STABLE LATTICES

PART II

HARVEY COHN

10. Introduction to Part II. The most interesting cases of stable lattices, introduced in an earlier volume of this journal **(12)**, were the (algebraic) modules of stable norm, or modules whose ratio of minimum absolute non-zero norm to lattice determinant (i.e., to the square root of module-discriminant) is a local maximum for small variations of the basis. We soon found that these modules were perhaps more numerous than we should have desired if we were interested only in finding an absolute maximum. Nevertheless stable lattices acquire a certain amount of intrinsic interest once we reach the stage where the *continuous* variable concept of "neighborhood of a lattice" leads to *algebraic* criteria of stability. In both these respects the situation displays some similarity to the more classical subject of extremal (quadratic) forms **(2)**.

If the module in question is the module of all integers (i.e., the so-called *integer-module*) of a *totally real* field of degree n, then the criterion of stability depends on the relative signs of the conjugates of the units. This is a specialization, (*weaker* when $n > 3$), of the classical concept of "(maximum) signature rank 2^n," used by Weber **(13)** for instance. We shall merely show, as a significant illustration, that the integer-module of the totally real field $K_N = R(\cos 2\pi/N)$, over the rationals R, has stable norm (except for a few small N).

If we consider fields that are *not totally real*, the classical problem of signature rank becomes vacuous for the imaginary (conjugate) fields while the stability criterion that we use becomes more complicated. We shall, however, demonstrate a refinement of the "unit star" method of Part I **(12**; p. 265**)**, to obtain a criterion that can be readily used to test more general modules. We shall carry this through the cubic case.

The big difficulty arises when "too many" roots of unity occur. We shall, therefore, consider as a final example the integer-module of the cyclotomic field $K^N = R(\exp 2\pi i/N)$. This module turns out to have a stable norm if and only if N is square-free. This result, which essentially uses the presence or absence of a normal basis for K^N, should further attest to the algebraic aspect of stability.

11. A totally-real illustration. If we specialize somewhat to integer-modules of a totally real *normal* field K, then the criterion of stability (of the

Received September 29, 1953. Presented to the American Mathematical Society September 2, 1952. Research sponsored by the Office of Ordnance Research, U.S. Army, under contract DA-20-018-ORD-12332.

The bibliographical items and section headings are numbered consecutively with items in Part I, otherwise referred to as **(12)**.

norm), given in Part I **(12**, p. 269**)**, reduces to the following: *For any non-identical automorphism S of K, (over the rationals), at least one unit u exists for which u/u^S is negative.*

For instance, consider the totally real field $K_N = R(\cos 2\pi/N)$ of degree $n = \frac{1}{2}\phi(N)$ (when $N > 2$). Here $\phi(N)$ is the Euler totient function (not to be confused with the gauge function of Part I **(12**, p. 261**)**, which has a vector argument). The field K_N is the maximal totally real field in the cyclotomic field $K^N = R(\exp 2\pi i/N)$. We shall show that *the integer-module of K_N has stable norm if*

$$N \neq 1, 2, 3, 4, 6, 12. \tag{11.1}$$

For the first five exceptional values of N, K_N is rational; while for $N = 12$, $K_{12} = R(\sqrt{3})$, which is unstable by the unsolvability **(12**, p. 267**)** of the diophantine equation $x^2 - 3y^2 = -1$.

For the field K_N, the Galois group consists of the $\frac{1}{2}\phi(N)$ operations

$$S\colon \zeta \to \zeta^{\pm g}, \qquad (g, N) = 1. \tag{11.2}$$

$$(\cos 2\pi M/N)^S = \cos 2\pi Mg/N. \tag{11.3}$$

To prove stability we make use of the following types of units:

$$\theta = 2\cos 2\pi M/N \qquad N \neq 2^k,\ 4p^k \quad (k \geqslant 0), \tag{11.4}$$

$$\psi = 1 + 2\cos 2\pi M/N \qquad N \neq 3p^k \quad (k \geqslant 0), \tag{11.5}$$

where $(M, N) = 1$ and p is a prime. (We note that this choice of units of K_N accounts for all N except the values (11.1).)

Now first of all we assert that for the special values of N:

$$N_1 = p^k (\neq 3), \quad N_2 = pq \tag{11.41}$$

the units θ are sufficient to establish stability; while for the special values:

$$N_3 = 4.2^k, \quad N_4 = 4p (\neq 12) \tag{11.51}$$

the units ψ are sufficient. In these cases p and q are odd primes and $k \geqslant 1$. We shall verify this just in a typical case, $N = N_1$. Here all we need to show is that for a given non-trivial automorphism S, a $M = M_1$ exists for which $\theta = \theta_1$ is positive and ${\theta_1}^S$ is negative. Thus all we need show is that for any $g \not\equiv \pm 1 \bmod N_1$, (for which $(g, N_1) = 1$), there exists an M_1 (for which $(M_1, N_1) = 1$), such that M_1 lies in the range $(-\frac{1}{4}N_1, \frac{1}{4}N_1)$, while $M_1 g$ is congruent (mod N_1) to a value in the range $(\frac{1}{4}N_1, \frac{3}{4}N_1)$. The existence of such an M_1 is assured from the fact that the possible values of M (i.e., the non-multiples of p), have such few gaps (i.e., the multiples of p), that the values of Mg cannot always "straddle" the range $(\frac{1}{4}N_1, \frac{3}{4}N_1)$ modulo N_1. Thus some value of Mg must lie in this range when $M = M_1$, a non-multiple of p. A similar argument holds for N_2, N_3, and N_4 (which were singled out for simplicity of proof, since they have few prime divisors and hence "small gaps").

We are now prepared to handle the general N in the following way: Suppose

that for the given S, $g \not\equiv \pm 1 \bmod N_1$, for N_1 (of type (11.41)) dividing N. Then the very same θ_1 used earlier is a unit of K_{N_1} (hence of K_N) for which $\theta_1/\theta_1{}^S$ is negative. Thus we see that the difficult case becomes the one in which, for each $p_i{}^{k_i}$ in the factorization $N = \Pi p_i{}^{k_i}$ the congruence

$$g \not\equiv \pm 1 \bmod p_i{}^{k_i}$$

is satisfied. In order that S still not be the identity, it is necessary that these ± 1 be "mixed" (e.g., that g not be congruent to (say) $+1$ for each $p_i{}^{k_i}$. Thus $g \not\equiv \pm 1$ for some composite modulus dividing N, of the type N_2 (see (11.41)) or N_4 (see (11.51)). Hence, once more, as in the preceding paragraph, a unit θ_2 or ψ_4 is determined for which $\theta_2/\theta_2{}^S$ or $\psi_4/\psi_4{}^S$ is negative. Q.E.D.

12. The stability configuration. In the last section, we obtained only an existence proof, i.e. a proof that $Q + 1$ $(= n(n-1)+1)$ *positively dependent* "gradient" vectors **(12**, pp. 263, 266**)**.

$$\mathbf{R}[\mathbf{u}] = (\ldots, u_l/u_j, \ldots) \qquad (l, j = 1, 2, \ldots, n; l \neq j), \tag{12.1}$$

exist, where $\mathbf{u} = (u_1, \ldots, u_n)$ is a vector of the module formed from each of $Q + 1$ properly chosen units u_1 of K_N. The set of $Q + 1$ vectors $\mathbf{R}[\mathbf{u}]$ will be called a *stability configuration*. The actual choice of the $Q + 1$ units u_1, as we shall indicate, is not only extremely difficult, but it accentuates irregularities in the infinitesimal behavior of the units of K_N for different N.

Nevertheless the finding of these $Q + 1$ vectors $\mathbf{u}$ or $\mathbf{R}[\mathbf{u}]$ would be desirable in view of the fact that a modular reduction theorem automatically enlarges the "neighborhood" of a stable lattice (*possibly* to the whole lattice space, thus establishing a critical lattice, as in the quadratic case **(12**, p. 268**)**). For instance, take the following simple-looking set of n units of K_N (for N prime $\geqslant 5$):

$$u_1 = \begin{cases} \zeta \quad + \zeta^{-1} \\ \zeta^3 \quad + \zeta + \zeta^{-1} + \zeta^{-3} \\ \ldots \qquad\qquad \ldots \\ \zeta^{N-4} + \zeta^{N-6} + \ldots + \zeta + \zeta^{-1} + \ldots + \zeta^{-N+6} + \zeta^{-N+4} \\ -1 \end{cases} \tag{12.2}$$

where $\zeta = \exp 2\pi i/N$. Each of the first $n - 1$ units listed above is taken with its conjugates and the last (rational) unit is taken once, forming $Q + 1 = n(n-1) + 1$ units.

It is found by very laborious calculations (which we omit) that the resulting $Q + 1$ vectors $\mathbf{R}[\mathbf{u}]$ provide a stability configuration when $N = 5, 7, 13$ but that these vectors are not even of rank Q when $N = 11$. The question of whether or not the integer-module of K_N provides a critical lattice for the norm in n real dimensions is answered positively for $N = 5, 7$ **(3)**, and negatively for $N = 13$ **(11)**, while for $N = 11$ the answer is still unknown. It would probably be wise to exhibit a sufficiently simple stability configuration for the integer-module in K_{11} before trying to establish it as a critical lattice.

13. Stability criterion for complex modules. Going to the complex case, we return to greater generality by considering as in §9 (above) any (non-degenerate) module $\mathfrak{M}$ (not necessarily consisting of *all* the integers of a field). The elements of $\mathfrak{M}$ are algebraic integers z with r real and $2s$ complex conjugates:

$$\begin{aligned} z_j &= x_j && (j = 1, 2, \ldots, r), \\ z_j &= x_j + i\,x_{j+s} && (j = r+1, \ldots, r+s), \\ z_{j+s} &= x_j - i\,x_{j+s}, \end{aligned} \tag{13.1}$$

making a total of $r + 2s = n$ conjugates. Then we are interested in stable modules for the norm (gauge) function

$$|\, x_1 \ldots x_r\, (x_{r+1}^2 + x_{r+s}^2) \ldots (x_{r+s+1}^2 + x_{r+2s}^2)\,|.$$

We consider the vector of $Q = n(n-1)$ generally complex components:

$$\mathbf{R}[\mathbf{z}] = (\ldots, z_l/z_j, \ldots) \quad (l, j = 1, 2, \ldots, n;\ l \neq j). \tag{13.2}$$

Then the criterion for stability is that the set of vectors $\mathbf{R}[\mathbf{z}]$ positively span a space of dimension Q as $\mathbf{z}$ varies over the set of module elements of minimum non-zero absolute norm. This criterion was established earlier **(12**, p. 266**)**, using $2Q$ real components, but the present form will prove simpler to use. As in the totally real case, the finding of $Q + 1$ positively dependent vectors $\mathbf{R}[\mathbf{z}]$ is so difficult that we must establish a new criterion relating to *projections of* $\mathbf{R}[\mathbf{z}]$.

Now every vector $\mathbf{R}[\mathbf{z}]$ can be expressed in terms of $n(n-1)$ *real* coordinates if we break the vector up into the following projections: Take any pair of distinct fields chosen from the first $r + s$ conjugate fields (conjugate complex repetitions being excluded). For every such pair, denoted by unequal subscripts $l, j (\leqslant r + s)$, a projection is determined. Specifically for l, j *both real*, there are $r(r-1)$ projections

$$\mathbf{R}_{l,j}[\mathbf{z}] = (z_l/z_j), \tag{13.31}$$

for l, j *both complex*, there are $s(s-1)$ projections

$$\mathbf{R}_{l,j}[\mathbf{z}] = (z_l/z_j,\ z_{l+s}/z_j) \tag{13.32}$$

for l, j *mixed* (i.e., one real and the other complex), there are $2rs$ projections

$$\mathbf{R}_{l,j}[\mathbf{z}] = (z_l/z_j). \tag{13.33}$$

Now, clearly, the projections of type (13.31) are of real dimension one; the projections of type (13.32) and (13.33) having two and one *complex* components, are of real dimension four and two respectively. We write this as dim $[l, j] = 1, 4$, and 2 respectively. If we were to sum the number of coordinates, we should find it accounts for

$$r(r-1) \cdot 1 + s(s-1) \cdot 4 + 2rs \cdot 2 = Q - 2s$$

coordinates. The remaining $2s$ coordinates are accounted for by a single projection called the "$2s$" projection,

$$\mathbf{R}_{2s}[\mathbf{z}] = (z_{r+1}/z_{r+s+1}, \ldots, z_{r+s}/z_{r+2s}), \tag{13.34}$$

of s complex components and of (real) dimension $2s$.

For some purposes it will be necessary to visualize all the real and imaginary parts written out as Q cartesian coordinates of a cartesian space $\mathfrak{S}^Q$ with projections $\mathfrak{S}^{\dim[l,j]}$ and $\mathfrak{S}^{2s}$. Thus we may introduce a (real) scalar product and with it length and angle. Furthermore any one of the projections may be imbedded (in the natural way) in $\mathfrak{S}^Q$ by setting the $Q - \dim[l,j]$ or $Q - 2s$ remaining coordinates equal to zero. Thus we may speak of the angle between $\mathbf{R}[\mathbf{z}]$ and any one of its projections, $\mathbf{R}_{l,j}[\mathbf{z}]$ or $\mathbf{R}_{2s}[\mathbf{z}]$.

The significance of the subspaces is then derived from the following fact: *Let any* $\mathbf{z}_0$ $(\neq 0)$ *be given. Then a* $\mathbf{z}_1$ *of equal norm exists for which* $\mathbf{R}[\mathbf{z}_1]$ *is arbitrarily close in direction to any preassigned* $[l,j]$ *projection* $\mathbf{R}_{l,j}[\mathbf{z}_0]$. To see this, take $\mathbf{z}_1 = \mathbf{z}_0\mathbf{u}$ where $\mathbf{u}$ is a unit of $\mathfrak{O}$ the order of $\mathfrak{M}$, so chosen (by Dirichlet's Theorem on units **(12**, p. 269**)**), that $|u_p/u_q|$ has the largest order of magnitude for the choice of sub-scripts $p = l$, $q = j$ $(p, q \leqslant r + s)$, and so that u_l/u_j lies arbitrarily close in argument to a *positive* real number. The main stability criterion will be a more complicated version of the "unit star" method of Part I **(12**, p. 265**)**, (which dealt entirely with one-dimensional $[l,j]$ projections). It is as follows:

The necessary and sufficient condition that the module $\mathfrak{M}$ *have a stable norm is that for* $\mathbf{z}$ *a variable element of minimum absolute non-zero norm in* $\mathfrak{M}$, *the projections* $\mathbf{R}_{l,j}[\mathbf{z}]$ *or* $\mathbf{R}_{2s}[\mathbf{z}]$ *each positively span a space of* $\dim[l,j]$ *or* $2s$ *dimensions.*

The *necessity* is immediate since a projection of a set of vectors positively spanning a space must necessarily positively span the projection. The *sufficiency* proof is the difficult one.

14. Sufficiency proof of stability criterion. We let $\mathbf{z}$ be a general element of $\mathfrak{M}$ of minimum absolute non-zero norm and we assume, as our hypothesis, that for certain values of $\mathbf{z}$, namely

$$\mathbf{z}_{l,j}^{(h)},\ \mathbf{z}_{2s}^{(k)} \qquad (1 \leqslant h \leqslant 1 + \dim[l,j],\quad 1 \leqslant k \leqslant 1 + 2s), \tag{14.1}$$

the sets of *projection* vectors $\{\mathbf{v}\}$, consisting of the subsets

$$\begin{aligned} \mathbf{R}_{l,j}[\mathbf{z}_{l,j}^{(h)}] &= \{\mathbf{v}\}_{l,j} && (1 \leqslant h \leqslant 1 + \dim[l,j]), \\ \mathbf{R}_{2s}[\mathbf{z}_{2s}^{(k)}] &= \{\mathbf{v}\}_{2s} && (1 \leqslant k \leqslant 1 + 2s), \end{aligned} \tag{14.2}$$

are positively dependent. The object is to show that for properly chosen units $\{\mathbf{U}\}$ of the order $\mathfrak{O}$ the vectors $\{\mathbf{W}\}$, consisting of the subsets

$$\begin{aligned} \mathbf{R}[\mathbf{Z}_{l,j}^{(h)}] &= \{\mathbf{W}\}_{l,j} && (1 \leqslant h \leqslant 1 + \dim[l,j]), \\ \mathbf{R}[\mathbf{Z}_{2s}^{(k)}] &= \{\mathbf{W}\}_{2s} && (1 \leqslant k \leqslant 1 + 2s), \end{aligned} \tag{14.3}$$

positively span the real cartesian space $\mathfrak{S}^Q$, where

$$\mathbf{Z}_{l,j}^{(h)} = \mathbf{z}_{l,j}^{(h)}\,\mathbf{U}_{l,j}^{(h)},\quad \mathbf{Z}_{2s}^{(k)} = \mathbf{z}_{2s}^{(k)}\,\mathbf{U}_{2s}^{(k)}. \tag{14.4}$$

The positive span will be established by means of the *projection* and *independence*

https://doi.org/10.4153/CJM-1954-027-6 Published online by Cambridge University Press

properties **(12**, p. 265**)**. We use the further set $\{\mathbf{V}\}$ to represent the projections of $\{\mathbf{W}\}$:

$$\begin{aligned} &\mathbf{R}_{l,j}[\mathbf{Z}_{l,j}^{(h)}] = \{\mathbf{V}\}_{l,j} && (1 \leqslant h \leqslant 1 + \dim[l,j]), \\ &\mathbf{R}_{2s}[\mathbf{Z}_{2s}^{(k)}] = \{\mathbf{V}\}_{2s} && (1 \leqslant k \leqslant 1 + 2s). \end{aligned} \tag{14.5}$$

The arguments used will be quite general (e.g., the values of the dimensionalities are of no importance).

First of all choose the $\mathbf{U}_{2s}{}^{(k)}$ $(1 \leqslant k \leqslant 1 + 2s)$ so that the $2s + 1$ projection vectors of the set $\{\mathbf{V}\}_{2s}$ are (still) positively dependent (in $\mathfrak{S}^{2s}$) while the vectors $\{\mathbf{W}\}_{2s}$ are independent (in the larger space $\mathfrak{S}^{Q}$). This can be done by the approximation technique of §13 (above), since the proper choice of the $\mathbf{U}_{2s}{}^{(k)}$ for each k will render each vector of $\{\mathbf{v}\}_{2s}$ arbitrarily close in direction to the corresponding vector in $\{\mathbf{V}\}_{2s}$ while some one $[l, j]$ projection of one vector of $\{\mathbf{W}\}_{2s}$ can be made much larger than this projection of all the other vectors of $\{\mathbf{W}\}_{2s}$. By this double condition on the $\mathbf{U}_{2s}{}^{(k)}$, $(1 \leqslant k \leqslant 1 + 2s)$, we preserve the positive dependence of the set $\{\mathbf{V}\}_{2s}$ in $\mathfrak{S}^{2s}$ without having the positive dependence relation remain valid for the set $\{\mathbf{W}\}_{2s}$ in $\mathfrak{S}^{Q}$. Once these $\mathbf{U}_{2s}{}^{(k)}$ are chosen we keep them fixed for the remainder of the proof.

Next we assign a positive angle ϵ. Then for this ϵ we can choose units $\mathbf{U}_{l,j}{}^{(h)}$, $(1 \leqslant h \leqslant 1 + \dim[l, j])$, such that $\{\mathbf{V}\}_{l,j}$ are still positively dependent (for each $[l, j]$) in the smaller space $\mathfrak{S}^{\dim[l,j]}$ while $\{\mathbf{W}\}_{l,j}$ are linearly independent in the larger space $\mathfrak{S}^{Q}$. *At the same time*, each vector of the set $\{\mathbf{W}\}_{l,j}$ is to make an angle $< \epsilon$ with the corresponding vector of the set $\{\mathbf{V}\}_{l,j}$. This can be done, as in the preceding paragraph by the approximation technique of §13 (above).

We now show that for ϵ small enough the *projection* property is valid, or that any arbitrary (say) *unit* vector $\mathbf{T}$ of $\mathfrak{S}^{Q}$ has a positive projection on one or more vectors of the total set $\{\mathbf{W}\}$. For if $\mathbf{T}$ lies wholly in the $\mathfrak{S}^{2s}$ projection, the positive dependence of $\{\mathbf{V}\}_{2s}$ is sufficient. On the other hand if $\mathbf{T}$ has a non-zero projection in some other space $\mathfrak{S}^{\dim[l,j]}$ then for ϵ small enough some element of $\{\mathbf{W}\}_{l,j}$ (being sufficiently close in direction to an element of $\{\mathbf{V}\}_{l,j}$), must have a positive projection on $\mathbf{T}$. By compactness, a single ϵ should achieve this uniformly for all directions of $\mathbf{T}$.

We next show that for ϵ small enough, the *independence* property is valid, or any Q vectors of the set $\{\mathbf{W}\}$ are linearly independent. Consider first the projection vectors $\{\mathbf{V}\}$. Clearly any linear relationship among vectors in $\{\mathbf{V}\}$ must be decomposable into the sum of linear relationships among vectors of the individual sets $\{\mathbf{V}\}_{l,j}$ and $\{\mathbf{V}\}_{2s}$ (lying wholly in the corresponding projections $\mathfrak{S}^{\dim[l,j]}$ and $\mathfrak{S}^{2s}$). Now by continuity this will be true for vectors sufficiently close in direction to the vectors of $\{\mathbf{V}\}$. The $\{\mathbf{W}\}_{l,j}$ immediately meet this condition when ϵ is small enough (by our choice of the units $\mathbf{U}$). The $\{\mathbf{W}\}_{2s}$ will also meet this condition if at the same time that we make ϵ small we stretch each of the $2s$ coordinates in $\mathfrak{S}^{2s}$ to infinity sufficiently *slowly* so as not to ruin the approximation of $\{\mathbf{W}\}_{l,j}$ to $\{\mathbf{V}\}_{l,j}$. This will accentuate the $\mathfrak{S}^{2s}$ projection of the *fixed* vectors $\{\mathbf{W}\}_{2s}$ and (effectively) permit them to approximate $\{\mathbf{V}\}_{2s}$.

Thus any linear relationship among vectors of the set $\{\mathbf{W}\}$ will imply such relationships among vectors in the individual sets $\{\mathbf{W}\}_{2s}$ or $\{\mathbf{W}\}_{l,j}$ which, as we saw earlier, are trivial, by choice of $\{\mathbf{U}\}$, for ϵ small enough. Q.E.D.

Now the existence of $Q+1$ positively dependent vectors, chosen from the $\sum(1+\dim[l,j])+(2s+1)$ vectors $\{\mathbf{W}\}$, is assured by a general convexity argument **(12**, p. 265**)**, but in practice the difficulties in exhibiting these $Q+1$ vectors are, as in the real case, almost prohibitive. (Regrettably, our earlier bibliography failed to list the work of Carathéodory **(10)** and Steinitz **(15)** who seem to have used similar convexity arguments, in a different context. The method of approximating projections, so natural with Dirichlet's theory of units **(5)**, seems to have not been used previously.)

15. Quadratic and cubic modules. The question of stability in a totally real module has already been answered in Part I **(12**, p. 269**)**. For complex modules the answer becomes extremely involved as the degree n increases. We carry the investigation only as far as $n=3$.

Starting with *quadratic* (complex) modules, we find that stability requires first of all that the norm assume its minimum at three $(=Q+1)$ values (and their negatives), lying on a circle with center at the origin. This shows the lattice to be equivalent under rotation to the equilateral lattice. Thus the *only stable quadratic (complex) modules are given by the module* $\rho\mathfrak{O}$, *where* ρ *is a fixed integer and* $\mathfrak{O}$ *is the set of all integers, in* $R(\exp 2\pi i/3)$.

In the case of cubic modules with one real and two complex conjugates $(n=3, r=1, s=1)$, *we find*, as indicated earlier without proof **(12** p. 269**)**, *that all such modules have stable norms*. To see this we start with the observation that the order $\mathfrak{O}$ of $\mathfrak{M}$ has one fundamental unit $\mathbf{w}=(w_1, w_2, w_3)$. Now w_2 is not real nor is any power of w_2 real, since the only real numbers in a complex cubic field are rational. This shows that the argument of w_2 is incommensurable with 2π, and therefore the directions of the complex vectors w_2^m, $(m=0, \pm1, \pm2, \ldots)$ are everywhere dense mod 2π. Thus for every $\mathbf{z}_0$ of minimal norm, the set $\mathbf{z}=\mathbf{z}_0\mathbf{w}^n$ has the same norm while the projections $\mathbf{R}_{1,2}[\mathbf{z}]$, $\mathbf{R}_{2,1}[\mathbf{z}]$, $\mathbf{R}_{2s}[\mathbf{z}]$, each in two-dimensional space, are everywhere dense with respect to direction, thus establishing the positive span and stability. (For an illustrative stability configuration see **(7)**.)

When $n>3$ the criteria are dominated by the occurrence of units and combinations of units whose arguments are commensurable with 2π. Here, the subject of the geometry of numbers must await more results in algebra. We shall, however, give such a case as the final illustration.

16. Cyclotomic field. We conclude by proving the *stability of the integer module in* $K^N=R(\exp 2\pi i/N)$ *if and only if* N *is square-free*. Here we note that the arguments of all units u are commensurable with 2π **(14**, p. 334**)**. In fact, denoting the conjugate-complex of u by $\tilde{u}$, we find $u/\tilde{u}$ is always a root of unity

lying in K^N hence a positive or negative power of $(\zeta =) \exp 2\pi i/N$. In this section $\phi(N) = n$, the degree of K^N over R.

First we dispose of the case where N has a square factor, say p^2, for p a prime. Consider any $n + 1$ $(= 2s + 1)$ projection vectors $\mathbf{R}_{2s}[\mathbf{u}]$ for $n + 1$ units $\mathbf{u}$; we shall show that such a set of vectors can never be positively dependent. For the s complex coordinates of $\mathbf{R}_{2s}[\mathbf{u}]$ (see equation (13.34)) are the conjugates of some positive or negative power of ζ. Thus if we write out any $n + 1$ powers of ζ we find that some $(n/p) + 1$ of them belong to the same residue class module p and are therefore linearly dependent (with rational coefficients), by virtue of the fact that the cyclotomic equation of degree n, defining ζ, is really an equation of degree n/p in ζ^p. Hence, by conjugates, a linear (rational) dependence exists among a proper subset of any $n + 1$ vectors $\mathbf{R}_{2s}[\mathbf{u}]$, excluding positive dependence.

From now on, we assume N is square-free, hence necessarily odd (and greater than 3 for convenience). We build the positive dependence from the relation

$$\sum_{k=1}^{n} \zeta^{a_k} - \mu(N) = 0 \tag{16.1}$$

where the a_k are the $n(=\phi(N))$ residue classes relatively prime to N, and $\mu(N)$ is the Moebius inversion function. We then take the $2s + 1$ units (of which one conjugate is indicated):

$$\begin{aligned} u_1^{(k)} &= \zeta^{\frac{1}{2}a_k(N+1)} && (k = 1, 2, \ldots, n), \\ u_1^{(n+1)} &= 1 && \text{if } \mu(N) = -1, \\ &= (1 - \zeta)^N && \text{if } \mu(N) = +1, \end{aligned} \tag{16.2}$$

(since $1 - \zeta$ is a unit now if and only if N is no prime power). We further see that

$$\begin{aligned} u_1^{(k)}/\tilde{u}_1^{(k)} &= \zeta^{a_k} && (k = 1, 2, \ldots, n), \\ u_1^{(n+1)}/\tilde{u}_1^{(n+1)} &= -\mu(N), \end{aligned} \tag{16.3}$$

and hence from (16.1)

$$\sum_{k=1}^{n+1} \mathbf{R}_{2s}[\mathbf{u}^{(k)}] = 0. \tag{16.4}$$

Now equation (16.4) asserts positive span in the "$2s$" projection once we know that *all* linear relations among $\mathbf{R}_{2s}[\mathbf{u}^{(k)}]$ are proportional to the relation (16.4). Otherwise expressed, we assert there is only a trivial relationship among the $\mathbf{R}_{2s}[\mathbf{u}^{(k)}]$ if k takes the values $1 \leqslant k \leqslant n$. Assume, to the contrary, that the system

$$\sum_{k=1}^{n} A_k \zeta^{a_k a_j} = 0 \qquad 1 \leqslant k, \quad j \leqslant n, \tag{16.5}$$

has a real non-trivial solution in A_k. Then a relation must exist where the A_k belong to K^N and (say) $A_1 = 1$. By applying the Galois group operations to (16.5) we derive a system in which the A_k are rational and not all zero. Thus

https://doi.org/10.4153/CJM-1954-027-6 Published online by Cambridge University Press

the relationship (16.5) contradicts the fact that ζ and its conjugates ζ^{a_k} ($k = 1, 2, \ldots, n$) provide a (normal) basis of K^N. (This last result is best known **(14**, p. 351**)** when N is prime; when N is composite but square-free, the direct-product field decomposition extends the result).

Having disposed of the "$2s$" projection, we must show that the $[l, j]$ projections, (see equation (13.32) above), are positively spanned. As in the beginning of §11 (above), we can reduce the problem to the following:

Let S be any non-identical automorphism of K^N over the rationals, distinct from $i \to -i$, then five units $u^{(h)}$ ($1 \leqslant h \leqslant 5$) can be found for which the five vectors $\mathbf{R}_S{}^{(h)} = (u^{(h)}/u^{(h)S}, \tilde{u}^{(h)}/u^{(h)S})$ are positively dependent. Here S is given by the transformation:

$$S: \zeta \to \zeta^g \qquad (g, N) = 1,\ g \not\equiv \pm 1 \pmod{N}. \tag{16.6}$$

Then we can take as the five units $u^{(h)} = \zeta, \zeta^{-1}, \zeta^a, \zeta^{-a}, 1$ respectively, where a is chosen as a function of g in such a manner that $\mathbf{R}_S{}^{(h)}$ are positively dependent. The specific details are tedious and are omitted as they have no bearing on the square-free nature of N but rather depend on the "small gap" type of argument used to determine M_1 in §11.

References

10. C. Carathéodory, *Über den Variabilitätsbereich der Fourier'schen Konstanten*, Rend. Circ. Math. Palermo, *32* (1911), 216.

11. H. Cohn, *Note on fields of small discriminant*, Proc. Amer. Math. Soc., *3* (1952), 713–714.

12. ———, *Stable lattices*, Can. J. Math., *5* (1953), 261–270.

13. H. Hasse, *Über die Klassenzahl abelscher Zahlkörper* (Berlin, 1952), 26–30.

14. D. Hilbert, *Theorie der algebraischen Zahlkörper*, Jahresbericht der deutschen Mathematiker-Vereinigung, *4* (1894), 177–546.

15. E. Steinitz, *Bedingt konvergente Reihen und konvexe Systeme*, J. reine angew. Math., *144* (1914), 15.

Wayne University