta) = zw$ are integral multiples of $S_1, \cdots, S_k$.*

The theory of the correspondence* between classes of ideals and classes of quadratic forms and the theory of the composition of classes would seem to entitle us to pass from the preceding result to the following conjectured theorem.

THEOREM 7. *Select a representative $S = [e, f + \theta]$ of each class of ideals of the field $R(\sqrt{m})$, and define θ by* (1) *or* (1′). *Then all integral solutions of $N(x + y\theta) = zw$ are integral multiples of*

$$(15)\quad \begin{aligned} &x = eln + fnq - flr - gqr, \qquad y = lr + nq,\\ &z = el^2 + 2flq + gq^2, \qquad w = en^2 - 2fnr + gr^2,\\ &m \equiv 2 \text{ or } 3 \pmod 4, \qquad f^2 - eg = m, \end{aligned}$$

or of

$$(16)\quad \begin{aligned} &x = eln + fnq - (f+1)lr - gqr, \qquad y = lr + nq,\\ &z = el^2 + (2f+1)lq + gq^2, \qquad w = en^2 - (2f+1)nr + gr^2,\\ &m \equiv 1 \pmod 4, \qquad (2f+1)^2 - 4eg = m. \end{aligned}$$

* To S and its conjugate S' correspond z and w, while to their product (a principal ideal) corresponds $N(x + y\theta)$, which therefore can be obtained from z and w by composition. This suggests another, but more technical, approach to our whole subject.

When S is the principal ideal $\{1\}$, $e = 1, f = 0$, (15), and (16) with n replaced by $n + r$, become (5_1) and (5_2) for $l = c$, $q = d$, $n = a$, $r = b$.

I have verified Theorem 7 for $m = -14, -17, -46$, when there are 4 classes of ideals; for $m = -26$, when there are 6 classes; for all values of m numerically < 100 for which there are 2 or 3 classes (§ 7); and when there is a single class (§ 4). A general proof is being sought by one of my students, who is also applying the method to other types of Diophantine equations.

7. *Cases of* 2 *or* 3 *Classes of Ideals.* The following result, in connection with Theorem 3, disposes of all positive values of $m < 100$, except $m = 82$, in which case alone the number of classes of ideals exceeds 3.

THEOREM 8. *For the* 37 *values of* m *between* -100 *and* $+100$ *and without a square factor for which there are exactly* 2 *or* 3 *classes of ideals in the field* $R(\sqrt{m})$, *all integral solutions of* $N(x + y\theta) = zw$ *are integral multiples of* (5) *and* (15) *or* (16), *where* e *and* f *take the one set or the two sets of values in one or two ideals* $[e, f + \theta]$ *which together with* $\{1\}$ *give representatives of the* 2 *or* 3 *classes of ideals.*

For $m \equiv 2$ or $3 \pmod 4$, $\theta = \sqrt{m}$, we write

$$\delta = D + q\theta, \qquad \epsilon = E + r\theta. \tag{17}$$

Then

$$N(\delta) = D^2 - mq^2, \qquad N(\epsilon) = E^2 - mr^2,$$
$$\delta\epsilon = DE + mqr + (Dr + Eq)\theta. \tag{18}$$

First, consider an ideal $S = [e, f + \theta]$ for which e is a prime factor of m. By (8), $f \equiv 0 \pmod e$ and we may take $f = 0$. Note that every ideal, not a principal ideal, is equivalent to S when * $m = -6, -10, -22, -58, 10, 26, 30, 42, 58, 70, 74, 78$ with $e = 2$, and when $m = 51$ or 66 with $e = 3$. The numbers (18) are divisible by e if and only if D and E are. For $D = el$, $E = en$, (14) become (15) with $f = 0$.

Second, for $m \equiv 3 \pmod 4$, let $S = [2, f + \theta]$. By (8), we may take $f = 1$. Note that every ideal, not a principal ideal, is equivalent to S when $m = -5, -13, -37, 15, 35, 39, 55, 87, 91, 95$. Since (18) shall be divisible by 2, $D = q + 2l$, $E = -r + 2n$, and (14) with $e = 2$ become (15).

* Sommer, *Zahlentheorie*, 1907, pp. 346–358. (Tables.)

Third, for $m \equiv 2$ or $3 \pmod 4$, $m \equiv 1 \pmod 3$, let $S = [3, f + \theta]$. By (8), we may take $f = 1$ or -1. For $m = 31$ or 79, the three classes of ideals are represented by $\{1\}$ and the two S's; for $m = 34$, the two classes are represented by $\{1\}$ and S with $f = +1$. The numbers (18) are divisible by 3 if and only if $D \equiv \pm q, E \equiv \mp r \pmod 3$. For $D = \pm q + 3l$, $E = \mp r + 3n$, (14) with $e = 3$ become (15) with $f = \pm 1$.

These three main cases cover all the values of m between -100 and $+100$ for which $m \equiv 2$ or $3 \pmod 4$ and for which there are exactly 2 or 3 classes of ideals.

It remains to verify closure. Let $x, \cdots, w$ in (15) be divisible by e. For our first case, $f = 0$ and $g = -m/e$ is not divisible by e, whence $q \equiv r \equiv 0 \pmod e$. The last is true also in our second case $e = 2$, $f = 1$, $g = (1 - m)/2$ odd. For $q = ed$, $r = eb$, the quotients of (15) by e are of the form (5_1) with $a = n - fb$, $c = l + fd$. In the third case $e = 3$, $f = \pm 1$, either $q \equiv r \equiv 0$ (just treated) or $l \equiv fgq$, $n \equiv -fgr \pmod 3$.

First, let $g \equiv -1 \pmod 3$ and hence replace l by $-fq + 3l$, and n by $fr + 3n$; the quotients of (15) by 3 are of the form (15) with e replaced by 9, f by $-2f$, and g by $(g + 1)/3$. For $m = 31$, we apply to $z = (9, -2f, -3)$, with $f = \pm 1$, in succession the substitutions

$$\begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}, \qquad \delta = \pm 2, \mp 1, \pm 1, \mp 5,$$

and obtain $(-3, \pm 4, 5)$, $(5, \pm 1, -6)$, $(-6, \pm 5, 1)$, $(1, 0, -31)$. The product of these substitutions is $l = 2c \mp 11d$, $q = \mp 5c + 28d$. Using also $n = 2a \pm 11b$, $r = \pm 5a + 28b$, we see that our solution becomes (5_1).

Next, let $g \equiv +1 \pmod 3$ and hence replace l by $fq + 3l$, and n by $-fr + 3n$; the quotients of (15) by 3 are

$$\begin{aligned} x &= 9ln + 4fnq - 4flr - hqr, \qquad y = lr + nq, \\ z &= 9l^2 + 8flq + hq^2, \qquad w = 9n^2 - 8fnr + hr^2, \\ h &= (g + 5)/3. \end{aligned} \tag{19}$$

For $m = 79$, apply to $z = (9, \pm 4, -7)$ in turn

$$\begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix}, \qquad \delta = \pm 1, \qquad \delta = \mp 1.$$

We obtain

$$z = 10s^2 \pm 14st - 3t^2 \equiv \phi \quad \text{for} \quad l = -s \mp t,$$

$q = \mp s - 2t$. But our initial z in (15) with $e = 3, f = \pm 1$, $g = -10$, becomes $-\phi$ for $l = -t \pm 2s$, $q = s$. Eliminating s and t, we see that if we replace l by $\pm l - 3q$, q by $2l \mp 5q$, n by $\mp n - 3q$, and r by $2n \pm 5r$ in (19), we obtain $x, -y, -z, -w$ of our initial (15). But by the change of the signs of q and r in (15), y is changed in sign, while the effect on x, z, w is to change the sign of f.

Finally, let $m = 34$, $e = 3$, $f = +1$. In (19) we take $l = -c + 6d$, $q = c - 5d$, $n = c + 6b$, $r = a + 5b$, and obtain (5_1) with z and w changed in sign.

Let $m \equiv 1 \pmod 4$, $\theta = \frac{1}{2}(1 + \sqrt{m})$, and consider an ideal S of the field $R(\theta)$ for which e is a prime factor of m. By (8′), we may take $2f + 1 = e$. Note that every ideal, not a principal ideal, is equivalent to S when $m = -35, 65, 85$ with $e = 5$; $m = -51$, $e = 3$; and $m = -9$, $e = 7$. By (2′) and (17),

$$N(\delta) = D^2 + Dq + \tfrac{1}{4}(1 - m)q^2,$$

$$N(\epsilon) = E^2 + Er + \tfrac{1}{4}(1 - m)r^2, \tag{20}$$

$$\delta\epsilon = DE + \tfrac{1}{4}(m - 1)qr + (Dr + Eq + rq)\theta.$$

Thus

$$4N(\delta) \equiv (2D + q)^2 \equiv 0, \qquad 4N(\epsilon) \equiv (2E + r)^2 \equiv 0 \pmod e.$$

Hence write $D = fq + el$, $E = -\frac{1}{2}(e + 1)r + en$. Then (14) give (16). To prove closure, let the numbers (16) be divisible by e. Since m is not divisible by e^2, g is not divisible by e. Hence $q \equiv r \equiv 0 \pmod e$. For $q = ed$, $r = eb$, the quotients of (16) by e are of the form (5_2) for $a = n - (f + 1)b$, $c = l + fd$.

Let $m \equiv 1 \pmod{4e}$, where e is a prime. By (8′), we may take $f = 0$ or $f = -1$, and obtain conjugate ideals. The conditions that (20) be divisible by e are

$$D(D + q) \equiv 0, \qquad E(E + r) \equiv 0, \qquad DE \equiv 0,$$

$$(D + q)(E + r) \equiv 0 \pmod e.$$

Hence either $D \equiv E + r \equiv 0$ or $E \equiv D + q \equiv 0$. For $D = el$,

$E = -r + en$, (14) become (16) with $f = 0$. For $E = en$, $D = -q + el$, (14) become (16) with $f = -1$. We may restrict the proof of closure to the first case. For, our two cases are interchanged by the substitution $s = (DE)(qr)(nl)$, which by (17) and (14) gives rise to the interchange of δ with ϵ, and z with w. But s replaces x, y, z, w of (16) with $f = 0$ by x, y, w, z of (16) with $f = -1$. The numbers (16) with $f = 0$ are divisible by e if and only if either $q \equiv r \equiv 0$ (treated above), or $l \equiv -gq$, $n \equiv gr \pmod{e}$.

First, let $g \equiv 0 \pmod{e}$. Replacing l by el and n by en in (16), we see that the quotients by e are of the form (16) with e replaced by e^2 and g by g/e, while f remains zero. For $m = -31$, $e = 2$, whence $g = 4$, we replace l by q, q by $-l$, n by $-r$, and r by n, and obtain (16) with $f = -1$. For $m = -15$, $e = 2$, we replace l by $-d$, q by $c + d$, n by b, and r by $-a$, and obtain (5_2).

Next, let $g \equiv \pm 1 \pmod{e}$. Write $l = \mp q + eQ$, $n = \pm r + eR$. The quotients of (16) with $f = 0$ by e are

$$
\begin{aligned}
&x = e^2QR - (1 \mp e)rQ \mp eqR - \sigma qr, \quad y = Qr + Rq,\\
&z = e^2Q^2 + (1 \mp 2e)Qq + \sigma q^2, \quad w = e^2R^2 - (1 \mp 2e)Rr + \sigma r^2, \qquad (21)\\
&\sigma = 1 + (g \mp 1)/e.
\end{aligned}
$$

For $m = -23$, $e = 2$, we have $g = 3$ and may choose the upper signs. Replacing Q by $-q$, q by $l - q$, R by r, and r by $-n - r$, we obtain (16) with $f = -1$.

For $e = \sigma = 3$, the upper signs give $g = 7$, $m = -83$, and the lower signs give $g = 5$, $m = -59$. Replacing Q by q, q by $-l \pm q$, R by r, and r by $-n \mp r$, we obtain $-x$, $-y$, z, w of (16) with $f = -1$.

These values -15, -23, -31, -35, -51, -59, -83, -91, 65, 85 are the only ones of m between -100 and $+100$ which are $\equiv 1 \pmod{4}$ and for which there are exactly 2 or 3 classes of ideals. Hence Theorem 8 is proved.

THE UNIVERSITY OF CHICAGO,
February 15, 1920.