THE GROUP OF CLASSES OF CONGRUENT QUADRATIC INTEGERS WITH RESPECT TO A COMPOSITE IDEAL MODULUS*

BY

ARTHUR RANUM

Introduction.

If in the ordinary theory of rational numbers we consider a composite integer m as modulus, and if from among the classes of congruent integers with respect to that modulus we select those which are prime to the modulus, they form a well-known multiplicative group, which has been called by WEBER (*Algebra*, vol. 2, 2d edition, p. 60), the most important example of a finite abelian group. In the more general theory of numbers in an algebraic field we may in a corresponding manner take as modulus a composite ideal, which includes as a special case a composite principal ideal, that is, an integer in the field, and if we regard all those integers of the field which are congruent to one another with respect to the modulus as forming a class, and if we select those classes whose integers are prime to the modulus, they also will form a finite abelian group † under multiplication.

The investigation of the nature of this group is the object of the present paper. I shall confine my attention, however, to a quadratic number-field, and shall determine the structure of the group of classes of congruent quadratic integers with respect to any composite ideal modulus whatever. Several distinct cases arise depending on the nature of the prime ideal factors of the modulus; for every case I shall find a complete system of independent generators of the group.

Exactly as in the simpler theory of rational numbers it will appear that the solution of the problem depends essentially on the case in which the modulus is a prime-power ideal, that is, a power of a prime ideal. The most important case, however, is probably that in which the modulus is a rational principal ideal or in other words a rational integer; therefore a separate discussion will be given of this case. Another interesting case is that in which the group is

* Presented to the Society (Chicago), April 9, 1909.

† This group must not be confused with the group of classes of equivalent ideals in an algebraic field, which is also finite and abelian; the latter has been the subject of numerous investigations, in which, however, the *language* of the theory of groups has not usually been employed.

cyclic and primitive roots exist; this case arises in a variety of ways, all of which will be enumerated, and the corresponding primitive roots given.

Preliminary notions.

1. Let m be any rational integer whose prime factors are all distinct, and let $\omega = \sqrt{m}$, if $m \equiv 2$ or $3 \pmod 4$, and $\omega = \frac{1}{2}(1 + \sqrt{m})$, if $m \equiv 1 \pmod 4$; then in the quadratic number-field defined by $\sqrt{m}$ the numbers $a + b\omega$, where a and b are rational integers, are said to be the *integers of the field*, or simply *quadratic integers*. The factorization of quadratic integers, although apparently capricious and utterly lawless, has been shown to be really amenable to reason, when considered from the standpoint of, and in connexion with, certain artificial quantities called *ideals*. For an elementary and detailed discussion of ideals in a quadratic number-field, illustrated by concrete examples, see SOMMER's recent book *Vorlesungen über Zahlentheorie*,* especially pages 36–59.

Unless otherwise stated, the notation and nomenclature used by SOMMER will be followed in this paper. Thus rational integers will be denoted by Roman letters a, b, etc., quadratic integers by Greek letters α, β, etc., and *principal ideals* (Hauptideale) by the symbols (a), (α), etc. But ideals in general will be denoted by capitals A, P, etc., except that the particular letters G, H, J will be reserved for groups.

2. Let A be any ideal of the number-field (Zahlkörper) $\mathrm{k}(\sqrt{m})$; the number of integers of the field that form a complete system of residues with respect to the modulus A, that is, the number of classes of congruent integers with respect to A, is equal to the norm of A, $n(A)$. Among these classes those which are prime to A, $\Phi(A)$ in number, where the Φ-function is a generalization of Euler's ϕ-function,† evidently form an *abelian multiplicative group* G, of order $\Phi(A)$. However, it will be more convenient to let the group be made up, not of the classes themselves, but of $\Phi(A)$ quadratic integers, one chosen from each class. In other words we shall select from a complete system of residues those which are prime to the modulus, thus forming what will be called a *reduced system of residues*, and regard them as the elements of the group. This is legitimate, provided we agree that the product of two elements α and β of the group is congruent to a third element γ of the group, $\alpha\beta \equiv \gamma \pmod A$, and not necessarily equal to it. The rational integer 1 can always be taken to be the identical element of the group.

* The reader of this book should be on the lookout for a number of minor errors and some rather misleading statements. Reference will also be made to HILBERT's *Bericht* in the Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4 (1897), pages 181–194, for the source of much of the material in SOMMER's book, and to BACHMANN's *Neuere Zahlentheorie*, Sammlung Schubert, for an introduction to the theory of algebraic numbers, in which the author, like SOMMER, confines himself to the quadratic field.

† SOMMER, l. c., pp. 78–81.

Modulus a Power of a Prime Ideal.

3. In studying this group we shall first take up the case in which the modulus A is a power of a prime ideal P, say $A = P^k$. If A is itself prime ($k = 1$), it is known that the group is *cyclic*, and therefore that *primitive roots* exist with respect to a prime ideal P (Sommer, l. c., pp. 84–86).

In order to investigate the case $k > 1$, it will be necessary to consider separately the three kinds of prime ideals, those of the first grade, both unambiguous and ambiguous, and those of the second grade (Sommer, l. c., p. 48 and p. 53). Let p be a rational prime such that the principal ideal (p) is divisible by the prime ideal P, and let P' be the conjugate of P; then the three kinds of prime ideals may be briefly characterized as follows:

First grade; unambiguous, $PP' = (p)$, $P' \neq P$,

ambiguous, $P^2 = (p)$.

Second grade; $P = (p)$.

Again, if P is of the first grade, $n(P^k) = p^k$ and $\Phi(P^k) = p^{k-1}(p-1)$, and if P is of the second grade, $n(P^k) = p^{2k}$ and $\Phi(P^k) = p^{2k-2}(p^2-1)$.

It will also be necessary to distinguish between different values of the rational prime p, according as $p = 2$, $p = 3$, or $p > 3$, and again between different forms of m, according as $m \equiv 1$, 2, or $3 \pmod 4$.

From the canonical forms of the bases of the different kinds of prime ideals, as given by Hilbert (*Bericht*, pp. 282–283) and Sommer (pp. 59–63), the corresponding canonical forms of the bases of their kth powers are easily derived and will be assumed in what follows.

Case I. *P an Unambiguous Prime of the First Grade.*

4. In this case $P = (p, a + \omega)$ and $P^k = (p^k, a_k + \omega)$; since the coefficient of ω in the basis of the modulus is 1, every integer in the field is congruent to some rational integer, and we may choose as a complete system of residues with respect to the modulus the rational integers $0, 1, \cdots, p^k - 1$. Now those which are prime to P^k are precisely those which are prime to p; so if we strike out from this complete system of residues those integers which are divisible by p, we shall have left $p^{k-1}(p-1)$ residues, one from each of the classes forming the group in question. In this first case, therefore, the group is simply isomorphic with the corresponding group in the rational number-field, and its generators can be written down immediately. There are two types, depending on the value of p.

Type 1. $p > 2$.

5. Thus, if $p > 2$, G is a cyclic group and can be generated by a single element of period $p^{k-1}(p-1)$. But it can also be generated by two indepen-

dent elements, one of period $p-1$ and the other of period p^{k-1}; and the latter choice of generators will be found more convenient for our purpose. Throughout this paper, similarly, the periods of the generators will always be chosen in such a way that no period shall be divisible both by p and by another prime factor.

Let us take $1+p$ as generator of period p^{k-1}, if $k>1$; if $k=1$, it reduces to the identical element and no longer figures as a generator. To find a generator of period $p-1$, let f_1 be a primitive root of the rational prime p; with respect to the modulus P^k, f_1 will be of period $p^i(p-1)$, where $i<k$, and $f=f_1^{p^i}$ will be of period $p-1$. *Therefore we shall take f and $1+p$ as the two required independent generators, of periods $p-1$ and p^{k-1}, respectively.*

Type 2. $p=2$.

6. If $p=2$, we obtain the second type, which is a non-cyclic group of order 2^{k-1}, having the invariants $2, 2^{k-2}(k>2)$. *Its generators will be taken to be -1 of period 2, and 5 of period 2^{k-2}. If $k=2$, there is only one generator, -1 of period 2; and if $k=1$, the group is of order 1.*

Case II. *P an Ambiguous Prime Ideal.*

7. In this case P is necessarily of the first grade and its norm p is a factor of the discriminant d of the number-field. Since $P^2=(p)$, every even power of P is a rational principal ideal, $P^{2s}=(p^s)$, and every odd power is equal to P multiplied by a rational principal ideal, $P^{2s+1}=(p^s)\cdot P$. This case will be found to give rise to five distinct types of groups, in two of which $p>2$ and in the other three $p=2$.

Subcase II_a. $p>2$.

8. By reference to Sommer's text, pages 59–63, we see that if $m\equiv 2$ or $3 \pmod 4$, $P=(p, \sqrt{m})$, and that if $m\equiv 1 \pmod 4$, then

$$\omega=\frac{1+\sqrt{m}}{2}, \qquad P=\left(p, \frac{p-1}{2}+\omega\right)=\left(p, \frac{p+\sqrt{m}}{2}\right).$$

It will be convenient to combine these two cases into one by introducing the symbol ω_1, defined by the equations

$$\omega_1=\omega=\sqrt{m}, \qquad \text{if } m\equiv 2 \text{ or } 3 \pmod 4,$$

$$\omega_1=\frac{p-1}{2}+\omega=\frac{p+\sqrt{m}}{2}, \qquad \text{if } m\equiv 1 \pmod 4.$$

In both cases, therefore, we may write

$$P=(p, \omega_1).$$

9. Further, raising both sides of this equation to even and to odd powe s, respectively, we have

$$(1) \qquad P^{2s} = (p^s, p^s\omega_1), \qquad P^{2s+1} = (p^{s+1}, p^s\omega_1).$$

In order to obtain a notation by means of which the even and the odd powers of P can be considered together, we again introduce new symbols, r and s, defined by the equations

$$\left[\frac{k}{2}\right] = s, \qquad \left[\frac{k+1}{2}\right] = r,$$

where k is a positive rational integer, and $[x]$ means the largest rational integer $\leqq x$. It follows that if $k = 2s$, $r = s$, and if $k = 2s+1$, $r = s+1$, and in either case $k = r+s$. By means of these symbols the two equations (1) can be replaced by the single equation

$$P^k = (p^r, p^s\omega_1).$$

10. Since $m \equiv 0 \pmod{p}$ and (ω_1) is not prime to (p), we can select as a reduced system of residues with respect to the modulus P^k the quadratic integers $u + v\omega_1$, in which v takes all rational integral values from 0 to $p^s - 1$, inclusive, and u takes all rational integral values from 1 to $p^r - 1$, inclusive, except those which are divisible by p. This gives p^s values to v and $p^{r-1}(p-1)$ values to u, and therefore furnishes $p^{r+s-1}(p-1)$ residues for the reduced system. This agrees with the formula $\Phi(P^k) = p^{k-1}(p-1)$ for the order of the group, since $r+s = k$.

A more convenient choice of residues for our purpose, however, is $u + v\sqrt{m}$, where u and v have the same values as before. If $m \equiv 2$ or $3 \pmod 4$, $\omega_1 = \sqrt{m}$ and the residues are also the same as before; if $m \equiv 1 \pmod 4$, $\omega_1 = \frac{1}{2}(p + \sqrt{m})$ and the residues are different, but still form a reduced system, as is evident from the formulæ

$$\sqrt{m} = -p + 2\omega_1,$$

$$\omega_1 \equiv -p\frac{p^{r-1}-1}{2} - \frac{p^s-1}{2}\sqrt{m} \pmod{P^k}.$$

11. Under this subcase all the groups are, for $p > 3$, of a single type, the third; while if $p = 3$, another type, the fourth, also occurs. In either type, however, it is immediately evident that the quadratic integers having rational residues form a cyclic subgroup analogous to type 1, and generated, therefore, by two rational integers, viz., g, of period $p-1$, and (if $r > 1$) $1 + p$, of period p^{r-1}. If $p = 3$, $g = -1$.

12. Among the irrational elements of the group (if $k > 1$) the integer $1 + \sqrt{m}$ suggests itself as probably an available independent generator of period p^s. This conjecture will be found to be correct, if $p > 3$, and sometimes, but not always,

correct, if $p = 3$. Here the word *independent* means *independent of the rational residues.*

THEOREM. *If $k > 1$, $1 + \sqrt{m}$ is an independent generator of period p^s with respect to the modulus $P^k = (p^r, p^s\omega_1)$ in every case except that in which $p = 3$ and $m \equiv -3 \pmod 9$.*

Proof. By means of the binomial theorem we obtain the formula

$$(2)\quad (1+\sqrt{m})^{p^i} \equiv 1 + p^{i+1}\cdot\frac{p^i-1}{2}\cdot\frac{m}{p} + p^i\left[1 + \frac{p(p^i-1)(p^i-2)}{2\cdot 3}\cdot\frac{m}{p}\right]\sqrt{m} \quad (\text{modd } p^{i+2},\ p^{i+2}\sqrt{m}),$$

where the coefficients are apparently rational fractions, but really integers. Putting $i = s$ in this congruence, and noting that $i + 1 \geqq r$, we see that $(1 + \sqrt{m})^{p^s} \equiv 1 \pmod{P^k}$ and therefore that $1 + \sqrt{m}$ has a period which is a divisor of p^s and will have a period exactly equal to p^s and will be independent of the rational residues, if its (p^{s-1})th power is irrational. Putting $i = s - 1$ in formula (2), we see that

$$(1+\sqrt{m})^{p^{s-1}} \equiv 1 + p^s\cdot\frac{p^{s-1}-1}{2}\cdot\frac{m}{p} + p^{s-1}\cdot y\cdot\sqrt{m} \quad (\text{modd } p^{s+1},\ p^{s+1}\sqrt{m}),$$

where

$$y = 1 + \frac{p(p^{s-1}-1)(p^{s-1}-2)}{2\cdot 3}\cdot\frac{m}{p}.$$

Hence $(1 + \sqrt{m})^{p^{s-1}}$ will have an irrational residue with respect to the modulus $(p^r, p^s\omega_1)$, if $y \not\equiv 0 \pmod p$. This is the case when $p > 3$; for then $y \equiv 1 \pmod p$: it is also the case, when $p = 3$ and $m \equiv 3 \pmod 9$; for then $y \equiv 1 + \frac{1}{3}m \equiv 2 \pmod 3$. The only other possibility, since $p > 2$, is $p = 3$ and $m \equiv -3 \pmod 9$. But this supposition makes $y \equiv 0 \pmod 3$, and the argument fails. The theorem is therefore proved.

Type 3. $p > 3$, *or* $p = 3$ *and* $m \equiv 3 \pmod 9$.

13. This theorem enables us to complete the determination of the third type of group. *Thus if P is an ambiguous prime ideal and if either $p > 3$ or $p = 3$ and $m \equiv 3 \pmod 9$, then the group of reduced residues with respect to the modulus $P^k = (p^r, p^s\omega_1)$ is generated by the three independent elements g, $1 + \sqrt{m}$* (if $k > 1$), *and $1 + p$ (if $k > 2$), whose periods are $p - 1$, p^s, and p^{r-1}, respectively.*

In other words every quadratic integer α, prime to the modulus, is expressible in one and only one way as a product of the form

$$\alpha \equiv g^{n_1}(1+\sqrt{m})^{n_2}(1+p)^{n_3} \pmod{P^k},$$

* It is to be noticed that if $m \equiv 1 \pmod 4$, $1 + \sqrt{m} = 2\omega$.

where the exponents n_1, n_2, and n_3 are residues with respect to the corresponding periods $p-1$, p^s, and p^{r-1}, respectively, and will be called the *indices* of α. If these indices range independently over complete systems of residues as to their respective moduli, the quadratic integer α will range over the entire group G. A similar definition of indices applies, of course, to every type of group.

14. It is evident that the elements whose periods are powers of p all have residues of the form $1+pu+v\sqrt{m}$ and constitute a Sylow subgroup H of order p^{k-1}, generated by $1+\sqrt{m}$ and $1+p$. It may easily be verified that the system of residues of the form $1+p^iu+p^jv\sqrt{m}$, where i and j are fixed exponents such that $1\leqq i\leqq r$ and $0\leqq j\leqq s$, constitute a group (a subgroup of H of order p^{k-i-j}), if, and only if, $i\leqq 2j+1$. Again, an element α is of period $p^i\,(i\leqq s)$, if, and only if, it is expressible in the form

$$\alpha\equiv 1+p^{r-i}u+p^{s-i}v\sqrt{m}\pmod{P^k},$$

where u and v are not both divisible by p.

Type 4. $p=3$, $m\equiv -3 \pmod 9$.

15. We now come to the exceptional case in which $p=3$, $m\equiv -3 \pmod 9$, and therefore $P^k=(3^r,\ 3^s\omega_1)$; it gives rise to another type of group, the fourth; $1+\sqrt{m}$ is no longer available as a generator, because it is not, in general, independent of the rational residues.

Let H, as before, be the subgroup of G whose elements are of the form $1+3u+v\sqrt{m}$ and whose order is 3^{k-1}, and let $J\,(k>1)$ be the subgroup of H whose elements are of the form $1+3u+3v\sqrt{m}$ and whose order is 3^{k-2}. From the formula

$$(1+3\sqrt{m})^{3^i}\equiv 1+3^{i+1}\sqrt{m}\quad(\text{modd } 3^{i+3},\ 3^{i+3}\sqrt{m})$$

it is immediately clear that $1+3\sqrt{m}$ is of period 3^{s-1} and independent of the rational residues, and consequently that if $k>3$, J has two independent generators, which can be taken to be 4 and $1+3\sqrt{m}$, of periods 3^{r-1} and 3^{s-1}, respectively.

16. We wish to show that, if $k>3$, H has the invariants $(3^{r-1},\ 3^{s-1},\ 3)$ and three independent generators, including those of J and one additional generator λ of period 3. This conclusion can be drawn the moment it is proved that H contains an element of period 3 not contained in J, that is, an element

$$\lambda=x+y\sqrt{m}, \tag{3}$$

such that

$$\lambda^3\equiv 1\pmod{P^k} \tag{4}$$

and

$$y\not\equiv 0\pmod 3. \tag{5}$$

It is unnecessary to write $1 + 3u$ for x; the conditions (4) and (5) are sufficient to show that λ occurs in H. From the abstract properties of the group H we know that if there exists one such element λ, *there must exist exactly eighteen*, any one of which will suffice as an independent generator of H and therefore also of G.

17. THEOREM. *If x and y are rational integers satisfying the congruences*

$$2x \equiv -1 \pmod{3^{r-1}}, \qquad r > 1, \tag{6}$$

$$4 \cdot \frac{m}{3} \cdot y^2 \equiv -1 \pmod{3^{s-1}}, \qquad s > 1, \tag{7}$$

then $\lambda = x + y\sqrt{m}$ will satisfy conditions (4) *and* (5).

Proof. (5) is an immediate consequence of (7). To show that (4) is also satisfied, we use the formula

$$8\lambda^3 = (2x)^3 + 9 \cdot 2x \cdot 4 \cdot \frac{m}{3} \cdot y^2 + 6y\left(4x^2 + 4\frac{m}{3}y^2\right)\sqrt{m},$$

from which, in view of (6) and (7) and the congruence $(2x)^3 \equiv -1 \pmod{3^r}$, derived from (6), we obtain the result

$$8\lambda^3 \equiv -1 + 9(-1)(-1) + 6y(1-1)\sqrt{m} \equiv 8 \quad (\text{modd } 3^r, 3^s\sqrt{m}),$$

and therefore also (4).

18. Since in (6) and (7) the coefficients of x and y are prime to 3, and since in (7) $4m/3$ and -1 are both non-squares, mod 3, therefore these two congruences can always be solved for x and y, and λ exists. Moreover, they have one and two solutions, respectively, which give three and six incongruent solutions, with respect to the moduli 3^r and 3^s, and determine eighteen distinct values of λ of the form $(x \pm y\sqrt{m}) + (3^{r-1}u + 3^{s-1}v\sqrt{m})$, where $u, v = 0, 1, 2$. These are precisely the eighteen residues of period 3 not contained in J. Hence (6) and (7) are necessary as well as sufficient conditions that $\lambda = x + y\sqrt{m}$ be an independent generator of period 3.

19. In order to extend the application of the theorem to the cases $k = 2$ and $k = 3$, in which $s = 1$, we shall restrict x and y, in those cases, to the value 1. This will agree with the obvious fact that $1 + \sqrt{m}$ is an independent generator of period 3 with respect to the moduli $(3, 3\omega_1)$ and $(9, 3\omega_1)$. Moreover, when the modulus is $(9, 9\omega_1)$, congruences (6) and (7) show that $1 + \sqrt{m}$ is again a generator of period 3; but when the modulus is $(27, 9\omega_1)$, $4 + \sqrt{m}$ is the corresponding generator. It is to be noticed that the solution of (6) can be written $x \equiv 1 + 3 + \cdots + 3^{r-2} \pmod{3^{r-1}}$.

There is one case in which the generator of period 3 is a rational multiple of $1 + \sqrt{m}$ for all values of k, and that is when $m = -3$; in that case (7) takes the form $(2y)^2 \equiv 1 \pmod{3^{s-1}}$ and is satisfied by $y = x$; therefore $\lambda = x(1 + \sqrt{m})$, where x is a root of the congruence (6).

20. The results obtained for type 4 may be summarized as follows: *If* $m \equiv -3 \pmod 9$ *and if* $P^k = (3^r, 3^s\omega_1)$ *is a power of an ambiguous prime ideal whose norm is* 3, *then the group of reduced residues, mod* P^k, *is generated by* -1 *of period* 2, *if* $k = 1$; *if* $k > 1$, *the quadratic integer* λ *determined by* (3), (6), *and* (7), *is an independent generator of period* 3; *if* $k > 2$, 4 *is another independent generator of period* 3^{r-1}; *and if* $k > 3$, $1 + 3\sqrt{m}$ *is still another, and the last, independent generator of period* 3^{s-1}.

The third power of every element of H is obviously equal to the third power of some element of J and is therefore of the form $1 + 9(u + v\sqrt{m})$. More generally, the 3^i-th power of every element of H is of the form $1 + 3^{i+1}(u + v\sqrt{m})$.

21. *Examples.* To illustrate the difference between the third and fourth types, take first the case where $m = -6$, $p = 3$, and $A = P^4 = (9, 9\sqrt{-6})$; here G is of type 3 and is generated by -1 of period 2, 4 of period 3, and $\alpha = 1 + \sqrt{-6}$ of period 9. The cyclic subgroup of order 9 generated by α may be written out as follows:

$$\begin{array}{lll} 1 = 1, & \alpha^3 \equiv 1 + 6\sqrt{-6}, & \alpha^6 \equiv 1 + 3\sqrt{-6}, \\ \alpha = 1 + \sqrt{-6}, & \alpha^4 \equiv 1 + 7\sqrt{-6}, & \alpha^7 \equiv 1 + 4\sqrt{-6}, \pmod{P^4}. \\ \alpha^2 \equiv 4 + 2\sqrt{-6}, & \alpha^5 \equiv 4 + 8\sqrt{-6}, & \alpha^8 \equiv 4 + 5\sqrt{-6}, \end{array}$$

Then take the case where $m = 6$, $p = 3$, and $A = P^4 = (9, 9\sqrt{6})$; G is of type 4 and is generated by -1 of period 2, 4 of period 3, $\lambda = 1 + \sqrt{6}$ of period 3, and $\beta = 1 + 3\sqrt{6}$ of period 3. The non-cyclic subgroup of order 9 generated by λ and β may be written out as follows:

$$\begin{array}{lll} 1 = 1, & \beta = 1 + 3\sqrt{6}, & \beta^2 \equiv 1 + 6\sqrt{6}, \\ \lambda = 1 + \sqrt{6}, & \beta\lambda \equiv 1 + 4\sqrt{6}, & \beta^2\lambda \equiv 1 + 7\sqrt{6}, \pmod{P^4}. \\ \lambda^2 \equiv 7 + 2\sqrt{6}, & \beta\lambda^2 \equiv 7 + 5\sqrt{6}, & \beta^2\lambda^2 \equiv 7 + 8\sqrt{6}, \end{array}$$

Subcase II_b. $p = 2$.

22. Here we shall find three new types of groups, the fifth, sixth, and seventh, depending on the value of m. If $m \equiv 2 \pmod 4$, $P = (2, \sqrt{m})$, $A = P^k = (2^r, 2^s\sqrt{m})$, and G is of the fifth type; while if $m \equiv 3 \pmod 4$, $P = (2, 1 + \sqrt{m})$, $A = P^k = (2^r, 2^s + 2^s\sqrt{m})$, and G is of the sixth or seventh type according as $m \equiv 3$ or $7 \pmod 8$; m cannot be $\equiv 1 \pmod 4$, since in that case p would not be a factor of the discriminant d. In all three types the rational residues form a subgroup J of order 2^{r-1} generated by -1, of period 2, and (if $r > 2$) 5, of period 2^{r-2}. In all three types, also, the case $k = 1$ is trivial and will be left out of account, since G is then of order 1.

Type 5. $m \equiv 2 \pmod 4$.

23. In this case the modulus is $P^k = (2^r, 2^s\sqrt{m})$, and since m is even, the elements of G are the residues $u + v\sqrt{m}$, where u takes the odd values $1, 3, \cdots, 2^r - 1$, and v ranges over *all* the integral values from 0 to $2^s - 1$. The group is easily disposed of, because only one irrational generator, $1 + \sqrt{m}$, is needed. The latter is of period 2^s and independent of the rational residues, exactly as in type 3 (§ 12, Theorem). For in the formula

$$(1 + \sqrt{m})^{2^i} \equiv 1 + 2^i\sqrt{m} \pmod{2^{i+1}, 2^{i+1}\sqrt{m}},$$

which is easily verified, we see, by putting $i = s$ and $s - 1$ in turn, that the 2^s-th power of $1 + \sqrt{m}$ is $\equiv 1 \pmod{P^k}$ and that the 2^{s-1}-th power is irrational.

Therefore the independent generators of G can be taken to be $1 + \sqrt{m}$ (*if* $k > 1$), -1 (*if* $k > 2$), *and* 5 (*if* $k > 4$), *and their periods are* 2^s, 2, *and* 2^{r-2}, *respectively.*

24. On the other hand, if $m \equiv 3 \pmod 4$, the modulus is $P^k = (2^r, 2^s + 2^s\sqrt{m})$.

In both the resulting types of groups the elements are of the form $u + v(1 + \sqrt{m})$ in which u is odd, or in other words they are of the form $u + v\sqrt{m}$ in which one of the coefficients u, v is odd and the other even. In both types there is the same subgroup J formed by the rational residues, and also the same independent irrational generator of period 2^{s-1}, namely $1 + 2\sqrt{m}$. For by expanding in powers of $1 + \sqrt{m}$ and noting that

$$(1 + \sqrt{m})^2 = 2\left(\frac{m-1}{2} + (1 + \sqrt{m})\right),$$

we easily derive the formula

$$(1 + 2\sqrt{m})^{2^i} = [-1 + 2(1 + \sqrt{m})]^{2^i} \equiv 1 - 2^{i+1}(1 + \sqrt{m}) \pmod{2^{i+2}, 2^{i+2}(1 + \sqrt{m})};$$

and by putting $i = s - 1$ and $s - 2$ in turn, we infer that the 2^{s-1}-th power of $1 + 2\sqrt{m}$ is $\equiv 1 \pmod A$ and that the 2^{s-2}-th power is irrational.

So far we have accounted for just half the group G; for J and $1 + 2\sqrt{m}$ generate a subgroup H of index 2 formed by those residues $u + v\sqrt{m}$ for which u is odd and v even. The other half of the group consists of the residues for which u is even and v odd. It will now be necessary to distinguish between the two cases $m \equiv 3$ and $m \equiv 7 \pmod 8$.

Type 6. $m \equiv 3 \pmod 8$.

25. Recalling the well-known fact that in the rational subgroup J the elements which are $\equiv \pm 3 \pmod 8$ are all of period 2^{r-2} ($r > 2$), while those which are $\equiv \pm 1 \pmod 8$ are all of lower period ($r > 3$), we see that in this case m is of

period $2^{r-2}(r>2)$ and that J is generated by -1 and m. Now $\sqrt{m}$ is an element of G, but not of H, whose square is m. It is therefore of period $2^{r-1}(r>2)$ and independent of -1; since its even powers are rational, it is also independent of $1+2\sqrt{m}$. Consequently, if $r>2$, we may choose as three independent generators of the group G, $\sqrt{m}$, $1+2\sqrt{m}$, and -1, whose periods are 2^{r-1}, 2^{s-1}, and 2, respectively.

This conclusion requires a slight modification to cover the cases $r=1$ and $r=2$. It is easy to verify the following: if $k=2$ $(r=1, s=1)$, G is generated by $\sqrt{m}$, of period 2; if $k=3$ $(r=2, s=1)$, G is generated by $\sqrt{m}$, of period 4; if $k=4$ $(r=2, s=2)$, G is generated by $\sqrt{m}$, of period 4, and $1+2\sqrt{m}$, of period 2. Every case will be included in the statement that $\sqrt{m}$ *is an independent generator of* G, *whose period is* 2^r, *if* $k=2, 3,$ *or* 4, *and* 2^{r-1}, *if* $k>4$; *if* $k>3$, $1+2\sqrt{m}$ *is another independent generator, of period* 2^{s-1}; *and if* $k>4$, -1 *is still another independent generator, of period* 2.

Type 7. $m\equiv 7 \pmod 8$.

26. In this case the period of m is $<2^{r-2}$ $(r>3)$ and that of $\sqrt{m}$ is $<2^{r-1}$. But it is easy to find an element μ of period 4, not contained in H, which, together with 5 and $1+2\sqrt{m}$, will generate G. If one such element exists, *there must be exactly thirty-two*, if $r>2$, since the invariants of G are 2^{r-2}, 2^{s-1}, and 4.

It will be sufficient to put

$$\mu = x\sqrt{m} \tag{8}$$

and determine x as a rational integer satisfying the congruence

$$mx^2 \equiv -1 \pmod{2^{r-1}}. \tag{9}$$

For since $\mu^2 \equiv -1 \pmod{2^{r-1}}$, therefore $\mu^4 \equiv 1 \pmod{2^r}$, and μ is of period 4; since the powers of 5 are all congruent to 1 (mod 8), μ is independent of 5; and since μ^2 is rational, μ is independent of $1+2\sqrt{m}$. Moreover, since $m\equiv -1 \pmod 8$, the congruence $mx^2 \equiv -1 \pmod 8$ and therefore also the congruence (9), can always be solved, and the element μ can always be found.

27. If $r=2$, the congruence (9) evidently still holds and determines the generator $\sqrt{m}$, of period 4. But if $r=1$ and $k=2$, it will be necessary to define $x=1$ as the corresponding root of (9) in order to obtain the generator $\sqrt{m}$; and moreover, its period in this case is 2 instead of 4.

Our final result is, therefore, that *the quadratic integer* μ, *defined by* (8) *and* (9), *is an independent generator whose period is* 2, *if* $k=2$, *and* 4, *if* $k>2$; *if* $k>3$, $1+2\sqrt{m}$ *is another independent generator, of period* 2^{s-1}; *and if* $k>4$, 5 *is still another independent generator, of period* 2^{r-2}.

If $k<9$, and therefore $r<5$, the simplest solution of (9) is $x=1$ and the

simplest choice of the generator μ is $\sqrt{m}$. If $k \geqq 9$, this simple form is no longer in general available; but there is one case in which it is available for every value of k, and that is when $m = -1$. In that case the elements $\sqrt{-1}$, $1 + 2\sqrt{-1}$, and 5 always generate the group.

28. *Examples.* To illustrate types 5, 6, and 7, let m be chosen to be 2, 3, and -1, respectively. If $m = 2$ and $k = 5$, so that $P^5 = (8, 4\sqrt{2})$, then G is of type 5 and order 16 and is generated by $\alpha = 1 + \sqrt{2}$, of period 4, $b = -1$, of period 2, and $c = 5$, of period 2. Thus:

$$\begin{array}{llll} 1 = 1, & \alpha = 1 + \sqrt{2}, & \alpha^2 \equiv 3 + 2\sqrt{2}, & \alpha^3 \equiv 7 + \sqrt{2}, \\ c = 5, & \alpha c \equiv + 5\sqrt{2}, & \alpha^2 c \equiv 7 + 2\sqrt{2}, & \alpha^3 c \equiv 3 + \sqrt{2}, \\ b = 7, & \alpha b \equiv 7 + 3\sqrt{2}, & \alpha^2 b \equiv 5 + 2\sqrt{2}, & \alpha^3 b \equiv 1 + 3\sqrt{2}, \\ bc \equiv 3, & \alpha bc \equiv 3 + 3\sqrt{2}, & \alpha^2 bc \equiv 1 + 2\sqrt{2}, & \alpha^3 bc \equiv 5 + 2\sqrt{2}, \end{array} \pmod{P^5}.$$

By way of contrast to this consider a corresponding group of type 7. E. g., take $m = -1$, $k = 5$, and $P^5 = (8, 4 + 4i)$, where $i = \sqrt{-1}$; then G is of order 16 and is generated by $\alpha = i$, of period 4, $\beta = 1 + 2i$, of period 2, and $c = 5$, of period 2. Thus:

$$\begin{array}{llll} 1 = 1, & \alpha = i, & \alpha^2 \equiv 7, & \alpha^3 \equiv 4 + 3i, \\ \beta = 1 + 2i, & \alpha\beta \equiv 6 + i, & \alpha^2\beta \equiv 3 + 2i, & \alpha^3\beta \equiv 6 + 3i, \\ c = 5, & \alpha c \equiv 4 + i, & \alpha^2 c \equiv 3, & \alpha^3 c \equiv 3i, \\ \beta c \equiv 5 + 2i, & \alpha\beta c \equiv 2 + i, & \alpha^2\beta c \equiv 7 + 2i, & \alpha^3\beta c \equiv 2 + 3i, \end{array} \pmod{P^5}.$$

To illustrate the difference between types 6 and 7 it will be better to take groups of higher order. E. g., put $m = 3$, $k = 8$, and $P^8 = (16, 16 + 16\sqrt{3})$; then G is of type 6 and order 128 and is generated by $\alpha = \sqrt{3}$ of period 8, $\beta = 1 + 2\sqrt{3}$ of period 8, and $c = -1$ of period 2. The subgroup $\{\alpha, c\}$ of order 16 may be written out as follows:

$$\begin{array}{llll} 1 = 1, & \alpha = \sqrt{3}, & c \equiv 15, & \alpha c \equiv 15\sqrt{3}, \\ \alpha^2 \equiv 3, & \alpha^3 \equiv 3\sqrt{3}, & \alpha^2 c \equiv 13, & \alpha^3 c \equiv 13\sqrt{3}, \\ \alpha^4 \equiv 9, & \alpha^5 \equiv 9\sqrt{3}, & \alpha^4 c \equiv 7, & \alpha^5 c \equiv 7\sqrt{3}, \\ \alpha^6 \equiv 11, & \alpha^7 \equiv 11\sqrt{3}, & \alpha^6 c \equiv 5, & \alpha^7 c \equiv 5\sqrt{3}, \end{array} \pmod{P^8}.$$

On the other hand, if $m = -1$, $k = 8$, and $P^8 = (16, 16 + 16i)$, then G is of the same order 128, but of type 7, and is generated by $\alpha = i$ of period 4, $\beta = 1 + 2i$ of period 8, and $c = 5$ of period 4. The subgroup $\{\alpha, c\}$ of

order 16 may be written out as follows:

$$\begin{array}{llll} 1 = 1, & \alpha = i, & \alpha^2 \equiv 15, & \alpha^3 \equiv 15i, \\ c = 5, & \alpha c \equiv 5i, & \alpha^2 c \equiv 11, & \alpha^3 c \equiv 11i, \\ c^2 \equiv 9, & \alpha c^2 \equiv 9i, & \alpha^2 c^2 \equiv 7, & \alpha^3 c^2 \equiv 7i, \\ c^3 \equiv 13, & \alpha c^3 \equiv 13i, & \alpha^2 c^3 \equiv 3, & \alpha^3 c^3 \equiv 3i, \end{array} \pmod{P^3}.$$

Case III. *P a prime ideal of the second grade.*

29. In this case $P = (p) = (p, p\omega)$, that is, the prime ideal is a rational principal ideal, and its norm is p^2. Further, $P^k = (p^k) = (p^k, p^k\omega)$. Since ω and p are relatively prime, every quadratic integer $u + v\omega$ is prime to P^k unless u and v are both divisible by p. The number of residues in G is therefore $p^{2k-2}(p^2 - 1)$. If $k > 1$, the residues $1 + p(u + v\omega)$ obviously form a Sylow subgroup H of order p^{2k-2} comprising all the elements whose periods are powers of p.

Since d, the discriminant of the field, is a non-square modulo p, the congruence $x^2 - d \equiv 0 \pmod{p}$ is irreducible and defines a *Galois field* of order p^2 whose elements may therefore be concretely represented by a complete system of residues $u + v\omega$ with respect to the modulus $(p, p\omega)$. But these residues, excepting 0, are precisely the elements of the group G in the case $k = 1$; hence the latter is a cyclic group of order $p^2 - 1$.

30. *Therefore any complete system of residues with respect to a prime ideal P of the second grade constitutes a Galois field F of order* p^2. It goes without saying that a complete system of residues with respect to a prime ideal of the first grade may also be looked upon as a Galois field of order p, and that with respect to a composite ideal the residues do not form a field at all.

Let δ_1 be a primitive root of the Galois field F, or in other words a generator of the group G, mod P. With respect to the modulus P^k, $\delta_1^{p^2-1}$ will be of period a power of p, say p^i, and $\delta = \delta_1^{p^i}$ will be of period $p^2 - 1$. We shall therefore choose δ to be a generator of the group G, mod P^k. In order to generate the entire group, it will only be necessary in addition to find generators of the subgroup H. At this point two cases must be distinguished, the case $p > 2$ in which G is of type 8, and the case $p = 2$ in which G is of type 9.

Type 8. $p > 2$.

31. In this case H is evidently generated by the two independent elements $1 + p$, and $1 + p\omega$, both of period p^{k-1}; hence *the entire group G, if* $k > 1$, *has the three independent generators* δ, $1 + p$, *and* $1 + p\omega$, *whose periods are* $p^2 - 1$, p^{k-1}, *and* p^{k-1}, *respectively.*

The elements having rational residues form a subgroup of order $p^{k-1}(p-1)$ generated by δ^{p+1} of period $p-1$, and $1+p$ of period p^{k-1}. It is easy to see that the system of residues of the form $1+p^iu+p^jv\omega$, where i and j are fixed exponents such that $1 \leqq i \leqq k$ and $1 \leqq j \leqq k$, constitute a group (a subgroup of H of order p^{2k-i-j}), if and only if $i \leqq 2j$. An element α is of period p^i $(i < k)$, if and only if it is expressible in the form

$$\alpha \equiv 1 + p^{k-i}(u + v\omega) \pmod{P^k},$$

where u and v are not both divisible by p.

Type 9. $p = 2$.

32. In this case $m \equiv 5 \pmod 8$, $\omega = \frac{1}{2}(1+\sqrt{m})$, $P^k = (2^k, 2^k\omega)$, and $\Phi(P^k) = 2^{2k-2}\cdot 3$. In the subgroup H whose elements are of the form $1+2(u+v\omega)$, the rational elements $1, 3, \cdots, 2^k-1$, which are now the only rational elements in the entire group G, are generated as usual by -1 and 5; but the irrational element $1+2\omega$ will no longer serve as the additional generator of H, as it is not independent of the rational elements. Now if $k > 2$, $1+4\omega$ is plainly of period 2^{k-2} and independent of the rational elements, so that -1, 5, and $1+4\omega$ generate just half of H.

Since m, being a non-square (mod 8), is of period 2^{k-2} $(k > 2)$, $\sqrt{m} = -1+2\omega$ is an irrational element of period 2^{k-1} independent of -1 and $1+4\omega$. So H is generated by $\sqrt{m}$, -1, and $1+4\omega$, if $k > 2$, and evidently by $\sqrt{m}$ and -1, if $k = 2$.

Summing up, we may say that *if P is a prime ideal of the second grade whose norm is* 4, *then in the group of reduced residues, mod P^k, the element δ defined in* § 30 *is an independent generator of period* 3; *if $k > 1$ the elements $\sqrt{m}$ and -1 are independent generators of periods 2^{k-1} and* 2, *respectively; and if $k > 2$, $1+4\omega$ is an independent generator of period 2^{k-2}.*

33. It may easily be proved that every residue of the form $1+2^{k-i}(u+v\omega)$, where $i < k$ and where u and v are not both even, is of period 2^i, except in the case where $i = k-1$, u is odd, and v is even.

While the generator δ must in general be determined separately for each value of k, there is one simple case in which the same determination of δ will hold for all values of k. Namely, if $m = -3$, $-\omega = -\frac{1}{2}(1+\sqrt{-3})$ is of period 3 irrespective of k, and can be taken to be the generator δ.

34. *Examples.* To illustrate type 8, we take $m = -1$, $p = 3$, and therefore $\omega = \sqrt{-1}$, $P^k = (3^k, 3^k\omega)$. When $k = 1$, G is cyclic, of order 8, and generated by $\delta = 1+\omega$. When $k = 2$, $\delta_1 = 1+\omega$ is of period 24, $\delta = \delta_1^3 \equiv -2+2\omega$ is of period 8, and G, of order 72, is generated by δ, 4, and $1+3\omega$, the last two being of period 3; the rational residues are generated

by $\delta^4 \equiv -1$ and 4; the powers of δ are

$$\begin{aligned} 1 &= 1, & \delta &= -2+2\omega, \\ \delta^2 &\equiv \omega, & \delta^3 &\equiv -2-2\omega, \\ \delta^4 &\equiv -1, & \delta^5 &\equiv 2-2\omega, \\ \delta^6 &\equiv -\omega, & \delta^7 &\equiv 2+2\omega, \end{aligned} \pmod{P^2}.$$

To illustrate type 9, we take $m = -3$ and therefore $\omega = \frac{1}{2}(1+\sqrt{-3})$ and $P^k = (2^k, 2^k\omega)$. When $k=2$, G is of order 12 and is generated by $\delta = -\omega$, $\epsilon = \sqrt{-3}$, and $b = -1$, of periods 3, 2, and 2, respectively; written out in full, it is

$$\begin{aligned} &1 = 1, && \epsilon = -1+2\omega, && b = -1, && \epsilon b \equiv 1+2\omega, \\ &\delta = -\omega, && \delta\epsilon \equiv 2-\omega, && \delta b \equiv \omega, && \delta\epsilon b \equiv 2+\omega, \\ &\delta^2 \equiv -1+\omega, && \delta^2\epsilon \equiv -1-\omega, && \delta^2 b \equiv 1-\omega, && \delta^2\epsilon b \equiv 1+\omega, \end{aligned} \pmod{P^2}.$$

When $k=3$, G is of order 48 and is generated by $\delta = -\omega$ of period 3, $\sqrt{-3}$ of period 4, -1 of period 2, and $1+4\omega$ of period 2.

Table of Moduli, Elements, and Generators.

35. For convenience of reference we shall now exhibit in tabular form the principal results already obtained, namely those relating to the nine types of groups, mod P^k, and in addition, for the sake of completeness, those relating to two other types, the tenth and eleventh, to be treated in §§ 46–51.

Modulus $A = P^k$.

I. P unambiguous, of the first grade; $PP' = (p)$, $(d/p) = 1$.

Type 1. $p > 2$, $m \equiv 1, 2$, or $3 \pmod 4$. $P = (p, a_1+\omega)$, $P^k = (p^k, a_k+\omega)$, $\Phi(P^k) = p^{k-1}(p-1)$. Elements $u = 1, 2, \cdots, p^k-1$; $u \not\equiv 0 \pmod p$. Generators f, defined in § 5, and $1+p$; periods $p-1$ and p^{k-1}.

Type 2. $p=2$, $m \equiv 1 \pmod 8$. $P=(2,\omega)$, $P^k=(2^k, a_k+\omega)$, $\Phi(P^k)=2^{k-1}$. Elements $u = 1, 3, \cdots, 2^k-1$. Generators -1 and 5; periods 2 and 2^{k-2}.

II. P ambiguous, of the first grade; $P^2 = (p)$, $(d/p) = 0$.

II$_a$. $p > 2$, $m \equiv 1, 2$, or $3 \pmod 4$.

Type 3. Either $p > 3$ and $m \equiv 0 \pmod p$, or $p = 3$ and $m \equiv 3 \pmod 9$. $P = (p, \omega_1)$, $P^k = (p^r, p^s\omega_1)$, $\Phi(P^k) = p^{k-1}(p-1)$. Elements $\alpha = u + v\sqrt{m}$; $u = 1, 2, \cdots, p^r-1$; $u \not\equiv 0 \pmod p$; $v = 0, 1, \cdots, p^s-1$. Generators g, defined in § 11, $1+\sqrt{m}$, and $1+p$; periods $p-1$, p^s, and $1+p^{r-1}$.

Type 4. $p=3$ and $m\equiv -3 \pmod 9$. $P=(3,\ \omega_1)$, $P^k=(3^r,\ 3^s\omega_1)$, $\Phi(P^k)=3^{k-1}\cdot 2$. Elements $\alpha=u+v\sqrt{m}$; $u=1, 2, \cdots, 3^r-1$; $u\not\equiv 0 \pmod 3$; $v=0, 1, \cdots, 3^s-1$. Generators -1, λ, defined in § 17, 4, and $1+3\sqrt{m}$; periods 2, 3, 3^{r-1}, and 3^{s-1}, if $k>1$; 2, 1, 1, and 1, if $k=1$.

II$_b$. $p=2$.

Type 5. $m\equiv 2 \pmod 4$. $P=(2, \sqrt{m})$, $P^k=(2^r, 2^s\sqrt{m})$, $\Phi(P^k)=2^{k-1}$. Elements $\alpha=u+v\sqrt{m}$; $u=1, 3, \cdots, 2^r-1$; $v=0, 1, \cdots, 2^s-1$. Generators $1+\sqrt{m}$, -1, and 5; periods 2^s, 2, and 2^{r-2}, if $k>2$; 2, 1, and 1, if $k=2$.

Type 6. $m\equiv 3 \pmod 8$. $P=(2, 1+\sqrt{m})$, $P^k=(2^r, 2^s+2^s\sqrt{m})$, $\Phi(P^k)=2^{k-1}$. Elements $\alpha=u+v\sqrt{m}$; $u=0, 1, \cdots, 2^r-1$; $v=0, 1, \cdots, 2^s-1$; $u+v\equiv 1 \pmod 2$. Generators $\sqrt{m}$, $1+2\sqrt{m}$, and -1; periods 2^{r-1}, 2^{s-1}, and 2, if $k>4$; 2^r, 2^{s-1}, and 1, if $k=2$, 3, or 4.

Type 7. $m\equiv 7 \pmod 8$. $P=(2, 1+\sqrt{m})$, $P^k=(2^r, 2^s+2^s\sqrt{m})$, $\Phi(P^k)=2^{k-1}$. Elements $\alpha=u+v\sqrt{m}$, as in type 6. Generators μ, defined in § 26, $1+2\sqrt{m}$, and 5; periods 4, 2^{s-1}, and 2^{r-2}, if $k>2$; 2, 1, and 1, if $k=2$.

III. P of the second grade; $P=(p)$, $(d/p)=-1$.

Type 8. $p>2$, $m\equiv 1$, 2, or 3 $\pmod 4$. $P=(p, p\omega)$, $P^k=(p^k, p^k\omega)$, $\Phi(P^k)=p^{2k-2}(p^2-1)$. Elements $\alpha=u+v\omega$; $u, v=0, 1, \cdots, p^k-1$; u and v not both $\equiv 0 \pmod p$. Generators δ, defined in § 30, $1+p$, and $1+p\omega$; periods p^2-1, p^{k-1}, and p^{k-1}.

Type 9. $p=2$, $m\equiv 5 \pmod 8$. $P=(2, 2\omega)$, $P^k=(2^k, 2^k\omega)$, $\Phi(P^k)=2^{2k-2}\cdot 3$. Elements $\alpha=u+v\omega$; $u, v=0, 1, \cdots, 2^k-1$; u and v not both even. Generators δ, defined in § 30, $\sqrt{m}=-1+2\omega$, -1, and $1+4\omega$; periods 3, 2^{k-1}, 2, and 2^{k-2}, if $k>1$; 3, 1, 1, and 1, if $k=1$.

Modulus $A=P^kP'^k$, $P\neq P'$.

P unambiguous, of the first grade; $PP'=(p)$, $(d/p)=1$.

Type 10. $p>2$, $m\equiv 1$, 2, or 3 $\pmod 4$. $P=(p, a+\sqrt{m})$, if $m\equiv 2$ or 3 $\pmod 4$; $P=(p, \frac{1}{2}a+\frac{1}{2}\sqrt{m})$, if $m\equiv 1 \pmod 4$. $P^kP'^k=(p^k)$, $\Phi(A)=p^{2k-2}(p-1)^2$. Elements $\alpha=u+v\sqrt{m}$; $u, v=0, 1, \cdots, p^k-1$; $u\not\equiv \pm av \pmod p$. Generators h, defined in § 48, ζ, defined in § 48, $1+p$, and $1+p\sqrt{m}$; periods $p-1$, $p-1$, p^{k-1}, and p^{k-1}.

Type 11. $p=2$, $m\equiv 1 \pmod 8$. $P=(2, \frac{1}{2}+\frac{1}{2}\sqrt{m})$, $P^kP'^k=(2^k)$, $\Phi(A)=2^{2k-2}$. Elements $\alpha=u+v\sqrt{m}$; $u, v=0, 1, \cdots, 2^k-1$; $u+v\equiv 1 \pmod 2$. Generators -1, θ, defined in § 50, 5, and $1+2\sqrt{m}$; periods 2, 2, 2^{k-2}, and 2^{k-2}.

MODULUS ANY COMPOSITE IDEAL.

36. Having found the structure of the group G in every case in which the modulus is a power of a prime ideal, we now have sufficient material at hand for constructing the group in the general case in which the modulus is any composite ideal whatever. This is easily accomplished in a similar manner to that used in the rational number-field.*

Let $A = P_1^{k_1} \cdots P_n^{k_n}$ be any ideal whose distinct prime factors are $P_1, \cdots, P_n$. Then the order of the group G formed by a reduced system of residues with respect to the modulus A is $\Phi(A) = \Phi(P_1^{k_1}) \cdots \Phi(P_n^{k_n})$ and the group itself is the direct product of n subgroups $G_i\,(i = 1, \cdots, n)$, each of which is simply isomorphic with a corresponding group $\bar{G}_i$, whose elements form a reduced system of residues, mod $P_i^{k_i}$. Every quadratic integer α, prime to A, uniquely determines n residues $\alpha_1, \cdots, \alpha_n$, belonging respectively to $\bar{G}_1, \cdots \bar{G}_n$, which satisfy the congruences

$$\alpha \equiv \alpha_1 \pmod{P_1^{k_1}}, \quad \cdots, \quad \alpha \equiv \alpha_n \pmod{P_n^{k_n}}. \tag{10}$$

When every residue α_i ranges over the elements of its group $\bar{G}_i$, α, determined uniquely by congruences (10), will range once and only once over all the elements of the group G. When every $\alpha_j = 1\ (j \neq i)$, and α_i ranges over the elements of its group $\bar{G}_i$, α will range over the elements of the subgroup G_i $(i = 1, \cdots, n)$.

37. Let $\bar{\lambda}_i, \bar{\mu}_i$, etc., be a *complete set of independent generators* of the group $\bar{G}_i\,(i = 1, \cdots, n)$, and let their periods be l_i', m_i', etc., respectively. Then every element α_i of $\bar{G}_i$ is expressible in the form $\alpha_i \equiv \bar{\lambda}_i^{l_i} \bar{\mu}_i^{m_i} \cdots \pmod{P_i^{k_i}}$, where the exponents l_i, m_i, etc., are residues with respect to the corresponding periods, l_i', m_i', etc. The congruences (10) now become

$$\begin{aligned} \alpha &\equiv \bar{\lambda}_1^{l_1} \bar{\mu}_1^{m_1} \cdots \pmod{P_1^{k_1}}, \\ &\cdots\cdots\cdots \\ \alpha &\equiv \bar{\lambda}_n^{l_n} \bar{\mu}_n^{m_n} \cdots \pmod{P_n^{k_n}}. \end{aligned}$$

Corresponding to the generators $\bar{\lambda}_i, \bar{\mu}_i$, etc., of the groups $\bar{G}_i\,(i = 1, \cdots, n)$, we now define generators λ_i, μ_i, etc., of the subgroups $G_i\,(i = 1, \cdots, n)$, and therefore of the entire group G, by means of the congruences

$$\begin{aligned} \lambda_i &\equiv \bar{\lambda}_i \pmod{P_i^{k_i}} \\ &\equiv 1 \pmod{P_j^{k_j}} \quad (j = 1, \cdots, n;\ j \neq i), \\ \mu_i &\equiv \bar{\mu}_i \pmod{P_i^{k_i}} \\ &\equiv 1 \pmod{P_j^{k_j}} \quad (j = 1, \cdots, n;\ j \neq i), \\ &\cdots\cdots\cdots \end{aligned} \qquad (i = 1, \cdots, n).$$

* Cf. WEBER, *Algebra*, vol. 2, 2nd edition, pp. 60–61.

The generators $\lambda_1, \mu_1, \cdots, \lambda_n, \mu_n$, etc., so defined, are of periods $l_1', m_1', \cdots, l_n', m_n'$, etc., and form a complete set of independent generators of G, in terms of which every element α of the group can be written as follows

$$\alpha \equiv (\lambda_1^{l_1}\mu_1^{m_1}\cdots), \cdots, \alpha \equiv (\lambda_n^{l_n}\mu_n^{m_n}\cdots), \mod A.$$

The exponents $l_1, m_1, \cdots, l_n, m_n$, will be called the *indices* of the quadratic integer α with respect to the modulus A.

This completes the solution of the general problem of determining the group of classes of congruent quadratic integers with respect to any composite modulus. But there are certain special cases that merit separate treatment.

Cyclic Groups.

38. If the group G, whose modulus is the ideal A, can be generated by a single element η and is therefore *cyclic*, η is said to be a *primitive root* of A. The number of primitive roots of A, if there is one such, is $\phi[\Phi(A)]$, where ϕ is Euler's ϕ-function. If G is not cyclic, A does not possess primitive roots.

The object of this part of the paper, §§ 38–45 inclusive, is to enumerate all the cases in which G is cyclic and to give at least one primitive root in every case. G will be cyclic, (1) if there is only one independent generator, and (2) if the periods of each pair of independent generators are relatively prime. In examining for cyclic groups, therefore, it will be well to note (1) that p and $p-1$ are relatively prime, (2) if p is an odd prime, $p-1$ and p^2-1 are even, and (3) if $p>3$, p^2-1 is divisible by 3.

Case I. *Modulus a Power of a Prime Ideal;* $A = P^k$.

39. (a) Ideal P unambiguous, of the first grade.

(a_1) $p>2$, $m\equiv 1, 2,$ or $3 \pmod 4$. Modulus $P^k=(p^k, a_k+\omega)$. In this case G is of type 1 and is cyclic for all values of k. We choose as primitive root of A the rational integer $f(1+p)$, of period $p^{k-1}(p-1)$, where f is defined in § 5.

(a_2) $p=2$, $m\equiv 1 \pmod 8$. Here G is of type 2 and is cyclic, only if $k=2$ or 1.

Modulus $P^2=(4, 2a+\omega)$. Primitive root -1, of period 2.

Modulus $P=(2, \omega)$. Primitive root 1, of period 1. This case would be trivial except for its application to Case II.

(b) Ideal P ambiguous, of the first grade.

(b_1) $p>2$, $m\equiv 1, 2,$ or $3 \pmod 4$, $m\equiv 0 \pmod p$. G is of type 3 or 4, and can only be cyclic when $k=2$ or 1.

Modulus $P^2=(p, p\omega)$. Primitive root $g(1+\sqrt{m})$ (§ 11), of period $p(p-1)$.

Modulus $P=(p, \omega_1)$. Primitive root g, of period $p-1$.

(b_2) $p=2$, $m\equiv 2 \pmod 4$. G is of type 5, and is cyclic when $k=2$ or 1.

Modulus $P^2 = (2, 2\sqrt{m})$. Primitive root $1 + \sqrt{m}$, of period 2.

Modulus $P = (2, \sqrt{m})$. Primitive root 1, of period 1.

(b_3) $p = 2$, $m \equiv 3 \pmod 4$. G is of type 6 or 7 and is cyclic, when $k = 3$, 2, or 1.

Modulus $P^3 = (4, 2 + 2\sqrt{m})$. Primitive root $\sqrt{m}$, of period 4.

Modulus $P^2 = (2, 2 + 2\sqrt{m})$. Primitive root $\sqrt{m}$, of period 2.

Modulus $P = (2, 1 + \sqrt{m})$. Primitive root 1, of period 1.

(c) Ideal P of the second grade.

G is of type 8 or 9 and is cyclic only when $k = 1$.

Modulus $P = (p, p\omega)$. Primitive root δ, defined in § 30, of period $p^2 - 1$. In the two simplest cases in which $p = 3$ and $p = 2$, δ can be found easily by means of a formula. Namely, if $p = 3$, $1 + \sqrt{m}$ is always a primitive root of P, of period 8, and if $m \equiv 1 \pmod 4$, $\omega = \frac{1}{2}(1 + \sqrt{m})$ is also a primitive root; again, if $p = 2$ and therefore $m \equiv 5 \pmod 8$, $\omega = \frac{1}{2}(1 + \sqrt{m})$ is a primitive root of P, of period 3.

40. Summarizing these results, we observe first that G is always cyclic when the modulus is the first power of P whether P is of the first or second grade. This agrees with the well-known fact that every prime ideal possesses primitive roots. Next we observe that *when P is a prime ideal of the first grade, whether ambiguous or not, P^2 as well as P possesses primitive roots; and when P is an ambiguous prime whose norm is 2, and $m \equiv 3 \pmod 4$, then P, P^2, and P^3 all have primitive roots. Finally, the only case in which P^k has primitive roots for all values of k is that in which P is an unambiguous prime of the first grade whose norm p exceeds 2.*

Case II. *Cyclic Groups with Modulus Divisible by Two Distinct Prime Ideals;* $A = P^k Q^l$.

41. To obtain the moduli that come under this case, we multiply together any two (more than two are evidently impossible) prime-power moduli coming under Case I, which occur for the same value of m and which are so related that the periods of their primitive roots are relatively prime. If P^k and Q^l are two such moduli, and if ρ, of period r, and σ, of period s, are a pair of their respective primitive roots, then a primitive root η of the modulus $A = P^k Q^l$ is defined by the congruences

$$\eta \equiv \rho \pmod{P^k}, \qquad \eta \equiv \sigma \pmod{Q^l}.$$

For, since r and s are relatively prime, η is of period rs.

42. Examining the moduli of case 1, we find that they fall into three classes: first, those whose primitive roots are of period 3, namely those for which P is of the second grade, $p = 2$, $k = 1$, and therefore $m \equiv 5 \pmod 8$; second, those

whose primitive roots are of period 1, namely those for which P is of the first grade, $p = 2$, $k = 1$, and therefore $m \equiv 1, 2, 3, 6$, or $7 \pmod 8$; and third, those whose primitive roots are of even period, namely all the remainder of the moduli.

Now it is clear that for a given value of m there exists just one modulus (or at most two, in a certain exceptional case) of either the first or second class, and an infinite number of moduli of the third class. But the product of two moduli of the third class will not have primitive roots. Therefore, to obtain a modulus having primitive roots we are restricted (with one exception) to multiplying a modulus of the third class by the particular modulus of the first or second class that happens to exist for the given value of m.

Subcase II_a. $m \equiv 5 \pmod 8$.

43. In this case there exists a modulus of the first class, namely a prime ideal $Q = (2, 2\omega)$ of the second grade having a primitive root $\omega = \frac{1}{2}(1 + \sqrt{m})$ of period 3. We proceed to construct moduli of the form $P^k Q$ by selecting from the third class an ideal P^k such that $\mathrm{p} > 2$ and the period of its primitive roots is not divisible by 3. If ρ is a primitive root of P^k, then the congruences

$$\eta \equiv \rho \pmod{P^k}, \qquad \eta \equiv \omega \pmod{Q}$$

determine a primitive root η of $P^k Q$.

(a) Ideal P unambiguous, of the first grade, $(m/p) = 1$.

(a_1) $p > 3$, $p \equiv 2 \pmod 3$, $P^k = (p^k, a_k + \omega)$.

Modulus $P^k Q = (2p^k, 2a_k + 2\omega)$. Primitive root $\eta = f(1 + p) + ep^k + a_k + \omega$ of period $3p^{k-1}(p - 1)$, where f is defined in § 5, and $e = 0$ or 1 according as a_k is even or odd.

(a_2) $p = 3$, $m \equiv 13 \pmod{24}$, $P = (3, \omega)$.

Modulus $PQ = (6, 2\omega)$. Primitive root $\eta = 2 + \omega$ of period 6.

(b) Ideal P ambiguous, of the first grade, $m \equiv 0 \pmod p$.

(b_1) $p > 3$, $p \equiv 2 \pmod 3$, $P = (p, \frac{1}{2}p - \frac{1}{2} + \omega)$, $P^2 = (p, p\omega)$.

Modulus $P^2 Q = (2p, 2p\omega)$. Primitive root $\eta = (2g + p)\omega$ (see § 11) of period $3p(p - 1)$.

Modulus $PQ = (2p, p - 1 + 2\omega)$. Primitive root $\eta = g + ep + \frac{1}{2}(p - 1) + \omega$ of period $3(p - 1)$, where $e = 0$ or 1 according as $g + \frac{1}{2}(p - 1)$ is even or odd.

(b_2) $p = 3$, $m \equiv -3 \pmod{24}$, $P = (3, 1 + \omega)$.

Modulus $PQ = (6, 2 + 2\omega)$. Primitive root $\eta = \omega$, of period 6.

(c) Ideal P of the second grade.

$p = 3$, $m \equiv 5 \pmod{24}$, $P = (3, 3\omega)$.

Modulus $PQ = (6, 6\omega)$. Primitive root ω of period 24.

Subcase II_b. $m \equiv 1, 2, 3, 6$, or $7 \pmod 8$.

44. In this case there exists a modulus of the second class, namely a prime ideal $Q = (2, b + \omega)$ of the first grade, having a primitive root 1 of period 1. Any modulus of the form $P^k Q$ for which P^k belongs to the third class and $p > 2$ will obviously have a primitive root η whose period is equal to that of the primitive roots of P^k. If ρ is one of the latter, then η can be defined by the congruences

$$\eta \equiv \rho \pmod{P^k}, \qquad \eta \equiv 1 \pmod{Q}.$$

(*a*) Ideal P unambiguous, of the first grade, $p > 2$, $P^k = (p^k, a_k + \omega)$.

Modulus $P^k Q = (2p^k, b_k + \omega)$. Primitive root $\eta = f(1 + p) + p^k$ (see § 5), of period $p^{k-1}(p - 1)$.

In the two remaining cases, in which P is ambiguous or of the second grade, it is evident that η will be equal to ρ or $\rho + p$; therefore in every case $\eta = \rho + ep$, where $e = 0$ or 1.

(*b*) Ideal P ambiguous, $p > 2$, $m \equiv 0 \pmod p$, $P = (p, a + \omega)$, $P^2 = (p, p\omega)$.

Modulus $P^2 Q = (2p, bp + p\omega)$. Primitive root $\eta = g(1 + \sqrt{m}) + ep$ (see § 11), of period $p(p - 1)$.

Modulus $PQ = (2p, c + \omega)$. Primitive root $\eta = g + ep$, of period $p - 1$.

(*c*) Ideal P of the second grade, $p > 2$, $P = (p, p\omega)$.

Modulus $PQ = (2p, bp + p\omega)$. Primitive root $\eta = \delta + ep$ (see § 30), of period $p^2 - 1$.

Subcase II_c.

45. This is the exceptional case mentioned in § 42, in which the modulus is divisible by two distinct conjugate primes P and P'. P is therefore an unambiguous prime of the first grade, $p = 2$, and $m \equiv 1 \pmod 8$. $P = (2, \omega)$ and $P' = (2, \omega')$.

Modulus $P^2 P' = (4, 2\omega)$. Primitive root -1, of period 2.

Modulus $PP' = (2, 2\omega)$. Primitive root 1, of period 1.

We have now exhausted all the possible cases of cyclic groups.

Modulus $(p^k) = P^k P'^k$.

46. A rational prime p, considered as a principal ideal (p), may be either a prime ideal of the second grade, or the square of an ambiguous prime of the first grade, or finally the product of an unambiguous prime of the first grade and its conjugate. The corresponding group of residues with respect to the modulus (p^k) has been considered for the first two cases in §§ 29–34 and 7–28, respectively. For the last case, in which the modulus contains two distinct conjugate primes, the general procedure of §§ 36, 37 is applicable, but a special direct method will now be developed, giving simpler results.

Let P be any unambiguous prime ideal of the first grade and P' its conjugate; then $(d/p) = 1$, and $PP' = (p) = (p, p\omega)$. Let

$$A = P^k P'^k = (p^k) = (p^k, p^k\omega),$$

and let G be the group of residues prime to the modulus A. G will be of two distinct types, depending on the value of p. Continuing the former numbering, we shall call them types 10 and 11. The results to be obtained have already been tabulated in § 35.

Type 10. $p > 2$.

47. In this case m may be $\equiv 1, 2$, or $3 \pmod 4$, and $P = (p, a_1 + \omega)$, $P' = (p, a_1 + \omega')$. If $m \equiv 2$ or $3 \pmod 4$, $\omega = \sqrt{m}$, $\omega' = -\sqrt{m}$, and, putting $a_1 = a$, we have

$$P = (p, a + \sqrt{m}), \qquad P' = (p, a - \sqrt{m}). \tag{11}$$

If $m \equiv 1 \pmod 4$,

$$a_1 + \omega = \frac{2a_1 + 1 + \sqrt{m}}{2}, \qquad a_1 + \omega' = \frac{2a_1 + 1 - \sqrt{m}}{2};$$

putting $2a_1 + 1 = a$, we have

$$P = \left(p, \frac{a + \sqrt{m}}{2}\right), \qquad P' = \left(p, \frac{a - \sqrt{m}}{2}\right). \tag{12}$$

Instead of writing the elements of G in the form $u + v\omega$, it will be allowable and convenient, exactly as in the similar case of § 10, to write them in the form $u + v\sqrt{m}$, where u and v are rational integers, residues with respect to the modulus p^k.

Since every element $u + v\sqrt{m}$ must be prime to P and also to P', therefore in view of (11) and (12) u and v must satisfy the condition $u \not\equiv \pm av \pmod p$. This gives $p^{2k-2}(p-1)^2$ as the order of the group, in accord with the value of $\Phi(A)$ and also with the fact (see § 36) that G is the direct product of two cyclic subgroups of order $p^{k-1}(p-1)$, which are simply isomorphic with groups whose moduli are P^k and P'^k, respectively.

48. As generators we could choose two independent elements of period $p^{k-1}(p-1)$, but we shall rather, in accordance with our former rule, choose four independent generators, two of period $p-1$ and, if $k > 1$, two others of period p^{k-1}. It is obvious that the two latter can be chosen to be $1 + p$ and $1 + p\sqrt{m}$, and that they generate a subgroup H, of order p^{2k-2}, comprising the residues $1 + pu + pv\sqrt{m}$, where u and v range from 0 to $p^{k-1} - 1$.

Let h be a rational residue of period $p-1$, like the generator f in type 1 (§ 5), and let ζ be a residue, necessarily irrational, satisfying the congruences

$$\zeta \equiv h \pmod{P^k}, \qquad \zeta \equiv 1 \pmod{P'^k}. \tag{13}$$

Then ζ is also of period $p-1$ and is evidently independent of h (cf. § 37).

Hence G is generated by the following four elements: h and ζ, both of period $p-1$, and if $k>1$, $1+p$ and $1+p\sqrt{m}$, both of period p^{k-1}. The rational residues are generated by $1+p$ and h; if we add to the rational residues the rational multiples of $\sqrt{m}$, we obtain a subgroup of order $2p^{k-1}(p-1)$, which is generated by $1+p$, h, and $\zeta^{\frac{1}{2}(p-1)}$. Every residue of period p^i $(0\leqq i<k)$ is of the form $1+p^{k-i}(u+v\sqrt{m})$, where u and v are not both divisible by p.

49. *Example.* Let $m=-1$, $p=5$, and $k=1$; then $P=(5, 2+i)$, $P'=(5, 2-i)$, $A=PP'=(5, 5i)$, and $\Phi(A)=16$. The elements of G are $u+vi$, where $u, v=0, \pm 1, \pm 2$, and $u \not\equiv \pm 2v \pmod 5$. Its generators are $h=2$ and $\zeta=-1+i$, defined by (13), both of period 4. In terms of h and ζ, G may be written out, as follows:

$$\begin{array}{llll} 1=1, & \zeta=-1+i, & \zeta^2\equiv -2i, & \zeta^3\equiv 2+2i, \\ h=2, & h\zeta\equiv -2+2i, & h\zeta^2\equiv i, & h\zeta^3\equiv -1-i, \\ h^2\equiv -1, & h^2\zeta\equiv 1-i, & h^2\zeta^2\equiv 2i, & h^2\zeta^3\equiv -2-2i, \\ h^3\equiv -2, & h^3\zeta\equiv 2-2i, & h^3\zeta^2\equiv -i, & h^3\zeta^3\equiv 1+i, \end{array} \pmod{PP'}.$$

If we had used the general method of § 37, the generators would have been $-1+i$ and $-1-i$.

Type 11. $p=2$.

50. In this case $m\equiv 1 \pmod 8$, $P=(2, \omega)=(2, \frac{1}{2}+\frac{1}{2}\sqrt{m})$, and $P'=(2, \omega')=(2, \frac{1}{2}-\frac{1}{2}\sqrt{m})$; also $A=(2^k, 2^k\omega)=(2^k, 2^{k-1}+2^{k-1}\sqrt{m})$. Since the residues $u+v\sqrt{m}$ are subject to the condition $u \not\equiv v \pmod 2$, it follows that either u is odd and v even, or u is even and v odd. Except for this restriction u ranges from 0 to 2^k-1 and v ranges from 0 to $2^{k-1}-1$. G is therefore of order 2^{2k-2}, which agrees with the value of $\Phi(A)$. If $k>1$, the residues for which u is odd and v even, namely those of the form $1+2u+2v\sqrt{m}$, obviously constitute a subgroup H of index 2 and order 2^{2k-3}. H is generated by the rational residues and the irrational residue $1+2\sqrt{m}=-1+4\omega$, of period 2^{k-2}; and the former are generated, as usual, by -1 and 5, of periods 2 and 2^{k-2}, respectively. Finally, G is generated by H and a single element θ of period 2 of the form $2u+(2v+1)\sqrt{m}$; if $k>2$, θ *can be chosen in eight different ways*, the simplest of which is the following:

$$\theta = x\sqrt{m}, \tag{14}$$

where x is a root of the congruence

$$mx^2 \equiv 1 \pmod{2^k}. \tag{15}$$

This congruence can always be solved for x, since m, being congruent to

$1 \pmod 8$, is necessarily a square, mod $2^k (k > 2)$; if $k = 2$, the same is true. Therefore, if $k > 1$, θ is a generator of period 2 of the required form.

Summing up, we may say that *the group G of reduced residues with respect to the modulus $(2^k) = P^k P'^k$ is of order 1, if $k = 1$* (cf. § 45, cyclic groups); *if $k > 1$, it has the two independent generators -1, of period 2, and θ defined by* (14) *and* (15), *also of period 2; if $k > 2$, it has the two additional independent generators 5 and $1 + 2\sqrt{m}$, both of period 2^{k-2}.*

The residues $1 + 4u + 2v\sqrt{m}$ evidently form a subgroup of order 2^{2k-4} generated by 5 and $1 + 2\sqrt{m}$.

51. *Example.* If $m = -7$ and $k = 3$, then $P = (2, \frac{1}{2} + \frac{1}{2}\sqrt{-7})$ and $A = P^3 P'^3 = (8, 4 + 4\sqrt{-7})$. G is of order 16 and is generated by the four independent elements $a = -1$, $b = 5$, $\theta = \sqrt{-7}$, and $\lambda = 1 + 2\sqrt{-7}$, all of period 2. Thus:

$$\begin{array}{llll} 1 \equiv 1, & \theta \equiv \sqrt{-7}, & \lambda \equiv 1 + 2\sqrt{-7}, & \theta\lambda \equiv 2 + \sqrt{-7}, \\ a \equiv 7, & a\theta \equiv 4 + 3\sqrt{-7}, & a\lambda \equiv 3 + 2\sqrt{-7}, & a\theta\lambda \equiv 2 + 3\sqrt{-7}, \\ b \equiv 5, & b\theta \equiv 4 + \sqrt{-7}, & b\lambda \equiv 5 + 2\sqrt{-7}, & b\theta\lambda \equiv 6 + \sqrt{-7}, \\ ab \equiv 3, & ab\theta \equiv 3\sqrt{-7}, & ab\lambda \equiv 7 + 2\sqrt{-7}, & ab\theta\lambda \equiv 6 + 3\sqrt{-7}, \end{array} \pmod{P^3 P'^3}.$$

Considerations of Rationality.

52. We shall now take up certain considerations of rationality that naturally give rise to two special kinds of moduli. Let $A = (gl, hl + l\omega)$ be any ideal in the number-field $k(\sqrt{m})$; then $A = A_1 A_2$, where $A_1 = (l)$ and $A_2 = (g, h + \omega)$. Thus A_1 is a rational principal ideal and A_2 will be called a *completely irrational ideal*, because it contains no rational factors. If the unit ideal (1) is regarded as belonging to both classes, then every ideal whatever can be factored in one and essentially only one way into two factors, one of which is a rational principal ideal and the other a completely irrational ideal. Evidently the norm of A is $n(A) = gl^2$, and $n(A_1) = l^2$, $n(A_2) = g$.

Let us examine the character of the prime factors of A_1 and of A_2. Since a completely irrational ideal A_2 cannot be divisible by a prime of the second grade, or by a power of an ambiguous prime of the first grade higher than the first, or finally by the conjugate of any of its unambiguous prime factors of the first grade, and since the converse evidently holds, therefore A_2 is characterized by being expressible in the form

$$A_2 = P_1^{s_1} \cdots P_i^{s_i} \cdot Q_1 \cdots Q_j, \tag{16}$$

where $P_1, \cdots, P_i$ are distinct unambiguous primes of the first grade, no two of which are conjugate, and $Q_1, \cdots, Q_j$ are distinct ambiguous primes.

53. On the other hand, if a rational principal ideal A_1 contains an unambig-

uous prime factor of the first grade, it must contain the same power of its conjugate, and if it contains an ambiguous prime factor Q, the highest power of Q which it contains must be an even power. Therefore A_1 is characterized by being expressible in the form

$$A_1 = (P_1 P_1')^{u_1} \cdots (P_i P_i')^{u_i} \cdot Q_1^{2v_1} \cdots Q_j^{2v_j} \cdot R_1^{w_1} \cdots R_k^{w_k}, \tag{17}$$

where P_1 and P_1' are conjugate unambiguous primes of the first grade, $Q_1, \cdots, Q_j$ are ambiguous primes, and $R_1, \cdots, R_k$ are primes of the second grade.

In other words, *an ideal A_1 is a rational principal ideal if, and only if, its unambiguous prime factors of the first grade enter in pairs of conjugates and its ambiguous prime factors are raised to even powers.*

We now turn to the consideration of the groups whose moduli are A_1 and A_2, respectively, and their special peculiarities. It is obvious that the group whose modulus is $A_1 A_2$ is not, in general, the direct product of two subgroups simply isomorphic with the groups whose moduli are A_1 and A_2, respectively.

Modulus a completely irrational ideal.

54. First, let G be the group of reduced residues with respect to a completely irrational modulus $A_2 = (g, h + \omega)$ whose prime factors are given by formula (16). Evidently $g = n(A_2) = p_1^{s_1} \cdots p_i^{s_i} \cdot q_1 \cdots q_j$, and the order of G is $\Phi(A_2) = \phi(g) = \phi[n(A_2)]$. Now since the coefficient of ω in the canonical form of A_2 is 1, the elements of G all have rational residues and G is simply isomorphic with the group of rational residues, mod g. Conversely, if A_2 is not completely irrational, the elements of G cannot all have rational residues. For by reference to the groups of types 8–11, and to those groups of types 3–7 in which $k > 1$, we see that they all contain elements whose residues are necessarily irrational. We have therefore proved the following theorem:

A necessary and sufficient condition that the elements of a group of quadratic integers with respect to an ideal modulus all have rational residues is that the modulus be a completely irrational ideal.

Modulus a rational principal ideal.

55. Again, consider the group G of reduced residues with respect to a rational principal ideal $A_1 = (l, l\omega)$ whose prime factors are given by formula (17). In this case the group is of peculiar interest because *its elements can be defined without using the language of ideals at all.* Thus the congruence $a + b\omega \equiv a' + b'\omega \pmod{A_1}$ is equivalent to the pair of rational congruences $a \equiv a', b \equiv b' \pmod{l}$, and the quadratic integer $a + b\omega$ will be prime to the ideal A_1 if, and only if, it is prime to the rational integer l. Therefore *G is really the group of classes of congruent quadratic integers with respect to a rational modulus l.*

56. In order to determine its structure when the field $k(\sqrt{m})$ and the rational integer l are given, we proceed as follows. First factor l and classify its prime factors into p's, q's, and r's in such a way that d, the discriminant of the field, is a square with respect to every p, a multiple of every q, and a non-square with respect to every r (if $p = 2$ or $r = 2$, d is a square or non-square, respectively, with respect to 8, instead of 2), or, briefly, so that $(d/p) = 1$, $(d/q) = 0$, and $(d/r) = -1$ for every p, q, and r, respectively. Suppose the result to be

$$l = p_1^{\mu_1} \cdots p_i^{\mu_i} \cdot q_1^{\nu_1} \cdots q_j^{\nu_j} \cdot r_1^{\omega_1} \cdots r_k^{\omega_k}.$$

Then the prime factors of the ideal A_1 will be precisely those given by (17), since l^2 is the norm of A_1, and since the unambiguous primes of the first grade enter in pairs of conjugates.

Now determine the groups whose moduli are the prime-power factors of A_1, except that simplicity will be gained by substituting for the pair of groups of types 1 or 2, whose moduli are $P_1^{\mu_1}$ and $(P_1')^{\mu_1}$, respectively, the single group of type 10 or 11, whose modulus is $(P_1 P_1')^{\mu_1}$, and by doing the same in the case of the other P's. Find the generators, therefore, of the groups of types 10 and 11, whose moduli are $(P_1 P_1')^{\mu_1}$, etc., of the groups of types 3–7, whose moduli are $Q_1^{2\nu_1}$, etc., and of the groups of types 8 and 9, whose moduli are $R_1^{\omega_1}$, etc. Finally, find the corresponding generators of the group G, whose modulus is (1), by using the method of § 37. In this way we obtain *a complete set of independent generators of any group of quadratic integers, whose modulus is a rational integer.*

57. *Example* 1. In the field $k(\sqrt{-35})$ find the group G whose modulus is the rational principal ideal $A_1 = (30)$. Here $\omega = \frac{1}{2}(1 + \sqrt{-35})$, $l = 30$, $d = -35$, and the elements of G are residues $a + b\omega$, mod 30, namely those which are prime to 30. Since $30 = 2 \cdot 5 \cdot 2$, and $(d/3) = 1$, $(d/5) = 0$, $(d/2) = -1$, therefore $p = 3$, $q = 5$, and $r = 2$; consequently $(3) = PP'$, $(5) = Q^2$, $(2) = R$, and $(30) = PP \cdot Q^2 \cdot R$. The group whose modulus is PP' is of type 10 and is generated by -1 and $-1-\omega$, both of period 2: the group whose modulus is Q^2 is of type 3 and is generated by 2, of period 4, and 2ω, of period 5; the group whose modulus is R is of type 9 and is generated by ω, of period 3. The corresponding generators, λ_1, μ_1, λ_2, μ_2, λ_3, of G itself are therefore defined by the congruences

$$\begin{aligned}
\lambda_1 &\equiv -1 \pmod 3 \equiv 1 \pmod 5 \equiv 1 \pmod 2,\\
\mu_1 &\equiv -1-\omega \text{ “ } \equiv 1 \text{ “ } \equiv 1 \text{ “ },\\
\lambda_2 &\equiv 1 \text{ “ } \equiv 2 \text{ “ } \equiv 1 \text{ “ },\\
\mu_2 &\equiv 1 \text{ “ } \equiv 2\omega \text{ “ } \equiv 1 \text{ “ },\\
\lambda_3 &\equiv 1 \text{ “ } \equiv 1 \text{ “ } \equiv \omega \text{ “ }.
\end{aligned}$$

The simplest solutions of these congruences are $\lambda_1 = 11$, $\mu_1 = 11 - 10\omega$, $\lambda_2 = 7$, $\mu_2 = -5 + 12\omega$, $\lambda_3 = 16 + 15\omega$. These are therefore independent generators of G and their periods are 2, 2, 4, 5, and 3, respectively; G is of order 240.

Example 2. By way of strong contrast to the first example take the same modulus (30), but a different field $\mathrm{k}(\sqrt{-1})$. In this case $\omega = \sqrt{-1}$, $d = -4$, $l = 30$, $(d/5) = 1$, $(d/2) = 0$, $(d/3) = -1$, $(5) = PP'$, $(2) = Q^2$, $(3) = R$. Mod PP', the group is of type 10 and is generated by 2 and $1 + \omega$; mod Q^2, the group is of type 7 and is generated by ω; mod R, the group is of type 8 and is generated by $1 + \omega$. G is of order 256, and is generated by $\lambda_1 = 7$, $\mu_1 = 1 + 6\omega$, $\lambda_2 = 16 + 15\omega$, $\lambda_3 = 1 + 10\omega$, whose periods are 4, 4, 2, and 8, respectively.

It is to be noticed that out of the 900 residues $a + b\omega$, mod 30, those which are prime to 30 form two entirely different groups in these two examples, groups which differ in their elements, their orders, their generators, and their invariants. Even residues that are common to the two groups are not necessarily of the same period; e. g., the generator $16 + 15\omega$, which is of period 3 in the first example, is of period 2 in the second.

58. Since completing the above paper I have found in §§ 96–98 of the third volume of Weber's *Algebra*, which was published last year, some results that are rather closely connected with §§ 52–57 of this paper. The immense advantage gained by the theory of numbers from a liberal use of the group concept has been clearly shown by Weber throughout his Algebra (as well as by Bachmann in his books and by G. A. Miller in his memoirs); and although the particular kind of group that I have here investigated is, I believe, entirely new, still Weber approaches very close to it in § 98 of the third volume. His groups O, O', and O_0 are of infinite order, but the quotient-group O/O_0 is of finite order and is a special case of my group G, namely the case in which the modulus is a rational principal ideal; and the quotient-group O'/O_0 is the subgroup of G whose elements have rational residues. Moreover, his "primary ideals," of § 97, are my "completely irrational ideals" of § 52, and his "4. Satz," page 354, is practically the same as my theorem of § 54.

CORNELL UNIVERSITY, *July*, 1909.