INTRODUCTORY REMARKS ON COMPLEX MULTIPLICATION

HARVEY COHN

Department of Mathematics
City College of New York
New York, N.Y. 10023 USA

(Received May 24, 1982)

ABSTRACT. Complex multiplication in its simplest form is a geometric tiling property. In its advanced form it is a unifying motivation of classical mathematics from elliptic integrals to number theory; and it is still of active interest. This interrelation is explored in an introductory expository fashion with emphasis on a central historical problem, the modular equation between $j(z)$ and $j(2z)$.

KEY WORDS AND PHRASES. Complex multiplication, class number, elliptic integrals, modular functions, modular equation.

1980 MATHEMATICS SUBJECT CLASSIFICATION CODE. 10D05.

1. GEOMETRIC ILLUSTRATION.

We begin with an observation scarcely requiring college level mathematics:

"If a room has a rectangular floor plan in which the ratio of its sides r is $\sqrt{2}$, then it may be partitioned into two rectangular rooms by a wall down the middle of the longer side (see Fig. 1a) in such a fashion that each half has the same shape as the original room (seen by using a 90° rotation)."

Clearly this is a unique phenomenon as stated. Only that ratio $r = \sqrt{2}$ will still be present after division into two halves ($2/r = r$), and a (nonrectangular) parallelogram-shaped room could not permit this kind of a subdivision (since its angles are not all equal).

Yet we can construct some kind of nontrivial parallelogram generalization, and once we do this there is no place to stop short of describing a major part of pure mathematics! What is involved is a synthesis of number theory, algebra, analysis, and topology which now all comes under the heading of complex multiplication. Our purpose is to offer a minimal description of this phenomenon using only "generally known" results.

2. THE PARALLELOGRAM GENERALIZATION.

We replace the rectangle by a parallelogram with a periodic structure (torus). This means that the parallelogram may now be subdivided into pieces which may be moved and reassembled according to the group of vectors generated by the sides of the parallelogram.

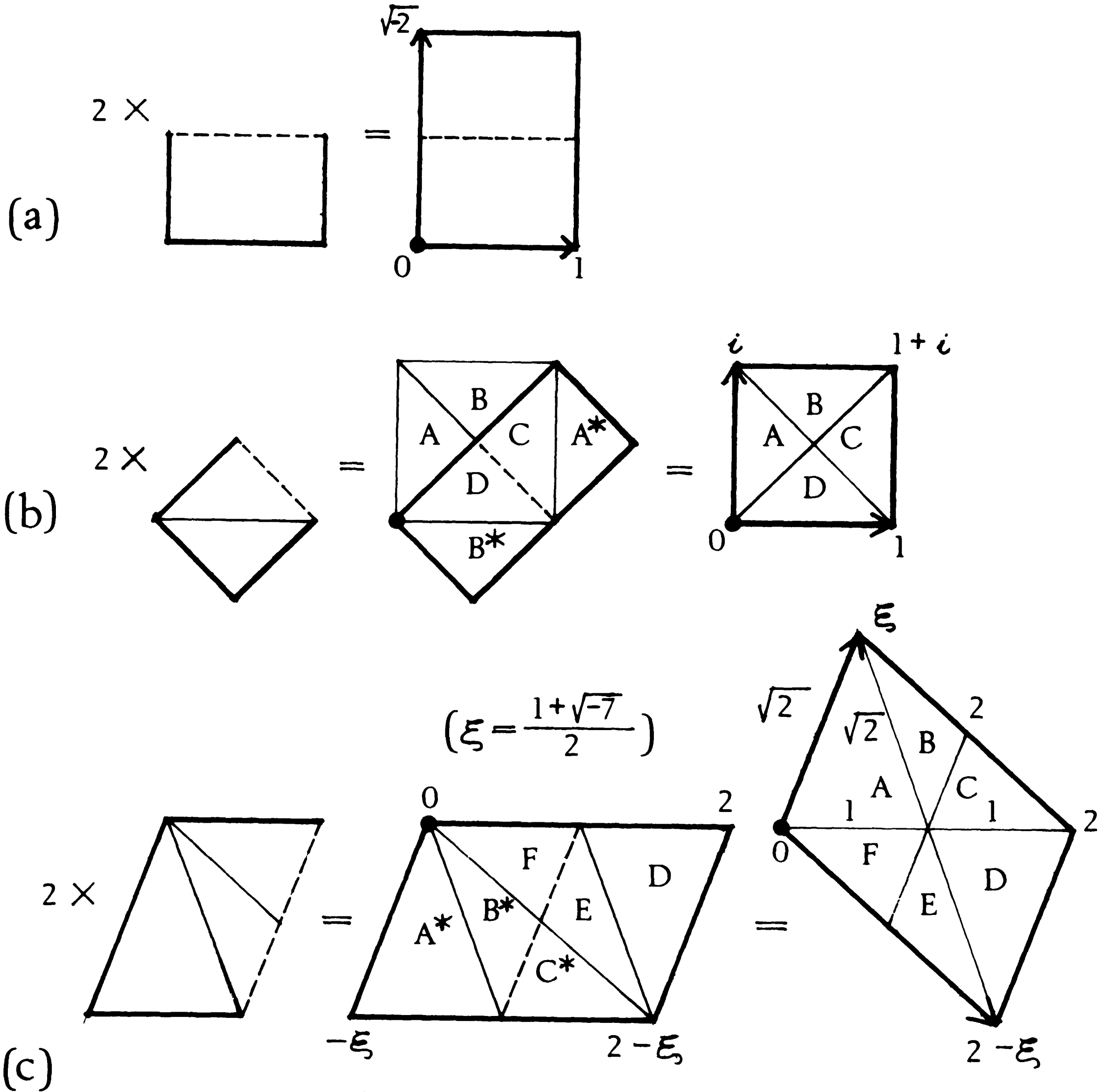

FIGURE 1 - THREE COMPLEX MULTIPLICATIONS OF NORM TWO

For instance, in Fig. 1b, the square A + B + C + D (on the right) can be reassembled as the rectangle A* + B* + C + D, where A* (or B*) is the right-hand (or downward) translate of A (or B). This new rectangle A* + C + D + B* can be cut in half to produce D + B* and A* + C, each of which has half the size but the same shape as the original (as seen by a 45° rotation).

If this looks too obvious, consider the parallelogram on the right in Fig. 1c. It is made up of isoscles triangles A and D of sides $1, \sqrt{2}, \sqrt{2}$ and scalene triangles B + C and E + F of sides $1, \sqrt{2}, 2$. Thus the parallelogram A + B + C + D + E + F is equivalent to A* + B* + C* + D + E + F and each half (namely A* + B* + F and C* + E + D) is similar to the original (as seen by a rotation of $\arccos 1/\sqrt{8} = 69^\circ \ldots$).

When we introduce complex numbers we see that these are essentially the only shapes for division of a parallelogram "modulo translations" into two equal similar parts, and we also see why the configurations are described as "complex multiplications of norm two".

3. LATTICE FORMULATION.

We consider two elements of $\mathbb{C}^*$ (nonzero complex numbers) which are independent over $\mathbb{R}$, namely ω_1 and ω_2 (with a nonreal ratio). We define this ratio τ as

$$\tau = \omega_2/\omega_1 \ , \ \operatorname{Im} \tau > 0 \quad (\tau \in H_+). \tag{3.1}$$

Thus the ordering of ω_1 and ω_2 is chosen to make τ lie in the upper-half plane H_+. Using ω_1 and ω_2 we generate the lattice L, which is thought of either as a set of points or as an abelian group of translations. We write

$$L = [\omega_1, \omega_2] = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\} \tag{3.2}$$

(or the $\mathbb{Z}$-module of rank two generated by ω_1 and ω_2 in $\mathbb{C}$).

The lattice L has many equivalent bases, i.e., it may be written as

$$L = [\lambda_1, \lambda_2] \tag{3.3a}$$

where, symbolically, $\lambda = A\omega$, for a matrix A in $PSL_2(\mathbb{Z})$, the modular group, (the matrices A and -A are identified). In detail,

$$\begin{aligned} \lambda_1 &= a_{11}\omega_1 + a_{12}\omega_2 \qquad & a_{ij} \in \mathbb{Z},\ A = (a_{ij}) \\ \lambda_2 &= a_{21}\omega_1 + a_{22}\omega_2 \qquad & a_{11}a_{22} - a_{12}a_{21} = 1 \ . \end{aligned} \tag{3.3b}$$

The determinant of A is +1 (not ± 1) to preserve ordering, i.e., so that $\omega_2/\omega_1 \in H_+$ also. The changes of bases are generated by the operations indicated as follows:

$$[\omega_1,\omega_2] = [-\omega_2,\omega_1] \ ; \ [\omega_1 \ , \ \omega_2] = [\omega_1,\omega_2 \pm \omega_1] \ . \tag{3.4}$$

The group $PSL_2(\mathbb{Z})$ is more complicated than L, and nonabelian. (For further details see Jacobson [12] or Gunning [9]).

The advantage of complex numbers comes with the concept of "shape" (or euclidean similarity). It can be defined as the <u>equivalence class</u> of lattices $\{L\} = \{L_1\}$ related by

$$\mu \ L = L_1, \ \mu \in \mathbb{C}^*, \tag{3.5a}$$

which denotes the lattice attained by multiplying each element of L by μ. Thus, in the symbols of (3.2) and (3.3a),

$$L_1 = [\mu \ \omega_1,\mu \ \omega_2] = [\mu \ \lambda_1,\mu \ \lambda_2] \ . \tag{3.5b}$$

Thus each L is equivalent (using $\mu = 1/\omega_1$) to

$$L_1 = [1,\tau], \quad \operatorname{Im} \tau > 0, \tag{3.6a}$$

where many different τ (e.g., τ, τ_0) may be used, all related by $PSL_2(\mathbb{Z})$(see (3.3)),

$$[1,\tau] = [1,\tau_0]\mu \Leftrightarrow \tau_0 = (a_{11}\tau + a_{12})/(a_{21}\tau + a_{22}) \ . \tag{3.6b}$$

We finally note the inclusion symbol

$$L_0 \subseteq L_1 \tag{3.7a}$$

for L_0 a sublattice of L_1. Actually, when L_0 is viewed as an additive subgroup of L_1, the index $|L_1/L_0|$ is easily interpreted as the (finite) ratio of areas of the parallelograms formed by the basis vectors of L_1 and L_0. Thus when similarity occurs, we easily recognize

$$|L/\mu \ L| = |\mu|^2 \ . \tag{3.7b}$$

Thus we now verbalize Fig. 1 as the display of lattices L and <u>complex multipliers</u> ξ with norm given by

$$|L/\xi \ L| = |\xi|^2 = 2 \ . \tag{3.8}$$

We seem to be doing even better; we can arrange to have

$$L = [\omega_1,\omega_2], \qquad L = [\omega_1,2 \ \omega_2] \ . \tag{3.9}$$

For example, in Figs. 1abc (respectively we can recognize this by using (3.4) as follows:

$$\xi = \sqrt{-2}, \ \omega_1 = 1, \ \omega_2 = \sqrt{-2}/2 \ , \tag{3.10a}$$

$$\sqrt{-2}[1,\sqrt{-2}/2]^* = [\sqrt{-2},-1] = [1,\sqrt{-2}]^* ;$$

$$\xi = 1 + i,\ \omega_1 = 1,\ \omega_2 = (1 + i)/2, \tag{3.10b}$$

$$(1 + i)[(1-i)/2,(1 + i)/2] = (1 + i)[1,(1 + i)/2]^* = [1 + i,i] = [1,i] = [1,1+i]^*;$$

$$\xi = (1 + \sqrt{-7})/2,\ \omega_1 = -\xi, \omega_2 = 1 (\xi^2 = \xi -2), \tag{3.10c}$$

$$\xi[-\xi,1]^* = [-\xi^2,\xi] = [2-\xi,\xi] = [2,\xi] = [-\xi,2]^* .$$

(In each case, the analogues of (3.9) are indicated by a*).

4. THE MULTIPLIER RING.

We now consider $R\{L\}$, the set of all multipliers of L, i.e.,

$$R\{L\} = \{\rho \in \mathbb{C} | \rho L \subseteq L\} . \tag{4.1}$$

We include $\rho = 0$ in the sense that $0L$ is trivially in L. Thus it is clear that $R\{L\}$ is a ring:

$$\rho_1 L \subseteq L,\ \rho_2 L \subseteq L \Rightarrow \rho_1\rho_2 L \subseteq L \tag{4.2a}$$

$$\rho_1 L \subseteq L,\ \rho_2 L \subseteq L \Rightarrow (\rho_1 \pm \rho_2)L \subseteq L \tag{4.2b}$$

since L is closed under addition and subtraction. From this, $R\{L\} \supseteq \mathbb{Z}$. Furthermore, as the notation indicates, $R\{L\}$ really depends on the equivalence class of $\{L\}$, (L and μL, above, have the same multipliers). Thus $R\{L\}$ is called the multiplier ring of each L or the class $\{L\}$. If $R\{L\} \neq \mathbb{Z}$, it is seen to contain a complex element, which performs complex multiplication. (Real multipliers must be integers by independence of the basis vectors of L).

THEOREM 4.3. Complex multiplication occurs in a lattice $L = [\omega_1,\omega_2]$ if and only if the ratio ω_2/ω_1 ($= \tau$) is a quadratic surd satisfying an equation over $\mathbb{Z}$

$$a\tau^2 - b\tau + c = 0,\quad d = b^2 - 4ac < 0, \tag{4.4}$$

normalized so that $a > 0$, $\gcd(a,b,c) = 1$. Then the multiplier ring is generated by a quadratic integer ξ, i.e.,

$$R\{L\} = \mathbb{Z}[\xi] . \tag{4.5}$$

Here ξ satisfied a monic equation of integral trace t and norm n, and, more important, with the same discriminant d,

$$\xi^2 - t\xi + n = 0,\quad d = t^2 - 4n\ (< 0). \tag{4.6}$$

To sketch the proof, write $[1,\tau] \supseteq \zeta[1,\tau]$, which has a subbasis in $[1,\tau]$ for each ζ ($\notin \mathbb{R}$) in $R\{L\}$,

$$\zeta[1,\tau] = [b_{11} + b_{12}\tau, b_{21} + b_{22}\tau] \subseteq [1,\tau] \tag{4.7}$$

$$\zeta = b_{11} + b_{12}\tau \qquad (4.8)$$
$$\zeta\tau = b_{21} + b_{22}\tau$$

where $b_{ij} \in \mathbb{Z}$, (but $b_{11}b_{22} - b_{12}b_{21} = |\zeta|^2$). We easily recognize ζ as an "eigenvalue" and $[1,\tau]$ as an "eigenvector", leading to equations of type (4.4) for τ, and monic for ζ. But here ζ is not necessarily a generator ξ of the ring $R\{L\}$, (it may be 2ξ, etc.). The main difficulty is showing that $R\{L\}$ has a generator ξ which necessarily leads to the <u>same</u> discriminant d. (In practice this is done by quadratic forms, see the next section). Note the dependence

$$d = d\{L\}\ ,\ R\{L\} = \mathbb{Z}[\xi] = R[d\{L\}]. \qquad (4.9)$$

We can show (4.9) by an explicit choice of generator $\xi_1 = \xi + m$, $(m \in \mathbb{Z})$ defined by the cases

$$d \equiv 0 \pmod 4,\quad \xi_1^2 - d/4 = 0, \qquad (4.10a)$$
$$d \equiv 1 \pmod 4,\quad \xi_1^2 - \xi_1 - (d-1)/4 = 0. \qquad (4.10b)$$

COROLLARY 4.11. If complex multiplication of L occurs by $\zeta (\in R\{L\}$ with norm $|\zeta|^2 = n$, then a basis of L can be chosen so that

$$\zeta[\omega_1,\omega_2] = m[\omega_1, n_0\,\omega_2],\quad n = m^2 n_0 \qquad (4.12)$$

where m is the maximum integer of $\mathbb{Z}$ for which $\zeta/m \in R\{L\}$.

For proof, consider the elementary divisor form of the mapping $\zeta L \to L$. Note the factor m by itself is a real multiplication, and $m = 1$ for the interesting cases.

We can now proceed to enumerate all complex multiplications. The first few are easy because they take place in lattices $[1,\xi]$ whose ring is just $\mathbb{Z}[\xi]$. For norm - we have units for $d = -4$ and -3, namely

$$\xi = i,\ \xi = (-1 + \sqrt{-3})/2\ . \qquad (4.13)$$

The complex multiplications of norm 2 are in (3.10abc), and have discriminants $d = -8, -4, -7$ respectively. It can be verified that for a given norm n, only a limited number of ξ occur in (say) (4.6), (since $t^2 = 4n + d < 4n$).

5. CLASS NUMBER.

We define $h = h(d)$, the <u>class number</u> of d as the number of inequivalent lattices $L_1,\ldots,L_h$ with complex multiplication and the common discriminant $d = d\{L_i\}$. Each $R\{L_i\}$ is the same $\mathbb{Z}[\xi_1]$ from (4.10ab), so we can always write $L_1 = [1,\xi_1]$, the so-called <u>principal lattice</u>, and we call $\{L_1\}$ the <u>principal lattice class</u>.

To see a nonprincipal lattice class, we take $d = -20$, where $h = 2$. We have'

$$L_1 = [1, \sqrt{-5}], \quad L_2 = [2, 1 + \sqrt{-5}], \tag{5.1a}$$

$$R\{L_1\} = R\{L_2\} = \mathbb{Z}[\sqrt{-5}]. \tag{5.1b}$$

The fact that L_2 is not in the principal class (of L_1) is seen first "algebraically" and later on (see 6.9)) "transcendentally".

Historically lattices were treated by Gauss (1800) by a correspondance with binary positive quadratic forms $\Phi(n_1,n_2)$. This is done by writing $L = [\omega_1,\omega_2]$ with

$$L \to \Phi(n_1,n_2) = t|n_1\omega_1 + n_2\omega_2|^2 , \tag{5.2a}$$

where $t \in \mathbb{R}$ is chosen so that Φ takes the form, in integers of $\mathbb{Z}$,

$$\Phi(n_1,n_2) = an_1^2 + bn_1n_2 + cn_2^2 , \quad a > 0, \ \gcd(a,b,c) = 1, \tag{5.2b}$$
$$d = b^2 - 4ac < 0 .$$

(The details are omitted). The forms lie in h equivalence classes under $PSL_2(\mathbb{Z})$ on n_1 and n_2, which correspond uniquely to the classes $\{L_i\}$. (For details, see Borel etc. [2] and deSeguier [15]).

We bypass a wealth of technique to concentrate on the case (5.1ab) for $d = -20$. There

$$L_1 \to n_1^2 + 5n_2^2 = \Phi_1(n_1,n_2) \tag{5.3a}$$
$$L_2 \to 2n_1^2 + 2n_1n_2 + 3n_2^2 = \Phi_2(n_1,n_2). \tag{5.3b}$$

These forms must be inequivalent since they represent different sets of integers. For instance, Φ_1 represents 1 (and is indeed called <u>principal</u> accordingly, while Φ_2 does not, i.e., $2\Phi_2(n_1,n_2) = (2n_1 + n_2)^2 + 5n_2^2 \neq 2$ for n_1 and n_2 in $\mathbb{Z}$. (The term <u>principal</u> <u>ideal</u> arose deviously in this context; L_1 is principal in $\mathbb{Z}[\sqrt{-5}]$ while L_2 is not).

THEOREM 5.4. For the discriminants $d = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$ and more remarkably for no other, there is a unique equivalence class of forms or lattices ($h = 1$).

This result is the "Gauss-Heegner-Stark Theorem", (see Stark [18]). It is a major illustration of the use of transcendental functions for algebraic purposes. We shall merely define its main analytic tool, the <u>modular</u> <u>invariant</u> $j\{L\}$ with emphasis on the more manipulatively available aspects, rather than venturing into topology and becoming absorbed in a different world, (e.g., of forms and Riemann Surfaces, see Gunning [9]).

6. THE MODULAR INVARIANT.

By definition, we are demanding that the <u>modular invariant</u> $j\{L\}$ be analytic in τ ($\in H_+$), if $[1,\tau] \in \{L\}$. Thus we ask for invariance under $PSL_2(\mathbb{Z})$, see (3.6b),

$$j\{L\} = j(\tau) = j\left(\frac{a_{11}\tau + a_{12}}{a_{21}\tau + a_{22}}\right), \quad a_{ij} \in \mathbb{Z},\ a_{11}a_{22}-a_{12}a_{21} = 1, \quad \text{Im } \tau > 0. \tag{6.1}$$

We know from the generator properties in (3.4), that it suffices to show

$$j(-1/\tau) = j(\tau + 1) = j(\tau). \tag{6.2}$$

To form this invariant, we start for symmetry's sake with $L = [\omega_1,\omega_2]$. We consider the aggregate of lattice points

$$\{\Omega\} = \{n_1\omega_1 + n_2\omega_2 | n_1, n_2 \in \mathbb{Z}\} = L \tag{6.3}$$

and define two invariants of L by double summation on n_1 and n_2

$$g_2 = g_2(\omega_1,\omega_2) = 60\ \Sigma^* \Omega^{-4}, \tag{6.4a}$$

$$g_3 = g_3(\omega_1,\omega_2) = 140\ \Sigma^* \Omega^{-6}, \tag{6.4b}$$

where the Σ^* denotes the omission from the sum of $(n_1,n_2) = (0,0)$. (The strange constants 60 and 140 are explained by (8.3) below). Now g_2 and g_3 depend on L but not on $\{L\}$; nevertheless, g_2^3/g_3^2 depend only on $\{L\}$ (or on $\omega_1/\omega_2 = \tau$). With additional strange constants introduced, we write

$$j = j\{L\} = j(\tau) = 1728g_2^3/(g_3^2 - 27g_3^2 \tag{6.5}$$

THEOREM 6.6. The modular invariant $j(\tau)$ satisfies (6.1) and has the further properties that

(a) $j(\tau)$ is analytic (free of poles) when $\text{Im } \tau > 0$, (in particular $g_2^3 - 27g_3^2 \neq 0$), and $j\{L\}$ is biunique onto $\mathbb{C}$.

(b) by the invariance under $\tau \to \tau + 1$, $j(\tau)$ is a Laurent series in $q = \exp 2\pi i\tau$, convergent for $\text{Im } \tau > 0$, and with integral coefficients starting with

$$j(\tau) = 1/q + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots \tag{6.7}$$

(c) any other analytic function of τ invariant under $PSL_2(\mathbb{Z})$ and with polar bounds at ∞ ($< \text{const}|q|^{-m}$, $m \in \mathbb{Z}$), is a polynomial in $j(\tau)$.

We do not attempt the proof here, although part (c) is particularly the key to the connection with topology and Riemann Surfaces. We note the uncanny accuracy of

(6.7) in computing j for the multipliers of norm 2, namely,

$$j(\sqrt{-2}) = 8000 = 20^3,\ j(i) = 1728 = 12^3,\ j\left(\frac{-1+\sqrt{-7}}{2}\right) = -3375 = -15^3. \qquad (6.8)$$

In addition, in reference to (5.1ab), for $d = -20$, we compute

$$j(\sqrt{-5}) = (50 + 26\sqrt{5})^3,\ j\left(\frac{1+\sqrt{-5}}{2}\right) = (50 - 26\sqrt{5})^3 \qquad (6.9)$$

which should further reassure us that $\{L_1\} \neq \{L_2\}$. It may seem precarious, in (6.9), to guess irrationals from decimals, but the sum and product of the entries in (6.9) are integers.

THEOREM 6.10. For every discriminant $d(< 0)$, let ξ_1 denote the generator in (4.10ab). Then the value of $j(\xi_1)$ is an algebraic integer of degree h over the field

$$k_0 = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\xi_1). \qquad (6.10a)$$

It generates a field over $\mathbb{Q}$ (of degree $2h$), namely,

$$K = k_0(j(\xi_1)) \qquad (6.10b)$$

which is abelian over k_0. The h conjugates of $j(\xi_1)$ over k_0 are $j\{L_i\}$, $(i = 1,\dots,h)$, the various classes of discriminant d. Thus from the fact that $j(\xi_1)$ is real, it is a rational integer precisely when $h = 1$, (see (5.4)).

This is part of a startling result in number theory of Weber (1890) (actually, "ring class field theory"). We need the further definition that a prime p splits in K if for every element γ of K the defining equation (over $\mathbb{Q}$) must, on reduction modulo p, contain only linear factors, possibly repeated. (One linear factor implies all factors of the defining equation are linear since $K/\mathbb{Q}$ is normal. We could even assume γ is restricted to integers whose defining equation has no multiple factors). In the most familiar case (see Cohn [3]) we say that p splits in $k_0 = \mathbb{Q}(\sqrt{d})$ exactly when d is a quadratic residue of $p, (d/p) = 1$, (excluding those p which divide d). The result is as follows:

THEOREM 6.11. If the prime p does not divide d, then the condition for p to split in K, see (6.10b), is that we can represent p by the principal quadratic form $|n_1 + n_2\xi_1|^2$, i.e., that we can solve for n_1 and n_2 in $\mathbb{Z}$ whichever applies:

$$p = n_1^2 - dn_2^2/4,\quad d \equiv 0 \pmod 4), \qquad (6.12a)$$

$$p = n_1^2 + n_1n_2 - (d-1)n_2^2/4,\quad d \equiv 1 \pmod 4). \qquad (6.12b)$$

Thus for $h(d = 1$, (6.12ab) follows exactly when p satisfies $(d/p) = 1$.

Weber [19] "almost" constructed all fields relatively abelian over the base field k_0 by using $j(\tau)$, but a later modification of Fueter [6] and Hasse [10] was required to do it. (Kronecker had called for such a construction as his "Jugendtraum"). Hilbert saw the phenomenon of a transcendental generator of algebraic fields and formulated his famous "twelfth problem" (see Langlands [14]) to investigate it further. Instead of describing the enormous complications to which this has lead, we retreat to the complex multiplications of norm 2 to show how they affect the j-function.

7. THE MODULAR EQUATION.

For any positive integer n, $j(n\tau)$ can be seen to be a root of a polynomial equation with integral coefficients and powers of $j(\tau)$. Going directly to $n = 2$, we define three functions j_1, j_2, and j_3 by

$$j_1(\tau) = j(2\tau),\ j_2(\tau) = j(\tau/2),\ j_3(\tau) = j(\tfrac{\tau + 1}{2}). \tag{7.1}$$

These are seen to be conjugates over the field of $j(\tau)$; indeed, we verify the following for the generators of $PSL_2(\mathbb{Z})$ in (6.2):

$$j_1(\tau + 1) = j_1(\tau),\ j_1(-1/\tau) = j_2(\tau) \tag{7.2a}$$

$$j_2(\tau + 1) = j_3(\tau),\ j_2(-1/\tau) = j_1(\tau) \tag{7.2b}$$

$$j_3(\tau + 1) = j_2(\tau),\ j_3(-1/\tau) = j_3(\tau). \tag{7.2c}$$

The last one is not quite immediate,

$$j_3(-\tfrac{1}{\tau}) = j\left(\frac{-1 + \tau}{2\tau}\right) = j\left(\frac{2\tau}{1 - \tau}\right) = j(-2 + \frac{2}{-\tau + 1}) = j\left(\frac{2}{-\tau + 1}\right) =$$

$$j\left(\frac{\tau - 1}{2}\right) = j\left(\frac{\tau + 1}{2}\right) = j_3(\tau). \tag{7.3}$$

From Theorem 6.6c we conclude that the symmetric functions of j_1, j_2, j_3 are the roots of a polynomial equation with integral polynomials in $j(\tau)$ as coefficients, the modular equation of order 2,

$$F_2(j_i, j(\tau)) = 0 \tag{7.4}$$

Our final tour de force will be the evaluation (see Fueter [6], Yui [21])

$$\begin{aligned} F_2(X,Y) = {} & X^3 + Y^3 - X^2Y^2 + 2^4.3.31(X^2Y + Y^2X) - 2^4.3^4.5^3(X^2 + Y^2) \\ & + 3^4.5^3.4027XY + 2^8.3^7.5^6(X + Y) - 2^{12}.3^9.5^9. \end{aligned} \tag{7.5}$$

On setting $Y = X$ and factoring, we are reassured again by

$$-F_2(X,X) = (X - 20^3)(X + 15^3)^2(X - 12^3). \tag{7.6}$$

Here we have the three complex multiplications of norm 2 (see (6.8)), where $X = Y = j(\tau) = j(2\tau)$, (see (3.9)).

Before evaluating $F_2(X,Y)$, we note the symmetry in X and Y, because of the reciprocal role of $j_1 = j(2\tau)$ and $j_2 = j(\tau/2)$. The symmetry might worry us because $F_2(j(2\tau), j(\tau)) = 0$ and $F_2(j(2\tau), j(4\tau)) = 0$, leaving the impression that $j(4\tau)$ is a conjugate of $j(\tau)$. To explain this "paradox" requires a careful accounting of the Galois group permutations of the j_i (seen in (7.2abc) to be 3-dihedral). Klein [13] introduced his solutions of equations by polyhedra precisely in this context, (the "icosahedron" entering for $j(5\tau)$, see Cohn [5]).

8. ELLIPTIC INTEGRALS.

The classic way to forge a relation between $j(\tau)$ and $j(2\tau)$ is to find two elliptic integrals, one of which has periods in a lattice belonging to τ (e.g., $L = [\omega_1,\omega_2]$) and the other of which has periods in a lattice belonging to 2τ, (i.e., $L' = [\omega_1, 2\omega_2]$). Incredibly, the relations between such integrals are manageable by "undergraduate calculus".

We use the Weierstrass method of starting with the lattice $L = [\omega_1,\omega_2]$ of periods and constructing elliptic functions with these periods. We start with (6.3) and define (see Whittaker and Watson [20])

$$z = p(u) = 1/u^2 + \Sigma^*(1/(u - \Omega)^2 - 1/\Omega^2). \tag{8.1}$$

Then all elliptic functions with period lattice L are the field $\mathbb{C}(z,w)$, where, (disdaining to discuss convergence), we set

$$w = p'(u) = -2/u^3 -2\ \Sigma^*\ 1/(u - \Omega)^3. \tag{8.2}$$

Next, using the special coefficients in (6.4ab), we find

$$w^2 = 4z^3 - g_2 z - g_3 \tag{8.3}$$

$$du = dz/w = dz/\sqrt{4z^3 - g_2 z - g_3}\quad . \tag{8.4}$$

Thus, for any constant $\mu(\neq 0)$, $\mu\int du$ is an elliptic integral of the <u>first kind</u> (always finite) and its periods form the lattices in the class $\{L\}$, as μ varies. The polynomial $P(z) = 4z^3 - g_2 z - g_3$ has three distinct roots (since $g_2^3 - 27g_3^2 \neq 0$ from Theorem 6.6a). Hence a typical period of $\int du$ itself is

$$2\int_{z=e_1}^{e_2} du \quad = \quad 2\int_{e_1}^{e_2} dz/\sqrt{P(z)} \tag{8.5}$$

where, $P(z)$ is now a cubic (and later on a biquadratic) with e_1 and e_2 as roots, (for a cubic, ∞ also behaves like a root). The factor 2 in (8.5) comes from the fact that a period path does not really join two roots, but rather it encircles them so that the value of $\sqrt{P}(z)$ can return to its original sign. Then the period path contracts to a doubled value.

To manipulate $\int du$, it is necessary to change it to the Legendre form so $du =$ const dv, where

$$dv = dz/\sqrt{(1 - Z^2)(1 - k^2Z^2)}, \quad k \neq \pm 1. \tag{8.6a}$$

We can do this by a linear transformation

$$z = (\alpha Z + \beta)/(\gamma Z + \delta), \quad \alpha,\beta,\gamma,\delta \in \mathbb{C}, \quad \alpha\delta - \beta\gamma \neq 0. \tag{8.6b}$$

Fortunately, this transformation need not be specified! All we need note is that we are transforming the roots

$$e_1,\ e_2,\ e_3,\ \infty \tag{8.7a}$$

of $4z^3 - g_2z - g_3$ into those of $(1 - Z^2)(1 - k^2Z^2)$, namely,

$$1,\ -1,\ 1/k,\ -1/k\ . \tag{8.7b}$$

We choose the right value of k for this by the cross-ratio. The cross-ratio of r_1, r_2, r_3, r_4 is defined as

$$\lambda = (r_1 - r_2)(r_3 - r_4)/(r_1 - r_4)(r_3 - r_2). \tag{8.7c}$$

So we define k to satisfy

$$\lambda = (e_1 - e_2)/(e_3 - e_2) = 4k/(k + 1)^2. \tag{8.7d}$$

Actually, there are six values of λ associated with each other by permuting r_1, r_2, r_3, r_4. These are also functions of e_1, e_2, e_3,

$$\lambda_j = \{\lambda, 1/\lambda,\ 1 - \lambda,\ 1/(1 - \lambda), (\lambda-1)/\lambda, \lambda/(\lambda - 1)\},\ j = 1,\ldots,6, \tag{8.8}$$

so symmetric functions of the λ_j should return us to g_2 and g_3. Thus it is no surprise to obtain $j(\tau)$ as

$$\begin{aligned} j(\tau) = 128\ \Sigma\ \lambda_j^{\ 2} + 384 &= 256(\lambda^2 - \lambda + 1)^3/\lambda^2(\lambda - 1)^2 \\ &= 16(k^4 + 14k^2 + 1)^3/k^2(k^2 - 1)^4. \end{aligned} \tag{8.9}$$

Now we use the Gauss-Landen transformation in (8.6a):

$$kZ = 2/(Z'\sqrt{k'} + 1/Z'\sqrt{k'}), \tag{8.10a}$$

with k' chosen so $k^2 = 4k'/(k' + 1)^2$, or,

$$k = 2/(\sqrt{k'} + 1/\sqrt{k'}). \tag{8.10b}$$

This transformation is (remarkably) one-to-two from Z to Z', yet it transforms dv to $(k' + 1)\,dv'$, where, after some hard work,

$$dv' = dZ'/\sqrt{(1-Z'^2)(1 - k'^2Z'^2)} \quad (= dv/(k' + 1)). \tag{8.11}$$

A further property of the transformation is that the lattice L' of periods of $dv'(k'+1)$ is the same as that of the lattice L of dv in the direction of ω_1 but doubled in the other, ω_2 . Thus $j(\tau)$ for L becomes $j(2\tau)$ for L'. Specifically, we note that as Z' goes from -1 to 1, Z goes from -1 to 1 in one-to-one fashion. On the other hand, when Z' goes from 1 to $1/k'$, Z goes from 1 to $1/k$ and back to 1 (doubling the period). Thus in (8.10ab),

$$\begin{aligned} Z' &= 1 &&\Rightarrow\ Z = 1\\ Z' &= 1/\sqrt{k'} &&\Rightarrow\ Z = 1/k\\ Z' &= 1/k' &&\Rightarrow\ Z = 1. \end{aligned} \tag{8.12}$$

Finally, using (8.9) and (8.10b) for $j(2\tau)$, we have

$$j(\tau) = 16(k^4 + 14k^2 + 1)^3/k^2(k^2 - 1)^4 \tag{8.13a}$$

$$\begin{aligned} j(2\tau) &= 16(k'^4 + 14k'^2 + 1)^3/k'^2\,(k'^2 - 1)^4 =\\ &= 256(k^4 - k^2 + 1)^3/k^4(k^2 - 1)^2 . \end{aligned} \tag{8.13b}$$

To eliminate k in (8.13ab), we write

$$s = (k - 1/k)^2/4; \tag{8.14}$$

$$j(\tau) = 64(s+4)^3/s^2 = 64(64/s^2 + 48/s + 12 + s), \tag{8.15a}$$

$$j(2\tau = 64(4s+1)^3/s = 64(1/s + 12 + 48s + 64s^2). \tag{8.15b}$$

There is a clear symmetry under $s \to 1/s$ (only to be expected from the symmetry of $F_2(X,Y)$). So $j(\tau)$ and $j(2\tau)$ are now replaced by symmetric functions in $t = s + 1/s$,

$$(j(\tau) + j(2\tau))/64 = 64t^2 + 49t - 116, \tag{8.16a}$$

$$j(\tau)\,j(2\tau)/64^2 = 64t^3 + 816t^2 + 3468t + 4913. \tag{8.16b}$$

The modular equation (7.5) (now in $X + Y$ and XY) emerges from a hand-calculation as the condition for a quadratic and a cubic polynomial (in t) to have a common root.

9. SOME FOLKLORE AND HISTORY.

The discovery of complex multiplication is connected with a legend which typically portrays C. F. Gauss as always the Übermensch and never the Münchhausen in his claims to prescience and omniscience. At the age of 14, in 1791, Gauss invented the arithmetic-geometric mean (agm), as a mere curiousity. Here one starts with two positive quantities a and b and transforms them by

$$T(a',b'),\ a' = (a+b)/2,\ b' = \sqrt{ab}\ . \tag{9.1}$$

Then $a' - b'$ has the order $(a-b)^2$ so the iteration of T easily converges as $n \to \infty$ to

$$\lim T^n(a,b) = (M,M),\ M = \operatorname{agm}(a,b). \tag{9.2}$$

Gauss calculated a few cases including

$$\operatorname{agm}(1,\sqrt{2}) = 1.198140234735592207439\ \ldots\ . \tag{9.3}$$

Now, eight years later, in 1799, Gauss [8] calculated $\int_0^1 dx/\sqrt{1-x^4}$, and naturally took the ratio to its cognate $\int_0^1 dx/\sqrt{1-x^2} = \pi/2$, only to recall that this ratio agreed to 11 decimal places with the reciprocal of $\operatorname{agm}(1,\sqrt{2})$. He justified this by proving that (under (9.1)),

$$I = \int_0^{\pi/2} d\theta/\sqrt{a^2\cos^2\theta + b^2\sin^2\theta} = \int_0^{\pi/2} d\theta/\sqrt{a'^2\cos^2\theta + b'^2\sin^2\theta} \tag{9.4}$$

$$= \pi/(2\operatorname{agm}(a,b))$$

as it would follow by iterating $T^n(a,b)$, while a and b approached a common limit. In terms of the integrals of type (8.6a), we can set $\sin\theta = Z$ and find

$$aI = \int_0^1 dZ/\sqrt{(1-Z^2)(1-k^2Z^2)},\quad k^2 = (a^2 - b^2)/a^2\ . \tag{9.5}$$

Thus for $a = 1$, $b = \sqrt{2}$, $k = i$, we obtain the arc length of the (figure-eight) lemniscate, $1 + r^2 = 2\cos^2\theta$ in polar coordinates. Gauss prove (9.4), essentially, by using the undoubled period in (8.10ab). The doubled period occurred even more strongly in the form of theta-function identities (akin to the modular equation). Remarkably, Gauss [7] did not publish this work until 1818, when he related it to the problem in astronomy of approximating the perturbation of a slow planet by a fast planet, by replacing the fast planet's orbit by an elliptical ring. Meanwhile, in 1795, J. Landen in Cambridge had essentially produced the integral transformation of (8.10ab), but presumably not with the modular interpretation.

There is a conflicting view that the credit for complex multiplication must be reserved to N. H. Abel [1] who first used period lattices and complex multipliers, but only in 1828 (see Cohn [4]). Thus it would be within Abel's scope to show complex multiplication by (1 + i) by presenting the integral transformation of Gauss and Landen in the form of the statement that the differential equation

$$dz/\sqrt{1 - z^4} = (1 + i)dz'/\sqrt{1 - z'^4} \qquad (9.6a)$$

has the <u>algebraic</u> integral in z and z'

$$z^2 = -2i/(z'^2 - 1/z'^2). \qquad (9.6b)$$

(Some minor changes of variable are required). Euler had previously shown in 1751 how to produce a (real) factor of 2 (rather than 1 + i), but C. L. Siegel [16] credits Fagnano who found such a formula as early as 1718!

In this century, Hecke [11] attempted to extend Weber's Theorem (6.11) to other fields, but this led mostly to a theory of modular functions of several variables. Weber's original program is still being pursued on a much more abstract level by G. Shimura [17], R. Langlands [14], and others, (but it can scarcely be given a status report here).

ACKNOWLEDGMENTS. Based on research supported by NSF Grant MCS 7903060. Earlier versions of this work were presented at the University of Copenhagen in January 1977 under a visit sponsored by the Danish National Research Council.

BIBLIOGRAPHICAL NOTE

An excellent exposition from an older vantage point was given by G. N. Watson in the Mathematical Gazette 17(1933)5-17 under the title "The Marquis and the Land-agent, A Tale of the Eighteenth Century". (He refers in the title to Fagnano and Landen, respectively).

REFERENCES

1. Abel, N.H. Recherches sur les fonctions elliptiques, Journ. reine angew. Math, 3(1828)160-190.
2. Borel, A., Chowla, S., Herz, C.S., Iwasawa, K. and Serre, J-P., Seminar of Complex Multiplication, Springer Lect. Notes., #21, 1966.
3. Cohn, H., Second Course in Number Theory, Wiley, 1962, (Dover reprint, 1980, under the title "Advanced Number Theory").
4. Cohn, H., Diophantine equations over $\mathbb{C}(t)$ and complex multiplication, (Number Theory, Carbondale, 1979), Springer Lecture Notes #751, 1979, 70-81.
5. Cohn, H., Iterated ring class fields and the icosahedron, Math. Annalen, 225 (1981) 107-122.

6. Fueter, R., Vorlesungen über die Singulären Moduln und die Komplexe Multiplikation, I, II, Teubner, 1924, 1927.

7. Gauss, C.F., Bestimmung der Anziehung eines elliptischen Ringes, 1818, (Reprint by Ostwalds Klassiker, Leipzig, 1927).

8. Gauss, C.F., Gedenkband Anlässich des 100 Todestages am 23 Februar 1955, Teubner, 1957.

9. Gunning, R.C., Lectures on Modular Forms, Princeton, 1962.

10. Hasse, H., Neue Begrundung der komplexe Multiplikation, Journal reine angew. Math., 157(1927)115-139, 165(1931)64-88.

11. Hecke, E., Höhere Modulfunktionen und ihre Anwendung auf die Zahlentheorie, Math. Annalen, 71(1912) 1-37.

12. Jacobson, N., Basic Algebra I, Freeman, 1974.

13. Klein, F., Über die Transformation der elliptischen Funktionen und die Auflösung fünften Grades, Math. Annalen, 14(1878)111-172.

14. Langlands, R., Some contemporary problems with origins in the Jugendtraum, (Mathematical Developments arising from Hilbert's Problems), Proc. Symp. Pure Math. Vol. 28, 1976, 401-418.

15. De Seguier, J., Sur deux Formules Fondamentales dans la Théorie des Formes Quadratiques et de la Multiplication Complexe apres Kronecker, Berlin, 1894.

16. Siegel, C.L., Vorlesungen über Ausgewählte Kapitel der Funktionentheorie, Lecture Notes, Gottingen, 1965, (Engl. Trans. "Topics in Complex Function Theory", Wiley, 1971).

17. Shimura, G., Automorphic Functions and Number Theory, Springer Lecture Notes, #54, 1968.

18. Stark, H.M., Class numbers of complex quadratic fields, (Modular Functions of One Variable I, Antwerp, 1972). Springer Lecture Notes, #320, 1973, 153-174.

19. Weber, H., Elliptische Funktionen und Algebraische Zahlen, Vieweg, 1891.

20. Whittaker, E.T., and Watson, G.N., A Course in Modern Analysis, Cambridge, 1940.

21. Yui, N., Explicit form of the modular equation, Jour. reine angew. Math. 299/300(1978) 185-200.