STABLE LATTICES

HARVEY COHN

1. Introduction. The consideration of *relative extrema* to correspond to the *absolute extremum* which is the critical lattice has been going on for some time. As far back as 1873, Korkine and Zolotareff [**6**] worked with the ellipsoid in hyperspace (i.e., with quadratic forms), and later Minkowski [**8**] worked with a general convex body in two or three dimensions. They showed how to find critical lattices by selection from among a finite number of relative extrema. They were aided by the long-recognized premise that only a finite number of lattice points can enter into consideration [**1**] when one deals with lattices "admissible to convex bodies."

In the realm of the more general star body, such as that involved in the product of homogeneous forms, there is no finiteness principle of equal scope. Mahler [**7**] has, however, developed a local property for the critical lattices established by Davenport [**3**; **4**], by using "bounded reducibility."

We shall develop a similar property which we shall call *stability* and we shall extend it to a large class of lattices for star bodies. We shall do this by introducing a formalism of *positively dependent differentials*. Then as an illustration, we shall give a condition for stability of the norm in an algebraic module (a condition which can be considerably simplified by the use of units in the Dedekind order [**5**]).

2. Critical lattices. A lattice $\mathfrak{L}$, in n-space, is determined by a $n \times n$ matrix (a_{ij}) of (say) positive determinant $||a_{ij}||$, the points of the lattice being denoted by the vectors $\mathbf{x}$ with components

$$x_i = \sum_{j=1}^{n} a_{ij} m_j \qquad (i = 1, 2, \ldots, n) \tag{2.1}$$

corresponding to the integral n-tuple $(m_j) = (m_1, \ldots, m_n)$. A real continuously differentiable function, $\phi(\mathbf{x})$, homogeneous of positive degree h in its variables, is defined in the space. The locus $|\phi| = 1$ is the boundary of the star body under consideration. Then we consider the function defined by

$$F(m_j, \mathfrak{L}) = \phi(\mathbf{x})/||a_{ij}||^{h/n}. \tag{2.2}$$

For each lattice $\mathfrak{L}$, an infimum of $|F|$ is defined over (m_j), excluding the origin of course. Call it $M(\mathfrak{L})$. Let the values $M(\mathfrak{L})$ have a finite supremum M_0. Now if a lattice $\mathfrak{L}_0$ exists for which $M(\mathfrak{L}_0) = M_0$, then $\mathfrak{L}_0$ is called a *critical* lattice. Thus

$$M(\mathfrak{L}) = \inf |F(m_j, \mathfrak{L})| \qquad (m_j) \neq 0 \tag{2.3}$$

Received December 17, 1951 and in revised form Febraury 15, 1952. Presented to the American Mathematical Society February 24, 1951. Research currently sponsored by the U.S. Army Office of Ordnance Reseach.

and

$$M_0 = M(\mathfrak{L}_0) = \sup_{\mathfrak{L}} M(\mathfrak{L}). \tag{2.4}$$

The *stable* lattices $\mathfrak{L}^*$ will be presently defined using the geometrically simplest (rather than the most general) type of relative maximum to replace the (absolute) maximum required in the last formula.

3. Dimension of differentials. First of all let us consider the function F defined in formula (2.2). If it refers to the n-tuple $(m_j^{(k)})$ of a finite or infinite set indexed by k then it will be called $F^{(k)}$ $(= F(m_j^{(k)}, \mathfrak{L}))$ for short. Now we regard the a_{ij} as the variables, leading to differentials da_{ij} around a fixed lattice (a_{ij}); the (m_j) or $(m_j^{(k)})$ remaining fixed in this process. Thus a total differential $d|F|$ or $d|F^{(k)}|$ is defined. (Since we are excluding lattices where $M(\mathfrak{L}) = 0$, the presence of the absolute value sign creates no difficulties.)

We now define dimension: The set (finite or infinite) of differentials $d|F^{(k)}|$ is of *dimension* q if a certain subset of q differentials are linearly independent and provide a basis for all differentials. In particular, the set of $q + 1$ differentials $d|F^{(k)}|$ $(k = 1, 2, \ldots, q + 1)$ is of dimension q if and only if the values of $A^{(k)}$ for which

$$\sum_1^{q+1} A^{(k)}\, d|F^{(k)}| = 0 \tag{3.1}$$

are a set of dimension one (i.e., proportional to the components of a single non-zero vector $\mathbf{A}_0$).

We next consider the actual calculation of dimension. We write the sum

$$\sum_{(k)} A^{(k)}\, d|F^{(k)}| = 0 \tag{3.11}$$

over some finite set of indices. Clearly the $A^{(k)}$ must be independent of the coordinates describing the $F^{(k)}$, but in terms of the a_{ij}, for instance,

$$\sum_{(k)} A^{(k)} \frac{\partial |F^{(k)}|}{\partial a_{ij}} = 0, \qquad 1 \leqslant i, j \leqslant n, \tag{3.2}$$

where the partial derivatives, as agreed earlier, are evaluated at some fixed lattice (a_{ij}). But $F^{(k)} = \phi(\mathbf{x}^{(k)})/\Delta^{h/n}$ where the $x_i^{(k)}$ were given in formula (2.1) (with $m_i = m_i^{(k)}$) and $\Delta = ||a_{ij}||$, assumed positive for convenience. Now

$$\frac{\partial |F^{(k)}|}{\partial a_{ij}} = \Delta^{-h/n} \frac{\partial |\phi^{(k)}|}{\partial x_j^{(k)}} m_i^{(k)} - \frac{h}{n} \Delta^{-(h/n)-1} |\phi^{(k)}|\, a^{ij}, \tag{3.3}$$

where a^{ij} means the cofactor of a_{ij} in the matrix (a_{ij}) and $\phi^{(k)}$ means $\phi(\mathbf{x}^{(k)})$. Thus we can take system (3.2), multiply by a_{il}, and sum over i, obtaining on substitution of the result in (3.3),

$$\begin{gathered} \sum_{(k)} A^{(k)} R_{jl}^{(k)} = 0, \\ R_{jl}^{(k)} = \frac{\partial |\phi^{(k)}|}{\partial x_j^{(k)}} x_l^{(k)} - \frac{h}{n} |\phi^{(k)}| \delta_{jl}, \end{gathered} \qquad 1 \leqslant j, l \leqslant n, \tag{3.4}$$

https://doi.org/10.4153/CJM-1953-029-5 Published online by Cambridge University Press

where δ_{jl} is the Kronecker delta. Since $\Delta \neq 0$, system (3.4) must be equivalent to system (3.2). Note, however, that system (3.4) does not contain a_{ij} or $m_i^{(k)}$ explicitly, and indeed the dimension can be determined as the rank of the $n^2 \times \Omega$ matrix of $R_{jl}^{(k)}$ where j, l takes on n^2 indices and k takes on Ω indices, finite or infinite.

Since, conversely, the system (3.4) leads to the system (3.11), the differentials depend essentially only on the lattice points $\mathbf{x}^{(k)}$.

4. Free dimension. Now if our set of $(m_j^{(k)})$ took on all *integral* n-tuples (except the origin), a dimension would be defined for these $d|F^{(k)}|$. Its value will be called *the free dimension of the fixed lattice* (a_{ij}) *with respect to the function* $\phi(\mathbf{x})$. We shall now see that the free dimension depends only on ϕ and not on the a_{ij}.

First of all the definition of free dimension would not change if the $(m_j^{(k)})$ took on all *real* values (except the origin). To see this, we must ask if the rank of the system $R_{jl}^{(k)}$ becomes any *greater* if the $(m_j^{(k)})$ are real instead of integral. Suppose a certain $q \times q$ minor of $R_{jl}^{(k)}$ is non-vanishing for a real set of $(m_j^{(k)})$. By homogeneity this depends on the $n - 1$ ratios of the n components of each $(x_i^{(k)})$ $(i = 1, 2, \ldots, n)$; but certainly any such ratios can be approximated arbitrarily closely by ratios from n components of integral lattice points. This is a simple consequence of the Dirichlet boxing-in principle. Hence this same $q \times q$ minor will be non-vanishing for an integral set of $(m_j^{(k)})$.

Thus in determining the *free dimension* from system (3.4) we may regard $R_{jl}^{(k)}$ as a function of the *free variables* $\mathbf{x}^{(k)}$ no longer subjected to membership in a lattice. The coefficients $A^{(k)}$, for instance, can be taken as polynomials in $x_i^{(k)}$ when ϕ is a rational function, by virtue of the fact that a polynomial in several variables vanishes for all values of the variables only when it vanishes identically. The free dimension will be denoted by Q.

Our only general information about ϕ is that it is homogeneous; hence in formula (2.2) one of the variables a_{ij} can be cancelled out, making F dependent on only $n^2 - 1$ of them. In a corresponding way, from formula (3.4),

$$\sum_{jl} R_{jl}^{(k)} \delta_{jl} = 0$$

by Euler's theorem on homogeneous functions. Hence, clearly, $Q \leqslant n^2 - 1$.

From the theory of implicit functions it follows that the free dimension is the minimum number of variables, on which the various $F^{(k)}$ really depend as the a_{ij} vary, the $(m_j^{(k)})$ remaining fixed. (See equation (3.2).)

5. Stable lattices. We first define a set of vectors $\{\mathbf{g}^{(k)}\}$ $(k = 1, 2, \ldots, Q + 1)$ to be *positively dependent* if all the linear relations

$$\sum_{(k)} A^{(k)} \mathbf{g}^{(k)} = 0 \tag{5.1}$$

are such that, $A^{(k)} = \sigma A_0^{(k)}$, where $A_0^{(k)}$ is a set of $Q + 1$ positive numbers and σ is scalar. This definition is affine-invariant and it can be realized only if

https://doi.org/10.4153/CJM-1953-029-5 Published online by Cambridge University Press

the set of vectors has dimension Q. An equivalent definition is that an arbitrary vector in $\mathfrak{S}^Q$, the Q-dimensional space determined by the $\{\mathbf{g}^{(k)}\}$, will have a positive projection (in the sense of any ordinary scalar product) on at least one $\mathbf{g}^{(k)}$.

We now come to the major definition. Assume the function ϕ to have the free dimension Q. A lattice $\mathfrak{L}^* = (a^*_{ij})$ is called *stable with respect to* ϕ if $Q+1$ n-tuples $(m_i^{(k)})$ exist such that

$$|F(m_j^{(k)}, \mathfrak{L}^*)| = M(\mathfrak{L}^*) > 0 \qquad (k = 1, 2, \ldots, Q+1) \tag{5.2}$$

and

$$\text{the } d|F^{(k)}| \text{ are positively dependent at } \mathfrak{L}^*. \tag{5.3}$$

We next develop the most important property of the stable lattice. For the free dimension Q, we can, by the implicit function theorem select $n^2 = Q + t$ variables

$$b_1, \ldots, b_Q, c_1, \ldots, c_t$$

functionally equivalent to the a_{ij} and such that the $|F^{(k)}|$ actually depend (locally) on the b_i only, (i.e., $\partial|F^{(k)}|/\partial c_j \equiv 0$), for all non-zero n-tuples $(m_i^{(k)})$, integral or even real (see §4). Having found such variables, we describe the $F^{(k)}$ locally in terms of just the b_i, in the neighborhood of b^*_i, c^*_j (the variables corresponding to a^*_{ij}). We define

$$|\mathfrak{L} - \mathfrak{L}^*| = \left(\sum_{i=1}^{Q} (b_i - b^*_i)^2\right)^{\frac{1}{2}} \tag{5.4}$$

as the *distance between lattices* (corresponding to the local coordinate system). Then if a lattice $\mathfrak{L}^* = (a^*_{ij})$ is stable with respect to the function ϕ of free dimension Q, then an $\epsilon > 0$ and an $\eta > 0$ exist together with $Q + 1$ n-tuples $(m_i^{(k)})$ $(k = 1, 2, \ldots, Q + 1)$ such that

$$|F(m_i^{(k)}, \mathfrak{L}^*)| = M(\mathfrak{L}^*) \tag{5.2}$$

and

$$|F(m_i^{(k)}, \mathfrak{L})| \leqslant |F(m_i^{(k)}, \mathfrak{L}^*)| - \eta|\mathfrak{L} - \mathfrak{L}^*| \tag{5.31}$$

for some index k depending on $\mathfrak{L}$ providing only that $|\mathfrak{L} - \mathfrak{L}^*| < \epsilon$.

Conversely, if a lattice has these properties for some ϵ, η and $Q + 1$ n-tuples as described, then the lattice is stable.

This is the type of property that Mahler **[7]** established for certain cases where his theory of "bounded reducibility" applies. The property is an easy consequence of the definition of stability given above. As a simple corollary we note that when $\mathfrak{L}^*$ is stable, then for some positive ϵ, η, and all $|\mathfrak{L} - \mathfrak{L}^*| < \epsilon$, we have $M(\mathfrak{L}) \leqslant M(\mathfrak{L}^*) - \eta|\mathfrak{L} - \mathfrak{L}^*|$.

Thus, in a sense, $M(\mathfrak{L}^*)$ is a local maximum by virtue of the $Q + 1$ specific lattice points for which the value is assumed.

6. Positive span. Now there are often infinitely many vectors of a lattice satisfying condition (5.2) for stability. Hence it would seem precarious to expect to discover $Q + 1$ vectors satisfying the further condition (5.3). We shall simplify the criterion of stability by referring it to the aggregate of *all* vectors satisfying the condition (5.2).

Let the finite or infinite set of vectors $\{\mathbf{w}\}$ determine a space $\mathfrak{S}^Q$ of Q dimensions, in which unit basis vectors and any ordinary scalar product are introduced. Then the set $\{\mathbf{w}\}$ is said to *positively span* this space if it has both the (*projection*) property that every arbitrary vector of $\mathfrak{S}^Q$ has a positive projection on at least one vector of $\{\mathbf{w}\}$ and the (*independence*) property that every Q vectors of $\{\mathbf{w}\}$ are linearly independent. (The properties are easily seen to be affine-invariant.)

Now every set of $Q + 1$ positively dependent vectors will positively span its space $\mathfrak{S}^Q$. (See §5.) Conversely, *every set of vectors* $\{\mathbf{w}\}$ *that positively spans the space* $\mathfrak{S}^Q$ *contains* $Q + 1$ *vectors which are positively dependent.* To see this, note that the set $\{\mathbf{w}\}$ determines a set of end-points of the various vectors, whose convex closure, a polytope $\mathfrak{P}$ in $\mathfrak{S}^Q$, contains the origin by the projection property. (The set $\{\mathbf{w}\}$ may be considered as a finite set by the compactness of the hypersphere in $\mathfrak{S}^Q$.) But the polytope $\mathfrak{P}$ can then be reduced to a single simplex of $Q + 1$ vertices which contains the origin, if we merely triangulate $\mathfrak{P}$, introducing no new vertices and recalling that the triangulating hyperplanes will not contain the origin (by the independence property). These $Q + 1$ vertices of course determine the positively dependent vectors.

The applications that follow (see §9) will stem from the following result: Let the (infinite) set of vectors $\{\mathbf{v}\}$ of $\mathfrak{S}^Q$ contain vectors arbitrarily close in direction to $2Q$ vectors consisting of Q basis vectors and their negatives. We shall call this latter configuration a *unit star*. (Compare the "eutactic star" of Coxeter [**2**, p. 401].) Suppose that a subsequence of $\{\mathbf{v}\}$ can be selected which comes increasingly close in direction to any designated one of the $2Q$ vectors of the unit star, without coinciding in direction. Let us further suppose that the last property still holds if we exclude from consideration all vectors of $\{\mathbf{v}\}$ that lie in an arbitrary set of fixed hyperplanes (through the origin). Then *the set* $\{\mathbf{v}\}$ *has a subset that positively spans* $\mathfrak{S}^Q$ *and hence a further subset of* $Q + 1$ *positively dependent vectors.*

To see this, first note that the *projection* property is easy to obtain from the unit star. To establish the *independence* property we select as our subset of $\{\mathbf{v}\}$ the sequence of vectors chosen by the following inductive procedure: The vectors are to come increasingly close to the $2Q$ vectors of the unit star in some order (without coinciding). Furthermore each vector is selected to be linearly independent of the set consisting of earlier chosen vectors (if any) together with the $2Q$ vectors of the unit star. This process will at every step leave cones about the vectors of the unit star inside one of which the next vector of the sequence may be chosen.

7. Stability of the norm in a module. Probably the most investigated non-convex star body is that given by $\phi(\mathbf{x}) = x_1 x_2 \ldots x_n$ and the most important lattices for it are those for which each row of the matrix in (2.1) namely

$a_{i1}, a_{i2} \ldots, a_{in}$, is the i conjugate of a set of n basis numbers of a (non-singular) module $\mathfrak{M}$ in a totally real field of degree n. The x_i is the i conjugate of a general number $\mathbf{x}$ in the module and ϕ is the norm. The minimum absolute value of ϕ (when $(x_i) \neq (0)$), is of course actually achieved for some $\mathbf{x}$ and is denoted by $M'(\mathfrak{M}) > 0$.

Now for this ϕ, from (3.4), $R_{j,l}^{(k)} = |\phi^{(k)}| x_l^{(k)}/x_j^{(k)}$ when $j \neq l$, and 0 when $j = l$. Thus Q, the free dimension, is $n(n-1)$ according to either of two reasons given in §4. *The condition for stability of the norm is simply that some set of vectors* $\mathbf{x}^{(k)}$ *of the module* $\mathfrak{M}$ *is such that*

$$\text{norm } \mathbf{x}^{(k)} = \pm M'(\mathfrak{M}) \tag{7.1}$$

and the set of vectors indexed by k and with $n(n-1)$ *components*

$$(\ldots, x_l^{(k)}/x_j^{(k)}, \ldots) \qquad (l, j = 1, 2, \ldots, n; l \neq j), \tag{7.2}$$

positively spans a space of $n(n-1)$ *dimensions.*

If the field has r real conjugates and $2s$ complex conjugates $(r + 2s = n)$, then we proceed similarly, writing

$$\begin{aligned} z_j &= x_j & (j = 1, 2, \ldots, r), \\ z_j &= x_j + ix_{j+s} & (j = r+1, \ldots, r+s), \\ z_{j+s} &= x_j - ix_{j+s}, \end{aligned} \tag{7.3}$$

where z_i represents the n conjugates of a number $\mathbf{z}$ in the field. Then the norm is

$$\phi^*(\mathbf{x}) = x_1 \ldots x_r(x_{r+1}^2 + x_{r+s}^2) \ldots (x_{r+s+1}^2 + x_{r+2s}^2)$$

and the lattice (or module $\mathfrak{M}$) is this time determined by the n^2 different real and imaginary components of the matrix a_{ij}. Then a repetition of the earlier calculation yields the same Q and the convenient new *condition for stability of the norm as simply that some set of vectors* $\mathbf{z}^{(k)}$ *of the module* $\mathfrak{M}$ *is such that*

$$\text{norm } \mathbf{z}^{(k)} = \pm M'(\mathfrak{M}), \tag{7.11}$$

and the set of vectors, indexed by k and given by the following $2n(n-1)$ *components:*

$$(\ldots, \Re\, z_l^{(k)}/z_j^{(k)}, \Im\, z_l^{(k)}/z_j^{(k)}, \ldots) \qquad (l, j = 1, 2, \ldots, n; l \neq j), \tag{7.21}$$

positively spans a space of $n(n-1)$ *dimensions.*

Of these $2n(n-1)$ components, some may vanish and others may be repeated with or without change of sign. Taking this into account we find the total, in general, is still $Q = n(n-1)$ essentially distinct non-vanishing components.

8. Quadratic forms. A simple illustration of stable lattices can be given for the indefinite form $\phi = x_1 x_2$ of free dimension $Q = 2$. (Compare §7.) Expanding $\phi = \Phi(m_1, m_2)$, in the notation of (2.1) and (2.2) we obtain:

$$\begin{aligned} F &= \Phi(m_1, m_2)/d^{\frac{1}{2}}, \\ \Phi(m_1, m_2) &= am_1^{\,2} + bm_1 m_2 + cm_2^{\,2}, \qquad d = b^2 - 4ac > 0. \end{aligned} \tag{8.1}$$

The lattice basis is involved by means of the relations

$$\begin{aligned} a_{11}a_{21} &= a, \quad a_{12}a_{22} = c, \\ a_{11}a_{22} + a_{12}a_{11} &= b, \qquad d = \Delta^2. \end{aligned} \tag{8.2}$$

Following §7, we would restrict ourselves to the case where Φ is proportional to the norm function in a quadratic module, or a, b, c are rational and d is not a perfect square. (Actually this would follow automatically from the stability conditions (5.2) and (5.3).) At any rate we assume Φ to be stable and let $Q + 1 = 3$ integer couples $(m_1^{(k)}, m_2^{(k)})$ $(k = 1, 2, 3)$ occur for which $|F|$ assumes its minimum value M, that is,

$$F^{(k)} = \epsilon^{(k)}M \neq 0, \qquad (\epsilon^{(k)} = \pm 1). \tag{8.3}$$

Then we consider the vector space spanned by the vectors of two components

$$R_{jl}^{(k)} = |\phi^{(k)}|x_l^{(k)}/x_j^{(k)} \qquad (j, l) = (1, 2), (2, 1). \tag{8.4}$$

In particular we look for relations of the type

$$\sum_{k=1}^{3} A^{(k)}R_{jl}^{(k)} = 0, \tag{8.5}$$

valid for both of the above choices of (j, l). But by virtue of relation (8.3), or $x_1^{(k)}x_2^{(k)} = d^{\frac{1}{2}}M\epsilon^{(k)}$, it follows that relations of the type (8.5) are the same as the following conditions for stability:

$$\sum_{k=1}^{3} A^{(k)}\mathbf{W}^{(k)} = 0, \tag{8.6}$$

where $\mathbf{W}^{(k)} = \epsilon^{(k)}((x_1^{(k)})^2, (x_2^{(k)})^2)$ is a vector of two components.

It is well known that the *critical* lattice for $\phi = x_1x_2$ belongs to the form

$$\Phi_o(m_1, m_2) = m_1^2 + m_1m_2 - m_2^2 = (m_1 - \theta_0 m_2)(m_1 - \theta'_0 m_2) \tag{8.7}$$

where $\theta_0, \theta'_0 = \frac{1}{2}(-1 \pm \sqrt{5})$, $d = 5$. For the corresponding lattice, $M(\mathfrak{L}_0) = 1/\sqrt{5}$, in the notation of (2.3). To verify that this $\mathfrak{L}_0$ is *stable* we make the choice, by trial and error: $(m_1^{(k)}, m_2^{(k)}) = (1, 0), (0, 1), (1, 1)$ for $k = 1, 2, 3$, respectively. Here

$$\epsilon^{(1)} = \epsilon^{(3)} = -\epsilon^{(2)} = 1; \quad x_1^{(k)} = m_1^{(k)} - \theta_0 m_2^{(k)}, \quad x_2^{(k)} = m_1^{(k)} - \theta'_0 m_2^{(k)}.$$

It is now easy to verify that from the equations in (8.6), $(A^{(1)}, A^{(2)}, A^{(3)}) = \sigma(1, 3, 1)$, for a scalar σ, whence the three $\mathbf{W}^{(k)}$ (or ultimately $d|F^{(k)}|$) are *positively dependent*. This establishes stability. From the results of §9, it will turn out that the presence of both positive and negative $\epsilon^{(k)}$ is actually necessary and sufficient. The result can be expressed as follows:

Let m be the smallest positive number which an indefinite irreducible quadratic form with integral coefficients represents in absolute value. Then the corresponding lattice is stable if and only if the form represents both $+m$ and $-m$.

In showing the lattice $\mathfrak{L}_0$ (of (8.7)) to be stable with respect to $\phi = x_1 x_2$, we showed according to §5 that a neighbourhood of $\mathfrak{L}_0$ in lattice space exists in which $M(\mathfrak{L}) \leqslant 1/\sqrt{5}$. If we ask about the size of this neighbourhood we find that, fortunately, it includes *all* lattices, provided we take into account images of the neighbourhood under change of basis. In other words, *$\mathfrak{L}_0$ is the critical lattice.* To see this, we set

$$F = x_1 x_2/(\theta - \theta'), \qquad 1 > \theta > 0 > \theta', \tag{8.8}$$

where $x_1 = m_1 - \theta m_2$, $x_2 = m_1 - \theta' m_2$. Here θ and θ' represent the two degrees of freedom of the lattice. We now go back to the proof of stability of $\mathfrak{L}_0$, and we use the same $(m_1^{(k)}, m_2^{(k)})$ and the corresponding $(x_1^{(k)}, x_2^{(k)})$ for $k = 1, 2, 3$. Then clearly,

$$\begin{cases} |F^{(1)}| \leqslant 1/\sqrt{5}, & \theta - \theta' \geqslant \sqrt{5}, \\ |F^{(2)}| \leqslant 1/\sqrt{5}, & \theta - \theta' \geqslant -\sqrt{5}\,\theta\theta', \\ |F^{(3)}| \leqslant 1/\sqrt{5}, & \theta - \theta' \geqslant \sqrt{5}\,(1 - \theta)(1 - \theta'), \end{cases} \tag{8.9}$$

and by drawing the $\theta\theta'$ plane we see that at least one of the three right-hand inequalities will hold at every point of the region $0 < \theta < 1$, $\theta' < -1$ (a rather ample neighbourhood of the critical values θ_0, θ'_0). But every lattice is equivalent under change of basis to one lying in this neighbourhood, by an extension of Gauss's criterion for reduction, i.e., that one root and the negative reciprocal of its conjugate lie between 0 and 1. Thus the lattice $\mathfrak{L}_0$ is critical.

If we turn our attention to the definite form $\phi = x_1^2 + x_2^2$ we find that ϕ is stable only for the critical (equilateral) lattice, in which case ϕ is proportional under rotation, to the norm function of the integers in the field of the cube roots of unity. For the larger problem of $\phi = x_1^2 + \ldots + x_n^2$, analogous types of extrema have been developed [**6**; **9**; **2**] manifesting themselves largely in the *coefficients of the expanded form.* (The reader is referred to [**2**] for recent developments as well as a sizable bibliography.) The present paper, however, will conclude with a treatment of the norm function of §7 as a *factored form*; thus we shall finally arrive at a criterion of stability in terms of the *multiplicative arithmetic* of a field.

9. Application of units of the order. The module $\mathfrak{M}$ determines [**5**] another (non-singular) module $\mathfrak{O}$, called its *order*, which consists of all algebraic integers $\mathbf{v}$ (in the corresponding field) such that $\mathbf{v}\mathfrak{M}$ lies in $\mathfrak{M}$. For instance, if $\mathfrak{M}$ were the module of all integers in a field (called an *integer-module* for short), then we should have $\mathfrak{O} = \mathfrak{M}$ and the minimizing $\mathbf{x}$ (or $\mathbf{z}$) satisfying equations (7.1) (or (7.2)) would be the units. In any case, $\mathfrak{O}$ is also a ring with unity, and according to the classical theory it contains $r + s - 1$ fundamental units. We shall denote any unit by $\mathbf{u}$ (with conjugates u_i). Thus for every solution $\mathbf{x}$ (or $\mathbf{z}$) to (7.1) (or (7.11)) another one is of the type $\mathbf{xu}$ (or $\mathbf{zu}$). We shall now use these units to make the vectors $\mathbf{R}$ follow a *unit star*. (See §6.)

https://doi.org/10.4153/CJM-1953-029-5 Published online by Cambridge University Press

For instance we start by assuming $\mathfrak{M}$ to be totally real and we concentrate on the (j, l) component of $\mathbf{R}$, whose sign agrees with x_l/x_j. (See §7.) By using fundamental units, we can choose a variable unit $\mathbf{u}$ so that of the $n(n-1)$ components u_q/u_p $(p \neq q)$, the fixed component u_l/u_j is positive and of *greater order of magnitude* than any other. This guarantees the *projection property*, i.e., that for the new minimal vector $\mathbf{xu}$, the new vector $\mathbf{R}$ comes arbitrarily close in direction to

$$(0, \ldots, 0, \operatorname{sgn} x_l/x_j, 0, \ldots, 0),$$

the "sgn" being at the (j, l) component. We can go further. Along with the last condition on the variable $\mathbf{u}$, we can have each u_q/u_p approaching 0 or ∞ with a *different order of magnitude*. This will guarantee the *independence property*, i.e., the vectors $\mathbf{R}$ can not then all lie on a finite set of hyperplanes through the origin (as the components are now of different orders of magnitude). Thus the positive span is established provided the "sgn" can be made positive and negative.

The norm in a totally real module is therefore stable if and only if the numbers $\mathbf{x}$ *of minimal absolute norm* ($\neq 0$) *are such that, for any two different conjugate fields denoted by* l *and* j, *the ratio* x_l/x_j *is positive for some* $\mathbf{x}$ *and negative for others.*

As an immediate consequence of this criterion, the integer-module of a *real quadratic field* is stable if and only if there is a unit of norm -1. The integer-module of a *totally real cubic field* is stable if and only if the units display all possible 2^3 arrays of sign among their conjugates. For instance the totally real cubic field generated by $2 \cos 2\pi/7$ (of minimal discriminant $= 49$) easily has the property, as we see by using as units conjugates of this generating element. Hence the field in question is stable [**7**].

In the case of modules which are not totally real it is harder to find a criterion as elegant as the last one, because $|u_l/u_j| = |u_q/u_p|$ not only when j and l refer to the *same* fields (respectively) as do p and q, but also when they refer to *conjugate complex* fields. Thus it is not so easy to accentuate just one component of $\mathbf{R}$. But since we are interested in the real or imaginary components of u_l/u_j (see (7.21)), we can make use of the incommensurability of π with the arguments of certain complex units. Thus by a modification of the unit star method as just used for the totally real case, we can see that *all cubic fields that are not totally real* have integer-modules with stable norms. Mahler [**7**] gave an analogous result only for the cubic field of (minimal) discriminant 23, but it curiously enough requires no special properties of that field!

Concluding in a simpler vein, we can see that if an integer-module is not totally real, but nevertheless has as units only totally real numbers (or even pure imaginary numbers) then it can not be stable, as the number of distinct non-zero components in (7.21) will fall short of the desired total, $Q = n(n-1)$, by at least s. Thus, once more, the *complex quadratic fields* do not have stable integer-modules, except when the field is that of the cube roots of unity.

https://doi.org/10.4153/CJM-1953-029-5 Published online by Cambridge University Press

Many other fields have been tested for stability but we shall defer the details for a later occasion as the techniques involved are rather specialized for the present stage of development.

References

1. H. Cohn, *On the finite determination of critical lattices*, Proc. Amer. Math. Soc., *2* (1951), 547–549.
2. H. S. M. Coxeter, *Extreme forms*, Can. J. Math., *3* (1951), 391-441.
3. H. Davenport, *On the product of three homogeneous linear forms* II, Proc. London Math. Soc. (2), *44* (1938), 412–431.
4. ——— *On the product of three homogeneous linear forms* III, Proc. London Math. Soc., *45* (1939), 98–125.
5. P. G. Dirichlet, *Vorlesungen über Zahlentheorie* (Braunschweig, 1894), 505 ff.
6. A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann., *11* (1877), 242–292.
7. K. Mahler, *Lattice points in n-dimensional star bodies* II, Proc. Koninklijke Nederlandsche Akademie van Wetenschappen, *49* (1946), 524–532, 622–631.
8. H. Minkowski, *Diophantische Approximationen* (Berlin, 1907), 51–58.
9. G. Voronoï, *Recherches sur les paralléloèdres primitifs*, J. Reine Angew. Math., *134* (1908), 198–287.

Wayne University