CYCLOTOMY WHEN e IS COMPOSITE*

BY

L. E. DICKSON

1. **Introduction.** This paper is a sequel to two earlier ones.† Let p be a prime and e a divisor of $p-1=ef$. We seek the e^2 cyclotomic constants (k, h). The difficulties increase roughly as e increases, but more exactly with Euler's function $\phi(e)$. We have $\phi(e) \leqq 4$ only when $e=1$-6, 8, 10, 12; for each of these e's a simple complete theory was given in D. It is known that $\phi(e)$ is even if $e>2$. We have $\phi(e)=6$ only when $e=7$, 9, 14, 18; $\phi(e)=8$ only when $e=15$, 16, 20, 24, 30; $\phi(e)=10$ only when $e=11$, 22. The case in which e is a prime or a double of a prime was treated in T.

Here we give a simple complete theory for $e=9$ and the further facts sufficient for a complete theory for $e=18$. We have overcome difficulties which did not arise in the earlier papers. We treat briefly the five cases having $\phi(e)=8$; there is now trouble in the determination of a unit factor.

2. **Subdivision of periods.** Let d be any divisor of e and write $E=e/d$. In the definition of the e periods η_k, replace e by E and f by df; we get the E periods

$$Y_k = \sum_{j=0}^{d-1} \eta_{k+jE} \qquad (k = 0, \cdots, E-1). \tag{1}$$

By T, (3),

$$Y_0 Y_k = \sum_{h=0}^{E-1} (k, h)_E Y_h + \text{const.}, \quad Y_h = \eta_h + \eta_{h+E} + \cdots .$$

The general term of the product is

$$\eta_{tE}\eta_{k+jE} = \sum_{n=0}^{e-1} (k + jE - tE, n)\eta_{n+tE} + \text{const.}$$

Let $0 \leqq k < E$, $0 \leqq h < E$. By the terms in η_h,

$$(k, h)_E = \sum_{t,j=0}^{d-1} (k + jE - tE, h - tE).$$

Since the two arguments may be reduced modulo e,

* Presented to the Society, April 20, 1935; received by the editors March 18, 1935.

† These Transactions, vol. 37 (1935), pp. 363–380, cited as T. American Journal of Mathematics, vol. 57 (1935), cited as D.

$$(2) \qquad (k, h)_E = \sum_{r,s=0}^{d-1} (k + rE, h + sE).$$

This proof is much simpler than that in D, §14, for the case $d=2$.

The primitive eth roots of unity satisfy an equation of degree $\phi(e)$ with integral coefficients. Its roots are β^k, where $0<k<e$ and k is prime to e. For the field of rational numbers, the general substitution of its Galois group G is induced by the replacement of β by β^k. Hence the latter yields a true relation when applied to a known one. But this may not be the case when k is not prime to e.

In T, (7), take $e=dE$, $m=dM$. In the terms with $j=tE, \cdots, tE+E-1$, take $j=J+tE$ and apply $\beta^{dE}=1$ and (1). We get

$$\sum_{J=0}^{E-1} \beta^{dMJ} \sum_{t=0}^{d-1} \eta_{J+tE} = \sum_{J=0}^{E-1} B^{MJ} Y_J = \phi(B^M),$$

where $B=\beta^d$ is a primitive Eth root of unity. Evidently $\phi(B^M)$ is derived from $F(\beta^M)$ in T, (7), by replacing e by E, β by B, η by Y. Hence $F(\beta^{dM})=\phi(B^M)$. Then T, (8), gives

$$(3) \qquad R(dr, ds, \beta)_e = R(r, s, \beta^d)_E.$$

PART I. THEORY FOR $e=9$

3. **The functions $R(m, n)$.** If $p=9f+1=$prime, t is even. When β is replaced by β^j, where j is prime to 9, it is known that $R(m,n)$ becomes $R(jm, jn)$, which is called a *conjugate* to $R(m, n)$. If m is prime to 3, we can choose j so that $jm\equiv 1 \pmod 9$. Hence unless m and n are both multiples of 3, $R(m, n)$ is conjugate to a certain $R(1, -)$. But $R(1, 1)=R(1, 7)$ is conjugate to $R(4, 28)=R(1, 4)$. Also $R(1, 6)=R(1, 2)$ is conjugate to $R(5, 10)=R(1, 5)=R(1, 3)$. Hence *every $R(m, n)$ is conjugate to one of* $R(1, 1)$, $R(1, 2)$, $R(3, 3)$.

We readily find $R(3, 3)$. By (32)-(34) of D,

$$(4) \qquad 2R(1, 1)_3 = L + 3M + 6\beta M, \quad M = (0, 1)_3 - (0, 2)_3,$$

$$(5) \qquad 4p = L^2 + 27M^2, \qquad L = 9(0, 0)_3 - p + 8 \equiv 7 \pmod 9.$$

By (3), $R(3, 3)_9=R(1, 1, \beta^3)_3$, whence

$$(6) \qquad 2R(3, 3) = L + 3M + 6\beta^3 M.$$

Jacobi* noted that if $\alpha^{p-1}=1$, $\alpha\neq 1$, and if γ is an imaginary cube root of unity, then

$$(7) \qquad F(\alpha)F(\gamma\alpha)F(\gamma^2\alpha) = \alpha^{-3m'}pF(\alpha^3), \qquad 3 \equiv g^{m'} \pmod p.$$

* Journal für Mathematik, vol. 30 (1846), p. 167.

We may take $\gamma=\beta^3, \alpha=\beta^4, p=F(\beta^4)F(\beta^5)$. We get

$$R(1, 7) = \beta^{-3m'}R(3, 5); \qquad R(1, 1) = R(1, 7),$$
$$R(3, 5, \beta^2) = R(6, 1) = R(1, 2),$$
$$R(1, 2) = \beta^{6m'}R(1, 1, \beta^2). \tag{8}$$

4. **Determination of the 81 cyclotomic constants** $(k, h)=kh$. The equalities T, (4), between the (k, h) become for $e=9$

$$11 = 08, 18 = 12, 22 = 07, 23 = 17, 27 = 24, 28 = 13, 33 = 06,$$
$$34 = 16, 35 = 26, 37 = 25, 38 = 14, 44 = 05, 45 = 15, 46 = 25,$$
$$47 = 26, 48 = 15, 55 = 04, 56 = 14, 57 = 24, 58 = 16, 66 = 03,$$
$$67 = 13, 68 = 17, 77 = 02, 78 = 12, 88 = 01, kh = hk.$$

The linear relations T, (5), now become

$$\sum_{h=0}^{8}(0, h) = f - 1, \qquad 01 + 08 + 2(12) + \sum_{h=3}^{7}(1, h) = f,$$
$$02 + 07 + 12 + 13 + 17 + 2(24) + 25 + 26 = f, \tag{9}$$
$$03 + 06 + 13 + 14 + 16 + 17 + 25 + 26 + 36 = f,$$
$$04 + 05 + 14 + 2(15) + 16 + 24 + 25 + 26 = f.$$

The sum of the last four less the first is

$$3(12 + 13 + 14 + 15 + 16 + 17 + 24 + 25 + 26) = 3f + 1 + (00) - (36). \tag{10}$$

In (4) and (5) we have by (2),

$$(0, 0)_3 = (0, 0) + 3(0, 3) + 3(0, 6) + 2(3, 6), \tag{11}$$

$$M = 01 - 02 + 04 - 05 + 07 - 08 + 2\{13 - 14 + 16 - 17 + 25 - 26\}. \tag{12}$$

Using T, (8), and checking by T, (16), we get after using

$$\beta^6 + \beta^3 + 1 = 0, \tag{13}$$

$$R(1, 1) = \sum_{i=0}^{5} c_i\beta^i, \qquad R(1, 2) = \sum_{i=0}^{5} b_i\beta^i, \tag{14}$$

$$c_0 = (00) - 3(06) + 2(36),$$
$$c_1 = 01 + 04 - 2(07) + 2(13) - 4(16) + 2(25),$$
$$c_2 = 2(02) - 05 - 08 + 4(14) - 2(17) - 2(26), \qquad c_3 = 3(03) - 3(06),$$
$$c_4 = -01 + 2(04) - 07 + 4(13) - 2(16) - 2(25),$$
$$c_5 = 02 + 05 - 2(08) + 2(14) + 2(17) - 4(26);$$

$$b_0 = 00 - 01 - 04 - 07 + 13 + 16 + 25 - 36,$$
$$b_1 = 01 + 05 - 07 - 08 + 12 - 2(15) + 16 - 17 + 24 - 25 + 26,$$
$$b_2 = 01 + 02 - 04 - 08 - 12 + 13 - 14 + 2(15) - 24 - 25 + 26,$$
$$b_3 = -01 + 02 - 04 + 05 - 07 + 08 + 13 - 14 + 16 - 17 + 25 - 26,$$
$$b_4 = 02 + 04 - 07 - 08 + 2(12) - 13 - 14 - 15 + 16 - 24 + 26,$$
$$b_5 = -04 + 05 + 07 - 08 + 12 + 13 + 15 - 16 - 17 - 2(24) + 26.$$

These twelve equations with the five in (9), and (11), (12), uniquely determine the nineteen "reduced" (k, h) involved in them and hence all the 81 cyclotomic constants.

We first give combinations which involve 01 and 08, 02 and 07, 04 and 05 only in their sums, which we eliminate by (9). Then $2b_0 - b_3$ is seen to involve the left member of (10), whence

$$2b_0 - b_3 = 1 + 3(0, 0) - 3(3, 6). \tag{15}$$

From this, (11), c_0 and c_3 we get

$$\begin{aligned} 9(0, 0) &= 2(2b_0 - b_3 - 1) + (0, 0)_3 - c_3 + 2c_0, \\ 9(0, 6) &= (0, 0)_3 - c_0 - c_3, \end{aligned} \tag{16}$$

$$(0, 3) = (0, 6) + \tfrac{1}{3}c_3, \qquad (3, 6) = (0, 0) - \tfrac{1}{3}(2b_0 - b_3 - 1). \tag{17}$$

These known $(0, 3t)$ and $(3, 6)$ are allowed in later answers. The new combinations are

$$b_1 - b_2 = 3(1, 2) - 6(1, 5) + 3(2, 4), \quad b_4 + b_5 - b_1 = 3(1, 2) + 3(1, 5) - 6(2, 4),$$
$$c_1 - c_2 = 3(1, 3) - 6(1, 4) - 3(1, 5) - 6(1, 6) + 3(1, 7) + 3(2, 4) + 3(2, 5) + 3(2, 6),$$
$$b_4 - c_1 = 3(1, 2) - 3(1, 3) + 6(1, 6) - 3(2, 4) - 3(2, 5),$$
$$c_5 - b_1 = 3(1, 4) + 3(1, 5) + 3(1, 7) - 3(2, 4) - 6(2, 6),$$
$$c_4 + b_5 = 3(1, 2) + 6(1, 3) - 3(1, 6) - 3(2, 4) - 3(2, 5),$$
$$A \equiv \tfrac{1}{2}\{M + 2b_0 + f - 1 - 3(0, 0) - 03 - 06 + 2(3, 6)\}$$
$$= 2(13 + 16 + 25) - 14 - 17 - 26.$$

From these and the fourth in (9), we get

$$9(2, 6) = 2B - C, \quad 9(1, 6) = B + C + 3D, \tag{18}$$

$$9(1, 3) = B + C + 3D + G, \qquad 9(2, 5) = B + C - 6D - G, \tag{19}$$
$$B = H - \tfrac{1}{3}(C_5 - b_1) + f - 03 - 06 - 36,$$
$$C = A - H + \tfrac{1}{3}(c_5 - b_1), \quad D = \tfrac{1}{3}(b_4 - c_1 - b_1 + b_2) - 2H,$$
$$G = c_4 + b_5 - b_4 + c_1, \; H = \tfrac{1}{3}\{b_4 + b_5 - b_1 - (b_1 - b_2)\} = 15 - 24.$$

Next, (10) yields

$$3(15+16+26) = f + \tfrac{1}{3}(1+00-36+b_2-b_1-c_5+b_1) + H + D, \tag{20}$$

which gives (1, 5). Then H gives (2, 4). Then b_1-b_2 gives (1, 2). We get (1, 4) from

$$2H + \tfrac{1}{3}(c_1 - c_2 - c_5 + b_1) = 13 - 3(1,4) - 2(1,6) + 25 + 3(2,6). \tag{21}$$

Then c_5-b_1 gives (1, 7). Finally, 01 and 08, 02 and 07, 04 and 05, whose sums are known by (9), are determined by them and c_1, c_4, b_0.

5. **Congruences.** After reductions by $\beta^9=1$, but not by (13), let

$$R(1, n) = \sum_{i=0}^{8} B_i\beta^i.$$

By* T, (17) and (18),

$$\sum_{i=0}^{8} B_i \equiv -1, \qquad \sum_{i=0}^{8} iB_i \equiv 0, \qquad \sum_{i=0}^{8} i^2B_i \equiv 0 \pmod 3. \tag{22}$$

We now reduce by (13) and get

$$R(1, n) = \sum_{i=0}^{5} C_i\beta^i, \qquad C_0 = B_0 - B_6,\ C_1 = B_1 - B_7,\ C_2 = B_2 - B_8,$$
$$C_3 = B_3 - B_6,\ C_4 = B_4 - B_7,\ C_5 = B_5 - B_8.$$

Hence (22) give

$$\sum_{i=0}^{5} C_i \equiv -1, \qquad \sum_{i=0}^{5} iC_i \equiv 0, \qquad \sum_{i=0}^{5} i^2C_i \equiv 0 \pmod 3. \tag{23}$$

These are equivalent to†

$$C_0 + C_3 \equiv -1, \qquad C_1 + C_4 \equiv 0, \qquad C_2 + C_5 \equiv 0 \pmod 3. \tag{24}$$

For $R(1, 1)$, $c_3 \equiv 0 \pmod 3$. By the fourth and first of (9),

$$c_1 - c_2 \equiv \sum_{h=1}^{8} (0, h) + (3, 6) - f = (3, 6) - (0, 0) - 1 \equiv 0 \pmod 3$$

by (10). Using also (24) in small letters, we see that for $R(1, 1)$

$$c_0 \equiv -1,\ c_2 \equiv c_1,\ c_3 \equiv 0,\ c_4 \equiv -c_1,\ c_5 \equiv -c_1 \pmod 3. \tag{25}$$

* Our conclusion is not altered by the fact that if r, s is 3, 6 or 6, 3, the six numbers in T, (20), now coincide in sets of three. The last two in (22) are multiples of 9.

† For $R(1, 2)$ every linear congruence modulo 3 is a combination of (24).

In Lemmas 1, 2, and their proofs, the summation index takes the values $0, 1, \cdots, 5$.

LEMMA 1. *Let* $\sum D_i \not\equiv 0 \pmod 3$ *in* $P = \sum D_i \beta^i$. *Then* $\pm \beta^n P = \sum C_i \beta^i$ *satisfies the first two congruences* (23) *for a single choice of the sign and for a single determination of* n *modulo* 3.

We have $\beta P = \sum S_i \beta^i$ where

$$S_0 = -D_5,\ S_1 = D_0,\ S_2 = D_1,\ S_3 = D_2 - D_5,\ S_4 = D_3,\ S_5 = D_4,$$

$$\sum S_i \equiv \sum D_i,\ \sum iS_i \equiv D_0 - D_1 + D_3 - D_4 \equiv \sum iD_i + \sum D_i \pmod 3.$$

Hence in $\beta^n P = \sum \sigma_i \beta^i$,

$$\sum \sigma_i \equiv \sum D_i,\ \sum i\sigma_i \equiv \sum iD_i + n \sum D_i \equiv 0 \pmod 3$$

by choice of n, uniquely modulo 3.

LEMMA 2. *Let* $C = \sum C_i \beta^i$ *satisfy the first two congruences* (23). *By Lemma* 1, *also* $\beta^3 C$ *and* $\beta^6 C$ *satisfy the same congruences. At most one of* $C, \beta^3 C, \beta^6 C$ *satisfy also* $C_3 \equiv 0,\ C_1 \not\equiv 0$.

In $\beta^3 C = \sum T_i \beta^i$,

$$T_0 = -C_3,\ T_1 = -C_4,\ T_2 = -C_5,\ T_3 = C_0 - C_3,\ T_4 = C_1 - C_4,\ T_5 = C_2 - C_5.$$

Hence in $\beta^6 C = \sum U_i \beta^i$, $U_0 = C_3 - C_0$, $U_3 = -C_0$. If two of C_3, T_3, U_3 are multiples of 3, then $C_0 \equiv C_3 \equiv 0 \pmod 3$ and the coefficients of both β^0 and β^3 in $C, \beta^3 C, \beta^6 C$ are all multiples of 3.

Lemmas 1 and 2 yield

THEOREM 1. *At most one of* $\pm \beta^s P$ *satisfies congruences* (25).

6. **Class number.** If q is any prime, the field defined by $\exp 2\pi i/q^h$ has the discriminant* $D = \pm q^m$, where $m = q^{h-1}(hq - h - 1)$ and the sign is plus except when $q^h = 4$ or $q \equiv 3 \pmod 4$. But Minkowski proved that every ideal class contains an ideal whose norm is $< (\pm D)^{1/2}$. For $q^h = 9$, the latter is $3^{9/2} < 140.3$. Tables† show that every prime < 1000 is a product of actual complex primes, whence every integer < 1000 is a product of principal ideals. Thus every ideal is a principal ideal.

THEOREM 2. *The field of the ninth roots of unity has the class number* 1.

7. **Complex factors of primes** $p = 9f + 1$. To p corresponds a polynomial $L(\beta)$ with integral coefficients which is a complex prime such that p is the

* Kummer. See Hilbert's Report on algebraic numbers, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4 (1894–95), p. 332.

† C. G. Reuschle, *Tafeln Complexer Primzahlen*, 1875, pp. 173–75.

product of a unit and the $L(\beta^i)$ for $i=1, 2, 4, 5, 7, 8$. Evidently the only possible factorizations

$$p = uf(\beta)f(\beta^{-1}), \quad u = \text{unit}, \quad f(\beta) \text{ with factor } L(\beta), \tag{26}$$

have the following four forms of $f(\beta)$:

(I) $L(\beta)L(\beta^2)L(\beta^4)$; (II) $L(\beta)L(\beta^2)L(\beta^5)$;

(III) $L(\beta)L(\beta^5)L(\beta^7)$; (IV) $L(\beta)L(\beta^4)L(\beta^7)$.

Since (IV) is unaltered when β is replaced by β^4 or β^7, it corresponds to $R(3, 3)$. When β is replaced by β^2, (III) becomes (II), (II) becomes (I), and (I) becomes the complement $L(\beta^8)\ L(\beta^4)\ L(\beta^2)$ to (III).

8. Diophantine equations determining $R(1, 1)$. As in T, §13, $u=1$ in (26), while $v=\pm\beta^s$ is the only unit such that

$$p = F(\beta)F(\beta^{-1}), \qquad F(\beta) = vf(\beta) = \sum_{i=0}^{5} c_i\beta^i. \tag{27}$$

By (13) this product is the sum of (28) and

$$(\beta + \beta^{-1})A + (\beta^2 + \beta^{-2})B + (\beta^4 + \beta^{-4} = -\beta - \beta^{-1} - \beta^2 - \beta^{-2})C,$$

where

$$p = \sum_{i=0}^{5} c_i^2 - c_0c_3 - c_1c_4 - c_2c_5, \qquad A = C, \quad B = C, \tag{28}$$

$$A = c_0c_1 + c_1c_2 + c_2c_3 + c_3c_4 + c_4c_5, \tag{29}$$

$$B = c_0c_2 + c_1c_3 + c_2c_4 + c_3c_5, \qquad C = c_0c_4 + c_1c_5 + c_0c_5. \tag{30}$$

By Theorem 1 there is at most one choice of v in (27) such that the c_i satisfy congruences (25), which must hold if $F(\beta)$ serves as $R(1, 1)$. Replace β by β^2 and write $F(\beta^2)=\sum b_i\beta^i$. Then

$$b_0 = c_0 - c_3,\ b_1 = c_5,\ b_2 = c_1 - c_4,\ b_3 = -c_3,\ b_4 = c_2,\ b_5 = -c_4. \tag{31}$$

Evidently (28)–(30) hold when the c_i are replaced by these b_i. If the c_i satisfy congruences (25), also the b_i satisfy them.

We saw that $R(1, 1)$ is the product of a unit by (I), (II), (III), or one of their complements, the six being permuted when β is replaced by β^2.

THEOREM 3. *Equations* (28) *have exactly six sets of integral solutions satisfying congruences* (25). *These sets are derived from any one set by applying the powers of substitution* (31) *of period* 6. *Any of the six sets may be chosen as the coefficients of* $R(1, 1)=\sum c_i\beta^i$. *Then* (8) *gives* $R(1, 2)$. *Except for the double sign of* M, $R(3, 3)$ *is defined by* (5) *and* (6). *Then all the cyclotomic constants are determined as in* §4.

The ambiguity in $R(3, 3)$ may be removed by using*

$$R(3, 3) = \beta^{-6m'}R(1, 1)R(1, 2, \beta^2)/R(1, 2), \tag{32}$$

viz.,

$$\beta^{6m'}F(\beta^2)F(\beta^3) = F(\beta)F(\beta^4),$$

which follows from (8).

Theorem 3 permits a six-fold choice for $R(1, 1)$. This is in accord with the fact that β may be chosen as any of the six roots of (13). The cyclotomic constants themselves have a six-fold ambiguity involved in the choice of the primitive root g of p. When g is replaced by a new primitive root g^r, $R(1, 1)$ becomes $R(t, t) = R(1, 1, \beta^t)$, where $tr \equiv 1 \pmod 9$. But t ranges with r over the six integers <9 and prime to 9. By (28),

$$\begin{aligned} &4p = C_0^2 + C_1^2 + C_2^2 + 3(c_3^2 + c_4^2 + c_5^2), \\ &C_0 = 2c_0 - c_3, \qquad C_1 = 2c_1 - c_3, \qquad C_2 = 2c_2 - c_5. \end{aligned} \tag{33}$$

By (25), $C_1 = 3y$, $C_2 = 3z$, $c_3 = 3w$, where y, z, w are integers. Thus

$$4p = C_0^2 + 9(y^2 + z^2) + 27w^2 + 3c_4^2 + 3c_5^2, \quad C_0 \equiv 1, \quad c_4 \equiv c_5 \pmod 3, \tag{34}$$

so that the five congruences (25) reduce to two after choosing our new variables.

Part II. Theory for $e = 18$

9. Unless m and n are both even or both multiples of 3, $R(m, n)$ is conjugate to some $R(1, -)$ and hence to a single one of

$$R(1, 1), R(1, 2), R(1, 3), R(1, 4), R(1, 5), R(1, 9). \tag{35}$$

The $R(3x, 3y)$ are conjugate to $R(3, 3)$, $R(3, 6)$, or $R(6, 6)$. The $R(2r, 2s)$ are given by (3). By T, §10,

$$\begin{aligned} &R(1, 9) = \beta^{2m}R(1, 1), \qquad R(1, 4) = (-1)^f\beta^{-6m}R(1, 1), \\ &R(2, 8) = (-1)^f\beta^{4m}R(1, 1). \end{aligned} \tag{36}$$

We regard $R(1, 1)_9$ as known by Theorem 3. Then our $R(2, 2)$ is known. Replacing β by β^{13}, we get $R(8, 8) = R(2, 8)$. Thus (36) give $R(1, 1)$, $R(1, 9)$, $R(1, 4)$. In (7) we may take $\gamma = \beta^6$, $\alpha = \beta^7$, $p = F(\beta^7)F(\beta^{11})$, and get

$$R(1, 13) = \beta^{-3m'}R(3, 11), \qquad R(1, 2) = \beta^{-3m'}R(1, 4, \beta^5), \tag{37}$$

since the latter is derived from the former by replacing β by β^5. By the value of R in terms of F, we get

* In case M is not divisible by 9, the change of the sign of M subtracts M from A above (18) and hence from C, whence by (18) the solution (26) is an integer for a single choice of $\pm M$.

$$R(m, t)R(n, m+t) = R(m, n)R(m+n, t), \tag{38}$$

$$R(1, 4)R(1, 5) = R(1, 1)R(2, 4), \quad R(2, 3)R(1, 5) = R(1, 3)R(2, 4). \tag{39}$$

By the first and (36_2), and then by the second,

$$R(1, 5) = (-1)^f\beta^{6m}R(2, 4), \quad R(1, 3) = (-1)^f\beta^{6m}R(2, 3). \tag{40}$$

We now know all functions (35) except $R(1, 3)$. While the case $R(1, 2)\,R(1, 3) = R(1, 1)\,R(2, 2)$ of (38) gives $R(1, 3)$, it is not found linearly.

10. We prove the following theorem:

THEOREM 4. *If $[x]$ denotes the least positive residue of x modulo e, we have the following decomposition into prime ideals*:

$$R(h, t) = \pm\,\beta^s\Pi\, f(\beta^Z), \quad zZ \equiv 1 \pmod{e}, \tag{41}$$

where z ranges over those positive integers $<e$ and prime to e such that

$$[hz] + [tz] > e. \tag{42}$$

Let r and g be primitive roots of

$$r^{p-1} = 1, \quad g^{p-1} \equiv 1 \pmod{p}, \quad p = ef + 1.$$

Write $\psi(r) = F(r^{-m})\,F(r^{-n})/F(r^{-m-n})$, where m and n are positive and $<p-1$. Jacobi noted that

$$\psi(g) \equiv 0 \pmod{p} \quad \text{if } m + n > p - 1.$$

Write

$$r^{-f} = \beta, \quad g^{-f} \equiv u \pmod{p}, \quad m \equiv hzf, \quad n \equiv tzf \pmod{(p-1)}.$$

Then $r^{-m} = \beta^{hz}$, $r^{-n} = \beta^{tz}$, and β is a primitive eth root of unity. Thus $\psi(r)$ becomes $R(h, t, \beta^z)$. Since m/f and n/f are positive integers $<e$ and are congruent modulo e to hz and tz, respectively, $m+n>p-1$ is equivalent to (42). Then $R(h, t, u^z) \equiv 0 \pmod{p}$. This implies* (41).

Since $R\,R(h, t) = p$ if $R = R(h, t, \beta^{-1})$, the solutions z of

$$[hz] + [tz] < e \tag{43}$$

yield the factors of R. We pass to the factors of $R(h, t)$ itself if we replace $f(\beta)$ by $f(\beta^{-1})$.

11. For $e = 18$, we use (43) and see that $R(1, 3)$ and $R(6, 6)$ are both prod-

* For e a prime, Kummer, Journal für Mathematik, vol. 35 (1847), p. 362, where there are two misprints of m for μ in the second line. Since we are taking his $f=1$, the periods η are the powers of α, and the symbolic "$f(\alpha) \equiv 0 \pmod{q}$ for $\eta = u_r$" on p. 339 now means $f(u_r) \equiv 0 \pmod{q}$ in the ordinary sense. For e composite, Kummer, Mathematische Abhandlungen, Akademie der Wissenschaften, Berlin (for 1856), 1857, p. 45, where he used (43).

ucts of $f(\beta)\ f(\beta^7)\ f(\beta^{13})$ by units $\pm\beta^s$. Hence $R(1, 3)=\beta^k R(6, 6)$. Replacing β by β^{13}, we get

$$R(13, 3) = (-1)^f R(2, 3) = \beta^{13} R(6, 6).$$

Then (40_2) gives $12k+6m\equiv 0 \pmod{18}$, $k=m+3t$. We omit the indirect determination of t, yielding

$$R(1, 3) = \pm \beta^{m+3m'} R(6, 6). \tag{44}$$

Since we know all the $R(m, n)$, we can find the cyclotomic constants as in D or T.

PART III. THEORY FOR $\phi(e)=8$, $e=15, 16, 20, 24, 30$

12. Let a, b, c, d denote the positive integers $<e/2$ and prime to e. Then $a'=e-a, \cdots, d'=e-d$ give the integers $>e/2$ and prime to e. Then p is the product of eight prime ideals $f(\beta^Z)$, denoted by Z, for $Z=a, \cdots, d'$. The following give $F(\beta)$ in the only decompositions $p=F(\beta)\ F(\beta^{-1})$, where $F(\beta)$ is a product of four of the prime ideals, one of which is $f(\beta^a)$:

$$\begin{aligned} &\text{I, II: } a, b, c, d \text{ or } d'; \qquad \text{III, IV: } a, b, c', d \text{ or } d'; \\ &\text{V, VI: } a, b', c, d \text{ or } d'; \qquad \text{VII, VIII: } a, b', c', d \text{ or } d'. \end{aligned} \tag{45}$$

If $F=F(\beta)$ is such a product of four, the product $F(\beta^{-1})$ of the complementary set of four is denoted by F'.

13. **Case** $e=16$. Every* ideal is a principal ideal (or the class number is 1). In §12, $a=1$, $b=3$, $c=5$, $d=7$. For the equation having the eight roots β^k, k odd and <16, the Galois group G for the domain of rational numbers is generated by

$$(\beta\beta^3\beta^9\beta^{11})(\beta^5\beta^{15}\beta^{13}\beta^7), \qquad (\beta\beta^5\beta^9\beta^{13})(\beta^3\beta^{15}\beta^{11}\beta^7). \tag{46}$$

These induce the respective substitutions

$$\begin{aligned} &(\text{II V' VIII III})(\text{I VII' to I'})(\text{IV})(\text{VI to VI'}), \\ &(\text{II III' VIII V})(\text{I VII' to I'})(\text{IV to IV'})(\text{VI}). \end{aligned} \tag{47}$$

Each $R(m, n)$ is conjugate to one and only one of $R(1, j), j=1, 2, 3, 6, 7$, $R(2, 2), R(2, 4), R(2, 6), R(4, 4)$. By T, (48)–(51),

$$(-1)^f R(1, 6) = R(1, 9) = \beta^{2m} R(2, 2), \quad R(1, 7) = (-1)^f \beta^{2m} R(1, 1), \tag{48}$$

where $g^m\equiv 2 \pmod{p}$. Applying Theorem 4 with (42) replaced by (43), we see that, apart from unit factors $\pm\beta^i$,

$$\begin{aligned} &R(1, 1) = \text{VII}, \ R(1, 2) = \text{VIII}, \ R(1, 3) = \text{III}, \ R(1, 6) = \text{IV}, \\ &R(2, 2) = R(2, 6) = R(1, 6), \ R(4, 4) = R(2, 2) = \text{VI}, \end{aligned}$$

* Weber, *Algebra*, 2d edition, vol. 2, 1899, p. 808, foot-note.

after a proper choice of $f(\beta)$ among the eight prime factors.

Consider the Diophantine equations found as in §8. A set of integral solutions which gives rise to 8 distinct sets under the group G generated by (46) may be taken as the coefficients of $R(1, 3)$. After choice of β among the eight roots of the octic satisfied by β^k, k odd and <16, we may assume that $R(1, 3)$ is the product of a unit $\pm\beta^i$ and III, rather than another of II, III, V, VII or the complements II′, $\cdots$ in the cycles of four in (47).

This unit is partially determined as follows. Write

$$R = (-1)^{n'}R(1, n) = \sum_{i=0}^{15} B_i\beta^i, \tag{49}$$

without reduction by $\beta^8 = -1$. As in T, §3,

$$\sum B_i = p - 2, \quad \sum iB_i \equiv 0 \pmod{16}, \quad \sum i^2 B_i \equiv 0 \pmod 8. \tag{50}$$

After reduction by $\beta^8 = -1$, we get

$$R = \sum_{i=0}^{7} C_i\beta^i, \quad C_i = B_i - B_{i+8}, \tag{51}$$

$$\sum C_i \equiv 1, \quad \sum iC_i \equiv C_1 + C_3 + C_5 + C_7 \equiv 0 \pmod 2. \tag{52}$$

By the difference of the last two in (50) taken modulo 4, we get

$$C_2 + C_3 + C_6 + C_7 \equiv 0 \pmod 2. \tag{53}$$

Consider any polynomial (51_1) with $\sum C_i$ odd. Then

$$\beta R = \sum_{i=0}^{7} D_i\beta^i, \quad D_0 = -C_7, \quad D_i = C_{i-1} \quad (i = 1, \cdots, 7),$$

$$\Delta = D_1 + D_3 + D_5 + D_7 = C_0 + C_2 + C_4 + C_6 \equiv 1 + s \pmod 2,$$

where $s = C_1 + C_3 + C_5 + C_7$. Hence if $s \equiv 1 \pmod 2$, βR has $\Delta \equiv 0 \pmod 2$. Hence by choice between R and βR we may assume that $s \equiv 0 \pmod 2$ in R. Then

$$\beta^2 R = \sum_{i=0}^{7} H_i\beta^i, \quad H_0 = -C_6, \quad H_1 = -C_7, \quad H_i = C_{i-2} \quad (i = 2, \cdots, 7),$$

$$H_1 + H_3 + H_5 + H_7 = C_1 + C_3 + C_5 - C_7 \equiv 0 \pmod 2,$$

$$\delta = H_2 + H_3 + H_6 + H_7 = C_0 + C_1 + C_4 + C_5 \equiv 1 + t \pmod 2,$$

where $t = C_2 + C_3 + C_6 + C_7$. Hence if t is odd, δ is even. Hence just one of $R, \beta R, \beta^2 R, \beta^3 R$ is a polynomial $\sum C_i\beta^i$ for which the three congruences (52) and (53) hold, viz.,

$$C_1 + C_5 \equiv C_3 + C_7 \equiv C_2 + C_6 \equiv 1 + C_0 + C_4 \pmod 2. \tag{54}$$

These four sums remain unaltered modulo 2 when we replace R by $\beta^4 R$. Thus $R(1, 3)$ is determined* up to a factor β^{4j}. We have not undertaken the investigation similar to that in §5, but much longer, to find further linear congruences which determine j. For a given p, j is probably determined by the formulas expressing (0, 0) or other cyclotomic constants (k, h) in terms of the coefficients of the $R(m, n)$.

The $R(2x, 2y)$ are known by the theory for $e=8$ in D. Then (48) gives $R(1, 6)$. We get $R(2, 3)$ from

$$R(1, 6) = R(33, 22) = R(2, 3, \beta^{11}). \tag{55}$$

The above discussion yielded $R(1, 3)$ and hence its conjugate $R(11, 33) = R(1, 11) = \pm R(1, 4)$. We get $R(1, 1)$ and $R(1, 2)$ from

$$R(1, 3)R(1, 4) = R(1, 1)R(2, 3), \qquad R(1, 2)R(1, 3) = R(1, 1)R(2, 2). \tag{56}$$

Also $R(1, 7)$ is known by (48). We now have a conjugate to every $R(m, n)$ and can find the (k, h) by linear equations as in T.

14. **Case** $e=15$. Let d_1, d_2, D be the discriminants of the fields defined by a primitive nth root of unity for $n=3, 5, 15$, respectively. Then $D=d_1^4 d_2^2$ by Hilbert's Report, loc. cit., p. 267. By §6, $d_1=-3$, $d_2=5^3$. Thus $D^{1/2}=1125$. By Reuschle's Tables, every integer <1000 is a product of principal ideals. If this were verified on to 1125, Minkowski's theorem (§6) would show that, in the field of the fifteenth roots of unity, every ideal is a principal ideal. A complete proof may be made by use of the real subfield of degree 4 as by Weber, loc. cit.

The $R(m, n)$ are conjugate to a single one of $R(1, j), j=1, \cdots, 5$, $R(3, 3)$, $R(5, 5)$. The last two may be regarded as known by (3).

Consider (7) with $\gamma=\beta^5$, $\alpha=\beta^6$ or β^{14}, $p=F(\alpha)\,F(\alpha^{-1})$. We get

$$R(1, 3) = \beta^{-3m'}R(3, 3), \qquad R(1, 6, \beta^4) = R(4, 9) = \beta^{3m'}R(1, 2). \tag{57}$$

Expressing the former in terms of F's we get

$$R(1, 6) = \beta^{-3m'}R(3, 4).$$

By the case $24\cdot 16=12\cdot 34$ of (38), we get

$$R(2, 4) = R(1, 2, \beta^2) = \beta^{3m'}R(1, 2). \tag{58}$$

In (41) denote $f(\beta^Z)$ by Z and use (43). Then, apart from factors $\pm\beta^s$,

$$R(1, 1) = 1\cdot 4\cdot 8\cdot 13, \qquad R(1, 2) = 1\cdot 2\cdot 4\cdot 8, \qquad R(1, 3) = 1\cdot 8\cdot 11\cdot 13,$$

while $R(1, 4)$ has the same factors as $R(1, 2)$, and $R(1, 5)$ the same as $R(1, 1)$.

* Likewise $R(1,5)$. While the factor for $R(1,4)$ is β^{-4j}, $R(1,1)$ is uniquely determined. See the later formulas.

Hence

$$R(1, 5) = \pm \beta^x R(1, 1). \tag{59}$$

Expressing the R's in terms of F's, we see that $R(2, 5) = \pm\beta^x R(1, 8)$. Replacing β by β^2, we get $R(1, 4) = \pm\beta^{2x} R(1, 2)$. The case $R(1, 4)\ R(1, 5) = R(1, 1) \cdot R(2, 4)$ of (38), and (58) give $3x \equiv 3m'$ (mod 15), whence $x = m' + 5y$.

In a formula due to Jacobi, loc. cit., p. 168, take $\lambda = 5$ and replace β by β^3, a primitive fifth root of unity. Then

$$F(\alpha)F(\beta^3\alpha)F(\beta^6\alpha)F(\beta^9\alpha)F(\beta^{12}\alpha) = \alpha^{-5M} p^2 F(\alpha^5) \tag{60}$$

if $5 \equiv g^M$ (mod p), $\alpha^{p-1} = 1$. We take

$$p = F(\alpha)F(\alpha^{-1}), \qquad p = F(\beta^3\alpha)F(\beta^{-3}\alpha^{-1}),$$

and have two equal products of three F's. Take $\alpha = \beta^{-1}$ and divide by $F(\beta^{11}) \cdot F(\beta^{13})$. We get

$$R(5, 8) = \beta^{5M} R(1, 10), \quad \text{or} \quad R(2, 8) = \beta^{5M} R(1, 4) = \pm \beta^{2x}\beta^{5M} R(1, 2).$$

Replacing β by β^2 in the earlier $R(1, 4)$, we get

$$R(2, 8) = \pm \beta^{4x} R(2, 4) = \pm \beta^{4x}\beta^{3m'} R(1, 2).$$

Hence $5M \equiv 2x + 3m'$ (mod 15). Thus $y \equiv m' - M$ (mod 3),

$$x = 6m' - 5M.$$

In §12, $a = 1$, $b = 2$, $c = 4$. By the replacement of β by either β^2 or β^7, I, IV, VI, VII (or their complements) are permuted in a cycle of four, while III and VIII are interchanged, and V is unaltered (or goes to V′). After a choice of β among the eight β^k, k prime to 15 and $k < 15$, we may take $R(1, 1)$ to be a product of a unit $\pm\beta^i$ by VI (rather than I, IV or VII). An equivalent choice for the Diophantine equations found as in §8 is that a set of integral solutions, which give rise to 8 distinct sets under the transformations induced by the Galois group generated by the replacements of β by β^2 and β^7, may be taken as the coefficients of $R(1, 1)$. But the unit factor cannot be determined as heretofore since there exists no linear congruence modulo 3 or 5 between the coefficients of $R(1, 1)$, after* reduction to a polynomial of degree 7 in β.

If we waive this difficulty and regard $R(1, 1)$ as known, we have $R(1, 5)$ by (59), $R(1, 3)$ by (57), and find $R(1, 2)$ by (56_2). Then $R(1, 4) = \pm\beta^{2x} R(1, 2)$. We now know a conjugate to every $R(m, n)$.

15. **Case** $e = 20$. The $R(m, n)$ are conjugate to $R(1, j)$, j = 1-5, 8, 9,

* Before that reduction by the octic in β, we have the congruences T, (18), and see that T, (69)–(71), apply also here.

$R(2, 2)$, $R(2, 4)$, $R(2, 8)$, $R(4, 4)$, $R(5, 5)$. The last five are found by (3). By T, (48)–(51),

$$R(1, 8) = \pm \beta^{-2m} R(2, 8), \qquad R(1, 9) = \pm \beta^{2m} R(1, 1).$$

By (60) with β^3 replaced by β^4, we get $R(2, 7) = rR(1, 2)$, $r = \beta^{5M}$. Then (38) gives $R(3, 6) = rR(1, 6)$. The factorizations into prime ideals yield only the facts that $R(1, 3)/R(1, 1)$, $R(1, 8)/R(1, 2)$, $R(2, 2)/R(1, 2)$ are units. The latter are found from one by use of (56_2), $18 \cdot 19 = 12 \cdot 28$, and $R(2, 8) = \beta^{4M} R(2, 2)$.

16. Case $e = 24$. The $R(m, n)$ are conjugate to $R(1, j)$, $j = 1\text{-}11$; $R(2, j)$, $j = 2, 4, 6, 8, 10$; $R(3, 3)$, $R(3, 6)$, $R(3, 9)$; $R(4, 4)$, $R(4, 8)$, $R(6, 6)$, $R(8, 8)$. By (7) with $\alpha = \beta^{17}$, $\gamma = \beta^8$, $R(1, 6) = \beta^{-3m'} R(3, 6)$. Expressed in F's, the latter gives $R(1, 9) = \beta^{-3m'} R(1, 2, \beta^7)$.

UNIVERSITY OF CHICAGO,
CHICAGO, ILL.