The density of integer points on homogeneous varieties

by

WOLFGANG M. SCHMIDT(1)

University of Colorado
Boulder, CO, U.S.A.

A. The setting

1. Introduction

Let V be a homogeneous algebraic set in $\mathbf{C}^s$ defined over the rationals, i.e. a set

$$V = V(\underline{\mathfrak{F}}) = V(\mathfrak{F}_1, \ldots, \mathfrak{F}_r),$$

consisting of the common zeros of given forms $\mathfrak{F}_1, \ldots, \mathfrak{F}_r$ of positive degrees, in s variables, and with rational coefficients. We are interested in

$$z_P(V) = z_P(\underline{\mathfrak{F}}),$$

the number of integer points $\underline{x}=(x_1, \ldots, x_s)$ on V with

$$|\underline{x}| := \max(|x_1|, \ldots, |x_s|) \leqslant P.$$

Not much is known in general about the behaviour of $z_P(V)$ as a function of P. In those cases where we do have information and where $z_P(V) \to \infty$ (i.e. where V contains an integer point besides $\underline{0}$) we have

$$z_P(V) \sim \mu P^\beta,$$

where $\mu>0$, $\beta>0$ and β is an integer.

Birch [1] could show that a system $\underline{\mathfrak{F}}$ of r forms of odd degrees $\leqslant k$ in $s>c_1(k, r)$ variables possesses a nontrivial integer zero. In particular, $z_P(\underline{\mathfrak{F}}) \to \infty$. It would be easy

(1) Partially supported by NSF-MCS-8015356.

to deduce that $z_P(\underline{\mathfrak{F}})$ tends to infinity quite fast if s is rather larger than c_1. However, the elementary diagonalization method of Birch is "wasteful" in the number of variables, and does not seem to yield our first theorem, which will be proved by analytic methods:

THEOREM I. *Suppose that $\underline{\mathfrak{F}}$ consists of r forms of odd degrees $\leqslant k$ in $s>c_2(k,r)$ variables. Then*

$$z_P(\underline{\mathfrak{F}}) \gg P^{s-c_2},$$

with a constant in $\gg$ which may depend on $\underline{\mathfrak{F}}$.

Let

$$\underline{\mathfrak{F}} = (\underline{\mathfrak{F}}^{(k)}, \dots, \underline{\mathfrak{F}}^{(1)}) \tag{1.1}$$

be a system of forms, with the subsystem $\underline{\mathfrak{F}}^{(d)}$ $(1\leqslant d\leqslant k)$ consisting of $r_d\geqslant 0$ forms of degree d and with rational coefficients. The number of integer points with $|\underline{x}|\leqslant P$ is $\sim(2P)^s$. When we substitute such a point into a form of degree d, we will in general obtain a value of the order of magnitude of P^d, and hence the "probability" for the form to vanish should be about P^{-d}. Therefore the probability for $\underline{\mathfrak{F}}$ to vanish simultaneously should be about P^{-R}, where

$$R = \sum_{d=1}^{k} dr_d. \tag{1.2}$$

Hence when $s>R$, one might expect (somewhat optimistically) that $z_P(\underline{\mathfrak{F}})$ will have the order of magnitude of P^{s-R}.

More generally, let $\mathfrak{B}$ be a box with sides parallel to the cordinate axes, i.e. a set $\mathfrak{B}=I_1\times\dots\times I_s$, where each I_i is an interval (open, closed, or half open) of finite positive length. We write $z_P(\underline{\mathfrak{F}},\mathfrak{B})$ for the number of zeros of $\underline{\mathfrak{F}}$ in the blown up box $P\mathfrak{B}$. We will call $\underline{\mathfrak{F}}$ a Hardy-Littlewood system (or briefly HLS) if for every box $\mathfrak{B}$,

$$z_P(\underline{\mathfrak{F}},\mathfrak{B}) = \mu P^{s-R} + O(P^{s-R-\delta}), \tag{1.3}$$

where $\delta>0$ and where $\mu=\mu(\underline{\mathfrak{F}},\mathfrak{B})$ is defined by an infinite product which will be explained in §3. We further will call $\underline{\mathfrak{F}}$ a proper Hardy-Littlewood system (or briefly PHLS) if $\mu(\underline{\mathfrak{F}},\mathfrak{E})>0$, where $\mathfrak{E}$ is the cube

$$\mathfrak{E}: |\underline{x}| \leqslant 1. \tag{1.4}$$

This terminology was chosen since up to now the Hardy-Littlewood circle method has been the most successful in estimating z_P.

Let us recall some known cases. Waring's problem, i.e. that of representing an integer m as a sum of dth powers of nonnegative integers, does not quite fall into our framework, since the equation $x_1^d+\ldots+x_s^d=m$ is not homogeneous (but see §9), and since the variables are restricted a priori to the bounded domain $0\leqslant x_i\leqslant m^{1/d}$ $(i=1,\ldots,s)$. In Waring's problem one is interested in the numbers of solutions as a function of m.

(A) Davenport and Lewis [5] have shown that a single additive form

$$\mathfrak{F}=a_1X_1^d+\ldots+a_sX_s^d$$

where $d\geqslant 18$, $s>d^2$ and $a_1a_2\ldots a_s\neq 0$, and where either d is odd or where the coefficients are not all of the same sign, is a PHLS.

Now if $\mathfrak{F}$ is a form of degree $d>1$, write $h(\mathfrak{F})$ for the least number h such that $\mathfrak{F}$ "splits into h products", i.e.

$$\mathfrak{F}=\mathfrak{A}_1\mathfrak{B}_1+\ldots+\mathfrak{A}_h\mathfrak{B}_h \tag{1.5}$$

with forms $\mathfrak{A}_i,\mathfrak{B}_i$ of positive degrees and with rational coefficients. When $\underset{\sim}{\mathfrak{F}}=(\mathfrak{F}_1,\ldots,\mathfrak{F}_r)$ consists of forms of equal degree $d>1$, write

$$h(\underset{\sim}{\mathfrak{F}})=\min h(\mathfrak{F}), \tag{1.6}$$

with the minimum taken over forms $\mathfrak{F}$ of the rational pencil of $\underset{\sim}{\mathfrak{F}}$, i.e. $\mathfrak{F}=c_1\mathfrak{F}_1+\ldots+c_r\mathfrak{F}_r=\underset{\sim}{c}\underset{\sim}{\mathfrak{F}}$, where $\underset{\sim}{c}\neq\underset{\sim}{0}$ has rational components.

(B) Although Davenport [4] did not give such a formulation, he did prove that a single cubic form $\mathfrak{F}$ with $h(\mathfrak{F})\geqslant 16$ is a PHLS.

(C) A system of r quadratic forms with $h(\underset{\sim}{\mathfrak{F}})>2r^2+3r$ is a HLS, and it is even a PHLS if $h(\underset{\sim}{\mathfrak{F}})>4r^3+4r^2$ and if it possesses a real nonsingular zero (i.e. a zero with $\partial\mathfrak{F}_j/\partial x_i$ $(1\leqslant j\leqslant r,\ 1\leqslant i\leqslant s)$ of rank r) (Schmidt [9]). Again, a system of r cubic forms with $h(\underset{\sim}{\mathfrak{F}})>c_3r^4>0$ is a PHLS (Schmidt [12]).

(D) Let $V^*(\underset{\sim}{\mathfrak{F}})$ be the set of $\underset{\sim}{x}\in\mathbf{C}^s$ for which the matrix $\partial\mathfrak{F}_j/\partial x_i$ $(1\leqslant j\leqslant r,\ 1\leqslant i\leqslant s)$ has rank less than r. When $r=1$, then $V^*(\underset{\sim}{\mathfrak{F}})\subseteq V(\underset{\sim}{\mathfrak{F}})$ by Euler's identity, but this need not be the case when $r>1$. Birch [2] showed that a system $\underset{\sim}{\mathfrak{F}}$ of r forms with $\dim V=s-r$ and with

$$s>\dim V^*+(d-1)2^{d-1}r(r+1)$$

is a HLS. It is even a PHLS if it possesses a nonsingular zero in each local field. (The dimension of an algebraic manifold is the maximum dimension of its irreducible components.)

Another result on "general" systems is due to Tartakovsky [14].

On the other hand, there are many examples of systems which are not HLS or PHLS. First of all, there may not be any local zeros. Or take $\mathfrak{F}=\mathfrak{L}^d$ where $\mathfrak{L}$ is a linear form, so that $z_P(\mathfrak{F})=z_P(\mathfrak{L})\sim\mu P^{s-1}$, rather then $\sim\mu P^{s-d}$. The trouble here is that R was defined in terms of $\underline{\mathfrak{F}}$ and not of $V=V(\underline{\mathfrak{F}})$. Perhaps one should replace R by $\hat{R}=\hat{R}(V)=\min R(\underline{\mathfrak{F}})$, over all systems $\underline{\mathfrak{F}}$ with $V=V(\underline{\mathfrak{F}})$. Another example with too many zeros is when $\mathfrak{F}=\mathfrak{F}(X_1,X_2)$. Then $z_P(\mathfrak{F})>>P^{s-2}$, no matter what the degree of $\mathfrak{F}$. As a final example take

$$\mathfrak{F}=\mathfrak{G}_1^D+\ldots+\mathfrak{G}_h^D$$

where D is even and where $\underline{\mathfrak{G}}=(\mathfrak{G}_1,\ldots,\mathfrak{G}_h)$ is a PHLS of forms of degree d. Here $z_P(\mathfrak{F})=z_P(\underline{\mathfrak{G}})\sim\mu P^{s-dh}$, whereas $R(\mathfrak{F})=dD$ may be both larger or smaller than dh. The trouble here seems to be that $h(\mathfrak{F})$ is small, namely $h(\mathfrak{F})\leqslant h$.

Linear equations can always be got rid of by elimination, and they will not quite fit into our general scheme. Hence we will deal with systems

$$\underline{\mathfrak{F}}=(\underline{\mathfrak{F}}^{(k)},\ldots,\underline{\mathfrak{F}}^{(2)}), \tag{1.7}$$

where $\underline{\mathfrak{F}}^{(d)}$ $(2\leqslant d\leqslant k)$ consists of $r_d\geqslant 0$ forms of degree d. The total number of forms is

$$r=r_k+\ldots+r_2. \tag{1.8}$$

We put

$$h_d=\begin{cases} h(\underline{\mathfrak{F}}^{(d)}) & \text{if } r_d>0,\\ +\infty & \text{if } r_d=0. \end{cases} \tag{1.9}$$

THEOREM II. *There is a function $\chi(d)$ such that a system $\underline{\mathfrak{F}}$ as in* (1.7) *with*

$$h_d\geqslant\chi(d)\,r_d\,kR \quad (2\leqslant d\leqslant k) \tag{1.10}$$

is a HLS. *For instance one may take $\chi(2)=2$, $\chi(3)=32$, $\chi(4)=1\,152$, and in general*

$$\chi(d)<2^{4d}\cdot d!.$$

Write $v(\underline{r})=v(r_k,\ldots,r_1)$ [or $v(r_k,\ldots,r_2,0)$] for the least number such that a system (1.1) [or a system (1.7)] in more than $v(\underline{r})$ variables has a nontrivial p-adic zero for each prime p. To obtain a PHLS we need the following

SUPPLEMENT. $\underline{\mathfrak{F}}$ *as in* (1.7) *is a* PHLS *provided, firstly,*

$$h_d \geqslant \chi(d)\, r_d\, kv(\underline{r}) \quad (2 \leqslant d \leqslant k), \tag{1.11}$$

and secondly,

$$\dim V_{\mathbf{R}} \geqslant s-r,$$

where $V_{\mathbf{R}}$ *is the manifold of real zeros of* $\underline{\mathfrak{F}}$. *This second condition is always satisfied if all the forms of* $\underline{\mathfrak{F}}$ *are of odd degree, i.e. if* $r_d=0$ *for d even.*

To prove Theorem II and its supplement we will need exponential sums. The following theorem is typical of the estimates which we will obtain.

THEOREM III. *Suppose* $\mathfrak{F}=\mathfrak{F}(X_1,\dots,X_s)$ *is a form of degree* $d>1$ *with integer coefficients and with* $h(\mathfrak{F})=h$, *say. Given* α *and given* $P>1$, *put*

$$S=\sum_{|\underline{x}|\leqslant P} e(\alpha\mathfrak{F}(\underline{x})),$$

where $e(z)=e^{2\pi iz}$. *Suppose that* $0<\Omega<h/\tau(d)$ *where* $\tau(2)=2$, $\tau(3)=8$, $\tau(4)=72$, *and in general* $\tau(d)<d\cdot 2^{2d}\cdot d!$. *Then for* $\Delta>0$ *and for* $P>P_0(\mathfrak{F},\Omega,\Delta)$, *either*

(i) $|S|\leqslant P^{s-\Delta\Omega}$,

or

(ii) *there is a natural* $q\leqslant P^{\Delta}$ *with* $\|q\alpha\|\leqslant P^{-d+\Delta}$, *where* $\|\cdot\|$ *denotes the distance to the nearest integer.*

The plan of the paper is as follows. In § 2 we will deduce Theorem I from Theorem II. In § 3 we will explain the product formula for the coefficient μ in (1.3). The proofs of Theorem II and III will be contained in parts B, C, D. In part B we will give an "axiomatic" exposition of the Hardy-Littlewood Method. In part C we will estimate exponential sums in terms of a certain invariant g. In part D, which is essentially algebraic in nature, we will derive a relation between g and h. Part B will be fairly routine, part C will be less so, and part D still less.

2. Deduction of Theorem I

Given odd k and given a vector $\underline{u}=(r_k, r_{k-2},\dots,r_1)$, we have to show that a system $\underline{\mathfrak{F}}=(\underline{\mathfrak{F}}^{(k)},\underline{\mathfrak{F}}^{(k-2)},\dots,\underline{\mathfrak{F}}^{(1)})$, with $\underline{\mathfrak{F}}^{(d)}$ consisting of $r_d\geqslant 0$ forms of degree d, has[1]

[1] The numbering of constants is started new in each section.

$$z_P(\underline{\mathfrak{F}}) \gg P^{s-c_1},$$

where $c_1=c_1(\underline{u})$. In what follows, c_1 will be the smallest number with this property.

We start with the observation that (when the right hand side is finite)

$$c_1(r_k, \dots, r_3, r_1) = c_1(r_k, \dots, r_3, 0)+r_1: \tag{2.1}$$

for there is an injective linear map $\tau: \mathbf{Q}^{s-r_1} \to \mathbf{Q}^s$ which maps integer points into integer points such that $\underline{\mathfrak{F}}^{(1)}(\tau \underline{Y})=\underline{0}$, identically in $\underline{Y}=(Y_1, \dots, Y_{s-r_1})$. Setting $c_2=c_1(r_k, \dots, r_3, 0)$, and $\underline{\mathfrak{F}}^*=(\underline{\mathfrak{F}}^{(k)}(\tau \underline{Y}), \dots, \underline{\mathfrak{F}}^{(3)}(\tau \underline{Y}))$, we have

$$z_P(\underline{\mathfrak{F}}^*) \gg P^{(s-r_1)-c_2}.$$

Since $|\tau \underline{Y}| \leqslant |\tau|\,|\underline{Y}|$, it follows that

$$z_P(\underline{\mathfrak{F}}) \geqslant z_{P/|\tau|}(\underline{\mathfrak{F}}^*) \gg P^{s-r_1-c_2}.$$

Thus $c_1(\underline{u}) \leqslant c_2+r_1$, and since the reverse inequality is obvious, (2.1) follows.

It remains for us to deal with the case when $\underline{u}=(r_k, r_{k-2}, \dots, r_3, 0)$. By Theorem II and its supplement, we have in fact a PHLS, unless some h_d is small. Thus we may suppose that some form of the pencil of $\underline{\mathfrak{F}}^{(d)}$ will be of the type (1.5) with $h \leqslant c_3(d, \underline{u})$. We may suppose that one of the forms of $\underline{\mathfrak{F}}^{(d)}$, say $\mathfrak{F}_1^{(d)}$, is of this type. Say $\mathfrak{A}_1, \dots, \mathfrak{A}_h$ are of odd degrees. Let $\mathfrak{C}_1, \dots, \mathfrak{C}_h$ be forms of degree $d-2$, obtained respectively from $\mathfrak{A}_1, \dots, \mathfrak{A}_h$ by multiplication by suitable powers of $x_1^2+\dots+x_s^2$. Then $V_{\mathbf{R}}(\underline{\mathfrak{F}}) \supseteq V_{\mathbf{R}}(\underline{\mathfrak{F}}^*)$, where $\underline{\mathfrak{F}}^*$ is obtained from $\underline{\mathfrak{F}}$ by replacing $\mathfrak{F}_1^{(d)}$ by $\mathfrak{C}_1, \dots, \mathfrak{C}_h$. The vector $\underline{u}^*$ belonging to $\underline{\mathfrak{F}}^*$ is

$$\underline{u}^* = \underline{u}^*(d) = (r_k, \dots, r_{d+2}, r_d-1, r_{d-2}+c_3(d, \underline{u}), r_{d-4}, \dots, r_1).$$

Thus whenever $r_k, \dots, r_3$ are not all zero, we have

$$c_1(\underline{u}) \leqslant \max c_1(\underline{u}^*(d)), \tag{2.2}$$

where the maximum is over odd d in $3 \leqslant d \leqslant k$ with $r_d>0$. By (2.1), the relation (2.2) is true whether $r_1=0$ or not.

Now we will write $\underline{u}^*<\underline{u}$ if there is some l with $r_l^*<r_l$ (possibly $\underline{u}^*=(r_t^*, r_{t-2}^*, \dots)$ with $t<l$), but $r_d^*=r_d$ for $d>l$. Since each nonempty set of vectors $\underline{u}$ contains a smallest element with respect to $<$, Theorem I may be proved by induction on $\underline{u}$. Since in (2.2), $\underline{u}^*(d)<\underline{u}$, and since the components of $\underline{u}^*(d)$ are bounded in terms of $\underline{u}$, the theorem follows.

By Theorem II and its supplement, we may take([2])

$$c_3(d, \underline{u}) = \chi(d)\, r_d k v(\underline{u}). \tag{2.3}$$

When $\underline{u}=(r_3, 0)$, we have $\underline{u}^*(3)=(r_3-1, c_3(3, \underline{u}))=(r_3-1, c_4 r_3 v(\underline{u}))$, hence by (2.1), (2.2),

$$c_1(r_3, 0) \leqslant c_1(r_3-1, 0)+c_4 r_3 v(\underline{u}).$$

Since $v(\underline{u})\ll r_3^3$ ([11]), one gets $c_1(r_3, 0)\leqslant c_1(r_3-1, 0)+O(r_3^4)$, hence

$$c_1(r_3, 0) \ll r_3^5,$$

as in [12].

For $k>3$ it is known (Leep and Schmidt [8]) that

$$v(r_k, \ldots, r_1) \leqslant c_5(k)\,(r_k+\ldots+r_1)^{2^{k-1}}. \tag{2.4}$$

Define $\exp_l x$ by $\exp_1 x=e^x$ and by $\exp_l x=\exp(\exp_{l-1} x)$. It may be shown that our estimates imply

$$c_1(r_k, \ldots, r_3, r_1) < \exp_{k-3}(c_6(k)\,(r_k+\ldots+r_1)). \tag{2.5}$$

3. The local densities

Suppose $\underline{\mathfrak{F}}$ has integer coefficients. Let p be a prime, and write $\nu_l=\nu_l(p)$ for the number of solutions of the system of congruences

$$\underline{\mathfrak{F}}(\underline{x}) \equiv \underline{0} \pmod{p^l}.$$

Further put $\mu_l=\nu_l p^{l(r-s)}$. The limit

$$\mu(p) = \lim_{l\to\infty} \mu_l, \tag{3.1}$$

when it exists, will be called the *p-adic density of zeros* of $\underline{\mathfrak{F}}$.

We note that, with the notation $\underline{a}\underline{\mathfrak{F}}=a_1\mathfrak{F}_1+\ldots+a_r\mathfrak{F}_r$,

$$\sum_{\underline{a} \pmod{p^l}} e(p^{-l}\underline{a}\underline{\mathfrak{F}}(\underline{x})) = \begin{cases} p^{lr} & \text{when } \underline{\mathfrak{F}}(\underline{x}) \equiv \underline{0} \pmod{p^l}. \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

([2]) In the notation of § 1, $v(\underline{u})=v(r_k, 0, r_{k-2}, \ldots, r_3, 0, r_1)$. Observe that the condition (1.11) is stronger than (1.10), since $v(\underline{r})>R$, as noted e.g. in (4.6) below.

For $\underline{\eta} \in p^{-l}\mathbf{Z}^r$ put

$$E(\underline{\eta}) = p^{-ls} \sum_{\underline{x} \pmod{p^l}} e(\underline{\eta}\underline{\mathfrak{F}}(\underline{x})). \tag{3.3}$$

In view of (3.2) we have

$$\mu_l = \sum_{\underline{a} \pmod{p^l}} E(p^{-l}\underline{a}). \tag{3.4}$$

Writing

$$A(p^m) = \sum_{\substack{\underline{a} \pmod{p^m} \\ (\underline{a}, p)=1}} E(p^{-m}\underline{a}) \tag{3.5}$$

where $(\underline{a}, p)=\gcd(a_1, \ldots, a_r, p)$, we obtain

$$\mu_l = 1+A(p)+\ldots+A(p^l),$$

and when the p-adic density exists, it is given by

$$\mu(p) = 1+A(p)+A(p^2)+\ldots. \tag{3.6}$$

Our formulae may be rewritten in the following more trendy way, which will however not be used in the sequel. (A more systematic exposition of this approach is given by Lachaud [6].) Let $\mathbf{Q}_p$ be the field of p-adic numbers, $\mathbf{Z}_p$ the ring of p-adic integers. Let $|\xi|_p$ be the p-adic absolute value on $\mathbf{Q}_p$. Let $\lambda(\eta)$ be the indicator function of $\mathbf{Z}_p$, i.e. $\lambda(\eta)=1$ when $\eta \in \mathbf{Z}_p$, and $\lambda(\eta)=0$ otherwise. Put

$$\lambda_l(\eta) = p^l\lambda(p^{-l}\eta) = \begin{cases} p^l & \text{when } |\eta|_p \leqslant p^{-l}, \\ 0 & \text{otherwise.} \end{cases}$$

Put $\lambda_l(\underline{\eta})=\lambda_l(\eta_1)\ldots\lambda_l(\eta_r)$ for $\underline{\eta}=(\eta_1, \ldots, \eta_r) \in \mathbf{Q}_p^r$. An element $\xi \in \mathbf{Q}_p$ may uniquely be written as $\xi=[\xi]+\{\xi\}$ where $[\xi] \in \mathbf{Z}_p$ and where $\{\xi\}=a_1p^{-1}+a_2p^{-2}+\ldots$ with $0 \leqslant a_i < p$. The character

$$e(\xi) := e(\{\xi\})$$

is sometimes called the *Tate* character. Let $d\xi$ be the Haar measure on $\mathbf{Q}_p$, normalized so that $\mathbf{Z}_p$ has measure 1. Further let $d\underline{\xi}$, $d\underline{\eta}$ be the Haar measure of $\mathbf{Q}_p^s$ and $\mathbf{Q}_p^r$, respectively.

With these conventions we have

$$\mu_l = p^{-ls} \sum_{\underline{x} \,(\mathrm{mod}\, p^l)} \lambda_l(\underline{\mathfrak{F}}(\underline{x})) = \int_{\mathbf{Z}_p^s} \lambda_l(\underline{\mathfrak{F}}(\underline{\xi}))\, d\underline{\xi}.$$

The formula (3.3) may be replaced by

$$E(\underline{\eta}) = \int_{\mathbf{Z}_p^s} e(\underline{\eta}\underline{\mathfrak{F}}(\underline{\xi}))\, d\underline{\xi}.$$

This definition in fact makes sense for every $\underline{\eta} \in \mathbf{Q}_p^r$. Further (3.4) becomes

$$\mu_l = \int_{p^{-l}\mathbf{Z}_p^r} E(\underline{\eta})\, d\underline{\eta}.$$

When the p-adic density $\mu(p)$ exists, then

$$\mu(p) = \int_{\mathbf{Q}_p^r} E(\underline{\eta})\, d\underline{\eta}.$$

We now turn to the *real density*. This density $\mu(\infty)=\mu(\infty, \mathfrak{B})$ will depend on the given box $\mathfrak{B}$. Write $\lambda(\eta)=1-|\eta|$ when $|\eta|\leqslant 1$, and $\lambda(\eta)=0$ otherwise. For $L>0$ put

$$\lambda_L(\eta) = L\lambda(L\eta) = \begin{cases} L(1-L|\eta|) & \text{when } |\eta| \leqslant L^{-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Put $\lambda_L(\underline{\eta})=\lambda_L(\eta_1)\ldots\lambda_L(\eta_r)$ for $\underline{\eta} \in \mathbf{R}^r$. Now set

$$\mu_L = \int_{\mathfrak{B}} \lambda_L(\underline{\mathfrak{F}}(\underline{\xi}))\, d\underline{\xi}.$$

The limit

$$\mu(\infty) = \mu(\infty, \mathfrak{B}) = \lim_{L \to \infty} \mu_L, \tag{3.7}$$

when it exists, will be called the real density.

Put

$$K(\underline{\eta}) = \int_{\mathfrak{B}} e(\underline{\eta}\underline{\mathfrak{F}}(\underline{\xi}))\, d\underline{\xi}. \tag{3.8}$$

We will see that under certain assumptions on $\underline{\mathfrak{F}}$ we have

$$K(\underline{\eta}) \ll \min(1, |\underline{\eta}|^{-r-1}). \tag{3.9}$$

Thus

$$\mu^*(\infty) := \int_{\mathbf{R}^r} K(\underline{\eta})\, d\underline{\eta}$$

exists. Moreover, as was shown in [9, § 11], it follows that

$$|\mu^*(\infty) - \mu_L| \ll L^{-1},$$

so that the limit $\mu(\infty)$ of (3.7) exists, and $\mu(\infty)=\mu^*(\infty)$.

The analogy in the definitions of $\mu(p)$ and $\mu(\infty)$ is clear. One difference is that only $\mu(\infty)$ depends on $\mathfrak{B}$. Under some further conditions, the local densities could be expressed as integrals along the manifold $\underline{\mathfrak{F}}=\underline{0}$, either in $\mathbf{Z}_p^s$ or in $\mathfrak{B}\subseteq\mathbf{R}^s$, by means of the Leray differential form. But these integrals offer no advantage for the purpose of this paper.

When defining a HLS in § 1, we postponed the definition of μ. We now give the following condition:

For a HLS *we postulate that the local densities as given by* (3.1) *and by* (3.7) *exist, that the product* $\mu(\infty, \mathfrak{B})\mu(2)\mu(3)\ldots$ *of these densities exists, and that the number* μ *of* (1.3) *is this product:*

$$\mu = \mu(\infty, \mathfrak{B})\mu(2)\mu(3)\ldots. \tag{3.10}$$

Hence a HLS is a PHLS precisely when all the local densities are positive. Classically, $\mathfrak{J}=\mu(\infty)$ is called the *singular integral*, and $\mathfrak{S}=\mu(2)\mu(3)\ldots$ is called the *singular series*.

So far we have defined the density μ only when $\underline{\mathfrak{F}}$ has integer coefficients. It may be seen that the local densities have simple transformation properties, and that the global density μ remains unchanged, when $\underline{\mathfrak{F}}$ is replaced by a proportional system $\underline{\mathfrak{G}}=c\underline{\mathfrak{F}}$ with integer coefficients. Hence in general we may define $\mu(\underline{\mathfrak{F}})=\mu(\underline{\mathfrak{G}})$, where $\underline{\mathfrak{G}}$ is proportional to $\underline{\mathfrak{F}}$ and has integer coefficients.

B. The Hardy-Littlewood method

4. A Hypothesis on exponential sums

Our goal in part B will be to show that the machinery of the Hardy-Littlewood method may be applied, provided we make a certain assumption on exponential sums. Let $\underline{\mathfrak{F}}=(\underline{\mathfrak{F}}^{(k)}, \ldots, \underline{\mathfrak{F}}^{(2)})$ be a system of $r=r_k+\ldots+r_2$ forms as in (1.7), with rational coeffi-

cients and in s variables $\underline{X}=(X_1,\dots,X_s)$. In proving Theorem II we can and we will suppose without loss of generality that the coefficients of $\underline{\mathfrak{F}}$ are in fact integers. Let T be the group $T=\mathbf{R}/\mathbf{Z}$, and T^r the r-dimensional torus. Elements $\underline{\alpha}$ of T^r will be written as

$$\underline{\alpha}=(\underline{\alpha}^{(k)},\dots,\underline{\alpha}^{(2)}) \tag{4.1}$$

with $\underline{\alpha}^{(d)}\in T^{r_d}$ $(2\leqslant d\leqslant k)$, where $T^0=\{0\}$. The inner product of $\underline{\alpha}$ and $\underline{\mathfrak{F}}$ may be written as

$$\underline{\alpha}\underline{\mathfrak{F}}=\underline{\alpha}^{(k)}\underline{\mathfrak{F}}^{(k)}+\dots+\underline{\alpha}^{(2)}\underline{\mathfrak{F}}^{(2)}.$$

For $\alpha\in T$, let $\|\alpha\|$ be the distance from α to the zero element of T. That is, when α consists of reals $\equiv\xi\,(\mathrm{mod}\,1)$, then $\|\alpha\|$ is the distance from ξ to the nearest integer. For $\underline{\alpha}\in T^l$ put $\|\underline{\alpha}\|=\max(\|\alpha_1\|,\dots,\|\alpha_l\|)$ when $l>0$, and $\|\underline{\alpha}\|=0$ when $l=0$.

Given a box $\mathfrak{B}$ and given $P>1$ we put

$$S(\underline{\alpha})=S(\underline{\alpha},\mathfrak{B})=\sum_{\underline{x}\in P\mathfrak{B}} e(\underline{\alpha}\underline{\mathfrak{F}}(\underline{x})). \tag{4.2}$$

Then

$$z_P=\int_{T^r} S(\underline{\alpha})\,d\underline{\alpha}. \tag{4.3}$$

Given a positive number Ω, we now introduce the following

HYPOTHESIS ON $\underline{\mathfrak{F}}$. *For any box $\mathfrak{B}$, any $\Delta>0$, and for $P>P_1(\underline{\mathfrak{F}},\Omega,\mathfrak{B},\Delta)$, each $\underline{\alpha}\in T^r$ satisfies at least one of the following two alternatives. Either*

(i) $|S(\underline{\alpha})|\leqslant P^{s-\Delta\Omega}$, *or*

(ii) *there is a natural $q=q(\underline{\alpha})\leqslant P^{\Delta}$ with*

$$\|q\underline{\alpha}^{(d)}\|\leqslant P^{-d+\Delta}\quad(2\leqslant d\leqslant k).$$

We will say that the *restricted* Hypothesis holds if the above condition holds for each Δ in $0<\Delta\leqslant 1$.

The r-tuples $\underline{\alpha}$ with (ii) form a subset $\mathfrak{M}(\Delta)$ of T^r which is the union of certain "boxes" (see below), traditionally called the *major arcs*. The complement $\mathfrak{m}(\Delta)$ of $\mathfrak{M}(\Delta)$ in T^r is called the *minor arcs* (although for $r>1$ this terminology, especially the plural, makes little sense). Thus the Hypothesis means that $S(\underline{\alpha})$ is small on the minor arcs. Our main task in part B will be a proof of the following

PROPOSITION I. *Suppose* $\mathfrak{F}$ *satisfies the Hypothesis with some*

$$\Omega > r+1, \tag{4.4}$$

or the restricted Hypothesis with some

$$\Omega > R. \tag{4.5}$$

Then $\mathfrak{F}$ *is a* HLS.

Given a prime p, define $v_p(\underline{r})=v_p(r_k, \dots, r_1)$ (or $v_p(r_k, \dots, r_2, 0)$) as the smallest number such that any system $\mathfrak{F}$ as in (1.1) (or as in (1.7)) in more than $v_p(\underline{r})$ variables has a nontrivial p-adic zero. The number $v(\underline{r})$ introduced in § 1 is then the maximum of $v_p(\underline{r})$ over all primes p. These quantities are known to be finite, and recursive estimates were derived in [8]. It is well known that (in the case (1.7))

$$v_p(\underline{r}) \geqq k^2 r_k + \dots + 2^2 r_2 > R > r+1. \tag{4.6}$$

FIRST SUPPLEMENT. *Suppose the restricted Hypothesis holds with*

$$\Omega > v_p(\underline{r}). \tag{4.7}$$

Then the p-adic density $\mu(p)$ *is positive.*

SECOND SUPPLEMENT. *Suppose the restricted Hypothesis holds with* (4.4), *and suppose that* $\dim V_{\mathbf{R}}(\mathfrak{B}) \geqq s-r$, *where* $V_{\mathbf{R}}(\mathfrak{B})$ *is the manifold of zeros of* $\mathfrak{F}$ *in the interior of* $\mathfrak{B}$. *Then the real density* $\mu(\infty, \mathfrak{B})$ *is positive. Moreover, we do have* $\dim V_{\mathbf{R}}(\mathfrak{E}) \geqq s-r$ *if* $\mathfrak{F}$ *consists only of forms of odd degree.*

Combining Proposition I and its supplements with what we said in § 3, and noting that $\dim V_{\mathbf{R}}(\mathfrak{E}) = \dim V_{\mathbf{R}}$, we obtain the

COROLLARY. *Suppose the restricted Hypothesis holds with*

$$\Omega > v(\underline{r}), \tag{4.8}$$

and suppose that $\dim V_{\mathbf{R}} \geqq s-r$. *Then* $\mathfrak{F}$ *is a* PHLS.

5. The minor arcs

We will assume that the assumption of Proposition I holds.

LEMMA 5.1. *For each* $\Delta>0$ *we have*

$$\int_{\mathfrak{m}(\Delta)} |S(\underline{\alpha})|\, d\underline{\alpha} \ll P^{s-R-\delta} \tag{5.1}$$

where $\delta=\delta(\Delta)>0$.

Proof. When the Hypothesis holds with $\Omega>r+1$, choose E so large that $E\Omega>R$; when the restricted hypothesis holds with $\Omega>R$, set $E=1$. At any rate, for $\underline{\alpha}\in\mathfrak{m}(E)$ we have $|S(\underline{\alpha})|\ll P^{s-E\Omega}\leqslant P^{s-R-\delta}$. Hence (5.1) is certainly true when $\Delta\geqslant E$, for then $\mathfrak{m}(\Delta)\subseteq\mathfrak{m}(E)$. When $\Delta<E$, pick numbers $\Delta=\Delta_0<\Delta_1<\ldots<\Delta_h=E$. Then $\mathfrak{m}(\Delta)$ is the union of $\mathfrak{m}(E)$ and the set-theoretic differences

$$\mathfrak{m}_i=\mathfrak{M}(\Delta_i)\setminus\mathfrak{M}(\Delta_{i-1}) \quad (i=1,\ldots,h).$$

The measure of $\mathfrak{m}_i$ is $\ll P^{-R+\Delta_i(r+1)}$. On the other hand, on the complement of $\mathfrak{M}(\Delta_{i-1})$, the integrand $|S(\underline{\alpha})|$ *is* $\ll P^{s-\Delta_{i-1}\Omega}$. Thus the integral over $\mathfrak{m}_i$ is

$$\ll P^{s-R-\Delta_{i-1}\Omega+\Delta_i(r+1)}.$$

But

$$-\Delta_{i-1}\Omega+\Delta_i(r+1)=-\Delta_i(\Omega-r-1)+(\Delta_i-\Delta_{i-1})\Omega<-\tfrac{1}{2}\Delta(\Omega-r-1)<0$$

if the sequence $\Delta_0<\ldots<\Delta_h$ was chosen with small enough differences $\Delta_i-\Delta_{i-1}$.

6. The major arcs

The major arcs $\mathfrak{M}(\Delta)$ are the union of the "boxes" $\mathfrak{M}(\Delta,q,\underline{a})$, consisting of $\underline{\alpha}$ with

$$|q\underline{\alpha}^{(d)}-\underline{a}^{(d)}|\leqslant P^{-d+\Delta} \quad (2\leqslant d\leqslant k), \tag{6.1}$$

where $q\leqslant P^{\Delta}$ and where $\underline{a}=(\underline{a}^{(k)},\ldots,\underline{a}^{(2)})$ runs through the integer points. In fact, since we are interested in $\underline{\alpha}\in T^r=(\mathbf{R}/\mathbf{Z})^r$, we may restrict ourselves to a set of points $\underline{a}\,(\mathrm{mod}\,q)$, and we further may suppose that $(\underline{a},q)=\gcd(a_2,\ldots,a_r,q)=1$. The union will then be disjoint if Δ is small and P is large.

Generalizing (3.3) we write

$$E(q^{-1}\underline{a})=q^{-s}\sum_{\underline{x}\,(\mathrm{mod}\,q)} e(q^{-1}\underline{a}\underline{\mathfrak{F}}(\underline{x})),$$

and we set

$$I(\underline{\beta}) = \int_{P\mathfrak{B}} e(\underline{\beta}\underline{\mathfrak{F}}(\underline{\xi}))\, d\underline{\xi}. \tag{6.2}$$

LEMMA 6.1. *Suppose* $\underline{\alpha}=q^{-1}\underline{a}+\underline{\beta}\in\mathfrak{M}(\Delta, q, \underline{a})$. *Then*

$$S(\underline{\alpha}) = q^{-s}S(q^{-1}\underline{a})\, I(\underline{\beta})+O(qP^{s-1+\Delta}).$$

The *proof* if as for Lemma 9 in [9].

Generalizing (3.5), put

$$A(q) = \sum_{\substack{a \pmod q \\ (a,q)=1}} E(q^{-1}\underline{a}),$$

and write

$$\mathfrak{S}(L) = \sum_{q\le L} A(q),$$

$$\mathfrak{J}(L) = \int_{|\eta|\le L} K(\underline{\eta})\, d\underline{\eta},$$

with $K(\underline{\eta})$ given by (3.8).

LEMMA 6.2. *For sufficiently small* $\Delta>0$ *there is a* $\delta>0$ *such that*

$$\int_{\mathfrak{M}(\Delta)} S(\underline{\alpha})\, d\underline{\alpha} = P^{s-R}\mathfrak{S}(P^{\Delta})\,\mathfrak{J}(P^{\Delta})+O(P^{s-R-\delta}).$$

The *proof* is as for Lemma 10 in [9].

In view of this and Lemma 5.1, and by (4.3), the proof of Proposition I will be complete if we can show that the local densities exist, that the infinite product

$$\mathfrak{S} = \mu(2)\mu(3)\mu(5)\ldots \tag{6.3}$$

is convergent, and that with suitable $\delta>0$

$$\mathfrak{S}(P^{\Delta})-\mathfrak{S} \ll P^{-\delta}, \tag{6.4}$$

$$\mathfrak{J}(P^{\Delta})-\mu(\infty) = \mathfrak{J}(P^{\Delta})-\mathfrak{J} \ll P^{-\Delta}. \tag{6.5}$$

This will be accomplished in the next two sections.

7. The singular series

LEMMA 7.1. *Suppose* $(a, q)=1$. *Now if the restricted Hypothesis holds with some* $\Omega>\Phi$, *then*

$$E(q^{-1}\underline{a}) \ll q^{-\Phi}. \tag{7.1}$$

The constant in $\ll$ *may depend on* $\mathfrak{F}$ *and* Φ.

Proof. $E(q^{-1}\underline{a})=q^{-s}S(\underline{a})$ with $\underline{a}=q^{-1}\underline{a}$, with $P=q$ and with $\mathfrak{B}$ the cube $0\leqslant\xi_i<1$. We now apply the Hypothesis with $\Delta=\Phi/\Omega<1$. Alternative (i) gives precisely (7.1). Alternative (ii) gives a number $\hat{q}\leqslant q^{\Delta}<q$ (when $q\neq 1$) with

$$\|\hat{q}q^{-1}\underline{a}^{(d)}\| \ll q^{-d+\Delta} \quad (2\leqslant d\leqslant k),$$

so that $\|\hat{q}q^{-1}\underline{a}^{(d)}\|<q^{-1}$ when q is large. Since $(a, q)=1$, this is impossible.

Now if the restricted Hypothesis holds with $\Omega>r+1$, we get $E(q^{-1}\underline{a})\ll q^{-r-1-\delta}$ where $\delta>0$, and hence $A(q)\ll q^{-1-\delta}$. Thus the sum

$$\mathfrak{S}(\infty)=\sum_{q=1}^{\infty} A(q)$$

is convergent, and

$$\mathfrak{S}(P^{\Delta})-\mathfrak{S}(\infty) \ll P^{-\delta}.$$

The densities $\mu(p)$ given by (3.6) exist, and since A is multiplicative,

$$\mathfrak{S}(\infty)=\prod_{p}\mu(p)=\mathfrak{S}.$$

Hence the assertions about the "singular series" $\mathfrak{S}$ made in the last section are correct.

Next, suppose that the restricted Hypothesis holds with $\Omega>v_p(\underline{r})$. Then $E(q^{-1}\underline{a})\ll q^{-v_p(\underline{r})-\delta}$, and $A(q)\ll q^{r-v_p(\underline{r})-\delta}$, so that

$$A(p^{l+1})+A(p^{l+2})+\ldots \ll p^{l(r-v_p(\underline{r})-\delta)}. \tag{7.2}$$

On the other hand the argument for Lemma 2 in [12] yields

$$v_l \gg p^{l(s-v_p(\underline{r}))}, \tag{7.3}$$

so that

$$1+A(p)+\ldots+A(p^l)=\mu_l=p^{l(r-s)}\nu_l \gg p^{l(r-v_p(\underline{r}))}.$$

This, together with (7.2), shows that the first supplement to Proposition I is correct.

We remark that (7.3) may be regarded as the analogue of Theorem I in the local field $\mathbf{Q}_p$. But (7.3) was very easy to prove.

8. The singular integral

LEMMA 8.1. *The restricted Hypothesis with* $\Omega>r+1$ *implies* (3.9).

As we had seen in § 3, it follows that the real density exists, and

$$\mu(\infty)=\mu^*(\infty)=\int_{\mathbf{R}^r} K(\underline{\eta})\,d\underline{\eta}.$$

Further,

$$\mu(\infty)-\mathfrak{I}(P^{\Delta})=\int_{|\underline{\eta}|>P^{\Delta}} K(\underline{\eta})\,d\underline{\eta}\ll P^{-\Delta},$$

so that (6.5) holds.

Moreover, as was shown in [9, Lemma 2], we have $\mu(\infty,\mathfrak{B})>0$ when $\dim V_{\mathbf{R}}(\mathfrak{B})\geqslant s-r$. And, as was shown in [12, § 2],

$$\dim V_{\mathbf{R}}=\dim V_{\mathbf{R}}(\mathfrak{E})\geqslant s-r \tag{8.1}$$

is certainly true if all the forms of $\underline{\mathfrak{F}}$ are of odd degree. Hence the second supplement follows.

Proof of the lemma. We proceed as in Lemma 11 of [9] and Lemma 12 of [12]. We may suppose that $|\underline{\eta}|>2$. Writing $\underline{\xi}=P^{-1}\underline{\xi}'$ we have

$$K(\underline{\eta})=P^{-s}I(\underline{\beta}) \tag{8.2}$$

where $I(\underline{\beta})$ is given by (6.2) and where

$$\underline{\beta}=(\underline{\beta}^{(k)},\ldots,\underline{\beta}^{(2)})=(P^{-k}\underline{\eta}^{(k)},\ldots,P^{-2}\underline{\eta}^{(2)}).$$

We are still free to choose P; we set

$$P=|\underline{\eta}|^{r+2}.$$

Put $\varphi=(r+2)^{-1}$. Then $\underline{\beta}$ lies on the boundary of the "box" $\mathfrak{M}(\varphi,1,\underline{0})$. The boxes

$\mathfrak{M}(\varphi, q, \underline{a})$ with $q \leqq P^{\varphi}$, with $\underline{a} \pmod q$ and with $(\underline{a}, q)=1$ are disjoint, at least when $|\underline{\eta}|$ and hence P is large. Hence β lies on the boundary of $\mathfrak{M}(\varphi)$, hence lies on the boundary of $\mathfrak{m}(\varphi)$. By the Hypothesis with $\Delta=\varphi$, we have

$$|S(\beta)| \leqq P^{s-\varphi\Omega} = P^s|\underline{\eta}|^{-\Omega} \ll P^s|\underline{\eta}|^{-r-1}.$$

But since β lies in $\mathfrak{M}(\varphi, 1, \underline{0})$, Lemma 6.1 yields

$$S(\beta) = I(\beta)+O(P^{s-1+\varphi}) = I(\beta)+O(P^s|\underline{\eta}|^{-r-1}).$$

The last two relations in conjunction with (8.2) yield (3.9).

We remark that (8.1) may be regarded as the analogue of Theorem I in the local field **R**. We also remark that the hypothesis was used for the minor arcs, for the singular series and the densities $\mu(p)$, as well as for the singular integral $\mathfrak{I}=\mu(\infty)$.

Incidentally, the restricted Hypothesis with some $\Omega>r$, and in consequence (3.9) weakened to $K(\underline{\eta}) \ll \min(1, |\underline{\eta}|^{-r-\delta_1})$ with $\delta_1>0$, would have been enough to prove the weaker version $\mathfrak{I}(P^{\Delta})-\mu(\infty) \ll P^{-\delta}$ of (6.5), and hence enough to deal with the singular integral.

9. Inhomogeneous polynomials

The results of part B easily generalize the systems

$$\underline{\mathfrak{P}} = (\underline{\mathfrak{P}}^{(k)}, \ldots, \underline{\mathfrak{P}}^{(2)}),$$

where $\underline{\mathfrak{P}}^{(k)}$ is a set of polynomials of degree d. Namely, let $\underline{\mathfrak{F}}=(\underline{\mathfrak{F}}^{(k)}, \ldots, \underline{\mathfrak{F}}^{(2)})$, where $\underline{\mathfrak{F}}^{(d)}$ consists of the forms of degree d belonging to $\underline{\mathfrak{P}}^{(d)}$. Define $\mu(p)$ as in § 3, but with $\underline{\mathfrak{F}}$ replaced by $\underline{\mathfrak{P}}$. On the other hand define $\mu(\infty, \mathfrak{B})$ exactly as in § 3, so that it depends only on the homogeneous part $\underline{\mathfrak{F}}$ of $\underline{\mathfrak{P}}$. Define $S(\underline{a})$ in terms of $\underline{\mathfrak{P}}$. Then if $\underline{\mathfrak{P}}$ satisfies the Hypothesis with $\Omega>r+1$ (or the restricted Hypothesis with $\Omega>R$), we may conclude that $\underline{\mathfrak{P}}$ is a HLS, in the sense that a formula analogous (1.3) holds. About the only extra line is in Lemma 6.1, where one has to note that

$$\int_{P\mathfrak{B}} e(\beta\underline{\mathfrak{P}}(\underline{\xi}))\, d\underline{\xi} = \int_{P\mathfrak{B}} e(\beta\underline{\mathfrak{F}}(\underline{\xi}))\, d\underline{\xi}+O(P^{s-1+\Delta}) = I(\beta)+O(P^{s-1+\Delta}).$$

There is no analogue to the first supplement. But the second supplement holds, with $V_{\mathbf{R}}(\mathfrak{B})$ the manifold of zeros of $\underline{\mathfrak{F}}$ (not $\underline{\mathfrak{P}}$) in $\mathfrak{B}$.

C. Estimation of exponential sums

10. Manifolds $\mathfrak{M}$ and invariants

With each form $\mathfrak{F}(\underline{X})$ of degree d we associate the unique symmetric multilinear form $\mathfrak{F}(\underline{X}_1|\dots|\underline{X}_d)$ with $\mathfrak{F}(\underline{X}|\dots|\underline{X})=(-1)^d d!\mathfrak{F}(\underline{X})$. Suppose $\underline{\mathfrak{F}}=(\mathfrak{F}_1,\dots,\mathfrak{F}_r)$ is a system of forms with complex coefficients and of equal degree $d>1$. The *complex pencil* of $\underline{\mathfrak{F}}$ consists of forms $\underline{\alpha}\underline{\mathfrak{F}}=\alpha_1\mathfrak{F}_1+\dots+\alpha_r\mathfrak{F}_r$ with nonzero $\underline{\alpha}\in\mathbf{C}^r$. Let $\underline{e}_1,\dots,\underline{e}_s$ be the basis vectors. When $d>1$ we associate with $\underline{\mathfrak{F}}$ the set $\mathfrak{M}=\mathfrak{M}(\underline{\mathfrak{F}})$ of $(d-1)$-tuples $(\underline{x}_1,\dots,\underline{x}_{d-1})\in\mathbf{C}^{s(d-1)}$ for which the matrix

$$(m_{ij})=(\mathfrak{F}_j(\underline{x}_1|\dots|\underline{x}_{d-1}|\underline{e}_i)) \quad (1\leqslant i\leqslant s,\ 1\leqslant j\leqslant r) \tag{10.1}$$

has rank $<r$. Thus $\mathfrak{M}$ is an algebraic manifold in $\mathbf{C}^{s(d-1)}$, consisting of the $(d-1)$-tuples for which some form $\mathfrak{F}$ of the complex pencil has

$$\mathfrak{F}(\underline{x}_1|\dots|\underline{x}_{d-1}|\underline{Z})=0, \tag{10.2}$$

identically in $\underline{Z}$. The manifold $\mathfrak{M}$ depends only on the complex pencil of $\underline{\mathfrak{F}}$, i.e. it is invariant under substitutions $\underline{\mathfrak{F}}\mapsto T\underline{\mathfrak{F}}$ where T is a nonsingular linear map of $\mathbf{C}^r$.

Birch [2] had defined $V^*=V^*(\underline{\mathfrak{F}})$ as the set of $\underline{x}\in\mathbf{C}^s$ for which the matrix $\partial\mathfrak{F}_j/\partial x_i$ $(1\leqslant i\leqslant s,\ 1\leqslant j\leqslant r)$ has rank less than r, i.e. for which the matrix

$$\mathfrak{F}_j(\underline{x}|\dots|\underline{x}|\underline{e}_i) \quad (1\leqslant i\leqslant s,\ 1\leqslant j\leqslant r)$$

has rank less than r. Hence V^* is the intersection of $\mathfrak{M}$ with the "diagonal" $\underline{x}_1=\dots=\underline{x}_{d-1}$. This diagonal has codimension $s(d-2)$, and hence V^*, interpreted in this way as a submanifold of $\mathbf{C}^{s(d-1)}$, has codimension

$$\leqslant \operatorname{codim}\mathfrak{M}+s(d-2).$$

(S. Lang [7, § II.7]). Hence if V^* is interpreted as a submanifold of $\mathbf{C}^s$, we get

$$\operatorname{codim} V^*\leqslant\operatorname{codim}\mathfrak{M}, \tag{10.3}$$

as had already been noted by Birch.

Suppose that the forms of $\underline{\mathfrak{F}}$ have rational coefficients. An integer $(s-1)$-tuple $(\underline{x}_1,\dots,\underline{x}_{d-1})$ now lies in $\mathfrak{M}$ precisely if there is a form $\mathfrak{F}$ of the *rational* pencil with (10.2). We write $g=g(\underline{\mathfrak{F}})$ for the largest real number such that

$$z_p(\mathfrak{M})\ll\ll P^{s(d-1)-g+\varepsilon} \tag{10.4}$$

holds for each $\varepsilon>0$. Since $z_P(\mathfrak{M})\ll P^{\dim \mathfrak{M}}$, we have

$$\operatorname{codim} \mathfrak{M} \leqslant g. \tag{10.5}$$

The number g is invariant under substitutions $\underline{\mathfrak{F}} \mapsto T\underline{\mathfrak{F}}$ where T is a nonsingular linear map of $\mathbf{Q}^r$. It is easily seen to be invariant also under substitutions $\underline{\mathfrak{F}}(\underline{X}) \mapsto \underline{\mathfrak{F}}(\tau(\underline{X}))$ where τ is a nonsingular linear map of $\mathbf{Q}^s$.

PROPOSITION II_0. *Let $\underline{\mathfrak{F}}=\underline{\mathfrak{F}}^{(d)}=(\mathfrak{F}_1, \ldots, \mathfrak{F}_r)$ be a system of forms of equal degree $d\geqslant 2$, with rational coefficients. The Hypothesis of* § 4 *is then true for any* Ω *in*

$$0<\Omega<g/(2^{d-1}(d-1)r). \tag{10.6}$$

In conjunction with Proposition I this shows that $\underline{\mathfrak{F}}$ is a HLS when

$$g>2^{d-1}(d-1)r(r+1).$$

By (10.3) and (10.5), this is certainly true if

$$\operatorname{codim} V^*>2^{d-1}(d-1)r(r+1).$$

Thus we have recovered the theorem of Birch quoted in § 1.

Now let $\underline{\mathfrak{F}}=(\underline{\mathfrak{F}}^{(k)}, \ldots, \underline{\mathfrak{F}}^{(2)})$, where $\underline{\mathfrak{F}}^{(d)}$ consists of $r_d\geqslant 0$ forms of degree d, with rational coefficients. For each d with $r_d>0$ put

$$g_d=g(\underline{\mathfrak{F}}^{(d)}). \tag{10.7}$$

Further set

$$\gamma_d=g_d^{-1}2^{d-1}(d-1)r_d \quad \text{when } r_d>0,\ g_d>0, \tag{10.8}$$

and $\gamma_d=0$ when $r_d=0$, and $\gamma_d=+\infty$ when $r_d>0$, $g_d=0$. Finally set

$$\tau=\gamma_2+4\gamma_3+\ldots+4^{k-2}\gamma_k. \tag{10.9}$$

PROPOSITION II. *The system $\underline{\mathfrak{F}}$ satisfies the restricted Hypothesis of* § 4 *for every* Ω *in*

$$0<\Omega<\tau^{-1}. \tag{10.10}$$

It follows via Proposition I that $\underline{\mathfrak{F}}$ is a HLS if

$$\tau R<1. \tag{10.11}$$

Furthermore, by the corollary to Proposition I, we have a PHLS if $\dim V_{\mathbf{R}} \geqslant s-r$, and if

$$\tau v(\underline{r}) < 1. \tag{10.12}$$

Noting the definition of τ, and $\Sigma_2^k(1+2^{1-d})<k$, we obtain the

COROLLARY. *$\underline{\mathfrak{F}}=(\underline{\mathfrak{F}}^{(k)}, \dots, \underline{\mathfrak{F}}^{(2)})$ is a* HLS *if*

$$g_d > (d-1)(1+2^{1-d})^{-1} 2^{3d-5} r_d k R \quad (2 \leqslant d \leqslant k). \tag{10.13}$$

It is even a PHLS *if* $\dim V_{\mathbf{R}} \geqslant s-r$ *and if*

$$g_d > (d-1)(1+2^{1-d})^{-1} 2^{3d-5} r_d k v(\underline{r}) \quad (2 \leqslant d \leqslant k). \tag{10.14}$$

In view of (10.3), (10.5), the conclusions remain valid if the g_d in (10.13), (10.14) is replaced by $\operatorname{codim} V_d^*$, with $V_d^* = V^*(\underline{\mathfrak{F}}^{(d)})$.

Part C will be devoted to a proof of Propositions II_0 and II.

Remark on inhomogeneous polynomials. It will be clear from our proofs that Propositions II_0 and II continue to hold for systems $\underline{\mathfrak{P}}$ of inhomogeneous polynomials as in §9, provided the sets $\mathfrak{M}_d$ and the invariants g_d, γ_d and τ are defined in terms of the "homogeneous part" $\underline{\mathfrak{F}}$ of $\underline{\mathfrak{P}}$.

11. Weyl's inequality

Given a function $\mathfrak{F}(\underline{X})$, define

$$\mathfrak{F}_d(\underline{X}_1, \dots, \underline{X}_d) = \sum_{\varepsilon_1=0}^{1} \dots \sum_{\varepsilon_d=0}^{1} (-1)^{\varepsilon_1+\dots+\varepsilon_d} \mathfrak{F}(\varepsilon_1 \underline{X}_1 + \dots + \varepsilon_d \underline{X}_d),$$

as in [10]. Then $\mathfrak{F}_d$ is symmetric in its d arguments, and $\mathfrak{F}_d(\underline{X}_1, \dots, \underline{X}_{d-1}, \underline{0})=0$. By [10, (2.1)], or directly,

$$\begin{aligned}\mathfrak{F}_{d+1}(\underline{X}_1, \dots, \underline{X}_{d+1}) \\ = \mathfrak{F}_d(\underline{X}_1, \dots, \underline{X}_{d-1}, \underline{X}_d) + \mathfrak{F}_d(\underline{X}_1, \dots, \underline{X}_{d-1}, \underline{X}_{d+1}) - \mathfrak{F}_d(\underline{X}_1, \dots, \underline{X}_{d-1}, \underline{X}_d + \underline{X}_{d+1}).\end{aligned}$$

Therefore, if for fixed $\underline{x}_1, \dots, \underline{x}_{d-1}$ we set $\mathfrak{G}(\underline{X}) = \mathfrak{F}_d(\underline{x}_1, \dots, \underline{x}_{d-1}, \underline{X})$, we obtain

$$\mathfrak{F}_{d+1}(\underline{x}_1, \dots, \underline{x}_{d-1}, \underline{X}_d, \underline{X}_{d+1}) = -\mathfrak{G}_2(\underline{X}_d, \underline{X}_{d+1}). \tag{11.1}$$

Given a finite set $\mathfrak{A}$ of integer points in $\mathbf{R}^s$, write $\mathfrak{A}-\underline{x}$ for the set of points $\underline{a}-\underline{x}$ with $\underline{a} \in \mathfrak{A}$. The difference set $\mathfrak{A}^D$ is of the union of the sets $\mathfrak{A}-\underline{x}$ with $\underline{x} \in \mathfrak{A}$. Define

$$\mathfrak{A}(\underline{x}_1, \dots, \underline{x}_t) = \bigcap_{\varepsilon_1=0}^{1} \dots \bigcap_{\varepsilon_t=0}^{1} (\mathfrak{A} - \varepsilon_1 \underline{x}_1 - \dots - \varepsilon_t \underline{x}_t).$$

Then $\mathfrak{A}(\underline{x}) = \mathfrak{A} \cap (\mathfrak{A} - \underline{x})$, and for $t \geq 2$,

$$\mathfrak{A}(\underline{x}_1, \dots, \underline{x}_t) = \mathfrak{A}(\underline{x}_1, \dots, \underline{x}_{t-1}) \cap (\mathfrak{A}(\underline{x}_1, \dots, \underline{x}_{t-1}) - \underline{x}_t).$$

LEMMA 11.1. *Let $\mathfrak{F}$ be defined on $\mathbf{Z}^s$ and real-valued, and put*

$$S = \sum_{\underline{x} \in \mathfrak{A}} e(\mathfrak{F}(\underline{x})).$$

Then for each $d \geq 2$,

$$|S|^{2^{d-1}} \leq |\mathfrak{A}^D|^{2^{d-1}-d} \sum_{\underline{x}_1 \in \mathfrak{A}^D} \dots \sum_{\underline{x}_{d-1} \in \mathfrak{A}^D} \left| \sum_{\underline{x}_d \in \mathfrak{A}(\underline{x}_1, \dots, \underline{x}_{d-1})} e(\mathfrak{F}_d(\underline{x}_1, \dots, \underline{x}_d)) \right|.$$

Here $|\mathfrak{A}^D|$ of course means the cardinality of $\mathfrak{A}^D$. The lemma is a modern formulation of Weyl's inequality.

Proof. In

$$|S|^2 = \sum_{\underline{x} \in \mathfrak{A}} \sum_{\underline{y} \in \mathfrak{A}} e(\mathfrak{F}(\underline{x}) - \mathfrak{F}(\underline{y}))$$

set $\underline{x}_1 = \underline{x} - \underline{y}$, $\underline{x}_2 = \underline{y}$. Then $\underline{x}_1 \in \mathfrak{A}^D$ and $\underline{x}_2 \in \mathfrak{A} \cap (\mathfrak{A} - \underline{x}_1) = \mathfrak{A}(\underline{x}_1)$. We note that $\mathfrak{F}(\underline{x}) - \mathfrak{F}(\underline{y}) = \mathfrak{F}(\underline{x}_1 + \underline{x}_2) - \mathfrak{F}(\underline{x}_2) = \mathfrak{F}_2(\underline{x}_1, \underline{x}_2) - \mathfrak{F}_1(\underline{x}_1)$. Thus

$$|S|^2 = \sum_{\underline{x}_1 \in \mathfrak{A}^D} e(-\mathfrak{F}_1(\underline{x}_1)) \sum_{\underline{x}_2 \in \mathfrak{A}(\underline{x}_1)} e(\mathfrak{F}_2(\underline{x}_1, \underline{x}_2)) \leq \sum_{\underline{x}_1 \in \mathfrak{A}^D} \left| \sum_{\underline{x}_2 \in \mathfrak{A}(\underline{x}_1)} e(\mathfrak{F}_2(\underline{x}_1, \underline{x}_2)) \right|,$$

which is the case $d=2$ of the lemma.

For the step from d to $d+1$, we square the inequality of the lemma, and use Cauchy's inequality, to obtain

$$|S|^{2^d} \leq |\mathfrak{A}^D|^{2^d - 2d + d - 1} \sum_{\underline{x}_1 \in \mathfrak{A}^D} \dots \sum_{\underline{x}_{d-1} \in \mathfrak{A}^D} \left| \sum_{\underline{x}_d \in \mathfrak{A}(\underline{x}_1, \dots, \underline{x}_{d-1})} e(\mathfrak{F}_d(\underline{x}_1, \dots, \underline{x}_d)) \right|^2. \tag{11.2}$$

Denote the sum over $\underline{x}_d$ on the inside by S_d. Then S_d is like S, except that $\mathfrak{F}(\underline{X})$ is replaced by $\mathfrak{G}(\underline{X}) = \mathfrak{F}_d(\underline{x}_1, \dots, \underline{x}_{d-1}, \underline{X})$, and $\mathfrak{A}$ is replaced by $\mathfrak{A}(\underline{x}_1, \dots, \underline{x}_{d-1})$. By applying the case $d=2$ of the lemma, and observing (11.1) as well as the relation $\mathfrak{A}(\underline{x}_1, \dots, \underline{x}_{d-1})^D \subseteq \mathfrak{A}^D$, we get

$$|S_d|^2 \leqslant \sum_{\underline{x}_d \in \mathfrak{A}^D} \left| \sum_{\underline{x}_{d+1} \in \mathfrak{A}(\underline{x}_1, \ldots, \underline{x}_d)} e(\mathfrak{F}_{d+1}(\underline{x}_1, \ldots, \underline{x}_{d+1})) \right|.$$

By substituting this into (11.2) we get the desired result.

LEMMA 11.2. *Suppose $\mathfrak{F}$ is a form of degree $j>0$. Then*

(a) $\mathfrak{F}_d=0$ *when* $d>j$.

(b) $\mathfrak{F}_j(\underline{X}_1, \ldots, \underline{X}_j)$ *is multilinear.*

(c) *When* $1 \leqslant d<j$, *then*

$$\mathfrak{F}_d(\underline{X}_1, \ldots, \underline{X}_d) = \sum_{l=1}^{j-d+1} \mathfrak{G}_{d,l}(\underline{X}_1, \ldots, \underline{X}_d),$$

where $\mathfrak{G}_{d,l}$ is a form of degree l in $\underline{X}_d$, and a form of total degree $j-l$ in $\underline{X}_1, \ldots, \underline{X}_{d-1}$.

Proof. Since $\mathfrak{F}_d(0, \underline{X}_2, \ldots, \underline{X}_d)=0$, each monomial occurring in $\mathfrak{F}_d(\underline{X}_1, \ldots, \underline{X}_d)$ has some component of $\underline{X}_1$ as a factor. The same is true for $\underline{X}_2, \ldots, \underline{X}_d$. Since the total degree is j, each monomial has a degree between 1 and $j-d+1$ in each of $\underline{X}_1, \ldots, \underline{X}_d$. (In the case $d=1$, all but $\mathfrak{G}_{1,j}$ vanish identically.)

Now if $\mathfrak{F}$ is a form of degree d, then by (b), $\mathfrak{F}_d(\underline{X}_1, \ldots, \underline{X}_d)$ is symmetric and multilinear. Each of the 2^d summands in the definition of $\mathfrak{F}_d(\underline{X}, \ldots, \underline{X})$ is a multiple of $\mathfrak{F}(\underline{X})$, so that $\mathfrak{F}_d(\underline{X}, \ldots, \underline{X})=\varrho(d)\mathfrak{F}(\underline{X})$ with a numerical factor $\varrho(d)$. Taking $\mathfrak{F}(X)=X^d$ we see that $\varrho(d)=(-1)^d d!$. Thus

$$\mathfrak{F}_d(\underline{X}_1, \ldots, \underline{X}_d) = \mathfrak{F}(\underline{X}_1 | \ldots | \underline{X}_d), \tag{11.3}$$

where the right hand side is the multilinear form of the last section.

Write $|\mathfrak{F}|$ for the maximum absolute value of the coefficients of a polynomial $\mathfrak{F}$ with real coefficients. Write $\|\mathfrak{F}\|$ for the maximum of $\|f\|$ over the coefficients f of $\mathfrak{F}$.

LEMMA 11.3. *Suppose $\mathfrak{F}$ is a form of degree j. Then*

$$\|\mathfrak{F}_d\| \leqslant 2^d \cdot d^j \|\mathfrak{F}\|.$$

Proof. We have $\|\mathfrak{F}(\underline{X}_1+\ldots+\underline{X}_p)\| \leqslant p^j \|\mathfrak{F}\|$. Since $\mathfrak{F}_d$ consists of 2^d summands, each of the form $\pm\mathfrak{F}(\varepsilon_1 \underline{X}_1+\ldots+\varepsilon_d \underline{X}_d)$, the assertion follows. (It would not be difficult to prove a stronger assertion.)

LEMMA 11.4. *Suppose*

$$\mathfrak{F}(\underline{X}) = \mathfrak{F}^{(0)}+\mathfrak{F}^{(1)}(\underline{X})+\ldots+\mathfrak{F}^{(k)}(\underline{X})$$

where $\mathfrak{F}^{(j)}$ $(0\leqslant j\leqslant k)$ *is a form of degree* j *with real coefficients. Then*

(A) $\mathfrak{F}_k(\underline{X}_1,\dots,\underline{X}_k)=\mathfrak{F}^{(k)}(\underline{X}_1|\dots|\underline{X}_k)$.

(B) *Suppose that* $1\leqslant d<k$ *and that* $\|\mathfrak{F}^{(j)}\|\leqslant P^{\theta-j}$ *for* $d<j\leqslant k$, *where* $\theta\geqslant 0$, $P>1$. *Also suppose that* $\underline{x}_1,\dots,\underline{x}_{d-1}$ *are integer points in* $P\mathfrak{E}$. *(This last supposition is empty when* $d=1$.*) Then*

$$\mathfrak{F}_d(\underline{x}_1,\dots,\underline{x}_{d-1},\underline{X})=\mathfrak{F}^{(d)}(\underline{x}_1|\dots|\underline{x}_{d-1}|\underline{X})+\sum_{l=1}^{k-d+1}\mathfrak{G}_d^{(l)}(\underline{x}_1,\dots,\underline{x}_{d-1},\underline{X}),$$

where $\mathfrak{G}_d^{(l)}(\underline{X})=\mathfrak{G}_d^{(l)}(\underline{x}_1,\dots,\underline{x}_{d-1},\underline{X})$ *is a form in* $\underline{X}$ *of degree* l *with*

$$\|\mathfrak{G}_d^{(l)}\|\ll P^{\theta-l}\quad(1\leqslant l\leqslant k-d+1),$$

and with the constant in $\ll$ *depending only on* k, s.

Proof. (A) follows from Lemma 11.2 and from (11.3). As for (B),

$$\begin{aligned}\mathfrak{F}_d&=\mathfrak{F}_d^{(d)}+\sum_{j=d+1}^{k}\mathfrak{F}_d^{(j)}\\&=\mathfrak{F}_d^{(d)}+\sum_{j=d+1}^{k}\sum_{l=1}^{j-d+1}\mathfrak{G}_{d,l}^{(j)}\\&=\mathfrak{F}_d^{(d)}+\sum_{l=1}^{k-d+1}\mathfrak{G}_d^{(l)},\end{aligned}$$

where

$$\mathfrak{G}_d^{(l)}=\sum_{j=\max(d+1,\,l+d-1)}^{k}\mathfrak{G}_{d,l}^{(j)}.$$

Since $\|\mathfrak{G}_{d,l}^{(j)}\|\leqslant\|\mathfrak{F}_d^{(j)}\|\ll\|\mathfrak{F}^{(j)}\|$, and since $\mathfrak{G}_{d,l}^{(j)}$ is a form of degree $j-l$ in $\underline{X}_1,\dots,\underline{X}_{d-1}$, and since further $|\underline{x}_1|,\dots,|\underline{x}_{d-1}|$ are bounded by P, we see that (as a form in $\underline{X}$ only)

$$\begin{aligned}\|\mathfrak{G}_d^{(l)}\|&\ll\sum_{j=d+1}^{k}P^{j-l}\|\mathfrak{F}^{(j)}\|\\&\ll\sum_{j=d+1}^{k}P^{j-l}P^{\theta-j}\\&\ll P^{\theta-l}\quad(1\leqslant l\leqslant k-d+1).\end{aligned}$$

12. Predominantly linear exponential sums

Write $\beta\underline{x}=\beta_1 x_1+\ldots+\beta_s x_s$ for the standard inner product.

LEMMA 12.1. *Suppose* $\mathfrak{G}(\underline{X})=\mathfrak{G}^{(0)}+\mathfrak{G}^{(1)}(\underline{X})+\ldots+\mathfrak{G}^{(m)}(\underline{X})$, *where* $\mathfrak{G}^{(j)}$ *is a form of degree* j *with* $\|\mathfrak{G}^{(j)}\|\leqslant Q^{-j}$ $(j=1,\ldots,m)$ *with some given* $Q>1$. *Suppose that* $0<\delta<1$ *and that* $M_1,\ldots,M_s$ *lie in* $1\leqslant M_i\leqslant Q^{1-\delta}$ $(1\leqslant i\leqslant s)$. *Given* $\underline{\beta}$, *put*

$$S=\sum_{\substack{\underline{x}\\ 1\leqslant x_i<M_i}} e(\beta\underline{x}+\mathfrak{G}(\underline{x})).$$

Then

$$|S|\ll\prod_{i=1}^{s}\min(M_i,\|\beta_i\|^{-1}),$$

with the constant in $\ll$ *depending only on* m, s, δ.

Proof. We may suppose that the constant term $\mathfrak{G}^{(0)}=0$. We further may suppose without loss of generality that $|\mathfrak{G}^{(j)}|\leqslant Q^{-j}$ $(j=1,\ldots,m)$. For the vectors $\underline{x}$ of the sum, $|\mathfrak{G}^{(j)}(\underline{x})|\ll Q^{-j}Q^{(1-\delta)j}=Q^{-\delta j}$ $(j=1,\ldots,m)$, so that $|\mathfrak{G}(\underline{x})|\ll Q^{-\delta}$. Let l be an integer with $l\delta>s$, and put

$$\mathfrak{H}(\underline{X})=\sum_{n=0}^{l}(2\pi i\mathfrak{G}(\underline{X}))^n/n!.$$

Then

$$e(\mathfrak{G}(\underline{x}))=\mathfrak{H}(\underline{x})+O(\mathfrak{G}(\underline{x})^l)=\mathfrak{H}(\underline{x})+O(Q^{-l\delta})=\mathfrak{H}(\underline{x})+O(Q^{-s}),$$

and therefore

$$S=\sum_{\substack{\underline{x}\\ 1\leqslant x_i\leqslant M_i}} e(\beta\underline{x})\,\mathfrak{H}(\underline{x})+O(1). \tag{12.1}$$

We now write

$$\mathfrak{H}(\underline{X})=1+\mathfrak{H}^{(1)}(\underline{X})+\ldots+\mathfrak{H}^{(ml)}(\underline{X}) \tag{12.2}$$

where $\mathfrak{H}^{(j)}$ is a form of degree j. Our hypothesis implies that

$$|\mathfrak{H}^{(j)}|\ll Q^{-j}\quad(1\leqslant j\leqslant ml). \tag{12.3}$$

Now

$$\sum_{x=1}^{M} e(\beta x)\, x^t = \sum_{x=1}^{M} (x^t-(x-1)^t)\,(e(\beta x)+e(\beta(x+1))+\ldots+e(\beta M))$$

$$\ll \sum_{x=1}^{M} x^{t-1} \min(M, \|\beta\|^{-1})$$

$$\ll M^t \min(M, \|\beta\|^{-1}).$$

Hence for a monomial $\mathfrak{M}(\underline{X})=X_1^{j_1}\ldots X_s^{j_s}$ of total degree $j_1+\ldots+j_s=j$, we have

$$\sum_{\substack{\underline{x} \\ 1\leqslant x_i\leqslant M_i}} e(\underline{\beta}\underline{x})\,\mathfrak{M}(\underline{x}) \ll Q^j \prod_{i=1}^{s} \min(M_i, \|\beta_i\|^{-1}).$$

This, together with (12.1), (12.2), and (12.3), gives the desired result.

LEMMA 12.2. *Suppose* $\mathfrak{G}(\underline{X})=\mathfrak{G}^{(0)}+\mathfrak{G}^{(1)}(\underline{X})+\ldots+\mathfrak{G}^{(m)}(\underline{X})$ *where* $\mathfrak{G}^{(j)}$ *is a form of degree* j. *Suppose* $0\leqslant\theta<1/4$, $P>1$, *and suppose there is a natural* q *with*

$$q\leqslant P^{\theta} \quad \text{and} \quad \|q\mathfrak{G}^{(j)}\|\leqslant cP^{\theta-j} \quad (j=1,\ldots,m),$$

where c *is a constant. Given* $\underline{\beta}$ *and given a box* $\mathfrak{B}$ *with sides at most* 1, *write*

$$S=\sum_{\underline{x}\in P\mathfrak{B}} e(\underline{\beta}\underline{x}+\mathfrak{G}(\underline{x})).$$

Then for $\varepsilon>0$,

$$S \ll P^{2\theta s+\varepsilon} \prod_{i=1}^{s} \min(P^{1-2\theta}, \|q\beta_i\|^{-1}),$$

with a constant in $\ll$ *which depends only on* m, s, c, ε.

Proof. Choose δ with $0<\delta<1/2$, and put

$$Q=P^{1-2\theta-\delta}, \quad M=Q^{1-\delta}.$$

The box $P\mathfrak{B}$ may be split into $\ll(P/Mq)^s$ boxes with sides $\leqslant Mq$. In each such small box write $\underline{x}=\underline{a}+q\underline{y}$, where $\underline{a}$ runs through a residue system modulo q, and $\underline{y}$ runs through a box with sides $\leqslant M$. Given the small box and given the residue class $\underline{a}$, we have $\underline{x}=\underline{b}+q\underline{z}$, where $\underline{z}$ runs through a box $\mathfrak{B}(\underline{b})$ of the type $1\leqslant z_i\leqslant M_i$ with $M_i\leqslant M$ $(i=1,\ldots,s)$. Put

$$S(\underline{b}) = \sum_{z \in \mathfrak{B}(\underline{b})} e(q\underline{\beta}z + \mathfrak{G}(\underline{b}+q\underline{z})).$$

Since the number of possibilities for $\underline{b}$ is

$$\ll (P/Mq)^s q^s = (P/M)^s \ll P^{2\theta s + 2\delta s},$$

and since δ may be chosen arbitrarily small, it will suffice for us to show that

$$S(\underline{b}) \ll \prod_{i=1}^{s} \min(P^{1-2\theta}, \|q\beta_i\|^{-1}).$$

Now $\mathfrak{G}^{(l)}(\underline{X}+\underline{Y}) = \mathfrak{H}^{(l)}(\underline{X}, \underline{Y}) = \mathfrak{H}_l^{(0)}(\underline{X}, \underline{Y}) + \ldots + \mathfrak{H}_l^{(l)}(\underline{X}, \underline{Y})$, say, where each term is a form of total degree l in $\underline{X}$, $\underline{Y}$, and where $\mathfrak{H}_l^{(j)}$ is of degree j in $\underline{Y}$ and of degree $l-j$ in $\underline{X}$. Clearly

$$\|q\mathfrak{H}_l^{(j)}\| \leqslant \|q\mathfrak{H}^{(l)}\| \leqslant 2^l \|q\mathfrak{G}^{(l)}\|.$$

For fixed $\underline{b}$ we have

$$\begin{aligned}\mathfrak{G}^{(l)}(\underline{b}+q\underline{Z}) &= \mathfrak{H}_l^{(0)}(\underline{b}) + q\mathfrak{H}_l^{(1)}(\underline{b}, \underline{Z}) + \ldots + q^l \mathfrak{H}_l^{(l)}(\underline{b}, \underline{Z}) \\ &= \mathfrak{R}_l^{(0)} + \mathfrak{R}_l^{(1)}(\underline{Z}) + \ldots + \mathfrak{R}_l^{(l)}(\underline{Z}),\end{aligned}$$

say, where $\mathfrak{R}_l^{(j)}$ is a form of degree j. Since $|\underline{b}| \ll P$, we obtain for $j = 1, \ldots, l$ that

$$\begin{aligned}\|\mathfrak{R}_l^{(j)}\| &\ll q^{j-1}|\underline{b}|^{l-j}\|q\mathfrak{G}^{(l)}\| \ll q^j P^{l-j} P^{\theta-l} \\ &= P^{\theta}(P/q)^{-j} \ll P^{\theta} P^{j(\theta-1)} \ll Q^{-j(1+\delta)}.\end{aligned}$$

Now

$$\mathfrak{G}(\underline{b}+q\underline{Z}) = \mathfrak{R}^{(0)} + \mathfrak{R}^{(1)}(\underline{Z}) + \ldots + \mathfrak{R}^{(m)}(\underline{Z})$$

with $\mathfrak{R}^{(j)} = \mathfrak{R}_j^{(j)} + \mathfrak{R}_{j+1}^{(j)} + \ldots + \mathfrak{R}_m^{(j)}$ $(j = 0, 1, \ldots, m)$, so that

$$\|\mathfrak{R}^{(j)}\| \leqslant Q^{-j} \quad (j = 1, \ldots, m)$$

if P and hence Q is large. Lemma 12.1 yields

$$S(\underline{b}) \ll \prod_{i=1}^{s} \min(M, \|q\beta_i\|^{-1}).$$

13. Exponential sums and multilinear inequalities

LEMMA 13.1. *Suppose* $\mathfrak{F}(\underline{X}) = \mathfrak{F}^{(0)} + \mathfrak{F}^{(1)}(\underline{X}) + \ldots + \mathfrak{F}^{(k)}(\underline{X})$, *where* $\mathfrak{F}^{(j)}$ *is a form of degree* j *with real coefficients. Let* $\mathfrak{B}$ *be a box with sides* $\leqslant 1$, *let* $P > 1$, *and put*

$$S = \sum_{\underline{x} \in P\mathfrak{B}} e(\mathfrak{F}(\underline{x})).$$

Now let $2 \leqslant d \leqslant k$ *and* $\varepsilon > 0$. *Suppose that either* $d=k$, *and put* $\theta=0$ *and* $q=1$. *Or else, suppose that* $2 \leqslant d < k$, *that* $0 \leqslant \theta < 1/4$, *and that there is a natural*

$$q \leqslant P^{\theta} \quad \text{with } \|q\mathfrak{F}^{(j)}\| \leqslant P^{\theta - j} \quad \text{for } d < j \leqslant k.$$

Then

$$|S|^{2^{d-1}} \ll P^{(2^{d-1}-d+2\theta)s+\varepsilon} \sum \left(\prod_{i=1}^{s} \min (P^{1-2\theta}, \|q\mathfrak{F}^{(d)}(\underline{x}_1|\dots|\underline{x}_{d-1}|\underline{e}_i)\|^{-1}) \right),$$

where the sum Σ *is over* $(d-1)$*-tuples of integer points* $\underline{x}_1, \dots, \underline{x}_{d-1}$ *in* $P\mathfrak{E}$, *where* $\underline{e}_1, \dots, \underline{e}_s$ *are the basis vectors, and where the constant in* $\ll$ *depends only on* s, k, ε.

Proof. The case $d=k$ is e.g. Lemma 2.1 of Birch [2]. But Birch does not give details of the proof and refers to Davenport [3], who did the case $k=3$. Hence it seems appropriate to go into the details.

Our hypothesis on $\mathfrak{B}$ implies that $(P\mathfrak{B})^D \subseteq P\mathfrak{E}$. Lemma 11.1 gives

$$|S|^{2^{d-1}} \ll (P^{(2^{d-1}-d)s} \sum_{\underline{x}_1 \in P\mathfrak{E}} \dots \sum_{\underline{x}_{d-1} \in P\mathfrak{E}} \left| \sum_{\underline{x} \in (P\mathfrak{B})(\underline{x}_1, \dots, \underline{x}_{d-1})} e(\mathfrak{F}_d(\underline{x}_1, \dots, \underline{x}_{d-1}, \underline{x}_d)) \right|. \quad (13.1)$$

In the case when $d=k$,

$$\mathfrak{F}_d(\underline{x}_1, \dots, \underline{x}_{d-1}, \underline{X}) = \underline{\beta} \underline{X}$$

with

$$\beta_i = \mathfrak{F}_d^{(d)}(\underline{x}_1, \dots, \underline{x}_{d-1}, \underline{e}_i) = \mathfrak{F}^{(d)}(\underline{x}_1|\dots|\underline{x}_{d-1}|\underline{e}_i) \quad (i = 1, \dots, s). \quad (13.2)$$

Hence a bound

$$\ll \prod_{i=1}^{s} \min (P, \|\beta_i\|^{-1})$$

holds for the inner sum in (13.1). In the case when $2 \leqslant d < k$, Lemma 11.4 tells us that

$$\mathfrak{F}_d(\underline{x}_1, \dots, \underline{x}_{d-1}, \underline{X}) = \underline{\beta} \underline{X} + \sum_{l=1}^{k-d+1} \mathfrak{G}_d^{(l)}(\underline{X})$$

where β is given by (13.2) and where $\mathfrak{G}_d^{(l)}$ is a form of degree l with

$$\|q\mathfrak{G}_d^{(l)}\| \ll P^{\theta-l} \quad (l=1,\dots,k-d+1).$$

Now Lemma 12.2 gives a bound

$$\ll P^{2\theta s+\varepsilon} \prod_{i=1}^{s} \min(P^{1-2\theta}, \|q\beta_i\|^{-1})$$

for the inner sum in (13.1).

LEMMA 13.2. *Make all the assumption of the preceding lemma. Suppose further that*

$$|S| \geqslant P^{s-K} \tag{13.3}$$

where $K>0$. Then the number N of $(d-1)$-tuples of integer points $\underline{x}_1,\dots,\underline{x}_{d-1}$ in $P\mathfrak{C}$ with

$$\|q\mathfrak{F}^{(d)}(\underline{x}_1|\dots|\underline{x}_{d-1}|\underline{e}_i)\| < P^{-1+2\theta} \quad (i=1,\dots,s) \tag{13.4}$$

satisfies

$$N \gg P^{s(d-1)-2^{d-1}K-\varepsilon}, \tag{13.5}$$

with a constant in $\gg$ depending only on s, k, ε.

Proof. Let $N_0(\underline{x}_1,\dots,\underline{x}_{d-2})$ be the number of points $\underline{x}_{d-1} \in P\mathfrak{C}$ with (13.4). Then $N=N_0$ when $d=2$, and

$$N = \sum_{\underline{x}_1 \in P\mathfrak{C}} \dots \sum_{\underline{x}_{d-2} \in P\mathfrak{C}} N_0(\underline{x}_1,\dots,\underline{x}_{d-2}) \tag{13.6}$$

when $d>2$. It will be convenient to set

$$J = P^{1-2\theta}, \tag{13.7}$$

and to write $\{\alpha\}$ for the fractional part of a real number α. Then for any set of integer points $\underline{x}_1,\dots,\underline{x}_{d-2}$ and any integers $a_1,\dots,a_s$ with $0 \leqslant a_i < J$, the inequalities

$$J^{-1}a_i \leqslant \{q\mathfrak{F}^{(d)}(\underline{x}_1|\dots|\underline{x}_{d-2}|\underline{x}_{d-1}|\underline{e}_i)\} < J^{-1}(a_i+1) \quad (1 \leqslant i \leqslant s)$$

cannot hold for more than $N_0(\underline{x}_1,\dots,\underline{x}_{d-2})$ integer points $\underline{x}_{d-1}$ lying in a prescribed

box of side P: for if $\underline{x}'_{d-1}$ is one solution of these inequalities, and if $\underline{x}_{d-1}$ denotes the general solution, then

$$\|q\mathfrak{F}^{(d)}(\underline{x}_1|\dots|\underline{x}_{d-2}|\underline{x}_{d-1}-\underline{x}'_{d-1}|\underline{e}_i)\| < J^{-1} \quad (i=1,\dots,s),$$

and $\underline{x}_{d-1}-\underline{x}'_{d-1}\in P\mathfrak{E}$. Thus the number of possibilities for $\underline{x}_{d-1}$ is indeed at most $N_0(\underline{x}_1,\dots,\underline{x}_{d-2})$.

Dividing the cube $P\mathfrak{E}$ into 2^s cubes of side P, we obtain

$$\begin{aligned}\sum_{\underline{x}_{d-1}\in P\mathfrak{E}} &\left(\prod_{i=1}^{s}\min(J, \|q\mathfrak{F}^{(d)}(\underline{x}_1|\dots|\underline{x}_{d-2}|\underline{x}_{d-1}|\underline{e}_i)\|^{-1})\right)\\ &\ll N_0(\underline{x}_1,\dots,\underline{x}_{d-2})\sum_{a_1=0}^{[J]}\dots\sum_{a_s=0}^{[J]}\left(\prod_{i=1}^{s}\min\left(J,\max\left(\frac{J}{a_i},\frac{J}{|J-a_i-1|}\right)\right)\right)\\ &\ll N_0(\underline{x}_1,\dots,\underline{x}_{d-2})J^s(\log J)^s.\end{aligned}$$

In conjunction with (13.6), (13.7), and the preceding lemma, this gives

$$|S|^{2^{d-1}} \ll NP^{(2^{d-1}-d+1)s+2\varepsilon}.$$

Since $\varepsilon>0$ is arbitrary here, the hypothesis (13.3) yields the desired conclusion.

14. An application of the geometry of numbers

LEMMA 14.1. *Let*

$$\mathfrak{L}_i(\underline{X}) = \lambda_{i1}X_1+\dots+\lambda_{is}X_s \quad (i=1,\dots,s)$$

be linear forms with $\lambda_{ij}=\lambda_{ji}$ $(1\leqslant i,j\leqslant s)$. Given $A>1$ and $Z>0$, let $N(Z)$ be the number of integer points $\underline{x}$ with

$$|\underline{x}|\leqslant ZA \quad \textit{and} \quad \|\mathfrak{L}_i(\underline{X})\|\leqslant ZA^{-1} \quad (i=1,\dots,s). \tag{14.1}$$

Then for $0<Z_1\leqslant Z_2<1$ we have

$$N(Z_1) \gg (Z_1/Z_2)^s N(Z_2),$$

with a constant in $\gg$ which depends only on s.

Proof. See Davenport [3, Lemma 3.3]. Davenport has strict inequalities in (14.1), but it is easily seen that this does not matter.

COROLLARY 1. *Suppose that* $1<R\leqslant P<J$, *and let*

$$N \text{ be the number of } |\underline{x}|\leqslant P \text{ with } \|\mathfrak{L}_i(\underline{x})\|\leqslant J^{-1} \quad (i=1,\dots,s)$$

$$N' \text{ be the number of } |\underline{x}|\leqslant R \text{ with } \|\mathfrak{L}_i(\underline{x})\|\leqslant J^{-1}RP^{-1} \quad (i=1,\dots,s).$$

Then

$$N' \gg (R/P)^s N. \tag{14.2}$$

Proof. Apply the lemma with $A=(PJ)^{1/2}$, $Z_2=(P/J)^{1/2}$, $Z_1=R/A$.

COROLLARY 2. *Suppose that* $6<R\leqslant J\leqslant P$. *Define* N *as in Corollary* 1, *and let*

$$N'' \text{ be the number of } |\underline{x}|\leqslant R \text{ with } \|\mathfrak{L}_i(\underline{x})\|\leqslant J^{-2}R \quad (i=1,\dots,s).$$

Then

$$N'' \gg (R/P)^s N.$$

Proof. Divide the cube $|\underline{x}|\leqslant P$ into cubes of side $\leqslant(1/3)J$, more precisely into $\ll(P/J)^s$ such cubes. One of these subcubes will contain $\gg(J/P)^s N$ points $\underline{x}$ with $\|\mathfrak{L}_i(\underline{x})\|\leqslant J^{-1}$ $(i=1,\dots,s)$. If $\underline{x}^*$ is a fixed one of these points and $\underline{x}$ any one of these points, then $\underline{y}=\underline{x}-\underline{x}^*\in(1/3)J\mathfrak{E}$ and $\|\mathfrak{L}_i(\underline{y})\|\leqslant(J/2)^{-1}$. By Corollary 1, applied with $(1/6)R$, $(1/3)J$, $(1/2)J$ in place of R, P, J, we find that the number of $|\underline{x}|\leqslant R$ with $\|\mathfrak{L}_i(\underline{x})\|\leqslant J^{-2}R$ $(i=1,\dots,s)$ is

$$\gg (R/2J)^s (J/P)^s N \gg (R/P)^s N.$$

LEMMA 14.2. *Make the same assumptions as in Lemma* 13.2. *Suppose* $\eta>0$, *and*

$$\eta+4\theta\leqslant 1. \tag{14.3}$$

Then the number $N(\eta)$ *of* $(d-1)$*-tuples*

$$\underline{x}_1,\dots,\underline{x}_{d-1} \quad \text{in } P^\eta\mathfrak{E}$$

with

$$\|q\mathfrak{F}^{(d)}(\underline{x}_1|\dots|\underline{x}_{d-1}|\underline{e}_i)\|\leqslant P^{-d+4\theta+(d-1)\eta} \quad (i=1,\dots,s)$$

satisfies

$$N(\eta)\gg P^{s(d-1)\eta-2^{d-1}K-\varepsilon},$$

with the constant in $\gg$ *dependent only on* s, k, η, ε.

Proof. For fixed $\underline{x}_2, \ldots, \underline{x}_{d-1}$, let

$$\mathfrak{L}_i(\underline{X}) = q\mathfrak{F}^{(d)}(\underline{X}|\underline{x}_2|\ldots|\underline{x}_{d-1}|\underline{e}_i).$$

Put $J=P^{1-2\theta}$, $R=\frac{1}{2}P^{\eta}$, and let $N_1(\underline{x}_2, \ldots, \underline{x}_{d-1})$ be the number of

$$\underline{x}_1 \in P\mathfrak{E} \quad \text{with } \|\mathfrak{L}_i(\underline{x}_1)\| \leqslant J^{-1} \quad (i=1, \ldots, s).$$

By Lemma 13.2,

$$\sum_{\underline{x}_2 \in P\mathfrak{E}} \cdots \sum_{\underline{x}_{d-1} \in P\mathfrak{E}} N_1(\underline{x}_2, \ldots, \underline{x}_{d-1}) \gg P^{s(d-1)-2^{d-1}K-\varepsilon}.$$

Let $N_1''(\underline{x}_2, \ldots, \underline{x}_{d-1})$ be the number of

$$\underline{x}_1 \in P^{\eta}\mathfrak{E} \quad \text{with } \|\mathfrak{L}_i(\underline{x}_1)\| \leqslant J^{-2}R = \tfrac{1}{2}P^{-2+4\theta+\eta} \quad (i=1, \ldots, s).$$

We infer from Corollary 2 that

$$N_1''(\underline{x}_2, \ldots, \underline{x}_{d-1}) \gg P^{(\eta-1)s} N_1(\underline{x}_2, \ldots, \underline{x}_{d-1}).$$

Therefore the number of $(d-1)$-tuples $\underline{x}_1, \ldots, \underline{x}_{d-1}$ with

$$\underline{x}_1 \in P^{\eta}\mathfrak{E}, \quad \underline{x}_2 \in P\mathfrak{E}, \quad \ldots, \quad \underline{x}_{d-1} \in P\mathfrak{E}$$

and with

$$\|q\mathfrak{F}^{(d)}(\underline{x}_1|\ldots|\underline{x}_{d-1}|\underline{e}_i)\| \leqslant \tfrac{1}{2}P^{-2+4\theta+\eta} \quad (i=1, \ldots, s)$$

is

$$\gg P^{s(d-2+\eta)-2^{d-1}K-\varepsilon}.$$

Next, for fixed $\underline{x}_1, \underline{x}_3, \ldots, \underline{x}_{d-1}$, let

$$\mathfrak{L}_i(\underline{X}) = q\mathfrak{F}^{(d)}(\underline{x}_1|\underline{X}|\underline{x}_3|\ldots|\underline{x}_{d-1}|\underline{e}_i) \quad (i=1, \ldots, s).$$

Put $J=2P^{2-4\theta-\eta}$, $R=P^{\eta}$, and let $N_2(\underline{x}_1, \underline{x}_3, \ldots, \underline{x}_{d-1})$ be the number of

$$\underline{x}_2 \in P\mathfrak{E} \quad \text{with } \|\mathfrak{L}_i(\underline{x}_2)\| \leqslant J^{-1} \quad (i=1, \ldots, s).$$

We have just seen that

$$\sum_{\underline{x}_1 \in P^{\eta}\mathfrak{E}} \sum_{\underline{x}_3 \in P\mathfrak{E}} \cdots \sum_{\underline{x}_{d-1} \in P\mathfrak{E}} N_2(\underline{x}_1, \underline{x}_3, \ldots, \underline{x}_{d-1}) \gg P^{s(d-2+\eta)-2^{d-1}K-\varepsilon}.$$

Let $N_2'(\underline{x}_1, \underline{x}_3, \dots, \underline{x}_{d-1})$ be the number of

$$\underline{x}_2 \in P^\eta \mathfrak{E} \quad \text{with } \|\mathfrak{L}_i(\underline{x}_2)\| \leqslant J^{-1}RP^{-1} = \tfrac{1}{2}P^{-3+4\theta+2\eta} \quad (i = 1, \dots, s).$$

We infer from Corollary 1 that

$$N_2'(\underline{x}_1, \underline{x}_3, \dots, \underline{x}_{d-1}) \gg P^{(\eta-1)s} N_2(\underline{x}_1, \underline{x}_3, \dots, \underline{x}_{d-1}).$$

Hence the number of $(d-1)$-tuples

$$\underline{x}_1 \in P^\eta \mathfrak{E}, \quad \underline{x}_2 \in P^\eta \mathfrak{E}, \quad \underline{x}_3 \in P\mathfrak{E}, \quad \dots, \quad \underline{x}_{d-1} \in P\mathfrak{E}$$

with

$$\|q\underline{\mathfrak{F}}^{(d)}(\underline{x}_1 | \dots | \underline{x}_{d-1} | \underline{e}_i)\| \leqslant \tfrac{1}{2}P^{-3+4\theta+2\eta} \quad (i = 1, \dots, s)$$

is

$$\gg P^{s(d-3+2\eta)-2^{d-1}K-\varepsilon}.$$

Continuing with this process, considering $\underline{x}_3, \dots, \underline{x}_{d-1}$ in turn, and applying Corollary 1 each time, we finally obtain the desired conclusion.

15. Systems of forms

Let $\underline{\mathfrak{F}} = (\underline{\mathfrak{F}}^{(k)}, \dots, \underline{\mathfrak{F}}^{(2)})$ be a system of forms as in (1.7) and with integer coefficients, and let $\underline{\alpha} = (\underline{\alpha}^{(k)}, \dots, \underline{\alpha}^{(2)})$ be as in (4.1). Further let $\mathfrak{M}_d = \mathfrak{M}(\underline{\mathfrak{F}}^{(d)})$ $(2 \leqslant d \leqslant k)$ be the manifolds of § 10.

LEMMA 15.1. *Suppose that $K>0$, $\varepsilon>0$, and that $2 \leqslant d \leqslant k$. Suppose that either $d=k$, in which case set $\theta=0$ and $q=1$. Or else, suppose that $2 \leqslant d < k$ with $r_d>0$, that $0 \leqslant \theta < 1/4$, and that there is a natural*

$$q \leqslant P^\theta \quad \text{with } \|q\underline{\alpha}^{(j)}\| \leqslant P^{\theta-j} \quad \text{for} \quad d < j \leqslant k. \tag{15.1}$$

Given a box $\mathfrak{B}$ with sides $\leqslant 1$, and given $P>1$, define the sum $S(\underline{\alpha})$ as in (4.2). *Given $\eta>0$ with* (14.3), *one of the following three alternatives must hold. Either*

(i) $|S(\underline{\alpha})| \leqslant P^{s-K}$, *or*

(ii) *there is a natural*

$$n \ll P^{r_d(d-1)\eta} \quad \text{with} \quad \|nq\underline{\alpha}^{(d)}\| \ll P^{-d+4\theta+r_d(d-1)\eta}, \quad \text{or}$$

(iii) $z_R(\mathfrak{M}_d) \gg R^{(d-1)s-2^{d-1}(K/\eta)-\varepsilon}$

holds with $R=P^{\eta}$. The constants in $\ll$ and $\gg$ here depend only on $s, k, r_k, \ldots, r_2, \eta, \varepsilon$, and $\underset{\sim}{\mathfrak{F}}$, and hence only on $\underset{\sim}{\mathfrak{F}}, \eta, \varepsilon$.

Proof. We have $\alpha\underset{\sim}{\mathfrak{F}}=\mathfrak{F}^{(2)}+\ldots+\mathfrak{F}^{(k)}$ with $\mathfrak{F}^{(d)}=\alpha^{(d)}\underset{\sim}{\mathfrak{F}}^{(d)}$. In the case when $2\leqslant d<k$, the hypothesis (15.1) implies that $\|q\mathfrak{F}^{(j)}\|\ll P^{\theta-j}$ for each j in $d<j\leqslant k$, with a constant in $\ll$ which depends only on $\underset{\sim}{\mathfrak{F}}^{(j)}$. It is clear that Lemmas 13.1, 13.2 and 14.2 hold with this slightly weaker assumption. In particular we may apply Lemma 14.2 when (i) fails. Then the number $N(\eta)$ of integer $(d-1)$-tuples $\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_{d-1}$ in $R\mathfrak{E}$ with

$$\|q\alpha^{(d)}\underset{\sim}{\mathfrak{F}}^{(d)}(\underset{\sim}{x}_1|\ldots|\underset{\sim}{x}_{d-1}|\underset{\sim}{e}_i)\| \leqslant 6P^{-d+4\theta+(d-1)\eta} \quad (i=1,\ldots,s) \tag{15.2}$$

satisfies

$$N(\eta) \gg R^{s(d-1)-2^{d-1}(K/\eta)-\varepsilon}.$$

Suppose $\underset{\sim}{\mathfrak{F}}^{(d)}=(\mathfrak{F}_1^{(d)}, \ldots, \mathfrak{F}_{r_d}^{(d)})$. Given $\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_{d-1}$ as above, form the matrix

$$(m_{ij}) = (\mathfrak{F}_j^{(d)}(\underset{\sim}{x}_1|\ldots|\underset{\sim}{x}_{d-1}|\underset{\sim}{e}_i)) \quad (1\leqslant i\leqslant s,\ 1\leqslant j\leqslant r_d).$$

Now if this matrix has rank less than r_d for each of the $(d-1)$-tuples counted by $N(\eta)$, then clearly alternative (iii) holds. Hence we may suppose that one at least of these matrices has rank r_d. We may suppose that the submatrix with $1\leqslant i\leqslant r_d$ is nonsingular. Write n for the absolute value of the determinant of this submatrix. We have

$$m_{ij} \ll R^{d-1},$$

and hence

$$n \ll R^{r_d(d-1)} = P^{r_d(d-1)\eta}.$$

From (15.2) we have

$$q\sum_{j=1}^{r_d} \alpha_j^{(d)} m_{ij} = b_i+\varrho_i \quad (1\leqslant i\leqslant s),$$

where the b_i are integers and the ϱ_i are bounded by the right hand side of (15.2). Let $a_1, \ldots, a_{r_d}$ be the solution of the system of linear equations

$$\sum_{j=1}^{r_d} a_j m_{ij} = nb_i \quad (1\leqslant i\leqslant r_d). \tag{15.3}$$

Then

$$\sum_{j=1}^{r_d} (qn\alpha_j^{(d)} - a_j)\, m_{ij} = n\varrho_i \quad (1 \leqq i \leqq r_d). \tag{15.4}$$

Cramér's rule applied to (15.3) shows that the a_j are integers, and applied to (15.4) it shows that

$$\|qn\alpha_j^{(d)}\| \leqq |qn\alpha_j^{(d)} - a_j| \ll R^{(d-1)(r_d-1)} P^{-d+4\theta+(d-1)\eta}$$
$$= P^{-d+4\theta+(d-1)r_d\eta}.$$

The proof of Lemma 15.1 is complete.

For d with $r_d > 0$, define $g_d = g(\underline{\mathfrak{F}}^{(d)})$ and γ_d as in § 10, and put

$$\gamma'_d = 2^{d-1}/g_d = \gamma_d/((d-1)r_d). \tag{15.5}$$

The third alternative of Lemma 15.1 may not happen for large P if $2^{d-1}K/\eta < g_d$. In particular it may not happen with $\eta = K\gamma'_d + \varepsilon$. The condition (14.3) is fulfilled when $4\theta + K\gamma'_d < 1$ and when $\varepsilon > 0$ is sufficiently small.

COROLLARY. *Let* $\underline{\mathfrak{F}} = (\underline{\mathfrak{F}}^{(k)}, \ldots, \underline{\mathfrak{F}}^{(2)})$, $\underline{\alpha} = (\underline{\alpha}^{(k)}, \ldots, \underline{\alpha}^{(2)})$ *and* P *be as above. Suppose either that* $d = k$, *in which case set* $\theta = 0$, $q = 1$. *Or suppose that* $2 \leqq d < k$, *that* $r_d > 0$, *that* $0 \leqq \theta < 1/4$, *and that there is a natural* q *with* (15.1). *Suppose that* $\varepsilon > 0$, *and that* $K > 0$ *satisfies*

$$4\theta + K\gamma'_d < 1 \tag{15.6}$$

Then either

(i) $|S(\underline{\alpha})| \leqq P^{s-K}$, *or*

(ii) *there is a natural* n *with*

$$n \ll P^{K\gamma_d+\varepsilon} \quad \text{and} \quad \|nq\underline{\alpha}^{(d)}\| \ll P^{-d+4\theta+K\gamma_d+\varepsilon}.$$

The constant in $\ll$ *depends only on* $\underline{\mathfrak{F}}, \eta$ *and* ε.

In particular, when $K\gamma'_k < 1$ and when

$$|S(\underline{\alpha})| > P^{s-K},$$

there is an n_k with

$$n_k \ll P^{K\gamma_k+\varepsilon} \quad \text{and} \quad \|n_k \underline{\alpha}^{(k)}\| \ll P^{-k+K\gamma_k+\varepsilon}. \tag{15.7}$$

Suppose now that $r_{k-1}>0$ and that $4K\gamma_k+K\gamma'_{k-1}<1$. When ε is sufficiently small we may apply the corollary with $d=k-1$, $\theta=K\gamma_k+\varepsilon$ and $q=n_k$. (Clearly everything works, even though the $\leqslant$ in (15.1) is replaced by $\ll$ in (15.7).) We infer that there is a natural n_{k-1} with

$$n_{k-1}\ll P^{K\gamma_{k-1}+\varepsilon} \quad \text{and} \quad \|n_k n_{k-1}\underline{\alpha}^{(k-1)}\|\ll P^{-(k-1)+4K\gamma_k+K\gamma_{k-1}+\varepsilon}. \tag{15.8}$$

(Actually one obtains multiples of ε in the exponents, but since $\varepsilon>0$ was arbitrary these multiples may be replaced by ε itself.) In the case when $r_{k-1}=0$ we have $\gamma_{k-1}=0$, and (15.8) is trivially satisfied with $n_{k-1}=1$. Now when $4^2K\gamma_k+4K\gamma_{k-1}+K\gamma'_{k-2}<1$, the argument may be repeated. Ultimately we obtain

LEMMA 15.2. *Put*

$$\tau_d=\gamma_d+4\gamma_{d+1}+\ldots+4^{k-d}\gamma_k \quad (2\leqslant d\leqslant k).$$

Suppose that $\varepsilon>0$, and that $K>0$ has

$$K\tau_2<1 \tag{15.9}$$

Given $\mathfrak{F}$, $\underline{\alpha}$ and P as above, we either have

(i) $|S(\underline{\alpha})|\leqslant P^{s-K}$, *or*

(ii) *there are natural numbers $n_k, n_{k-1}, \ldots, n_2$ with*

$$n_d\ll P^{K\gamma_d+\varepsilon} \tag{15.10}$$

and

$$\|n_k\ldots n_d\underline{\alpha}^{(d)}\|\ll P^{-d+K\tau_d+\varepsilon} \quad (2\leqslant d\leqslant k). \tag{15.11}$$

Proof of Proposition II_0. We apply the corollary to Lemma 15.1 with $d=k$. We suppose (10.6) to hold, so that $\Omega\gamma_d<1$. We set $K=\Delta\Omega$, so that $K\gamma_d+\varepsilon<\Delta$ when $\varepsilon>0$ is small. Thus when P is large, say when $P\geqslant P_1(\mathfrak{F},\Omega,\Delta)$, then either

(i) $|S(\underline{\alpha})|\leqslant P^{s-\Delta\Omega}$, or

(ii) there is a q with

$$q\leqslant P^{\Delta} \quad \text{and} \quad \|q\underline{\alpha}\|\leqslant P^{-d+\Delta}.$$

But what about the condition (15.6)? In our context this condition means that $K\gamma'_d<1$, and for this it suffices that $K\gamma'_d\leqslant\Omega\gamma_d$, i.e. that $\Delta\gamma'_d\leqslant\gamma_d$, i.e. that $\Delta\leqslant(d-1)r$. We are thus left with the case when

$$\Delta > (d-1)r.$$

But in this case (ii) (of the Hypothesis) is always true by Dirichlet's Theorem on approximation.

In our lemmas we supposed that $\mathfrak{B}$ had sides $\leqslant 1$. But clearly the proposition is true in general with $P \geqslant P_1(\underline{\mathfrak{F}}, \Omega, \Delta, \mathfrak{B})$.

Proof of Proposition II. We apply Lemma 15.2 with $K=\Delta\Omega$. In view of (10.10) we have $\Omega\tau<1$. Setting $q=n_k n_{k-1} \dots n_2$ we have

$$q \ll P^{K\tau+\varepsilon} \quad \text{and} \quad \|q\underline{\alpha}^{(d)}\| \ll P^{-d+K\tau+\varepsilon} \quad (2 \leqslant d \leqslant k),$$

since $\tau_d+\gamma_{d-1}+\dots+\gamma_2 \leqslant \tau_2=\tau$ $(2 \leqslant d \leqslant k)$. Here $K\tau+\varepsilon=\Delta\Omega\tau+\varepsilon<\Delta$ if $\varepsilon>0$ is sufficiently small. Thus, as in the proof of Proposition II_0, either (i) or (ii) holds. In our present context, (15.9) becomes $\Delta\Omega\tau<1$, which is true for $\Delta \leqslant 1$. Hence $\underline{\mathfrak{F}}$ satisfies the restricted Hypothesis.

D. The invariants g and h

16. Invariants $g_{\mathbf{C}}$ and $h_{\mathbf{C}}$

In this section we will introduce quantities $g_{\mathbf{C}}$ and $h_{\mathbf{C}}$ which are easier to handle than g and h.

If $\mathfrak{F}$ is a form of degree $d>1$ with complex coefficients, let $h_{\mathbf{C}}=h_{\mathbf{C}}(\mathfrak{F})$ be the least number h such that $\mathfrak{F}$ may be written in the form (1.5), where the $\mathfrak{A}_i$, $\mathfrak{B}_i$ are forms of positive degrees with *complex* coefficients. Given an r-tuple $\underline{\mathfrak{F}}$ of forms of degree d, let $h_{\mathbf{C}}(\underline{\mathfrak{F}})$ be the minimum of $h_{\mathbf{C}}(\mathfrak{F})$ over all forms of $\mathfrak{F}$ of the complex pencil of $\underline{\mathfrak{F}}$. Define the manifold $\mathfrak{M}=\mathfrak{M}(\underline{\mathfrak{F}})$ as in § 10, and put

$$g_{\mathbf{C}} = \operatorname{codim} \mathfrak{M}.$$

LEMMA 16.1. $g_{\mathbf{C}} \leqslant 2^{d-1} h_{\mathbf{C}}$.

Proof. We may suppose that $\underline{\mathfrak{F}}=(\mathfrak{F}_1, \dots, \mathfrak{F}_r)$ and that $\mathfrak{F}_1$ may be written as in (1.5) with $h=h_{\mathbf{C}}$. Write $e(i)=\deg \mathfrak{A}_i$, $f(i)=\deg \mathfrak{B}_i$, so that $e(i)+f(i)=d$ $(1 \leqslant i \leqslant h_{\mathbf{C}})$. It is easily seen that the multilinear form $\mathfrak{F}_1(\underline{X}_1|\dots|\underline{X}_d)$ is a sum of products

$$\mathfrak{A}_i(\underline{X}_{j_1}|\dots|\underline{X}_{j_{e(i)}})\,\mathfrak{B}_i(\underline{X}_{k_1}|\dots|\underline{X}_{k_{f(i)}}),$$

where $1 \leqslant i \leqslant h_{\mathbf{C}}$ and where $j_1<\dots<j_{e(i)}$ and $k_1<\dots<k_{f(i)}$ are disjoint subsets of $\{1, \dots, d\}$. A point $(\underline{x}_1, \dots, \underline{x}_{d-1})$ will certainly lie in $\mathfrak{M}$ if

$$\mathfrak{A}_i(\underline{x}_{j_1}|\dots|\underline{x}_{j_{e(i)}})=0$$

for $1\leqslant i\leqslant h_{\mathbf{C}}$ and any $1\leqslant j_1<\dots<j_{e(i)}\leqslant d-1$, and if furthermore

$$\mathfrak{B}_i(\underline{x}_{k_1}|\dots|\underline{x}_{k_{f(i)}})=0$$

for $1\leqslant i\leqslant h_{\mathbf{C}}$ and any $1\leqslant k_1<\dots<k_{f(i)}\leqslant d-1$. The number of all these equations is

$$\sum_{i=1}^{h_{\mathbf{C}}}\left(\binom{d-1}{e(i)}+\binom{d-1}{f(i)}\right)\leqslant 2^{d-1}h_{\mathbf{C}}.$$

PROPOSITION $\mathrm{III}_{\mathbf{C}}$. *For a single form $\mathfrak{F}$ of degree $d>1$,*

$$h_{\mathbf{C}}(\mathfrak{F})\leqslant\varphi(d)\,g_{\mathbf{C}}(\mathfrak{F}),$$

where $\varphi(2)=\varphi(3)=1$, $\varphi(4)=3$, $\varphi(5)=13$, and $\varphi(d)<(\log 2)^{-d}d!$ in general.

COROLLARY. *For a system $\underline{\mathfrak{F}}$ of r forms of degree $d>1$,*

$$h_{\mathbf{C}}(\underline{\mathfrak{F}})\leqslant\varphi(d)\,(g_{\mathbf{C}}(\underline{\mathfrak{F}})+r-1).$$

Proof. Since $\mathfrak{M}(\underline{\mathfrak{F}})$ is the union of $\mathfrak{M}(\mathfrak{F})$ over the forms $\mathfrak{F}$ of the pencil, and since $\mathfrak{M}(\lambda\mathfrak{F})=\mathfrak{M}(\mathfrak{F})$ for $\lambda\neq 0$, there is some $\mathfrak{F}$ in the pencil with

$$\dim\mathfrak{M}(\mathfrak{F})\geqslant\dim\mathfrak{M}(\underline{\mathfrak{F}})-(r-1),$$

or

$$g_{\mathbf{C}}(\mathfrak{F})=\operatorname{codim}\mathfrak{M}(\mathfrak{F})\leqslant g_{\mathbf{C}}(\underline{\mathfrak{F}})+r-1.$$

Then

$$h_{\mathbf{C}}(\underline{\mathfrak{F}})\leqslant h_{\mathbf{C}}(\mathfrak{F})\leqslant\varphi(d)\,g_{\mathbf{C}}(\mathfrak{F})\leqslant\varphi(d)\,(g_{\mathbf{C}}(\underline{\mathfrak{F}})+r-1).$$

17. The arithmetical case

Now let $\underline{\mathfrak{F}}$ be an r-tuple of forms of degree $d>1$ with rational coefficients, and define h, g as before, i.e. as in § 1, § 10. It is easily seen that

$$h_{\mathbf{C}}\leqslant h,\quad g_{\mathbf{C}}\leqslant g. \tag{17.1}$$

The proof of Lemma 16.1 does not seem to have an analogue in the arithmetical case, nor is such an analogue of importance for the main purpose of this investigation.

However, the analogue of Proposition III_C holds, i.e. for a single form $\mathfrak{F}$,

$$h(\mathfrak{F}) \leqslant \varphi(d)\,[g(\mathfrak{F})], \tag{17.2}$$

where [ ] denotes the integer part.

PROPOSITION III. *Suppose that $\mathfrak{F}$ is a form of degree $d>1$ with rational coefficients, and write $\mathfrak{M}=\mathfrak{M}(\mathfrak{F})$. Suppose that for some $P>1$,*

$$z_P(\mathfrak{M}) > AP^{s(d-1)-\gamma-1}, \tag{17.3}$$

where $A=A(d,s)$ is a constant independent of $\mathfrak{F}$, and where γ is an integer. Then

$$h(\mathfrak{F}) \leqslant \varphi(d)\,\gamma. \tag{17.4}$$

Now if $\gamma=[g(\mathfrak{F})]$, then (17.3) is certainly true for some arbitrarily large values of P, so that (17.4), and hence indeed (17.2) holds.

COROLLARY. *For a system $\underline{\mathfrak{F}}$ of r forms of degree d with rational coefficients,*

$$h(\underline{\mathfrak{F}}) \leqslant \varphi(d)\,([g(\underline{\mathfrak{F}})]+(d-1)\,r(r-1)).$$

Proof. Put $\gamma=[g(\underline{\mathfrak{F}})]+(d-1)\,r(r-1)$, and choose $\varepsilon>0$ with

$$\gamma+1 > g(\underline{\mathfrak{F}})+(d-1)\,r(r-1)+2\varepsilon. \tag{17.5}$$

By definition of $g=g(\underline{\mathfrak{F}})$, there are certain arbitrarily large values of P with

$$z_P(\mathfrak{M}(\underline{\mathfrak{F}})) \gg P^{s(d-1)-g-\varepsilon}. \tag{17.6}$$

The constant in $\gg$ here and in what follows may depend on $\underline{\mathfrak{F}}$.

Suppose $(x_1,\dots,x_{d-1})$ with $|x_i|\leqslant P$ lies in $\mathfrak{M}(\underline{\mathfrak{F}})$. The matrix (10.1) then has rank less than r. Thus there is a linear combination $\mathfrak{F}=a_1\mathfrak{F}_1+\dots+a_r\mathfrak{F}_r$ with (10.2). The coefficients a_i have to satisfy the system of linear equations

$$\sum_{j=1}^{r} m_{ij}a_j = 0 \quad (i=1,\dots,s). \tag{17.7}$$

The rank of the matrix (m_{ij}) is $\leqslant r-1$, and the entries m_{ij} are $\ll P^{d-1}$. Hence there is a nontrivial integer solution $\underline{a}=(a_1,\dots,a_r)$ of (17.7) with

$$|\underline{a}| \ll P^{(d-1)(r-1)}.$$

The number of possibilities for such $\underline{a}$ is $\ll P^{(d-1)r(r-1)}$. Hence there is a form $\mathfrak{F}$ in the rational pencil with

$$z_P(\mathfrak{M}(\mathfrak{F})) \gg P^{-(d-1)r(r-1)} z_P(\mathfrak{M}(\underline{\mathfrak{F}})).$$

In conjunction with (17.5), (17.6) this gives

$$z_P(\mathfrak{M}(\mathfrak{F})) \gg P^{s(d-1)-\gamma-1+\varepsilon},$$

and hence gives (17.3) when P is large. Thus (17.4) holds, and further

$$h(\underline{\mathfrak{F}}) \leqslant h(\mathfrak{F}) \leqslant \varphi(d)\gamma.$$

In the next section we will deduce Theorems II and III. Proposition III_C will be proved in §§ 19–23. The necessary modifications for the proof of Proposition III will be given in § 24.

18. Deduction of Theorems II and III

The corollaries of Propositions II and III, together with

$$(d-1)(1+2^{1-d})^{-1}2^{3d-5}r_d kR+(d-1)r_d(r_d-1)<(d-1)2^{3d-5}r_d kR$$

show that Theorem II is indeed true with

$$\chi(d) = (d-1)2^{3d-5}\varphi(d).$$

We have $\chi(2)=2$, $\chi(3)=32$, $\chi(4)=1152$, and in general $\chi(d)<2^{4d}\cdot d!$ The Supplement to Theorem II follows in the same way.

As for Theorem III, we had seen in Proposition II_0 that $\mathfrak{F}$ satisfies the Hypothesis with every $\Omega<g/(2^{d-1}(d-1))$, and hence it satisfies the Hypothesis with $\Omega<h/\tau(d)$, where $\tau(d)=(d-1)2^{d-1}\varphi(d)$. Here $\tau(2)=2$, $\tau(3)=8$, $\tau(4)=72$, and in general $\tau(d)<2^{2d}\cdot d!$

19. Simple points

Let

$$s = e+t, \tag{19.1}$$

and let V be an irreducible algebraic variety of dimension e embedded in $\mathbf{C}^s$. Let $\mathfrak{J}(V)$ be the ideal of polynomials $f(\underline{X}) \in \mathbf{C}[\underline{X}]=\mathbf{C}[X_1,\ldots,X_s]$ which vanish on V. We will write

$\partial f/\partial X_i$ for the partial derivatives, and $\partial f/\partial x_i$ for the partial derivatives evaluated at a particular point $\underline{x}$. Given $\underline{x} \in V$, let $G(\underline{x})$ be the set of vectors

$$\operatorname{grad} f(\underline{x}) = (\partial f/\partial x_1, \ldots, \partial f/\partial x_s)$$

where f runs through $\mathfrak{F}(V)$. Then $G(\underline{x})$ is a vector space (over $\mathbf{C}$). It is well known (see e.g. Lang [7], Chapter VIII.2) that

$$\dim G(\underline{x}) \leqslant t. \tag{19.2}$$

Points with $\dim G(\underline{x})=t$ are called *simple* or *non-singular,* points with $\dim G(x)<t$ are called *singular*. Again, it is well known that the singular points form a proper algebraic subset V_{sing} of V.

Let $\underline{C}=(C_1, \ldots, C_s)$ be a new vector of variables. For $\underline{x} \in V$, let $H(\underline{x})$ be the set of linear forms

$$f^{(1)}(\underline{C}) = \sum_{i=1}^{s} (\partial f/\partial x_i) C_i.$$

Then $H(\underline{x})$ is a vector space isomorphic to $G(\underline{x})$, and thus $\dim H(\underline{x}) \leqslant t$. This means that there are t linear forms (which depend on $\underline{x}$), say

$$k_1(\underline{C}), \ldots, k_t(\underline{C}),$$

which generate $H(\underline{x})$. In section 20 we will generalize this fact to higher derivatives.

LEMMA 19.1. *Suppose that $\underline{x}$ is a simple point on V. Suppose that, say, the vectors $(\partial f/\partial x_1, \ldots, \partial f/\partial x_t)$ where f ranges over $\mathfrak{F}(V)$, contain t independent ones. Write $\underline{x}=(x_1, \ldots, x_t, y_1, \ldots, y_e)$. Then there exist unique formal power series*

$$\mathfrak{X}_i \in \mathbf{C}[[Y_1, \ldots, Y_e]] \quad (i = 1, \ldots, t)$$

with constant term zero such that

$$f(x_1+\mathfrak{X}_1(\underline{Y}), \ldots, x_t+\mathfrak{X}_t(\underline{Y}), y_1+Y_1, \ldots, y_e+Y_e) = 0 \tag{19.3}$$

for each $f \in \mathfrak{F}(V)$.

Moreover, if V is defined over the rationals (i.e. if it is definable by polynomial equations with rational coefficients), and if $\underline{x}$ has rational components, then the series $\mathfrak{X}_i$ have rational coefficients.

Proof. Except possibly for the last assertion, this is well known (Lang [7], Chapter VIII.4). The uniqueness part of the lemma is obtained by a quite simple argument, which also gives the last assertion (about rational coefficients) without extra effort.

20. Higher derivatives

Again let $V \subseteq \mathbf{C}^s$ be an irreducible variety of dimension e and of codimension t. Let $\underline{x} \in V$. Given $f \in \mathfrak{J}(V)$ and given $n>0$, write

$$f^{(n)}(\underline{C}) = \frac{1}{n!} \sum_{i_1=1}^{s} \cdots \sum_{i_n=1}^{s} \frac{\partial^n f}{\partial x_{i_1} \cdots \partial x_{i_n}} C_{i_1} \cdots C_{i_n}, \tag{20.1}$$

so that $f^{(n)}$ is a form of degree n.

LEMMA 20.1. *Suppose $\underline{x}$ is a simple point of V. Then there are forms*

$$k_1^{(p)}(\underline{C}), \ldots, k_t^{(p)}(\underline{C}) \quad (p = 1, 2, \ldots)$$

which depend on $\underline{x}$, and where $k_j^{(p)}$ is of degree p, such that for $f \in \mathfrak{J}(V)$ and for $n=1,2,\ldots$ we have

$$f^{(n)}(\underline{C}) = \sum_{p=1}^{n} \sum_{q=1}^{t} h_q^{(n-p)}(\underline{C})\, k_q^{(p)}(\underline{C}), \tag{20.2}$$

where $h_q^{(n-p)}$ is a form of degree $n-p$ which depends on f, as well as on $n-p$ and q.

Moreover, when V is defined over the rationals and when $\underline{x}$ is rational, then the $k_q^{(p)}$ have rational coefficients. When further f has rational coefficients, then so do the $h_q^{(n-p)}$.

Proof. We make the same conventions as in Lemma 19.1. In particular, $\mathfrak{X}_1, \ldots, \mathfrak{X}_t$ will be the formal series of that lemma. We may suppose that $\underline{x}=\underline{0}$. Let $\mathfrak{R}$ be the ring

$$\mathfrak{R} = \mathbf{C}[\underline{X}][[\underline{Y}]] = \mathbf{C}[X_1, \ldots, X_t][[Y_1, \ldots, Y_e]],$$

consisting of formal series in $\underline{Y}$ whose coefficients are polynomials in $\underline{X}$. For $f=f(\underline{X}, \underline{Y}) \in \mathfrak{R}$ we have

$$f(\underline{X}, \underline{Y}) - f(\mathfrak{X}_1(\underline{Y}), X_2, \ldots, X_t, \underline{Y}) = (X_1 - \mathfrak{X}_1(\underline{Y}))\, h_1(\underline{X}, \underline{Y})$$

with $h_1 \in \mathfrak{R}$. Similarly,

$$f(\mathfrak{X}_1(\underline{Y}), X_2, \ldots, X_t, \underline{Y}) - f(\mathfrak{X}_1(\underline{Y}), \mathfrak{X}_2(\underline{Y}), X_3, \ldots, X_t, \underline{Y}) = (X_2 - \mathfrak{X}_2(\underline{Y}))\, h_2(\underline{X}, \underline{Y})$$

with $h_2 \in \mathfrak{R}$. Continuing in this manner we get

$$f(\underline{X}, \underline{Y}) = (X_1 - \mathfrak{X}_1(\underline{Y}))\, h_1(\underline{X}, \underline{Y}) + \ldots + (X_t - \mathfrak{X}_t(\underline{Y}))\, h_t(\underline{X}, \underline{Y}) + f(\mathfrak{X}(\underline{Y}), \underline{Y}).$$

In the case when $f \in \mathfrak{J}(V)$, this becomes

$$f(\underline{X}, \underline{Y}) = \sum_{q=1}^{t} (X_q - \mathfrak{X}_q(\underline{Y}))\, h_q(\underline{X}, \underline{Y}). \tag{20.3}$$

Now when $\underline{x}=\underline{0}$, then $f^{(n)}$ of (20.1) is just the form of degree n in the Taylor expansion

$$f(\underline{C}) = f(\underline{0}) + f^{(1)}(\underline{C}) + \ldots + f^{(n)}(\underline{C}) + \ldots .$$

Clearly in this way $f^{(n)}$ may be defined for $f \in \mathfrak{R}$, and not just for polynomials $f \in \mathbf{C}[X_1, \ldots, X_s] = \mathbf{C}[\underline{X}, \underline{Y}]$. Further it is clear that when $f = uv$ with $u, v \in \mathfrak{R}$, then

$$f^{(n)} = \sum_{p=0}^{n} u^{(p)} v^{(n-p)},$$

where $u^{(0)} = u(\underline{0})$, $v^{(0)} = v(\underline{0})$. Applying this remark to (20.3) we get

$$f^{(n)} = \sum_{q=1}^{t} \sum_{p=0}^{n} k_q^{(p)} h_q^{(n-p)}$$

where $k_q(\underline{X}, \underline{Y}) = X_q - \mathfrak{X}_q(\underline{Y})$. Note that k_q $(q=1, \ldots, t)$ is independent of f. Since $k_q^{(0)} = 0$, formula (20.2) follows.

In the case when V is defined over the rationals and when $\underline{x}$ is rational, the series $\mathfrak{X}_i$ will have rational coefficients by Lemma 19.1, and hence so will the $k_q^{(p)}$. In the case when f has rational coefficients, we may work in the ring $\mathfrak{R}_{\mathbf{Q}} = \mathbf{Q}[\underline{X}][[\underline{Y}]]$, and the series h_q will have rational coefficients.

Remark. The case $n=1$ of Lemma 20.1 is true for any $\underline{x} \in V$, simple or not, since (19.2) did not depend on the simplicity of $\underline{x}$. The general case, or at least the first assertion of the general case, is probably also true for any $\underline{x} \in V$. But this is not essential for the present paper.

21. Operators $\mathfrak{D}_\tau$

Given a multilinear form $h(\underline{C}_1, \ldots, \underline{C}_q)$, and given a set $\varrho = \{u_1 < \ldots < u_q\}$ of positive integers, put

$$h(\underline{C}_\varrho) = h(\underline{C}_{u_1}, \ldots, \underline{C}_{u_q}),$$

so that $h(C_\varrho)$ becomes a multilinear form in vectors $C_{u_1}, \dots, C_{u_q}$. Given a form $f^{(n)}(C)$ of degree n, define the multilinear form $f^{(n)}(C_1|\dots|C_n)$ as in § 10. When $f^{(n)}(C)=h^{(n-p)}(C)\,k^{(p)}(C)$ with forms of respective degrees $n-p, p$, then it is easily seen that

$$f^{(n)}(C_1|\dots|C_n)=\sum_{\varrho,\sigma} h^{(n-p)}(C_\varrho)\,k^{(p)}(C_\sigma) \tag{21.1}$$

where the sum is over the partitions of $\{1,\dots,n\}$ into subsets ϱ, σ with respective cardinalities $n-p, p$. (This fact was used in the proof of Lemma 16.1.) In particular it follows from (20.2) that

$$f^{(n)}(C_1|\dots|C_n)=\sum_{p=1}^{n}\sum_{\varrho,\sigma}\sum_{q=1}^{t} h_q^{(n-p)}(C_\varrho)\,k_q^{(p)}(C_\sigma). \tag{21.2}$$

Now suppose that

$$S=ws \tag{21.3}$$

and that V is an irreducible variety of codimension t in $\mathbf{C}^S$. We consider polynomials $f(\mathfrak{X})=f(\underline{X}_1,\dots,\underline{X}_w)$ where each $\underline{X}_i$ has s components. Given a simple point $\underline{\mathfrak{x}}=(\underline{x}_1,\dots,\underline{x}_w)$ of V, we may apply everyting we said above. We obtain forms $f^{(n)}(\mathfrak{C})$ (as in (20.1)) with $\mathfrak{C}=(C_1,\dots,C_w)$, and multilinear forms $f^{(n)}(\mathfrak{C}_1|\dots|\mathfrak{C}_n)$.

Given a subset

$$\tau\subseteq\{1,\dots,w\}$$

we introduce an operator $\mathfrak{D}_\tau(C_\tau)$ as follows. The operator acts on polynomials $f(\mathfrak{X})$. When $\tau=\emptyset$, then $\mathfrak{D}_\emptyset f=f(\underline{\mathfrak{x}})$, i.e. one substitutes $\underline{\mathfrak{x}}$ for $\mathfrak{X}$. When $\tau=\{u_1,\dots,u_n\}$, then

$$\mathfrak{D}_\tau(C_\tau)f=\frac{(-1)^n}{n!}f^{(n)}(\mathfrak{c}_{u_1}|\dots|\mathfrak{c}_{u_n}), \tag{21.4}$$

where

$$\mathfrak{c}_l=(0,\dots,\underset{\leftarrow\ l\ \rightarrow}{C_l},\dots,0)\quad(1\leqslant l\leqslant w).$$

Thus

$$\mathfrak{D}_\tau(C_\tau)f=\sum_{i_1=1}^{s}\dots\sum_{i_n=1}^{s} C_{u_1 i_1}\dots C_{u_n i_n}\frac{\partial^n f}{\partial x_{u_1 i_1}\dots\partial x_{u_n i_n}}. \tag{21.5}$$

Substituting (21.2) we get (for $f \in \mathfrak{F}(V)$ and $\mathfrak{x}$ simple on V) that

$$(-1)^n n! \mathfrak{D}_\tau(\underline{C}_\tau) f = \sum_{p=1}^{n} \sum_{\varrho,\sigma} \sum_{q=1}^{t} h_q^{(n-p)}(\mathfrak{c}_\varrho) k_q^{(p)}(\mathfrak{c}_\sigma),$$

where the sum is over partitions of τ into subsets ϱ, σ of cardinalities $|\varrho|=n-p$, $|\sigma|=p$. Put

$$h_{q\varrho}^{(n-p)}(\underline{C}_\varrho) = h_q^{(n-p)}(\mathfrak{c}_\varrho),$$

$$k_{q\sigma}^{(p)}(\underline{C}_\sigma) = k_q^{(p)}(\mathfrak{c}_\sigma),$$

so that $h_{q\varrho}^{(n-p)}$ and $k_{q\sigma}^{(p)}$ are multilinear forms in vectors $\underline{C}$ with s components. With this notation we finally get for $f \in \mathfrak{F}(V)$ that

$$(-1)^n n! \mathfrak{D}_\tau(\underline{C}_\tau) f = \sum_{p=1}^{n} \sum_{\varrho,\sigma} \sum_{q=1}^{t} h_{q\varrho}^{(n-p)}(\underline{C}_\varrho) k_{q\sigma}^{(p)}(\underline{C}_\sigma). \tag{21.6}$$

We recall that the $k_{q\sigma}^{(p)}$ are independent of $f \in \mathfrak{F}(V)$, while the $h_{q\varrho}^{(n-p)}$ depend on f. When $\mathfrak{x}$ is rational and V is defined over the rationals, then the k's have rational coefficients. If further $f \in \mathfrak{F}(V)$ has rational coefficients, then so do the h's.

22. Proof of Proposition $\mathrm{III}_\mathbf{C}$: Beginning

The case $d=2$ is easy. Here $\mathfrak{M}$ consists of $\underline{x}$ with $\mathfrak{F}(\underline{x}|\underline{Z})=0$, and hence $\mathfrak{M}$ is a subspace of $\mathbf{C}^s$ of codimension $g_\mathbf{C}$. Since neither $g_\mathbf{C}$ nor $h_\mathbf{C}$ are affected by a nonsingular linear transformation of the variables, we may suppose that $\mathfrak{M}$ is the subspace $x_1=\ldots=x_{g_\mathbf{C}}=0$. Each $\underline{X}$ may uniquely be written as $\underline{X}=\underline{X}_\mathfrak{M}+\underline{X}^\perp$, with $\underline{X}_\mathfrak{M} \in \mathfrak{M}$, and $\underline{X}^\perp$ in the orthogonal complement of $\mathfrak{M}$. We have

$$\mathfrak{F}(\underline{X}) = \tfrac{1}{2}\mathfrak{F}(\underline{X}_\mathfrak{M}+\underline{X}^\perp|\underline{X}_\mathfrak{M}+\underline{X}^\perp) = \mathfrak{F}(\underline{X}^\perp) = \sum_{i,j=1}^{g_\mathbf{C}} c_{ij} X_i X_j,$$

with certain coefficients c_{ij}. Since $X_1, \ldots, X_{g_\mathbf{C}}$ are linear forms in $\underline{X}$, we have $h_\mathbf{C} \leqq g_\mathbf{C}$.

We now commence with the proof for the case when $d>2$. Let M be an irreducible component of $\mathfrak{M}$, of codimension $g_\mathbf{C}$. Let K be a field of definition of M, containing the coefficients of $\mathfrak{F}$. From now on, $(\underline{x}_1, \ldots, \underline{x}_{d-1})$ will be a fixed generic point of M with respect to K. In particular, it will be a simple point of M. Write

$$u = \text{transc.deg. } K(\underline{x}_1, \ldots, \underline{x}_{d-2})/K, \tag{22.1}$$

$$v = \text{transc.deg. } K(\underline{x}_1, \ldots, \underline{x}_{d-1})/K(\underline{x}_1, \ldots, \underline{x}_{d-2}), \tag{22.2}$$

so that $u+v=\dim M$, and set

$$t = s(d-2)-u, \quad a = s-v. \tag{22.3}$$

Then

$$a+t = s(d-1)-\dim M = g_{\mathbf{C}}. \tag{22.4}$$

Let S be the subspace consisting of vectors $\underline{y}$ such that $\mathfrak{F}(\underline{x}_1|\ldots|\underline{x}_{d-2}|\underline{y}|\underline{Z})=0$, i.e. such that $(\underline{x}_1, \ldots, \underline{x}_{d-2}, \underline{y}) \in \mathfrak{M}$. Since $\underline{x}_{d-1}$ lies in S and has v components which are algebraically independent over $K(\underline{x}_1, \ldots, \underline{x}_{d-2})$, it follows that $\dim S \geqslant v$. If we had $\dim S > v$, then some $\underline{x}'_{d-1}$ in S would have more than v components which are independent over $K(\underline{x}_1, \ldots, \underline{x}_{d-2})$, and $(\underline{x}_1, \ldots, \underline{x}_{d-2}, \underline{x}'_{d-1})$ would have more than $u+v$ independent components over K, contradicting the fact that $\dim \mathfrak{M}=\dim M=u+v$. Thus $\dim S=v$ and

$$\operatorname{codim} S = a. \tag{22.5}$$

In what follows write $\mathfrak{X}=(\underline{X}_1, \ldots, \underline{X}_{d-2})$ for vectors of variables and

$$\underline{\mathfrak{x}} = (\underline{x}_1, \ldots, \underline{x}_{d-2}) \tag{22.6}$$

where $\underline{x}_1, \ldots, \underline{x}_{d-2}$ are the given vectors. Further introduce the matrix

$$A(\mathfrak{X}): \mathfrak{F}(\underline{X}_1|\ldots|\underline{X}_{d-2}|\underline{e}_i|\underline{e}_j) \quad (1 \leqslant i, j \leqslant s),$$

where $\underline{e}_1, \ldots, \underline{e}_s$ are the basis vectors. A vector $\underline{y}=y_1\underline{e}_1+\ldots+y_s\underline{e}_s$ lies in S precisely if

$$\sum_{i=1}^{s} \mathfrak{F}(\underline{x}_1|\ldots|\underline{x}_{d-2}|\underline{e}_i|\underline{e}_j)\, y_i = 0 \quad (1 \leqslant j \leqslant s).$$

In view of (22.5) the matrix $A(\underline{\mathfrak{x}})$ has

$$\operatorname{rank} A(\underline{\mathfrak{x}}) = a. \tag{22.7}$$

We may suppose without loss of generality that the submatrix $1 \leqslant i, j \leqslant a$ is nonsingular.

In general denote the subdeterminant of $A(\mathfrak{X})$ with $1 \leqslant i, j \leqslant a$ by $\Delta(\mathfrak{X})$, and let

$$\Delta^i_j(\mathfrak{X}) \quad (1 \leqslant i \leqslant s-a = v,\ 1 \leqslant j \leqslant a)$$

be the subdeterminant formed from the first a rows, and from the columns $1, 2, \ldots, j-1, a+i, j+1, \ldots, a$. Put

$$\underline{y}^1 = \underline{y}^1(\mathfrak{X}) = (\Delta_1^1, \ldots, \Delta_a^1, -\Delta, 0, \ldots, 0),$$

$$\underline{y}^2 = \underline{y}^2(\mathfrak{X}) = (\Delta_1^2, \ldots, \Delta_a^2, 0, -\Delta, \ldots, 0),$$

$$\ldots$$

$$\underline{y}^v = \underline{y}^v(\mathfrak{X}) = (\Delta_1^v, \ldots, \Delta_a^v, 0, 0, \ldots, -\Delta).$$

Now

$$\mathfrak{F}(\underline{X}_1 | \ldots | \underline{X}_{k-2} | \underline{y}^i(\mathfrak{X}) | \underline{e}_j) \quad (1 \leqslant i \leqslant v)$$

is identically zero (as a function of $\mathfrak{X}=(\underline{X}_1, \ldots, \underline{X}_{k-2})$) for $1 \leqslant j \leqslant a$, while for $a < j \leqslant s$ it is an $(a+1)\times(a+1)$ subdeterminant of $A(\mathfrak{X})$. So if these $(a+1)\times(a+1)$ subdeterminants are $D_1(\mathfrak{X}), \ldots, D_N(\mathfrak{X})$, in some order, and if $\underline{D}(\mathfrak{X})=(D_1(\mathfrak{X}), \ldots, D_N(\mathfrak{X}))$, then

$$\mathfrak{F}(\underline{X}_1 | \ldots | \underline{X}_{d-2} | \underline{y}^{(i)}(\mathfrak{X}) | \underline{Z}) = \mathfrak{B}^i(\underline{D}(\mathfrak{X}), \underline{Z}) \quad (1 \leqslant i \leqslant v), \tag{22.8}$$

where $\mathfrak{B}^i$ is a bilinear form, in the vector $\underline{D}$ with N components and the vector $\underline{Z}$ with s components.

In view of (22.7) we have $\underline{D}(\mathfrak{x})=\underline{0}$, but $\Delta(\mathfrak{x}) \neq 0$ by our remarks above. The vectors

$$\underline{y}^1(\mathfrak{x}), \ldots, \underline{y}^v(\mathfrak{x})$$

are independent and lie in S, in fact they span S. Now if $\underline{y}^1(\mathfrak{x}), \ldots, \underline{y}^v(\mathfrak{x})$ together with, say $\underline{z}^1, \ldots, \underline{z}^a$, span $\mathbf{C}^s$, each $\underline{X}$ is uniquely

$$\underline{X} = \mathfrak{N}_1(\underline{X})\underline{y}^1(\mathfrak{x}) + \ldots + \mathfrak{N}_v(\underline{X})\underline{y}^v(\mathfrak{x}) + \mathfrak{L}_1(\underline{X})\underline{z}^1 + \ldots + \mathfrak{L}_a(\underline{X})\underline{z}^a \tag{22.9}$$

with linear forms $\mathfrak{N}_1, \ldots, \mathfrak{N}_v, \mathfrak{L}_1, \ldots, \mathfrak{L}_a$. The space S is defined by $\mathfrak{L}_1=\ldots=\mathfrak{L}_a=0$.

23. Proof of Proposition III_C: End

We will use the notation of §21 with $w=d-2$. Let $\mathfrak{S}$ be the set $\mathfrak{S}=\{1, 2. \ldots, d-2\}$. Further let $\mathfrak{F}$ and $\mathfrak{x}=(\underline{x}_1, \ldots, \underline{x}_{d-2})$ be as in the last section. Let $V \subseteq \mathbf{C}^{s(d-2)}$ be the variety with generic point $\mathfrak{x}$ with respect to K; then $\operatorname{codim} V = s(d-2)-u=t$ by (22.1), (22.3). Given $\sigma \subseteq \mathfrak{S}$ we put

$$\mathfrak{F}_\sigma(C_\sigma, \underline{Y}, \underline{Z}) = \mathfrak{F}(\underline{w}_1 | \ldots | \underline{w}_{d-2} | \underline{Y} | \underline{Z})$$

with

$$\underline{w}_i = \begin{cases} \underline{C}_i & \text{for } i \in \sigma, \\ \underline{x}_i & \text{for } i \notin \sigma. \end{cases}$$

We are going to apply $\mathfrak{D}_\tau(\underline{C}_\tau)$ with $\tau \subseteq \mathfrak{S}$ to the identity (22.8). When $\tau = \emptyset$ we get nothing interesting: both sides become zero. Suppose now that τ consists of a single element u. In this case, applying $\mathfrak{D}_\tau(\underline{C}_\tau)$ to (22.8) we obtain

$$\mathfrak{F}(\underline{x}_1|\dots|\underline{C}_u|\dots|\underline{x}_{d-2}|\underline{y}^i(\underline{\mathfrak{x}})|\underline{Z}) + \mathfrak{F}(\underline{x}_1|\dots|\underline{x}_{d-2}|\mathfrak{D}_\tau(\underline{C}_\tau)\underline{y}^i|\underline{Z}) = \mathfrak{B}^i(\mathfrak{D}_\tau(\underline{C}_\tau)\underline{D}, \underline{Z}) \quad (1 \leqslant i \leqslant v),$$

where $\mathfrak{D}_\tau$ applied to a vector acts componentwise. The last relation may be rewritten as

$$\mathfrak{F}_\tau(\underline{C}_\tau, \underline{y}^i(\underline{\mathfrak{x}}), \underline{Z}) + \mathfrak{F}_\varnothing(\underline{C}_\varnothing, \mathfrak{D}_\tau(\underline{C}_\tau)\underline{y}^i, \underline{Z}) = \mathfrak{B}^i(\mathfrak{D}_\tau(\underline{C}_\tau)\underline{D}, \underline{Z}).$$

More generally, using (21.5) one sees that for arbitrary $\tau \subseteq \mathfrak{S}$ we have

$$\sum_{\sigma \subseteq \tau} \mathfrak{F}_\sigma(\underline{C}_\sigma, \mathfrak{D}_{\tau \setminus \sigma}(\underline{C}_{\tau \setminus \sigma})\underline{y}^i, \underline{Z}) = \mathfrak{B}^i(\mathfrak{D}_\tau(\underline{C}_\tau)\underline{D}, \underline{Z}) \quad (1 \leqslant i \leqslant v) \tag{23.1}$$

We observe that

$$\mathfrak{F}_\varnothing(\underline{C}_\varnothing, \underline{Y}, \underline{y}^j(\underline{\mathfrak{x}})) = \mathfrak{F}(\underline{x}_1|\dots|\underline{x}_{d-2}|\underline{Y}|\underline{y}^j(\underline{\mathfrak{x}})) = 0 \quad (1 \leqslant j \leqslant v).$$

Hence substituting $\underline{Z} = \underline{y}^j(\underline{\mathfrak{x}})$ into (23.1) we obtain

$$\sum_{\varnothing \neq \sigma \subseteq \tau} \mathfrak{F}_\sigma(\underline{C}_\sigma, \mathfrak{D}_{\tau \setminus \sigma}(\underline{C}_{\tau \setminus \sigma})\underline{y}^i, \underline{y}^j(\underline{\mathfrak{x}})) = \mathfrak{L}_{ij}(\mathfrak{D}_\tau(\underline{C}_\tau)\underline{D}) \tag{23.2}$$

with certain linear forms $\mathfrak{L}_{ij}$. This is an identity of multilinear forms in vectors $\underline{C}_u$ with $u \in \tau$.

For $\sigma \subseteq \mathfrak{S}$, we define a linear transformation $\mathfrak{A}_\sigma(\underline{C}_\sigma): \mathbf{C}^s \to \mathbf{C}^s$ as follows: $\mathfrak{A}_\varnothing(\underline{C}_\varnothing)$ is the identity map, and for $\sigma \neq \emptyset$ we stipulate that

$$\mathfrak{A}_\sigma(\underline{C}_\sigma)\underline{y}^i(\underline{\mathfrak{x}}) = \mathfrak{D}_\sigma(\underline{C}_\sigma)\underline{y}^i \quad (1 \leqslant i \leqslant v). \tag{23.3}$$

This contains a certain arbitrariness, since the $\underline{y}^i(\underline{\mathfrak{x}})$ $(i = 1, \dots, v)$ do not form a basis of $\mathbf{C}^s$ (except when $v = s$). For instance we may set $\mathfrak{A}_\sigma(\underline{C}_\sigma)\underline{y} = \underline{0}$ for $\underline{y}$ in the orthogonal complement of $\underline{y}^1(\underline{\mathfrak{x}}), \dots, \underline{y}^v(\underline{\mathfrak{x}})$. At any rate we can make our choice so that $\mathfrak{A}_\sigma(\underline{C}_\sigma)\underline{Y}$ is multilinear, i.e. linear in the $\underline{C}_i$ $(i \in \sigma)$ and in $\underline{Y}$. Let $\mathfrak{L}_1, \dots, \mathfrak{L}_a$ be the linear forms of (22.9).

LEMMA 23.1. $\mathfrak{F}_\tau(\underline{C}_\tau, \underline{Y}, \underline{Z})$ *(as a polynomial in* $\underline{C}_\tau, \underline{Y}, \underline{Z}$*) lies in the ideal generated by the forms*

$$\mathfrak{L}_i(\underline{Z}) \quad (1 \leqslant i \leqslant a), \tag{A}$$

by

$$\mathfrak{L}_i(\mathfrak{A}_{\sigma_1}(\underline{C}_{\sigma_1}) \dots \mathfrak{A}_{\sigma_p}(\underline{C}_{\sigma_p})\, \underline{Y}) \quad (1 \leqslant i \leqslant a) \tag{B}$$

where $\sigma_1, \dots, \sigma_p$ *are disjoint subsets of* τ *whose union has cardinality* $<|\tau|$*, and by*

$$k_{q\sigma}^{(p)}(\underline{C}_\sigma), \tag{C}$$

where $1 \leqslant p \leqslant |\tau|$, $1 \leqslant q \leqslant t$, $\sigma \subseteq \tau$ *with* $|\sigma| = p$*, and where the forms* $k_{q\sigma}^{(p)}$ *come from* (21.6).

Proof. We proceed by induction on $|\tau|$, beginning with the case when $\tau = \emptyset$. In this case

$$\mathfrak{F}_\emptyset(\underline{C}_\emptyset, \underline{Y}, \underline{Z}) = \mathfrak{F}(x_1 | \dots | x_{d-2} | \underline{Y} | \underline{Z}). \tag{23.4}$$

Writing $\underline{Y}, \underline{Z}$ in the form (22.9), we see that (23.4) is a bilinear form in $(\mathfrak{L}_1(\underline{Y}), \dots, \mathfrak{L}_a(\underline{Y}))$ and $(\mathfrak{L}_1(\underline{Z}), \dots, \mathfrak{L}_a(\underline{Z}))$, hence lies in the ideal generated by (A).

Next, let us consider the case when $|\tau| = 1$. Here (23.2) reduces to

$$\mathfrak{F}_\tau(\underline{C}_\tau, \underline{y}^i(\mathfrak{x}), \underline{y}^j(\mathfrak{x})) = \mathfrak{L}_{ij}(\mathfrak{D}_\tau(\underline{C}_\tau)\, \underline{D}) \quad (1 \leqslant i, j \leqslant v).$$

Again writing $\underline{Y}, \underline{Z}$ in the form (22.9), we find that $\mathfrak{F}_\tau(\underline{C}_\tau, \underline{Y}, \underline{Z})$ lies in the ideal generated by $\mathfrak{L}_i(\underline{Z})$ $(1 \leqslant i \leqslant a)$, by $\mathfrak{L}_i(\underline{Y}) = \mathfrak{L}_i(\mathfrak{A}_\emptyset(\underline{C}_\emptyset)\, \underline{Y})$ $(1 \leqslant i \leqslant a)$ of (B), and by $\mathfrak{L}_{ij}(\mathfrak{D}_\tau(\underline{C}_\tau)\, \underline{D})$. Now each component of D_l of $\underline{D}$ vanishes on the variety V whose generic point was $\mathfrak{x}$, i.e. each component lies in $\mathfrak{J}(V)$. So (21.6) may be applied, and $\mathfrak{D}_\tau(\underline{C}_\tau) D_l$ lies in the ideal generated by the forms $k_{q\sigma}^{(p)}(\underline{C}_\sigma)$ with $p = 1 = |\tau|$, with $1 \leqslant q \leqslant t$ and with $\sigma = \tau$.

Suppose now that $|\tau| > 1$ and that the lemma has been shown for the proper subsets of τ. We may rewrite (23.2) as

$$\mathfrak{F}_\tau(\underline{C}_\tau, \underline{y}^i(\mathfrak{x}), \underline{y}^j(\mathfrak{x})) = \mathfrak{L}_{ij}(\mathfrak{D}_\tau(\underline{C}_\tau)\, \underline{D}) - \sum_{\substack{\varrho \\ \emptyset \neq \varrho \subsetneq \tau}} \mathfrak{F}_\varrho(\underline{C}_\varrho, \mathfrak{D}_{\tau \setminus \varrho}(\underline{C}_{\tau \setminus \varrho})\, \underline{y}^i, \underline{y}^j(\mathfrak{x})).$$

Therefore $\mathfrak{F}_\tau(\underline{C}_\tau, \underline{Y}, \underline{Z})$ lies in the ideal generated by $\mathfrak{L}_i(\underline{Y}), \mathfrak{L}_i(\underline{Z})$ $(i = 1, \dots, a)$, by the forms

$$\mathfrak{L}_{ij}(\mathfrak{D}_\tau(\underline{C}_\tau)\, \underline{D}) \quad (1 \leqslant i, j \leqslant v), \tag{23.5}$$

plus forms

$$\mathfrak{F}_\varrho\left(\underline{C}_\varrho, \sum_{i=1}^{v} \mathfrak{N}_i(\underline{Y})\, \mathfrak{D}_{\tau\setminus\varrho}(\underline{C}_{\tau\setminus\varrho})\, \underline{y}^i, \sum_{j=1}^{v} \mathfrak{N}_j(\underline{Z})\, \underline{y}^j(\underline{x})\right) \tag{23.6}$$

with $\emptyset \neq \varrho \subsetneqq \tau$. We write $\hat{\underline{Z}} = \Sigma_{j=1}^{v} \mathfrak{N}_j(\underline{Z})\, \underline{y}^j(\underline{x})$, and note that $\hat{\underline{Z}}$ lies in S. We may replace (23.6) by

$$\mathfrak{F}_\varrho(\underline{C}_\varrho, \mathfrak{A}_{\tau\setminus\varrho}(\underline{C}_{\tau\setminus\varrho})\, \underline{Y}, \hat{\underline{Z}}), \tag{23.7}$$

since the difference lies in the ideal generated by the $\mathfrak{L}_i(\underline{Y})$. Again by (21.6), each $\mathfrak{D}_\tau(\underline{C}_\tau) D_l$, and hence each form (23.5), lies in the ideal generated by (C). By induction, $\mathfrak{F}_\varrho(\underline{C}_\varrho, \underline{Y}, \underline{Z})$ with $\emptyset \neq \varrho \subsetneqq \tau$ lies in the ideal generated by (A), by (B) with disjoint subsets $\sigma_1, \ldots, \sigma_p$ whose union is less than ϱ, and by (C) with $1 \leqslant p \leqslant |\varrho|$ and $\sigma \subseteq \varrho$. Since $\mathfrak{L}_i(\hat{\underline{Z}}) = 0$, the form (23.7) lies in the ideal generated by (C) and by

$$\mathfrak{L}_i(\mathfrak{A}_{\sigma_1}(\underline{C}_{\sigma_1}) \ldots \mathfrak{A}_{\sigma_p}(\underline{C}_{\sigma_p})\, \mathfrak{A}_{\tau\setminus\varrho}(\underline{C}_{\tau\setminus\varrho})\, \underline{Y}).$$

Since $\sigma_1, \ldots, \sigma_p, \tau\setminus\varrho$ are disjoint subsets of τ whose union is less than τ, this is of the type (B).

The lemma will now be applied with $\tau = \mathfrak{S} = \{1, \ldots, d-2\}$. The number of forms is as follows. The number of forms (A) is a. The number of forms (B) is

$$a(1+\theta_{d-2})$$

where θ_m is the number of disjoint *nonempty* subsets $\sigma_1, \ldots, \sigma_p$ of $\{1, \ldots, m\}$ whose union has cardinality less than m. Here the ordering of $\sigma_1, \ldots, \sigma_p$ matters, but each σ_l itself is an unordered set. The number of forms (C) is

$$t \sum_{p=1}^{d-2} \binom{d-2}{p} = t(2^{d-2}-1).$$

By the lemma, applied with $\tau = \mathfrak{S}$, the multilinear form $\mathfrak{F}(\underline{X}_1 | \ldots | \underline{X}_d)$ lies in the ideal generated by the

$$a + a(1+\theta_{d-2}) + t(2^{d-2}-1) \tag{23.8}$$

forms (A), (B) and (C).

Substituting $\underline{X}_1 = \ldots = \underline{X}_d = \underline{X}$ we see that $\mathfrak{F}(\underline{X})$ lies in an ideal generated by forms of degrees between 1 and $d-1$, the number of these forms given by (23.8). Since $\mathfrak{L}_i(\underline{X}_{d-1})$ from (B) and $\mathfrak{L}_i(\underline{X}_d)$ from (A) both become $\mathfrak{L}_i(\underline{X})$, we may in fact save the summand a in

(23.8). We remark that Lemma 23.1 is not symmetric in $\underline{X}_1, \dots, \underline{X}_d$, and that a subtler argument probably would lead to further, substantial savings. At any rate, we may infer that

$$h_{\mathbf{C}}(\mathfrak{F}) \leqq a(1+\theta_{d-2})+t(2^{d-2}-1),$$

so that by (22.4),

$$h_{\mathbf{C}}(\mathfrak{F}) \leqq g_{\mathbf{C}} \max(1+\theta_{d-2}, 2^{d-2}-1). \tag{23.9}$$

Proposition $\mathrm{III}_{\mathbf{C}}$ is now an immediate consequence of

LEMMA 23.2. *The quantity* $\eta_m=1+\theta_m$ *has* $\eta_1=1$, $\eta_2=3$, $\eta_3=13$, *and in general* $\eta_m<(\log 2)^{-m}m!$

Proof. Setting $q=p+1$ in the definition, we see that θ_m is the number of partitions of $\{1, \dots, m\}$ into nonempty subsets $\sigma_1, \dots, \sigma_q$ where $q \geqq 2$. Hence η_m is the number of partitions into nonempty subsets $\sigma_1, \dots, \sigma_q$ where $q \geqq 1$.

η_1 "counts" only $\{1\}$, so that $\eta_1=1$.

η_2 counts $\{1,2\}$, $\{1\} \cup \{2\}$, $\{2\} \cup \{1\}$, so that $\eta_2=3$.

Similarly, $\eta_3=13$. In general,

$$\eta_m = \sum_{q=1}^{m} \sum_{\substack{u_1+\dots+u_q=m \\ u_i>0}} \frac{m!}{u_1! \dots u_q!}.$$

Setting $u_1+\dots+u_{q-1}=u$ and $q-1=p$, we obtain

$$\begin{aligned} \eta_m &= 1+\sum_{u=1}^{m-1} \sum_{p=1}^{u} \sum_{u_1+\dots+u_p=u} \frac{u!}{u_1! \dots u_p!} \binom{m}{u} \\ &= 1+\sum_{u=1}^{m-1} \binom{m}{u} \eta_u = \sum_{u=0}^{m-1} \binom{m}{u} \eta_u \end{aligned}$$

if we put $\eta_0=1$. The quantities $\xi_m=\eta_m(\log 2)^m/m!$ have

$$\xi_m = \sum_{u=0}^{m-1} \frac{(\log 2)^{m-u}}{(m-u)!} \xi_u.$$

Hence when $\xi_0, \xi_1, \dots, \xi_{m-1}$ are $\leqq 1$, then $\xi_m < e^{\log 2}-1=1$. Therefore each of $\xi_1, \xi_2, \dots$ is <1, and the lemma follows.

24. Proof of Proposition III

Let us look at the case $d=2$ first. When $\mathfrak{F}$ has rational coefficients, then $\mathfrak{M}$ is a subspace defined over the rationals. The number of integer points $\underline{x}$ in $\mathfrak{M} \cap (P\mathfrak{E})$ is

$$\ll P^{\dim \mathfrak{M}},$$

with a constant in $\ll$ which depends only on s. Hence if A in (17.3) is sufficiently large, we have $s(d-1)-\gamma-1<\dim \mathfrak{M}$, so that $\operatorname{codim} \mathfrak{M} \leqslant \gamma$. Since for $d=2$ we have $h(\mathfrak{F}) \leqslant \operatorname{codim} \mathfrak{M}$, the estimate (17.4) follows.

Before dealing with the case $d>2$, we need some general facts. Suppose that V is an algebraic submanifold of $\mathbf{C}^S$. We will say that *V belongs to the class $\mathfrak{C}(l)$* if it is the set of zeros of polynomials $f_1, \ldots, f_l$, each of total degree $\leqslant l$. It is well known that

$$V = V_1 \cup \ldots \cup V_m, \tag{24.1}$$

where the V_i are irreducible algebraic varieties, and this representation is unique if no V_i is redundant, i.e. if $V_i \not\subseteq V_j$ for $i \neq j$.

LEMMA 24.1. *Suppose $V \in \mathfrak{C}(l)$. There is an $l^*=l^*(l, S)$ such that in the unique representation* (24.1) *we have $m \leqslant l^*$, and each V_i lies in $\mathfrak{C}(l^*)$.*

Proof. See A. Seidenberg [13, § 65].

LEMMA 24.2. *Suppose $V \in \mathfrak{C}(l)$ contains integer points in a given bounded domain $\mathfrak{D}$, and write $z_{\mathfrak{D}}(V)$ for the number of these integer points. There is a subset $V' \subseteq V$ such that*

(A) *V' is an irreducible algebraic variety,*

(B) *V' is defined over the rationals,*

(C) *there is an integer point in $V' \cap \mathfrak{D}$ which is a simple point of V',*

(D) $z_{\mathfrak{D}}(V') \geqslant c_1 z_{\mathfrak{D}}(V)$ *where* $c_1=c_1(l, S)>0$.

Proof. We will construct a sequence

$$V = V^0 \supset V^1 \supset V^2 \supset \ldots \tag{24.2}$$

where V^i is an algebraic manifold belonging to $\mathfrak{C}(l_i)$ with $l_i=l_i(l, S)$; and where $z_{\mathfrak{D}}(V^i) \geqslant m_i z_{\mathfrak{D}}(V)$ with $m_i=m_i(l, S)>0$.

Case (A). Suppose V^i is not an irreducible variety. Then let V^{i+1} be the irreduci-

ble component of V^i for which $z_{\mathfrak{D}}(V^{i+1})$ is largest possible. By Lemma 24.1 and by inductive hypothesis, V^{i+1} will have the desired properties.

Case (B). Suppose V^i is an irreducible variety, but is not defined over the rationals. Let $f_1, \dots, f_n$ be $n \leqslant l_i$ polynomials of degree $\leqslant l_i$ defining V^i. The total number of coefficients of $f_1, \dots, f_n$ is bounded in terms of S and l_i, and hence so is the dimension D of the $\mathbf{Q}$-vector space spanned by these coefficients. If $\beta_1, \dots, \beta_D$ is a basis of this vector space, we may write $f_m = \Sigma_j \beta_j f_{mj}$ $(1 \leqslant m \leqslant n)$, where the polynomials f_{mj} have rational coefficients. Let V^{i+1} be the algebraic set defined by $f_{mj}=0$ $(1 \leqslant m \leqslant n,$ $1 \leqslant j \leqslant D)$. Then V^{i+1} is defined over the rationals and hence is a proper subset of V^i, so that $\dim V^{i+1} < \dim V^i$ (Lang [7, § II.3, Corollary 1]). Further $V^{i+1} \in \mathfrak{C}(l_i D)$ and $z_{\mathfrak{D}}(V^{i+1}) = z_{\mathfrak{D}}(V^i)$.

Case (C). Suppose V^i is an irreducible variety which is defined over $\mathbf{Q}$, but all the integer points of $V^i \cap \mathfrak{D}$ are singular points of V^i. In this case let V^{i+1} be the set of singular points of V^i.

The chain (24.2) must end after a bounded number of steps, since the case (A) cannot occur twice in a row, and since in the cases (B) and (C) the dimension is reduced. The last set of the chain has the desired properties.

Proof of Proposition III. We suppose that $d>2$. For given $\underline{x}_1, \dots, \underline{x}_{d-2}$, the $\underline{x}_{d-1}$ with $(\underline{x}_1, \dots, \underline{x}_{d-2}, \underline{x}_{d-1}) \in \mathfrak{M}$ form a linear subspace $S(\underline{x}_1, \dots, \underline{x}_{d-2})$, with a certain codimension a. Given $\underline{x}_1, \dots, \underline{x}_{d-2}$, the number of integer points $\underline{x}_{d-1} \in P\mathfrak{E}$ with $(\underline{x}_1, \dots, \underline{x}_{d-1}) \in \mathfrak{M}$ is then $\leqslant c_2(s) P^{s-a}$. Let $V_a \subseteq \mathbf{C}^{s(d-2)}$ be the algebraic set consisting of $(\underline{x}_1, \dots, \underline{x}_{d-2})$ for which $\operatorname{codim} S(\underline{x}_1, \dots, \underline{x}_{d-2}) \leqslant a$. Then[1]

$$z_P(\mathfrak{M}) \leqslant c_2(s) \sum_{a=0}^{s} z_P(V_a) P^{s-a}.$$

By the hypothesis (17.3), there must be an a in $0 \leqslant a \leqslant s$ with

$$z_P(V_a) > c_3(s) A P^{s(d-2)-\gamma-1+a}.$$

Since $z_P(V_a) \leqslant c_4(s, d) P^{s(d-2)}$, it follows that for sufficiently large A we must have $a-\gamma-1<0$, i.e.

---

[1] *Added in proof.* Rather than $z_P(V_a)$ and $z_P(V')$ below, we should count only points in V_a but not in V_{a-1}.

$$0 \leqslant a \leqslant \gamma.$$

Now $V_a \subseteq \mathbf{C}^S = \mathbf{C}^{s(d-2)}$ is in some class $\mathfrak{C}(l)$ with $l = l(s, d)$. Define $V' \subseteq V_a$ according to Lemma 24.2. Thus V' is an irreducible algebraic variety, and is defined over the rationals. We have $z_P(V') \geqslant c_1 z_P(V_a)$, hence

$$z_P(V') \geqslant c_5(s, d) A P^{s(d-2)-\gamma-1+a}.$$

Since $V' \in \mathfrak{C}(l')$ where $l' = l'(s, d)$, it follows for a sufficiently large value of A that $\dim V' \geqslant s(d-2)+a-\gamma$, or that

$$a+t \leqslant \gamma, \tag{24.3}$$

where $t = \operatorname{codim} V'$.

Further by part (C) of Lemma 24.2, there is an integer point $\underset{\sim}{x} = (\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_{d-2}) \in V'$ which is simple on V'. The whole construction for the proof of Proposition $\mathrm{III}_{\mathbf{C}}$ can be carried over, but this time our point $\underset{\sim}{x}$ has integer components. All the polynomials occurring have rational coefficients. Whereas in § 23 we used the fact that each component D_l of D lay in $\mathfrak{J}(V)$, we now use the fact that $D_l \in \mathfrak{J}(V_a) \subseteq \mathfrak{J}(V')$. Thus (21.6) holds for $f = D_l$, where the forms k are defined in terms of V' and $\underset{\sim}{x}$. The inequality (24.3) takes the place of (22.4). We may indeed conclude that $h(\mathfrak{F}) \leqslant \gamma\varphi(d)$.

References

[1] BIRCH, B. J., Homogeneous forms of odd degree in a large number of variables. *Mathematika*, 4 (1957), 102–105.

[2] — Forms in many variables. *Proc. Roy. Soc. Ser. A*, 265 (1962), 245–263.

[3] DAVENPORT, H., Cubic forms in 32 variables. *Philos. Trans. Roy. Soc. London Ser. A*, 251 (1959), 193–232.

[4] — Cubic forms in 16 variables. *Proc. Roy. Soc. Ser. A*, 272 (1963), 285–303.

[5] DAVENPORT, H. & LEWIS, D. J., Homogeneous additive equations. *Proc. Roy. Soc. Ser. A*, 274 (1963), 443–460.

[6] LACHAUD, G., Une presentation adelique de la serie singuliere et du probleme de Waring. *Enseign. Math.* To appear.

[7] LANG, S., *Introduction to algebraic geometry*. Interscience Tracts in Pure and Applied Math., 1958.

[8] LEEP, D. & SCHMIDT, W. M., Systems of homogeneous equations. *Inventiones Math.*, 71 (1983), 539–549.

[9] SCHMIDT, W. M., Simultaneous rational zeros of quadratic forms. *Seminar Delange-Pisot-Poitou* 1981. Progress in Math., Vol. 22 (1982), 281–307.

[10] — On cubic polynomials II. Multiple exponential sums. *Monatsh. Math.*, 93 (1982), 141–168.

[11] — On cubic polynomials III. Systems of p-adic equations. *Monatsh. Math.*, 93 (1982), 211–223.

[12] — On cubic polynomials IV. Systems of rational equations. *Monatsh. Math.*, 93 (1982), 329–348.
[13] SEIDENBERG, A., Constructions in algebra. *Trans. Amer. Math. Soc.*, 197 (1974), 273–313.
[14] TARTAKOVSKY, W., Über asymptotische Gesetze der allgemeinen Diophantischen Analyse mit vielen Unbekannten. *Bull. Acad. Sci. USSR*, (1935), 483–524.

Received November 22, 1982