Werk

Titel: Journal für die reine und angewandte Mathematik
Verlag: de Gruyter
Jahr: 1990
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN243919689_0406
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0406

Übergeordnetes Werk

Werk Id: PPN243919689
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Journal für die reine und angewandte Mathematik

gegründet 1826 von

August Leopold Crelle

fortgeführt von
C. W. Borchardt, K. Weierstrass, L. Kronecker, L. Fuchs,
K. Hensel, L. Schlesinger, H. Hasse, H. Rohrbach

gegenwärtig herausgegeben von

Simon Donaldson · Willi Jäger
Martin Kneser · Horst Leptin · Samuel J. Patterson
Peter Roquette · Michael Schneider

unter Mitwirkung von
J. Arthur (Toronto), J. Cuntz (Heidelberg), T. tom Dieck (Göttingen), O. Forster (München),
P. R. Halmos (Santa Clara), F. Hirzebruch (Bonn), R. Howe (New Haven), Y. Ihara (Kyoto),
H. Koch (Berlin), J. Lindenstrauss (Jerusalem), A. N. Parshin (Moskau), R. Weissauer (Mannheim)

JRMAA8

Band 406

W
DE
G

Walter de Gruyter · Berlin · New York 1990

♾ Gedruckt auf säurefreiem Papier · Printed on acid-free paper

Microform editions are available from: University Microfilms International,
300 N. Zeeb Road, Ann. Arbor, MI 48106, USA.

Printed in Germany.
Satz und Druck: Arthur Collignon GmbH, Berlin.
Buchbinderische Verarbeitung: Lüderitz & Bauer GmbH, Berlin.
ISSN 0075-4102

Inhalt

Indexed in Current Contents, SCI, ASCA, MATH Database on STN International, and ISI/COMPUMATH. Covered by Current Mathematical Publications, Mathematical Reviews and Zentralblatt für Mathematik/Mathematics Abstract.

Ausgabedatum des Bandes 406

26. April 1990

J. reine angew. Math. **406** (1990), 1—4

Journal für die reine und angewandte Mathematik

Remarks on nilpotent Lie algebras of vector fields

By *Janusz Grabowski**) at Warsaw

1. Preliminaries and the statement of the theorem

In [1] a local description of analytic vector fields finitely generating a transitive nilpotent Lie algebra L on a manifold is given. Our aim is to generalize this result by

(i) omitting the analyticity assumption, i.e. we will admit the vector fields which are smooth only,

(ii) omitting the assumption that L is finitely generated,

(iii) giving more information about the coefficients of vector fields from $L^{(j)}$.

Moreover, our proof seems to be much simpler than the proof in [1].

We will refer to [1] for the definitions and some partial results. Before stating the main theorem let us introduce the notation.

Suppose that L is a nilpotent Lie algebra of smooth vector fields on an n-dimensional manifold M and $p \in M$. The central descending series of L is defined by $L^{(1)} = L$ and, recurrently, $L^{(k+1)} = [L, L^{(k)}]$. For $i = 1, \ldots, n$, define

$$r_i = \max \{ j \in \mathbb{Z}^+ : \dim L^{(j)}(p) \geqq n + 1 - i \},$$

$a_1 = \min \{ j \in \mathbb{Z}^+ : r_j = r_n \}$ and, recurrently, $a_{i+1} = \min \{ j \in \mathbb{Z}^+ : r_j = r_{a_i - 1} \}$. Thus

$$1 \leqq r_1 \leqq \cdots \leqq r_n,\ a_1 > a_2 > \cdots, \quad \text{and} \quad r_j = r_{a_i}, \quad \text{if} \quad a_{i-1} > j \geqq a_i.$$

Denote $r := r(L, p) := (r_1, \ldots, r_n)$ and let δ_t^r be the dilation of $\mathbb{R}^n$ given by r, i.e. $\delta_t^r(x_1, \ldots, x_n) = (t^{r_1} x_1, \ldots, t^{r_n} x_n)$.

The main result is the following.

Theorem 1. *Suppose that L is a nilpotent Lie algebra of smooth vector fields on an n-dimensional smooth manifold M such that $\dim L(p) = n$ for some $p \in M$. Let $Y^i \in L^{(r_i)}$, where $i = 1, \ldots, n$ and $r = r(L, p) = (r_1, \ldots, r_n)$ is defined as above, be chosen such that*

*) The author was supported by the Alexander von Humboldt-Stiftung.

$Y^1(p), \ldots, Y^n(p)$ are linearly independent. Then $r_1 = 1$ and in the local coordinates in a neighbourhood of p given by $(x_1, \ldots, x_n) \mapsto (\exp x_n Y^n) \circ \cdots \circ (\exp x_1 Y^1)(p)$, each $Y \in L^{(j)}$ is of the form $Y = \sum_{i=1}^{n} y_i(x)\partial_i$, where $\partial_i = \partial/\partial x_i$ and y_i are polynomials of degree $(r_j - j)$ with respect to the dilation δ_t^r, $i = 1, \ldots, n$.

In particular, vector fields from L are of degree (-1) with respect to δ_t^r and L has locally finite dimension.

2. Side results and the proof of theorem 1

We assume that $Y^1, \ldots, Y^n$ and local coordinates in a neighbourhood of p are chosen as in theorem 1.

In the sequel, $\deg(f) = k$ will mean that f is a polynomial of degree k with respect to the dilation δ_t^r.

Lemma 1. *We have $r_1 = 1$, i.e. $\dim L^{(2)}(p) < n$.*

Proof. Suppose $Z^1, \ldots, Z^n \in L^{(2)}$ and $Z^{(1)}(p), \ldots, Z^{(n)}(p)$ are linearly independent. Let $L_p = \{Y \in L : Y(p) = 0\}$ be the isotropy subalgebra of L at p. For each $i = 1, \ldots, n$ there are $X_1^i, Y_1^i, \ldots, X_{k(i)}^i, Y_{k(i)}^i \in L$ such that $Z^i = \sum_{j=1}^{k(i)} [X_j^i, Y_j^i]$ and thus

$$(1) \qquad Z^i = \sum_{k,l=1}^{n} a_{kl}^i [Z^k, Z^l] + \sum_{k=1}^{n} b_k^i [Z^k, V_k^i] \pmod{L_p}, \quad i = 1, \ldots, n,$$

for some $a_{kl}^i, b_k^i \in \mathbb{R}$ and $V_k^i \in L_p$.

Similarly as in [1], substituting for each Z^k and Z^l on the right side of (1) the k-th and the l-th equation of (1), we get $Z^i \in L^{(3)} \pmod{L_p}$, $i = 1, \ldots, n$, and inductively $Z^i \in L^{(s)} \pmod{L_p}$, $i = 1, \ldots, n$, $s = 2, 3, \ldots$.

Hence $\dim L^{(s)}(p) = n$ for all $s = 1, 2, 3, \ldots$; a contradiction. □

Lemma 2. i) *If $r_l \geqq j > r_{l-1}$, then $L^{(j)}(q) = \operatorname{span}\{Y^l(q), \ldots, Y^n(q)\}$ for q from a neighbourhood of p.*

ii) $Y^i = \partial_i + \sum_{j=i+1}^{n} c_{ij}(x)\partial_j$, *where c_{ij} are smooth functions of the form*

$$c_{ij}(x_1, \ldots, x_n) = \sum_{k=i+1}^{n} x_k c_{ij}^k(x_1, \ldots, x_n) \quad \text{for} \quad c_{ij}^k\text{-smooth}, \quad i = 1, \ldots, n.$$

Proof. The above facts are proved in [1] without use of the analyticity assumption. □

Lemma 3. *Let f be a smooth function in a neighbourhood of 0 in $\mathbb{R}^n$ such that $f(x_1, \ldots, x_n) = f(0) + \sum_{l=i}^{n} x_l g_l(x_1, \ldots, x_n)$ for some smooth g_l, and let $\deg(\partial_l(f)) = k - r_l$ for $n \geqq l \geqq i$. Then $\deg(f) = k$.*

Proof. We have $f(x_1, \ldots, x_n) = x_n \partial_n(f)(x_1, \ldots, x_n) + f_n(x_1, \ldots, x_{n-1})$, where

$\deg(x_n \partial_n(f)) = k$ and f_n is smooth and depends on $x_1, \ldots, x_{n-1}$ only. Inductively,

$$f(x) = x_n w_n(x) + \cdots + x_i w_i(x) + f_{i-1}(x),$$

where $\deg(x_n w_n(x) + \cdots + x_i w_i(x)) = k$ and f_{i-1} depends on $x_1, \ldots, x_{i-1}$ only. But

$$f_{i-1}(x_1, \ldots, x_{i-1}) = f(x_1, \ldots, x_{i-1}, 0, \ldots, 0) = f(0),$$

so $\deg(f) = k$. □

To prove theorem 1 we will use the induction with respect to n. For $n=1$, by lemma 1 and lemma 2, we have $L^{(2)} = \{0\}$ and $y^1 = \partial_1$. Since L is commutative, $0 = [Y^1, Y] = \partial_1(y)\partial_1$ for each $Y = y(x_1)\partial_1 \in L$, so $y(x_1) = \text{const}$ and L is one-dimensional generated by ∂_1.

Let now $n > 1$. By lemma 2, we know that $Y^{a_1} = \partial_{a_1}, \ldots, Y^n = \partial_n$.
Those vector fields belong to the center of L, so $[\partial_i, Y] = 0$ for all $Y \in L$ and $i = a_1, \ldots, n$. This implies that the coefficients of vector fields from L do not depend on $x_{a_1}, \ldots, x_n$.

Passing to the quotient manifold with respect to the foliation generated by $\partial_{a_1}, \ldots, \partial_n$, we get a Lie algebra homomorphism

$$\hat{}: L \to \hat{L}, \quad \text{where} \quad \left(\sum_{i=1}^{n} y_i(x)\partial_i\right)\hat{} = \sum_{i=1}^{a_1-1} y_i(x)\partial_i.$$

$\hat{L}$ can be considered as a nilpotent Lie algebra of vector fields on a manifold of dimension $(a_1 - 1)$ and it is easy to see that $\hat{r} := r(\hat{L}, 0) = (r_1, \ldots, r_{a_1-1})$. By the inductive assumption, if $Y \in \hat{L}^{(j)}$, then y_i, $i = 1, \ldots, a_1 - 1$, are polynomials of degree $(r_i - j)$ with respect to the dilation $\delta_t^{\hat{r}}$ and hence with respect to the dilation δ_t^r, since they do not depend on $x_{a_1}, \ldots, x_n$. This way we get that

(2) for each $Y \in L^{(j)}$, $Y = \sum_{i=1}^{n} y_i(x)\partial_i$, the coefficients y_i depend on $x_1, \ldots, x_{a_1-1}$ only and $\deg(y_i) = r_i - j$ for $i = 1, \ldots, a_1 - 1$.

We will get theorem 1 immediately by proving inductively the following.

Theorem 2. *For each* $k = 1, 2, \ldots,$

A_k) *if* $n \geqq i \geqq a_k$, *then* $\deg(c_{is}) = (r_s - r_i)$ *for* $s = n, \ldots, i+1$,

B_k) *if* $n \geqq i \geqq a_k$, *then* $\deg(\partial_i(c_{js})) = (r_s - r_j - r_i)$ *for* $j = n, \ldots, 1$ *and* $s = n, \ldots, j+1$,

C_k) *if* $j > r_{a_{k+1}}$, *then for each* $Y \in L^{(j)}$ *we have*

(3) $$Y=\sum_{i=a_k}^{n} y_i(x)\partial_i, \text{ where } \deg(y_i)=r_i-j.$$

Recall that c_{js} are coefficients of Y^j as in lemma 2.

Proof of theorem 2. A_1) $Y^i=\partial_i$ for $n\geqq i\geqq a_1$.

B_1) $\partial_i(c_{mj})=0$ for $n\geqq i\geqq a_1$.

Now we will show that A_k) and B_k) imply C_k).

Let $j>r_{a_{k+1}}$ and let $Y\in L^{(j)}$. Since $[Y^m, Y]\in L^{(r_m+j)}$, we can assume inductively that $[Y^m, Y]$ satisfies (3). The coefficient by ∂_s in $[Y^m, Y]$ equals $Y^m(y_s)-Y(c_{ms})$ and it is a polynomial of degree (r_s-r_m-j). Since

$$Y(c_{ms})=\sum_{i=a_k}^{n} y_i\,\partial_i(c_{ms})=\sum_{i=a_k}^{a_1-1} y_i\,\partial_i(c_{ms}),$$

$\deg(\partial_i(c_{ms}))=(r_s-r_m-r_i)$ by B_k) and $\deg(y_i)=(r_i-j)$ for $i=1,\ldots,a_1-1$ by (2), we get that $\deg(Y^m(y_s))=(r_s-j-r_m)$ for $m=n,\ldots,1$. Now, using (2), one can prove inductively that this implies that $\deg(\partial_m(y_s))=(r_s-j-r_m)$ for $m=n,\ldots,1$, and we conclude by lemma 3 that $\deg(y_s)=(r_s-j)$.

It remains to prove that C_k) implies A_{k+1}) and B_{k+1}).

Assume C_k) and let $n\geqq i\geqq a_{k+1}$. The coefficient by ∂_s in $[Y^j, Y^i]$ equals $Y^j(c_{is})-Y^i(c_{js})$ and, since $[Y^j, Y^i]\in L^{(r_j+r_i)}$ and $r_j+r_i>r_i\geqq r_{a_{k+1}}$, it is a polynomial of degree $(r_s-r_j-r_i)$ by C_k).

To prove A_{k+1}), assume inductively that $\deg(c_{js})=(r_s-r_j)$ for $j>i$. Hence $\deg(Y^i(c_{js}))=\deg\left(\partial_i(c_{js})+\sum_{l=i+1}^{a_1-1} c_{il}\,\partial_l(c_{jl})\right)=(r_s-r_j-r_i)$ by (2) and we conclude that $\deg(Y^j(c_{is}))=(r_s-r_j-r_i)$ and then, inductively, that $\deg(\partial_j(c_{is}))=(r_s-r_j-r_i)$ for $n\geqq j>i$.

Now, $\deg(c_{is})=(r_s-r_i)$ by lemma 2. ii) and lemma 3.

Finally, we will prove B_{k+1}). As above, $Y^i(c_{js})-Y^j(c_{is})$ is a polynomial of degree $(r_s-r_i-r_j)$. We get by A_{k+1}) that $\deg(Y^j(c_{is}))=(r_s-r_i-r_j)$, so $\deg(Y^i(c_{js}))=(r_s-r_i-r_j)$ and, inductively, $\deg(\partial_i(c_{js}))=(r_s-r_i-r_j)$ for $n\geqq i>a_{k+1}$. □

Bibliography

[1] *M. Kawski*, Nilpotent Lie algebras of vector fields, J. reine angew. Math. **388** (1988), 1—17.

Institute of Mathematics, Warsaw University, PKiN IXp., 00-901 Warsaw, Poland

Eingegangen 25. Januar 1989

J. reine angew. Math. **406** (1990), 5—9

Journal für die reine und angewandte Mathematik

Der Zentralisator einer Liealgebra in einer einhüllenden Algebra

Von *Friedrich Knop* in Basel

1. Einleitung

Sei $\mathfrak{g}$ eine halbeinfache Liealgebra und $\mathfrak{h}$ eine reduktive Unteralgebra. Der Zentralisator $\mathfrak{U}(\mathfrak{g})^{\mathfrak{h}}$ von $\mathfrak{h}$ in der universell einhüllenden Algebra von $\mathfrak{g}$ enthält dann sowohl das Zentrum von $\mathfrak{U}(\mathfrak{g})$ als auch das von $\mathfrak{U}(\mathfrak{h})$. In [5] hat K. Johnson bewiesen, daß im Falle $\mathfrak{g}=\mathfrak{su}(n, 1)$ und $\mathfrak{h}=\mathfrak{u}(n)$ der Zentralisator von den beiden Zentren erzeugt wird. Wir zeigen in dieser Arbeit, daß dies auch für $\mathfrak{g}=\mathfrak{so}(n, 1)$ und $\mathfrak{h}=\mathfrak{so}(n)$ zutrifft und daß dies im Prinzip die einzigen nichttrivialen Fälle sind, für die dies gilt (Satz 2. 3). Weiterhin zeigen wir, daß der Zentralisator immer ein flacher Modul über dem Erzeugnis der beiden Zentren ist (Satz 2. 2). Die Beweisidee besteht darin, zum zugehörigen graduierten Fall überzugehen. Die in Rede stehenden Algebren sind dann durch eine gewisse Momentabbildung miteinander verknüpft, die ich schon in [6] untersucht habe.

2. Ergebnisse

Alles sei im folgenden über einem Körper k der Charakteristik null definiert. Für eine Liealgebra $\mathfrak{g}$ sei $\mathfrak{U}(\mathfrak{g})$ ihre universell einhüllende Algebra. Sie besitzt eine kanonische Filtrierung $\mathfrak{U}_n(\mathfrak{g})$ und die zugehörige graduierte Algebra ist die symmetrische Algebra $S(\mathfrak{g})$. Für $x \in \mathfrak{U}_n(\mathfrak{g}) - \mathfrak{U}_{n-1}(\mathfrak{g})$ sei $\bar{x}$ das Bild von x in $S(\mathfrak{g})$. Der Kommutator auf $\mathfrak{U}(\mathfrak{g})$ induziert auf $S(\mathfrak{g})$ ein Poissonprodukt: Für $\bar{x} \in S^m(\mathfrak{g})$ und $\bar{y} \in S^n(\mathfrak{g})$ ist

$$\{\bar{x}, \bar{y}\} := \overline{xy - yx} \in S^{m+n-1}(\mathfrak{g}).$$

Das Zentrum $\mathfrak{U}(\mathfrak{g})^{\mathfrak{g}}$ der einhüllenden Algebra bezeichnen wir mit $\mathfrak{Z}(\mathfrak{g})$. Entsprechend sei $Z(\mathfrak{g}) := S(\mathfrak{g})^{\mathfrak{g}}$. Wenn $\mathfrak{g}$ halbeinfach ist, sind beide Algebren Polynomringe mit $\operatorname{rg}\mathfrak{g}$ Erzeugenden.

Sei ab jetzt $\mathfrak{g}$ halbeinfach und $\mathfrak{h} \subseteqq \mathfrak{g}$ eine reduktive Unteralgebra. Wir interessieren uns für den Zentralisator $\mathfrak{U}(\mathfrak{g})^{\mathfrak{h}}$ von $\mathfrak{h}$ in $\mathfrak{U}(\mathfrak{g})$. Es gibt einen kanonischen Homomorphismus

$$\mu : \mathfrak{Z}(\mathfrak{g}) \otimes_k \mathfrak{Z}(\mathfrak{h}) \longrightarrow \mathfrak{U}(\mathfrak{g})^{\mathfrak{h}}.$$

Sein Bild sei $\mathfrak{Z}_0$. Entsprechend haben wir einen Homomorphismus von Poissonalgebren

$$\mu' : Z(\mathfrak{g}) \otimes_k Z(\mathfrak{h}) \longrightarrow S(\mathfrak{g})^{\mathfrak{h}}$$

mit Bild Z_0.

Satz 2. 1. *Sei* $\mathfrak{k}$ *das größte Ideal von* $\mathfrak{g}$, *das in* $\mathfrak{h}$ *enthalten ist. Dann ist*

$$\mathfrak{Z}_0 = \mathfrak{Z}(\mathfrak{g}) \otimes_{\mathfrak{Z}(\mathfrak{k})} \mathfrak{Z}(\mathfrak{h}), \quad Z_0 = Z(\mathfrak{g}) \otimes_{Z(\mathfrak{k})} Z(\mathfrak{h}).$$

Insbesondere ist μ (*bzw.* μ') *genau dann injektiv, wenn* $\mathfrak{h}$ *kein echtes Ideal von* $\mathfrak{g}$ *enthält. Weiterhin sind* $\mathfrak{Z}_0$ *und* Z_0 *Polynomringe.*

Satz 2. 2. $\mathfrak{U}(\mathfrak{g})^{\mathfrak{h}}$ (*bzw.* $S(\mathfrak{g})^{\mathfrak{h}}$) *ist ein flacher* $\mathfrak{Z}_0$- (*bzw.* Z_0-)*Modul.*

Satz 2. 3. *Es sind äquivalent*:

1. μ *ist surjektiv.*

1′. μ' *ist surjektiv.*

2. $\mathfrak{h}$ *ist algebraisch, und* $\mathfrak{U}(\mathfrak{g})^{\mathfrak{h}}$ *ist kommutativ.*

2′. $\mathfrak{h}$ *ist algebraisch, und das Poissonprodukt auf* $S(\mathfrak{g})^{\mathfrak{h}}$ *verschwindet.*

3. *Über dem algebraischen Abschluß von* k *gilt* $\mathfrak{g} = \bigoplus_{i=1}^{s} \mathfrak{g}_i$, $\mathfrak{h} = \bigoplus_{i=1}^{s} \mathfrak{h}_i$ *mit* $\mathfrak{h}_i \subseteq \mathfrak{g}_i$, *wobei für jedes* i *einer der folgenden Fälle zutrifft*:

— $\mathfrak{h}_i = \mathfrak{g}_i$ *ist eine einfache Liealgebra,*

— $\mathfrak{g}_i = \mathfrak{sl}_n$, $\mathfrak{h}_i = \mathfrak{gl}_{n-1}$ *mit* $n \geqq 2$,

— $\mathfrak{g}_i = \mathfrak{so}_n$, $\mathfrak{h}_i = \mathfrak{so}_{n-1}$ *mit* $n \geqq 4$.

Wenn diese Bedingungen erfüllt sind, ist $\mathfrak{U}(\mathfrak{g})$ (*bzw.* $S(\mathfrak{g})$) *ein freier* $\mathfrak{U}(\mathfrak{g})^{\mathfrak{h}}$- (*bzw.* $S(\mathfrak{g})^{\mathfrak{h}}$-)*Modul.*

3. Beweise

Zunächst sei bemerkt, daß alle Behauptungen genau dann richtig sind, wenn sie über dem algebraischen Abschluß von k stimmen. Wir nehmen daher ab jetzt an, daß k algebraisch abgeschlossen ist.

Sei G die einfach zusammenhängende algebraische Gruppe mit Liealgebra $\mathfrak{g}$. Wenn es eine abgeschlossene Untergruppe $H \subseteq G$ mit $\mathfrak{h} = \operatorname{Lie} H$ gibt, so heißt $\mathfrak{h}$ algebraisch. In jedem Fall gibt es eine kleinste algebraische Unteralgebra $\bar{\mathfrak{h}} \supseteq \mathfrak{h}$, die algebraische Hülle. Sie ist ebenfalls reduktiv, $\mathfrak{h}$ ist ein Ideal, und der Quotient ist abelsch. Es gilt $\mathfrak{U}(\mathfrak{g})^{\mathfrak{h}} = \mathfrak{U}(\mathfrak{g})^{\bar{\mathfrak{h}}}$.

Wenn $\mathfrak{h}$ algebraisch ist, setzen wir $X := (G \times H)/H$, wobei H diagonal eingebettet ist. Mit anderen Worten ist $X = G$ und $G \times H$ operiert durch $s \mapsto gsh^{-1}$. Weiter sei $\pi : T_X^* \to X$ das Kotangentialbündel. Es gilt $T_X^* = G \times \mathfrak{g}^*$, π ist die Projektion auf den ersten Faktor, G operiert durch Linksmultiplikation auf dem ersten Faktor, und H operiert durch Rechtsmultiplikation auf dem ersten und durch Konjugation auf dem zweiten Faktor. Auf T_X^* ist die Momentabbildung definiert:

$$\Phi : T_X^* \to (\mathfrak{g} \oplus \mathfrak{h})^* : \alpha \mapsto (\xi \in \mathfrak{g} \oplus \mathfrak{h} \mapsto \alpha(\xi_{\pi(\alpha)})).$$

Für die Funktionenalgebren liefert das

$$S(\mathfrak{g} \oplus \mathfrak{h}) \to k[T_X^*] = k[G \times \mathfrak{g}^*] = k[G] \otimes_k S(\mathfrak{g}).$$

Der Übergang zu $\mathfrak{g} \oplus \mathfrak{h}$-Invarianten liefert genau

$$\mu' : Z(\mathfrak{g}) \otimes_k Z(\mathfrak{h}) = S(\mathfrak{g} \oplus \mathfrak{h})^{\mathfrak{g} \oplus \mathfrak{h}} \to (k[G] \otimes_k S(\mathfrak{g}))^{\mathfrak{g} \oplus \mathfrak{h}} = S(\mathfrak{g})^{\mathfrak{h}}.$$

Diesen Homomorphismus habe ich in [6] eingehend untersucht.

Beweis von Satz 2. 1. Sei $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{g}_0$ und $\mathfrak{h} = \mathfrak{k} \oplus \mathfrak{h}_0$. Dann ist

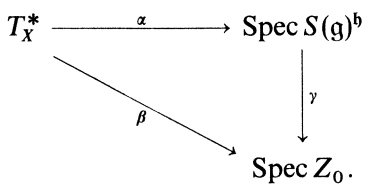
$$\mathfrak{Z}(\mathfrak{g}) \otimes_{\mathfrak{Z}(\mathfrak{k})} \mathfrak{Z}(\mathfrak{h}) = \mathfrak{Z}(\mathfrak{k}) \otimes_k \mathfrak{Z}(\mathfrak{g}_0) \otimes_k \mathfrak{Z}(\mathfrak{h}_0),$$

sowie $\mathfrak{U}(\mathfrak{g})^{\mathfrak{h}} = \mathfrak{Z}(\mathfrak{k}) \otimes_k \mathfrak{U}(\mathfrak{g}_0)^{\mathfrak{h}_0}$. Entsprechendes gilt für den graduierten Fall. Damit genügt es zu zeigen: $\mathfrak{k} = 0 \Rightarrow \mu, \mu'$ sind injektiv. Da μ' aus μ durch Übergang zur assoziierten graduierten Algebra entsteht, genügt es zu zeigen, daß μ' injektiv ist. Weiterhin können wir annehmen, daß $\mathfrak{h}$ algebraisch ist.

Sei $T \subseteqq G$ ein maximaler Torus. Da G lokal effektiv auf G/H operiert, ist die generische Standgruppe von T auf G/H endlich. Anders ausgedrückt gibt es einen maximalen Torus T_0, so daß $T_0 \cap H$ endlich ist. Wähle ein $\xi \in \mathfrak{g}^*$ mit $G_\xi = T_0$. Dann ist H_ξ und damit die generische Standgruppe von $G \times H$ auf T_X^* endlich. Aus [6], Korollar 8. 2 und Satz 5. 4 folgt, daß die Momentabbildung dominant ist. Insbesondere ist μ' injektiv. □

Beweis von Satz 2. 2. Sei $\bar{\mathfrak{h}} = \mathfrak{a} \oplus \mathfrak{h}$ die algebraische Hülle von $\mathfrak{h}$. Dann ist $\mathfrak{Z}(\mathfrak{g}) \otimes_{\mathfrak{Z}(\mathfrak{h})} \mathfrak{Z}(\bar{\mathfrak{h}}) = \mathfrak{Z}_0 \otimes_k \mathfrak{U}(\mathfrak{a})$ flach über $\mathfrak{Z}_0$. Entsprechendes gilt für den graduierten Fall. Es genügt also, den Satz für algebraisches $\mathfrak{h}$ zu beweisen. Ebenfalls genügt es, die Behauptung für den graduierten Fall zu beweisen.

Wir haben dann folgendes kommutatives Diagramm:



Nach [6], Satz 6. 6c ist β äquidimensional. Da α surjektiv ist, ist auch γ äquidimensional. Nach [4] oder [1] ist $S(\mathfrak{g})^{\mathfrak{h}}$ ein Cohen-Macaulay-Ring. Mit [3], § 15. 4. 2 folgt die Flachheit von $S(\mathfrak{g})^{\mathfrak{h}}$ über Z_0. □

Beweis von Satz 2. 3. $1' \Rightarrow 1$: trivial.

$1 \Rightarrow 2$: $\mathfrak{U}(\mathfrak{g})^{\mathfrak{h}} = \mathfrak{Z}_0$ ist kommutativ. Sei $\bar{\mathfrak{h}} = \mathfrak{a} \oplus \mathfrak{h}$ die algebraische Hülle von $\mathfrak{h}$. Wegen $\mathfrak{Z}_0 = \mathfrak{U}(\mathfrak{g})^{\mathfrak{h}} = \mathfrak{U}(\mathfrak{g})^{\bar{\mathfrak{h}}} \supseteq \mathfrak{Z}_0 \otimes_k \mathfrak{U}(\mathfrak{a})$ ist $\mathfrak{a} = 0$, und $\mathfrak{h}$ ist algebraisch.

$2 \Rightarrow 2'$: trivial.

$2' \Rightarrow 3$: Sei $B \subseteq G \times H$ eine Boreluntergruppe. Der Transzendenzgrad des Invariantenkörpers $k(X)^B$ heißt Kompliziertheit von X. Varietäten der Kompliziertheit null heißen sphärisch. Wenn X nicht sphärisch ist, folgt aus [6], Satz 7. 1, daß es eine $G \times H$-invariante rationale Funktion f auf T_X^* gibt, die algebraisch unabhängig von $S(\mathfrak{g} \oplus \mathfrak{h})$ ist. Nach [6], Satz 7. 6 folgt, daß f nicht mit allen $G \times H$-invarianten rationalen Funktionen auf T_X^* Poisson-kommutieren kann. Die Einschränkungsabbildung von $k(T_X^*)^{G \times H}$ auf $\mathfrak{g}^* = \{e\} \times \mathfrak{g}^* \subseteq G \times \mathfrak{g}^* = T_X^*$ liefert einen Poisson-Isomorphismus mit $k(\mathfrak{g}^*)^{\mathfrak{h}}$. Nach [7], Corollaire 7 ist die generische Bahn von H auf $\mathfrak{g}^*$ abgeschlossen. Insbesondere gilt $k(\mathfrak{g}^*)^{\mathfrak{h}} = \operatorname{Quot} k[\mathfrak{g}^*]^{\mathfrak{h}} = \operatorname{Quot} S(\mathfrak{g})^{\mathfrak{h}}$, d.h. $S(\mathfrak{g})^{\mathfrak{h}}$ ist nicht Poisson-kommutativ. Also ist X sphärisch. In [2] sind alle affinen, homogenen, sphärischen Varietäten klassifiziert. Aus dieser Tabelle liest man ab, daß $(G \times H)/H$ genau dann sphärisch ist, wenn $(\mathfrak{g}, \mathfrak{h})$ wie in Punkt 3 des Satzes ist.

$3 \Rightarrow 1'$: Wir können annehmen, daß $(\mathfrak{g}, \mathfrak{h})$ eines der drei Paare ist. Der erste Fall ist trivial.

$\mathfrak{g} = \mathfrak{sl}_n$, $\mathfrak{h} = \mathfrak{gl}_{n-1}$: Dieser Fall wurde in [5] behandelt. Ich möchte hier einen kürzeren Beweis vorstellen: Wir identifizieren $\mathfrak{g}^*$ und $\mathfrak{g}$ mit Hilfe der Killingform. $\mathfrak{h}$ ist die Menge aller Matrizen in $\mathfrak{sl}_n$, deren letzte Zeile und letzte Spalte bis auf das Diagonalelement aus Nullen besteht. Sei nun S die Menge aller Matrizen in $\mathfrak{g}$ von folgender Form:

$$\begin{pmatrix} 0 & & & & * & * \\ & \ddots & & & \vdots & \vdots \\ 1 & & \ddots & & \vdots & \vdots \\ & & & 0 & * & * \\ & & & 1 & * & * \\ & & & & 1 & * \end{pmatrix}.$$

Wir haben einen Morphismus

$$\Phi : \mathfrak{g} \longrightarrow \mathfrak{g}//G \times \mathfrak{h}//H := \operatorname{Spec} S(\mathfrak{g})^{\mathfrak{g}} \times \operatorname{Spec} S(\mathfrak{h})^{\mathfrak{h}}.$$

Die Nullfaser ist genau die Menge der nilpotenten Matrizen, die nilpotent bleiben, wenn man die letzte Zeile und Spalte fortläßt. Es gibt nur eine Matrix in S, die diese Bedingung erfüllt, nämlich die, bei der alle Sternchen gleich Null sind.

Für $t \in k^*$ sei $\lambda(t) := \operatorname{diag}(t^{n-1}, t^{n-3}, \ldots, t^{-n+3}, t^{-n+1}) \in H$. Wir lassen nun k^* folgendermaßen auf $\mathfrak{g}$ operieren: Für $t \in k^*$ und $A \in \mathfrak{sl}_n$ sei $t \cdot A := t^2 \lambda(t) A \lambda(t)^{-1}$. Diese Operation läßt S invariant. Genauer operiert k^* linear auf S mit den Gewichten $2, 4, \ldots, 2n-2, 4, 6, \ldots, 2n$. Dies sind aber genau die Gewichte, mit denen k^* auf

$\mathfrak{g}//G \times \mathfrak{h}//H$ operiert. Mit [9], 8.1, Lemma 3 erhalten wir, daß $S \to \mathfrak{g}//G \times \mathfrak{h}//H$ ein Isomorphismus ist. Dies liefert ein Inverses zum kanonischen Morphismus

$$\mathfrak{g}//H \to \mathfrak{g}//G \times \mathfrak{h}//H,$$

und damit ist die Behauptung gezeigt.

$\mathfrak{g} = \mathfrak{so}_n$, $\mathfrak{h} = \mathfrak{so}_{n-1}$: Diesen Fall könnte man im Prinzip genauso behandeln wie den vorherigen. Wir schlagen hier eine Variante ein: Es gibt einen kanonischen Morphismus $\Phi: \mathfrak{g}//H \to \mathfrak{g}//G \times \mathfrak{h}//H$. Da X sphärisch ist, ist Φ endlich ([6], Satz 7.1). Beide Räume sind glatt und tragen eine natürliche k^*-Operation, so daß Φ äquivalent ist. Die Gewichte dieser Operationen sind dieselben ([8], Table 3a, Zeile 2 und 5). Mit [9], 8.1, Lemma 3 erhalten wir wieder, daß es sich bei Φ um einen Isomorphismus handelt, was zu beweisen war.

Zum Beweis der letzten Aussage: Nach [6], Satz 6.6 ist $S(\mathfrak{g})$ flach über $Z_0 = S(\mathfrak{g})^{\mathfrak{h}}$. Sei $S(\mathfrak{g}) = \bigoplus_\chi M_\chi$ die Zerlegung des H-Moduls $S(\mathfrak{g})$ in isotypische Komponenten. Diese sind endlich erzeugte Z_0-Moduln und als direkte Summanden eines flachen Moduls flach, also projektiv, also frei. Der ungraduierte Fall folgt hieraus. □

Nachtrag bei der Korrektur. Mit denselben Methoden kann man folgendes beweisen: Sei $\mathfrak{h} \subseteq \mathfrak{g}$ algebraisch. Dann ist $\mathfrak{Z}_0$ das Zentrum von $\mathfrak{U}(\mathfrak{g})^{\mathfrak{h}}$.

Literatur

[1] *J.-F. Boutot*, Singularités et quotients par les groupes réductifs, Invent. Math. **88** (1987), 65–68.

[2] *M. Brion*, Classification des espaces homogènes sphériques, Compos. Math. **63** (1987), 189–208.

[3] *J. Dieudonné, A. Grothendieck*, Eléments de géométrie algébrique IV, Publ. Math. IHES **28** (1966).

[4] *M. Hochster, J. Roberts*, Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay, Adv. in Math. **13** (1974), 115—175.

[5] *K. Johnson*, The centralizer of a Lie algebra in an enveloping algebra, J. reine angew. Math. **395** (1989), 196—201.

[6] *F. Knop*, Weylgruppe und Momentabbildung, Invent. Math. **99** (1990), 1–23.

[7] *D. Luna*, Slices étales, Bull. Soc. Math. France, Mem. **33** (1973), 81–105.

[8] *G. Schwarz*, Representations of simple Lie groups with regular rings of invariants, Invent. Math. **49** (1978), 167—191.

[9] *P. Slodowy*, Simple singularities and simple algebraic groups, Lect. Notes in Math. **815**, Berlin-Heidelberg-New York 1980.

Mathematisches Institut, Rheinsprung 21, CH-4051 Basel

Eingegangen 1. April 1989

J. reine angew. Math. **406** (1990), 10—43

Journal für die reine und angewandte Mathematik

Quasilinear hyperbolic 2×2 systems with a free, damping boundary condition

By *Hans-Dieter Alber* at Darmstadt and *Jeffery Cooper* at College Park

1. Introduction

We consider the quasilinear system of equations for two functions $u(x, t)$, $v(x, t)$ and a "boundary function" $s(t)$

$$u_t - v_x = 0, \tag{1.1}$$

$$v_t - \sigma(u)_x = 0 \quad \text{in} \quad 0 < x < L, \ t \geqq 0, \tag{1.2}$$

$$v(L, t) = 0, \tag{1.3}$$

$$v(0, t) = s'(t), \tag{1.4}$$

$$ms'' + rs' + ks = \sigma(u(0, t)), \qquad m \geqq 0, \ r, k > 0, \tag{1.5}$$

with initial conditions

$$u(x, 0) = u^0(x), \ v(x, 0) = v^0(x), \qquad 0 \leqq x \leqq L, \tag{1.6}$$
$$s(0) = s^0.$$

In this paper we assume that $u \longrightarrow \sigma(u)$ is a smooth function on an open interval I with $0 \in I$. Furthermore

$$\sigma'(u) > 0 \quad \text{for} \quad u \in I \quad \text{and} \quad \sigma(0) = 0. \tag{1.7}$$

With this condition the system (1.1), (1.2) is hyperbolic. When $I = \mathbb{R}$, this system may be thought of as modelling a nonlinear string with vertical displacement function $\varphi(x, t)$ such that $(u, v) = (\varphi_x, \varphi_t)$. The boundary condition (1.3) means that the right end of the

string is fixed, while (1.4), (1.5) mean that the left end is attached to a sort of spring mass system with damping which controls the vertical displacement. (1.5) is the equation of motion of this system, m is the mass, r a damping constant, and k the spring constant. In section 4 of this paper we make the additional hypothesis

$$\int_0^L u^0(x)\,dx + s^0 = 0 \tag{1.8}$$

on the initial data. This amounts to assuming that the right end of the string is fixed at $\varphi(L, t)=0$ and the left end at $\varphi(0, t)=s(t)$ for all t. (1.8) determines the choice of s^0 in (1.6) uniquely.

It is well known that if σ is a nonlinear function, then smooth solutions of (1.1), (1.2) develop singularities after some time. One might expect, however, that the introduction of damping in (1.5) prevents the formation of singularities and assures the existence of a global smooth solution. In fact, this has been proved by Greenberg and Li Ta-tsien [2] and by Slemrod [8] for the system (1.1)—(1.5) with $m=k=0$ and $r>0$. In this case s' can be eliminated from (1.4) and (1.5). They proved the existence of C^1 solutions global in time provided the initial data (u^0, v^0) is sufficiently small in the C^1-norm. The basic idea in their proof is that the C^1-norm of disturbances propagating along characteristics decays upon reflection at the left boundary by a factor strictly less than one.

In the present paper we study the boundary condition (1.5) in the general case. Our result is that in the case $m=0$ and $r, k>0$ a global smooth solution still exists. However, in the case $m, r, k>0$, that is for nonvanishing mass of the spring, the situation changes and a smooth solution develops singularities after a finite time, in general.

Though in the case $m=0$, $r, k>0$ a global solution still exists, the situation is different from the Greenberg-Li Ta-tsien case, since the decay result for the C^1-norm mentioned above no longer holds. Instead, decay occurs in the energy norms. In section 2 we therefore derive the estimate

$$\frac{d}{dt}E(t) \leqq C_1[E(t)^{1/2}+E(t)]\,E(t) - C_2 r[|s'|^2+|s''|^2+|s'''|^2], \tag{1.9}$$

and in section 3 the estimate

$$\int_0^t E(t) \leqq C_3 \int_0^t (|s'|^2+|s''|^2+|s'''|^2)\,d\tau + C_4 \int_0^t E(\tau)^2\,d\tau, \tag{1.10}$$

which holds for all $t \geqq T^*$ with a suitable constant $T^*>0$, and with the energy $E(t)$ defined in (2.3)—(2.5). Combination of (1.9) and (1.10) yields the global existence and the exponential decay results from section 4 for C^3-solutions.

The derivation of (1. 9) is standard, but we present it in detail, since some care is necessary to estimate the boundary terms. This can be seen from the fact that (1. 9) is no longer valid for $m>0$. We note that the right hand side of (1. 10) does not contain the terms $\int_0^t s(\tau)^2 d\tau$, and some care is needed to show that this term can be avoided in this inequality.

As already mentioned, an essentially new situation occurs in the case $m, r, k>0$, which is considered in sections 5, 6, and 7 of this paper. For a C^2 solution (u, v) of (1. 1)—(1. 7) set

$$E_0(t)=\int_0^L \left[\frac{1}{2}v^2(x,t)+\int_0^{u(x,t)}\sigma(\eta)\,d\eta\right]dx+\frac{1}{2}(m|s'|^2+k|s|^2).$$

We note that $\frac{d}{dt}E_0(t)=-r(s')^2\leqq 0$ so that the initial boundary value problem is dissipative. Nevertheless, we show that for $m>0$ the global existence result of section 4 no longer holds and that for sufficiently small initial data u^0, v^0 singularities develop. More precisely, let μ be the diameter of support of (u_x^0, v_x^0), and assume that $u^0(0)=v^0(0)=s^0=0$. We prove that C^2 solutions of (1. 1)—(1. 7) with $\sigma''(0)\neq 0$ develop singularities in a finite time provided (u^0, v^0) is small in $C([0, L])$ and $D\equiv\mu/m$ is sufficiently small. Moreover, it is shown that asymptotically for $\mu\to 0$ and

$$\sup_{0\leqq x\leqq L}(|u^0(x)|, |v^0(x)|)\to 0$$

the time of existence is equal to the time of existence of the solution to the Cauchy problem for (1. 1), (1. 2). The method of proof is similar to that of Lax [3], but more complicated techniques are needed to estimate the solution as it interacts with the free boundary. The core of the proof is the equation (7. 6), which states that disturbances propagating along characteristics are reflected at the boundary unchanged up to integral terms, which can be made small by choosing the initial conditions as described above.

With a different choice of σ, the system (1. 1)—(1. 7) describes an initial-boundary value problem for one dimensional isentropic flow in Lagrangian coordinates, and in the remainder of this introduction we discuss this interpretation of (1. 1)—(1. 7). In Eulerian coordinates, the gas is contained in a tube along the y axis with a fixed wall at $y=b$. The left end of the tube is bounded by a piston of mass m on a damped spring mechanism. When the gas is at rest with a constant density $\varrho_0>0$ we take the equilibrium position of the piston to be $y=a$ and $s(t)$ denotes the displacement of the piston from equilibrium. The system of differential equations and boundary conditions in Eulerian coordinates for the density ϱ, velocity v and pressure P is

$$\varrho_t+(\varrho v)_y=0, \tag{1. 11}$$

$$\varrho[v_t+vv_y]+P_y=0, \tag{1. 12}$$

$$v(a+s(t), t)=s'(t), \tag{1.13}$$

$$v(b, t)=0, \tag{1.14}$$

$$ms''+rs'+ks=P_0-P(a+s(t), t). \tag{1.15}$$

Here $P_0=P(\varrho_0)$ is the pressure needed to balance the spring of the piston at equilibrium. The Lagrangian coordinate is

$$x=\int_{a+s(t)}^{y(x,t)} \varrho\, d\eta,$$

the mass of gas between the piston and y, and

$$L=\int_{a+s(t)}^{b} \varrho\, d\eta$$

is the total mass of gas in the tube. The system (1.11)—(1.15) transforms into (1.1)—(1.5) with

$$u=\frac{1}{\varrho(y(x, t), t)}-u_0$$

being the difference between the specific volume $1/\varrho$ and $u_0=1/\varrho_0$. We shall assume that

$$\sigma(u)=P_0-P\left[\frac{1}{u+u_0}\right]$$

satisfies (1.7). This would be true when the gas is polytropic in which case $P(\varrho)=A\varrho^\gamma$ and $\sigma(u)=P_0-A(u+u_0)^{-\gamma}$. The condition (1.8) becomes

$$\int_{s^0+a}^{b} \varrho(y, 0)\, dy=\varrho_0(b-a).$$

Note that μ has the units of mass so that $D=\mu/m$ is a dimensionless parameter. Our condition for the breakdown of solutions requires that the mass of gas in the non-constant part of the initial data must be small relative to the mass m of the piston. In this case, the free piston is in effect acting like a rigid wall, and the formation of singularities is to be expected.

Finally we note that in this paper we assume local existence of C^3 solutions of the system (1.1)—(1.7) to be known. This local existence result can be proved using classical methods due to Friedrichs [1]. Li Ta-tsien and Yu Wen-ci [5] have obtained such local existence results, and a modification of their method could be used to derive the local existence theorem needed here. We remark that Li Ta-tsien [4] has also studied some free boundary value problems with a view to proving global existence of discontinuous shock wave solutions.

Acknowledgement. We wish to acknowledge the support of two institutions which provided visiting opportunities: Alber at the University of Maryland, and Cooper at the University of Bonn under Sonderforschungsbereich 256.

2. Energy estimates

We shall derive energy estimates for solutions $(u, v) \in C^3([0, L]\times[0, T]; \mathbb{R}^2)$ of the system (1. 1)—(1. 6) when $m=0$, $r>0$, and $k>0$. We recall that the system we are considering is

$$u_t = v_x, \tag{2. 1}$$
$$v_t = \sigma(u)_x,$$

$$v(L, t) = 0, \tag{2. 2}$$
$$v(0, t) = s'(t),\ rs'(t) + ks(t) = \sigma(u(0, t)), \qquad t \geqq 0.$$

We introduce the following notation. Let $w=(u, v)$ and for $t \geqq 0$ set

$$E_0(t) = E_0(t, w) \tag{2. 3}$$
$$= \int_0^L \left[\frac{1}{2} v^2(x, t) + \int_0^{u(x,t)} \sigma(\eta)\, d\eta\right] dx + \frac{1}{2} k|s(t)|^2.$$

For a multi index $\alpha=(\alpha_1, \alpha_2)$, $0<|\alpha|=\alpha_1+\alpha_2 \leqq 2$, let

$$E_\alpha(t) = E_\alpha(t, w) \tag{2. 4}$$
$$= \frac{1}{2}\int_0^L [|D^\alpha v(x, t)|^2 + \sigma'(u(x, t))|\, D^\alpha u(x, t)|^2]\, dx$$
$$+ \frac{1}{2} k[\sigma'(u(0, t))]^{-\alpha_1} |\partial_t^{|\alpha|} s(t)|^2.$$

Finally, let

$$E(t) = \sum_{|\alpha| \leqq 2} E_\alpha(t). \tag{2. 5}$$

For functions $f, g : (0, L) \to \mathbb{R}^2$, we set

$$(f, g) = \int_0^L f(x) \cdot g(x)\, dx, \quad \|f\| = (f, f)^{1/2}$$

and

$$\|f\|_\infty = \sup_{0<x<L} |f(x)|.$$

If $w=(u, v)$ is a C^2 solution on $[0, L]\times[0, T]$, there are positive constants $\underline{\sigma}_1$, $\bar{\sigma}_1$, $\bar{\sigma}_2$, and $\bar{\sigma}_3$ such that

$$\underline{\sigma}_1 \leqq \sigma'(u(x, t)) \leqq \bar{\sigma}_1, \tag{2. 6}$$
$$|\sigma''(u(x, t))| \leqq \bar{\sigma}_2, \quad |\sigma'''(u(x, t))| \leqq \bar{\sigma}_3,$$

for $(x, t) \in [0, L]\times[0, T]$. Hence for a C^2 solution w, we have

$$E(t) \geqq \frac{1}{2} \min\{\underline{\sigma}_1, 1\} \sum_{|\alpha| \leqq 2} \|D^\alpha w\|^2.$$

Theorem 2. 1. *Let (u, v) be a C^3 solution of (2. 1)—(2. 2) on $[0, L]\times[0, T]$. Then there are constants C_1 and C_2 independent of r and k (but depending on $\sup_{\substack{0 \leqq t \leqq T \\ 0 \leqq x \leqq L}} |u(x, t)|$ through $\underline{\sigma}_1$, $\bar{\sigma}_1$, $\bar{\sigma}_2$, and $\bar{\sigma}_3$) such that*

$$\frac{d}{dt} E(t) \leqq C_1 \left[E(t)^{1/2} + \left[\frac{r^2+1}{r} \right] E(t) \right] E(t) - C_2 r[|s'|^2 + |s''|^2 + |s'''|^2]. \tag{2. 7}$$

Proof. From (2. 1)—(2. 3), we find

$$\frac{d}{dt} E_0(t) = \frac{d}{dt} \left[\int_0^L \left[\frac{1}{2} v^2 + \int_0^u \sigma(\tau)\, d\tau \right] dx + \frac{1}{2} k s^2 \right] \tag{2. 8}$$
$$= \int_0^L (v v_t + \sigma(u) u_t)\, dx + k s s' = -r(s')^2.$$

Next let

$$A_0(u) = \begin{bmatrix} \sigma'(u) & 0 \\ 0 & 1 \end{bmatrix}, \quad A_1(u) = \begin{bmatrix} 0 & \sigma'(u) \\ \sigma'(u) & 0 \end{bmatrix}.$$

By assumption, $w=(u, v) \in C^3$. Hence (2. 1) can be written as a symmetric hyperbolic system:

$$A_0(u) w_t = A_1(u) w_x \tag{2. 9}$$

and from (2. 4) we see that

$$\frac{d}{dt} E_\alpha = \frac{1}{2} \frac{d}{dt} (A_0(u) D^\alpha w, D^\alpha w) + \frac{1}{2} \frac{d}{dt} k[\sigma'(u(0, t))]^{-\alpha_1} |\partial_t^{|\alpha|} s(t)|^2. \tag{2. 10}$$

If we differentiate in (2. 9), the result is

$$A_0(u)D^\alpha w_t = A_1(u)D^\alpha w_x + B_\alpha(w) \tag{2. 11}$$

where

$$\begin{aligned} B_\alpha w &= D^\alpha(A_1(u)w_x - A_0(u)w_t) - A_1(u)D^\alpha w_x + A_0(u)D^\alpha w_t \\ &= \sum_{\beta<\alpha}\binom{\alpha}{\beta}[D^{\alpha-\beta}A_1(u)D^\beta w_x - (D^{\alpha-\beta}A_0(u))D^\beta w_t]. \end{aligned} \tag{2. 12}$$

The boundary condition at $x=L$ implies that

$$[D^\alpha w A_1(u)D^\alpha w](L, t)=0.$$

Hence if we multiply (2. 11) by $D^\alpha w$ and integrate, we deduce

$$\begin{aligned} \frac{1}{2}\frac{d}{dt}(A_0(u)D^\alpha w, D^\alpha w) &= \frac{1}{2}([A_0(u)_t - A_1(u)_x]D^\alpha w + B_\alpha(w), D^\alpha w) \\ &\quad - [\sigma'(u)D^\alpha u D^\alpha v](0, t). \end{aligned} \tag{2. 13}$$

Now

$$([A_0(u)_t - A_1(u)_x]D^\alpha w, D^\alpha w) = \int_0^L \sigma''(u_t|D^\alpha u|^2 - 2u_x D^\alpha u D^\alpha v)\,dx.$$

Hence Sobolev's inequality and the definition of $E(t)$ then yield

$$\begin{aligned} |([A_0(u)_t - A_1(u)_x]D^\alpha w, D^\alpha w)| &\leqq C\bar{\sigma}_2\|Du\|_\infty\|D^\alpha w\|^2 \\ &\leqq C\bar{\sigma}_2\max\left[1, \frac{1}{\underline{\sigma}_1}\right]E^{3/2}(t), \end{aligned} \tag{2. 14}$$

where $\|Du\|_\infty = \max_{0\leqq x\leqq L}\{|u_t(x, t)|, |u_x(x, t)|\}$.

To estimate the commutator $B_\alpha(w)$ we use the Moser type inequalities [6]:

$$\|D^\alpha(fg) - fD^\alpha g\| \leqq C(\|D^{|\alpha|}f\|\,\|g\|_\infty + \|Df\|_\infty\|D^{|\alpha|-1}g\|).$$

Here $\|D^s f\|^2 = \sum_{|\alpha|=s}\|D^\alpha f\|^2$. Now when $f=A_j(u)$, $j=0, 1$,

$$\|Df\|_\infty = \|D(A_j(u))\|_\infty \leqq C_1\bar{\sigma}_2\|Du\|_\infty$$

and

$$\|Df\| = \|D(A_j(u))\| \leqq C_2\bar{\sigma}_2\|Du\|$$

while

$$\|D^2 f\| = \|D^2(A_j(u))\| \leqq C_3\bar{\sigma}_3\|Du\|_\infty\|Du\| + C_4\bar{\sigma}_2\|D^2 u\|.$$

Hence with $g = Dw$, we obtain from (2. 12)

$$\text{(2. 15)} \qquad \begin{cases} \|B_\alpha(w)\| \leqq C\bar{\sigma}_2 \|Du\|_\infty \|Dw\| & \text{for } |\alpha| = 1 \text{ and} \\ \|B_\alpha(w)\| \leqq C\{(\bar{\sigma}_3 \|Du\|_\infty \|Du\| + \bar{\sigma}_2 \|D^2 u\|) \|Dw\|_\infty \\ \qquad + \bar{\sigma}_2 \|Du\|_\infty \|D^2 w\|\} & \text{for } |\alpha| = 2. \end{cases}$$

Now using Sobolev's inequality and the definition of $E(t)$, we have (for $\alpha \neq 0$):

$$|(B_\alpha(w), D^\alpha w)| \leqq C \max\left\{1, \frac{1}{\underline{\sigma}_1}\right\}^2 (\bar{\sigma}_2 E^{3/2}(t) + \bar{\sigma}_3 E^2(t)).$$

Combining (2. 13), (2. 14) and this last estimate we obtain

$$\text{(2. 16)} \qquad \frac{1}{2}\frac{d}{dt}(A_0(u)D^\alpha w, D^\alpha w) \leqq C \max\left\{1, \frac{1}{\underline{\sigma}_1}\right\}^2 (\bar{\sigma}_2 E^{1/2}(t) + \bar{\sigma}_3 E(t))\, E(t) - [\sigma'(u) D^\alpha u D^\alpha v]\,(0, t).$$

It remains to estimate the boundary terms in this inequality. For $\alpha = (0, 1)$, we use (2. 2) to obtain

$$\text{(2. 17)} \qquad \begin{aligned} -\sigma' D^\alpha u D^\alpha v &= -\sigma' u_t v_t = -\sigma(u)_t v_t \\ &= -\frac{k}{2}\frac{d}{dt}(s')^2 - r(s'')^2. \end{aligned}$$

For $\alpha = (1, 0)$, we use (2. 1) and (2. 17) to deduce

$$\begin{aligned} -\sigma' D^\alpha u D^\alpha v &= -\sigma' u_x v_x = -u_t v_t \\ &= \frac{1}{\sigma'}\left[-\frac{k}{2}\frac{d}{dt}(s')^2 - r(s'')^2\right] \\ &= -\frac{k}{2}\frac{d}{dt}\left[\frac{(s')^2}{\sigma'}\right] - \frac{r}{\sigma'}(s'')^2 - \frac{k}{2}\frac{\sigma''}{(\sigma')^2} u_t (s')^2. \end{aligned}$$

Then we use Sobolev's inequality to estimate u_t, and the fact that $E(t) \geqq \frac{1}{2} k |s'|^2$ to obtain

$$\text{(2. 18)} \qquad -\sigma' u_x v_x \leqq -\frac{k}{2}\frac{d}{dt}\left[\frac{(s')^2}{\sigma'}\right] - \frac{r(s'')^2}{\sigma'} + CE^{3/2}(t).$$

Next we turn to the case $\alpha=(0, 2)$. We find that

$$-\sigma' D^\alpha u D^\alpha v = -\sigma' u_{tt} v_{tt} = -\sigma(u)_{tt} v_{tt} + \sigma''(u) u_t^2 v_{tt} \tag{2.19}$$

$$= -\frac{k}{2}\frac{d}{dt}(s'')^2 - r(s''')^2 + \sigma''(u) u_t^2 s'''$$

$$\leqq -\frac{k}{2}\frac{d}{dt}(s'')^2 - r(1-\varepsilon)(s''')^2 + \frac{C}{\varepsilon r} E^2(t).$$

Here we have used Sobolev again to estimate u_t in terms of $E(t)$. The case $\alpha=(1, 1)$ is a bit more complicated. By virtue of (2. 1),

$$-\sigma' u_{xt} v_{xt} = -u_{tt} v_{tt} + \sigma''(u) u_x u_t u_{tt}.$$

Using (2. 19) we find

$$-u_{tt} v_{tt} \leqq \frac{1}{\sigma'}\left[-\frac{k}{2}\frac{d}{dt}(s'')^2 - r(1-\varepsilon)(s''')^2 + \frac{C}{\varepsilon r} E^2(t)\right] \tag{2.20}$$

$$\leqq -\frac{k}{2}\frac{d}{dt}\left[\frac{(s'')^2}{\sigma'}\right] - \frac{r(1-\varepsilon)}{\sigma'}(s''')^2 + C_1 E^{3/2}(t) + C(\varepsilon r)^{-1} E^2(t).$$

From the boundary condition (2. 2),

$$u_{tt} = \frac{1}{\sigma'}[r s''' + k s'' - \sigma'' u_t^2].$$

We note that $u_x = \frac{v_t}{\sigma'} = \frac{s''}{\sigma'}$ so that $k s'' u_x u_t = \frac{k(s'')^2}{\sigma'} u_t$. This yields

$$\sigma''(u) u_x u_t u_{tt} = \left[\frac{\sigma''}{\sigma'}\right][r s''' + k s'' - \sigma'' u_t^2] u_x u_t \tag{2.21}$$

$$\leqq \left[\frac{r}{\sigma'}\right]\left[\varepsilon (s''')^2 + \frac{1}{\varepsilon}(\sigma'')^2 u_x^2 u_t^2\right]$$

$$+ \frac{\sigma''}{(\sigma')^2} k (s'')^2 u_t - \frac{(\sigma'')^2}{\sigma'} u_t^3 u_x$$

$$\leqq r\frac{\varepsilon (s''')^2}{\sigma'} + C_1 E^{3/2}(t) + C_2\left[\frac{r}{\varepsilon} + 1\right] E^2(t).$$

Hence combining (2. 20) and (2. 21) we find

$$-\sigma' u_{xt} v_{xt} \leqq -\frac{k}{2}\frac{d}{dt}\left[\frac{(s'')^2}{\sigma'}\right] - \frac{r(1-2\varepsilon)}{\sigma'}(s''')^2 + C_1 E^{3/2}(t) + C_2\left[\frac{1}{\varepsilon r} + \frac{r}{\varepsilon} + 1\right] E^2(t). \tag{2. 22}$$

Finally, we tackle the case $\alpha = (2, 0)$. Again by virtue of (2. 1) we have

$$-\sigma' u_{xx} v_{xx} = -u_{xt} v_{xt} + \sigma'' u_x^2 u_{xt}.$$

From (2. 22) we see that

$$-u_{xt} v_{xt} \leqq -\frac{k}{2}\frac{d}{dt}\left[\frac{s''}{\sigma'}\right]^2 - \frac{r(1-2\varepsilon)}{(\sigma')^2}(s''')^2 + C_3 E^{3/2}(t) + C_2\left[\frac{1}{\varepsilon r} + \frac{r}{\varepsilon} + 1\right] E^2(t) \tag{2. 23}$$

and

$$\begin{aligned}
\sigma'' u_x^2 u_{xt} &= \frac{\sigma''}{\sigma'} u_x^2 [v_{tt} - \sigma'' u_t u_x] \\
&= \frac{\sigma''}{\sigma'} u_x^2 s''' - \frac{(\sigma'')^2}{\sigma'} u_t u_x^3 \\
&\leqq \frac{\varepsilon r}{(\sigma')^2}(s''')^2 + \frac{1}{\varepsilon r}(\sigma'')^2 u_x^4 + \frac{(\sigma'')^2}{\sigma'} u_t u_x^3 \\
&\leqq \frac{\varepsilon r}{(\sigma')^2}(s''')^2 + C_4 E^2(t) + \frac{1}{\varepsilon r} C_5 E^2(t).
\end{aligned}$$

Combining (2. 23) and this last inequality we have

$$-\sigma' u_{xx} v_{xx} \leqq -\frac{k}{2}\frac{d}{dt}\left[\frac{s''}{\sigma'}\right]^2 - \frac{r(1-3\varepsilon)}{(\sigma')^2}(s''')^2 + C_3 E^{3/2}(t) + C_6\left[\frac{1}{\varepsilon r} + \frac{r}{\varepsilon} + 1\right] E^2(t). \tag{2. 24}$$

To conclude we substitute (2. 17), (2. 18), (2. 19), (2. 22) and (2. 24) into (2. 16) and sum over $\alpha \neq 0$:

$$\frac{1}{2}\frac{d}{dt}\sum_{1\leqq|\alpha|\leqq 2}(A_0(u)D^\alpha w, D^\alpha w)+\frac{k}{2}\frac{d}{dt}\sum_{1\leqq|\alpha|\leqq 2}(\sigma')^{-\alpha_1}[\partial_t^{|\alpha|}s]^2$$

$$\leqq C_1 E^{3/2}(t)+C_2\left[\frac{1}{\varepsilon r}+\frac{r}{\varepsilon}+1\right]E^2(t)$$

$$-r\left\{\left[1+\frac{1}{\sigma'}\right](s'')^2+\left[(1-\varepsilon)+\frac{(1-2\varepsilon)}{\sigma'}+\frac{(1-3\varepsilon)}{(\sigma')^2}\right](s''')^2\right\}.$$

The statement of Theorem 2. 1 follows from this estimate and (2. 8) and (2. 10) if we fix the value of ε, at say $\varepsilon = 1/6$.

3. Dependence of the solution on the boundary values

If the negative terms on the right hand side of the inequality (2. 7) dominate the other terms, then the energy of the solution decreases and blow up does not occur. Therefore we prove in this section an estimate for these negative terms. In section 5 we combine this estimate and (2. 7) to obtain a differential inequality for $E(t)$.

As in the last section, we assume that $(u, v) \in C^3([0, L]\times[0, T])$ is a solution of (2. 1) and (2. 2). We set $\bar{E} = \sup_{0\leqq t\leqq T} E(t)$. In this section we shall prove the following theorem.

Theorem 3. 1. *Let* $T^* = 2L(\underline{\sigma}_1)^{-1/2}$ *and assume the initial data satisfies* (1. 8):

$$\int_0^L u^0(x)\,dx + s^0 = 0.$$

If $T > 2T^*$, *then there are constants* C *and* a_1 *independent of* r *and* k, *but which depend on* $\sup_{\substack{0\leqq x\leqq L\\ 0\leqq t\leqq T}}|u(x, t)|$, *such that for* $2T^* \leqq t \leqq T$,

$$\int_0^t E(\tau)\,d\tau \leqq C\exp(a_1\bar{E}^{1/2})\int_0^t [(r^2+k^2+1)(|s'|^2+|s''|^2)$$

$$+(1+r^2)|s'''|^2+E(\tau)^2]\,d\tau. \tag{3. 1}$$

The proof is based on several lemmas. For $(x, t) \in [0, L]\times[0, T]$ we let $\tau(\xi; x, t)$ be the solution of

$$\frac{d\tau}{d\xi} = \lambda(\xi, \tau), \qquad \tau(x; x, t) = t, \tag{3. 2}$$

where $\lambda(x, t) = [\sigma'(u(x, t))]^{-1/2}\cdot\xi \mapsto (\xi, \tau(\xi; x, t))$ is the positive characteristic through (x, t). Let $\tau_x = (\partial_x\tau)(\xi; x, t)$ and $\tau_t = (\partial_t\tau)(\xi; x, t)$.

Lemma 3. 2. *We have*

(i) (3. 3) $$\tau_x(\xi; x, t) = -\lambda(x, t)\,\tau_t(\xi; x, t).$$

(ii) *There exist constants C and a such that for* $0 \leqq \xi \leqq x \leqq L$, $0 \leqq t \leqq T$,

(3. 4) $$\exp(-a\bar{E}^{1/2}) \leqq |\tau_t(\xi; x, t)| \leqq \exp(a\bar{E}^{1/2}),$$

(3. 5) $$C^{-1}\exp(-a\bar{E}^{1/2}) \leqq |\tau_x(\xi; x, t)| \leqq C\exp(a\bar{E}^{1/2}),$$

and

(3. 6) $$|\tau_{xx}(\xi; x, t)| \leqq C\exp(3a\bar{E}^{1/2}) \times [E^{1/2}(t) + \int_\xi^x E(\tau(\eta; x, t))\,d\eta + \int_\xi^x |u_{tt}(\eta; \tau(\eta; x, t))|\,d\eta].$$

Proof. Note that τ_x and τ_t satisfy the same linear differential equation, but with different initial conditions:

(3. 7) $$\frac{d}{d\xi}\tau_x = \lambda_t(\xi, \tau)\tau_x, \quad \tau_x(x; x, t) = -\lambda(x, t),$$

(3. 8) $$\frac{d}{d\xi}\tau_t = \lambda_t(\xi, \tau)\tau_t, \quad \tau_t(x; x, t) = 1.$$

Equation (3. 3) follows from (3. 7) and (3. 8). Furthermore

(3. 9) $$\tau_t(\xi; x, t) = \exp\int_x^\xi \lambda_t(\eta, \tau(\eta; x, t))\,d\eta.$$

But $\lambda_t = \partial_t[\sigma'(u(x, t))]^{-1/2} = -\frac{1}{2}[\sigma'(u)]^{-3/2}\sigma'' u_t$, so

(3. 10) $$|\lambda_t| \leqq \frac{\bar{\sigma}_2 |u_t(x, t)|}{2(\underline{\sigma}_1)^{3/2}} \leqq aE^{1/2}(t, w)$$

where we have used the Sobolev embedding Theorem and the definition (2. 5) of $E(t)$. Inequality (3. 4) is an immediate consequence of (3. 9) and (3. 10), and (3. 5) follows from (3. 3) and (3. 4).

To derive (3. 6) we observe that τ_{xx} solves the initial value problem

(3. 11) $$\begin{cases} \dfrac{d}{d\xi}\tau_{xx} = \lambda_t\tau_{xx} + \lambda_{tt}(\tau_x)^2, \\ \\ \tau_{xx}(x; x, t) = -\lambda_x(x, t) + (\lambda\lambda_t)(x, t). \end{cases}$$

Indeed, the initial condition follows from differentiating the initial condition $\tau_x(x; x, t) = -\lambda(x, t)$ with respect to x:

$$\begin{aligned}\tau_{xx}(x; x, t) &= -\tau_{x\xi}(x; x, t) - \lambda_x(x, t)\\ &= -\lambda_t(x, t)\,\tau_x(x; x, t) - \lambda_x(x, t)\\ &= -\lambda_x(x, t) + \lambda_t(x, t)\,\lambda(x, t).\end{aligned}$$

Now we integrate (3. 11) from ξ to x and use (3. 5) and (3. 10) to obtain

$$\begin{aligned}(3.12)\qquad |\tau_{xx}(\xi; x, t)| &= |\tau_{xx}(x; x, t)\exp\left[\int_x^\xi \lambda_t\,d\eta\right]\\ &\quad + \int_x^\xi \exp\left[\int_\zeta^\xi \lambda_t\,d\eta\right]\lambda_{tt}(\tau_x)^2\,d\zeta|\\ &\leqq |\lambda_x + \lambda\lambda_t|\exp(a\bar{E}^{1/2}) + C^2\exp(3a\bar{E}^{1/2})\int_\xi^x |\lambda_{tt}|\,d\zeta.\end{aligned}$$

In the same manner as we obtained (3. 10), we may deduce that

$$|\lambda_x + \lambda\lambda_t| = |\lambda_x + \frac{1}{2}(\lambda^2)_t| \leqq C_1 E^{1/2}(t, w),$$

and

$$\begin{aligned}|\lambda_{tt}(x, t)| &\leqq C_2 u_t^2(x, t) + C_3|u_{tt}(x, t)|\\ &\leqq C_4 E(t, w) + C_3|u_{tt}(x, t)|.\end{aligned}$$

We insert these estimates into (3. 12) to arrive at (3. 6). This completes the proof of Lemma 3. 2.

Lemma 3. 3. *There exist constants C and a_1 independent of r, k and T such that*

$$\begin{aligned}(3.13)\qquad &\sum_{0\leqq|\alpha|\leqq 2}\int_0^t\int_0^L (|D^\alpha v|^2 + |D^\alpha u|^2)\,dx\,d\tau\\ &\qquad \leqq C\exp(a_1\bar{E}^{1/2})\int_0^t \sum_{i=0}^2 (|D_t^i v(0, \tau)|^2 + |D_t^i u(0, \tau)|^2)\,d\tau\end{aligned}$$

for $2T^* \leqq t \leqq T$.

Proof. We show how to estimate the integral of v_{xx}^2. The estimates for the other terms are similar or simpler. Fix $x \in [0, L]$ and $t \in [T^*, T]$. To simplify the notation, we shall denote the mapping $\eta \mapsto \tau(0; x, \eta)$ for $T^* \leqq \eta \leqq t$ by $\eta \mapsto \tau(\eta)$. The Riemann invariants are

$$\alpha = \frac{1}{2}(v - \int_0^u \sqrt{\sigma'(\eta)}\,d\eta), \quad \beta = \frac{1}{2}(v + \int_0^u \sqrt{\sigma'(\eta)}\,d\eta).$$

These functions satisfy $\alpha_t+\sqrt{\sigma'(u)}\,\alpha_x=0$, $\beta_t-\sqrt{\sigma'(u)}\,\beta_x=0$. Thus α is constant on positive characteristics, and β is constant on negative characteristics. Note that $v=\alpha+\beta$ and

$$\int_{T^*}^{t} v_{xx}^2(x,\eta)\,d\eta \leqq 2\int_{T^*}^{t} \alpha_{xx}^2(x,\eta)\,d\eta + 2\int_{T^*}^{t} \beta_{xx}^2(x,\eta)\,d\eta. \tag{3.14}$$

Because α is constant on positive characteristics we have

$$\begin{aligned}\int_{T^*}^{t} \alpha_{xx}^2(x,\eta)\,d\eta &\leqq 2\int_{T^*}^{t} \alpha_{tt}^2(0,\tau(\eta))\,\tau_x^4\,d\eta + 2\int_{T^*}^{t} \alpha_t^2(0,\tau(\eta))\,|\tau_{xx}|^2\,d\eta \\ &= 2(I_1+I_2).\end{aligned} \tag{3.15}$$

To estimate I_1 we use the inverse $\tau\mapsto\eta(\tau)$ of the mapping $\eta\mapsto\tau(\eta)$ to transform the integral to an integral over τ and observe that

$$\frac{d\eta}{d\tau}=\frac{1}{\dfrac{d\tau}{d\eta}}=\frac{1}{\tau_t(0;x,\eta)}.$$

Since $\tau(t)\leqq t$ we obtain by (3.3)—(3.5)

$$I_1 \leqq C^2(\underline{\sigma}_1)^{-1}\exp(3a\bar{E}^{1/2})\int_0^t \alpha_{tt}^2(0,\tau)\,d\tau. \tag{3.16}$$

To estimate I_2 we first assume $t-T^*\geqq 1$, choose N as the greatest integer in $(t-T^*)$ and set $l=(t-T^*)/(N+1)$. Then $1/2\leqq l\leqq 1$ and

$$\begin{aligned} I_2 &= \sum_{n=1}^{N+1}\int_{(n-1)l+T^*}^{nl+T^*} \alpha_t^2\,|\tau_{xx}|^2\,d\eta \\ &\leqq \sum_{n=1}^{N+1}\left[\int_{(n-1)l+T^*}^{nl+T^*} |\tau_{xx}|^2\,d\eta \sup_{(n-1)l\leqq\eta-T^*\leqq nl}\alpha_t^2(0,\tau(\eta))\right] \\ &\leqq \sup_{1\leqq n\leqq N+1}\left[\int_{(n-1)l+T^*}^{nl+T^*} |\tau_{xx}|^2\,d\eta\right]\left[\sum_{n=1}^{N+1}\int_{(n-1)l+T^*}^{nl+T^*}\left(\frac{1}{l}\,\alpha_t^2+|\partial_\eta\alpha_t^2|\right)d\eta\right] \\ &\leqq \sup_{1\leqq n\leqq N+1}\left[\int_{(n-1)l+T^*}^{nl+T^*} |\tau_{xx}|^2\,d\eta\right]\left[\int_{T^*}^{t}\left(3\alpha_t^2+\alpha_{tt}^2\left(\frac{d\tau}{d\eta}\right)^2\right)d\eta\right] \\ &\leqq \sup_{1\leqq n\leqq N+1}\Bigg\{C^2\exp(6a\bar{E}^{1/2}) \\ &\quad\cdot\int_{(n-1)l+T^*}^{nl+T^*}\left[\bar{E}^{1/2}+L\bar{E}+\int_0^x |u_{tt}(\zeta,\tau(\zeta;x,\eta))|\,d\zeta\right]^2 d\eta\Bigg\} \\ &\quad\cdot\int_{T^*}^{t}(3\alpha_t^2+\alpha_{tt}^2\,\tau_t(0;x,\eta)^2)\,d\eta. \end{aligned} \tag{3.17}$$

In the last step we used (3.6). If $0<t-T^*\leqq 1$, then obviously the same estimate holds. Let

$$\Gamma_n=\{(\zeta,\tau):0<\zeta<x \quad \text{and} \quad \tau(\zeta;x,(n-1)l+T^*)<\tau<\tau(\zeta;x,nl+T^*)\}$$

be the region bounded by the positive characteristics through $(x,(n-1)l+T^*)$ and $(x,nl+T^*)$. We have by (3.4) and Cauchy-Schwarz inequality

$$\begin{aligned}\int_{(n-1)l+T^*}^{nl+T^*}\left[\int_0^x |u_{tt}(\zeta,\tau(\zeta;x,\eta))|\,d\zeta\right]^2 d\eta &\leqq x\int_{\Gamma_n}|u_{tt}(\zeta,\tau)|^2\frac{d(\zeta,\tau)}{\tau_t(\zeta;x,\eta)}\\ &\leqq L\exp(a\bar{E}^{1/2})\int_{\Gamma_n}|u_{tt}(\zeta,\tau)|^2\,d(\zeta,\tau)\\ &\leqq L\exp(a\bar{E}^{1/2})\int_{t_1}^{t_2}\int_0^L|u_{tt}(\zeta,\tau)|^2\,d\zeta\,d\tau\\ &\leqq L\exp(a\bar{E}^{1/2})\,(t_2-t_1)\,2\underline{\sigma}_1^{-1}\bar{E}\\ &\leqq L\exp(a\bar{E}^{1/2})\,(1+L\underline{\sigma}_1^{-1/2})\,2\underline{\sigma}^{-1}\bar{E},\end{aligned}$$

with $t_1=\tau(0;x,(n-1)l+T^*)$ and $t_2=nl+T^*$. We also used that $l\leqq 1$ and

$$|\tau_\xi|=|\lambda|\leqq\underline{\sigma}_1^{-1/2}.$$

We combine this last inequality with (3.17) to deduce that

$$I_2\leqq C\exp(7a\bar{E}^{1/2})\int_{T^*}^{t}(3\alpha_t^2+\alpha_{tt}^2\tau_t(0;x,\eta)^2)\,d\eta.$$

The second factor in this inequality involving the integrals α_t^2 and α_{tt}^2 can be estimated in the same way as the term I_1 in (3.16). Putting together the last estimate and (3.15), (3.16), we finally arrive at

$$\int_{T^*}^{t}\alpha_{xx}^2(x,\eta)\,d\eta\leqq C\exp(7a\bar{E}^{1/2})\int_0^t[\alpha_t^2(0,\tau)+\alpha_{tt}^2(0,\tau)]\,d\tau. \tag{3.18}$$

β is constant on negative characteristics, and the boundary condition $v(L,t)=0$ implies $\beta(L,t)=-\alpha(L,t)$. Thus we have

$$\begin{aligned}\beta(x,\eta)_{xx}&=\beta(L,\tau_-(\eta))_{xx}=-\alpha(L,\tau_-(\eta))_{xx}\\ &=-\alpha(0,\tau(0;L,\tau_-(L;x,\eta)))_{xx}.\end{aligned}$$

The mapping $\eta \mapsto \tau(0; L, \tau_-(L; x, \eta))$ has the same properties as the mapping

$$\eta \mapsto \tau(0; x, \eta)$$

and by the choice of $T^* = 2L(\underline{\sigma}_1)^{-1/2}$, we have $\tau(0; L, \tau_-(L; x, \eta)) \geqq 0$ for $\eta \geqq T^*$. Thus we may derive an estimate for the integral of β_{xx}^2 which is analogous to (3. 18). From (3. 14) we thus obtain

$$\int_0^L \int_{T^*}^t v_{xx}^2(x, \eta)\, d\eta\, dx \leqq LC \exp(a_1 \bar{E}^{1/2}) \int_0^t [\alpha_t^2(0, \tau) + \alpha_{tt}^2(0, \tau)]\, d\tau. \tag{3. 19}$$

If we add together the estimates of the form (3. 19) over all the terms in (3. 13), and use the fact that α and its derivatives can be estimated by u, v and their derivatives, we obtain

$$\int_{T^*}^t \int_0^L \sum_{|\alpha| \leqq 2} (|D^\alpha u|^2 + |D^\alpha v|^2)\, dx\, d\eta \leqq C \exp(a_1 \bar{E}^{1/2}) \int_0^t \sum_{i=0}^2 |D_t^i u(0, \tau)|^2 + |D_t^i v(0, \tau)|^2\, d\tau. \tag{3. 20}$$

Finally, using the forward characteristics instead of the backward characteristics, we can derive an estimate identical to (3. 20) with the limits of integration being $[0, T^*]$ on the left, and $[0, 2T^*]$ on the right. This completes the proof of Lemma 3. 3.

Lemma 3. 4. *Suppose that* $\int_0^L u^0(x)\, dx + s_0 = 0$. *Then there is a constant* C *such that for* $2T^* \leqq t \leqq T$,

$$\int_0^t [|u(0, \tau)|^2 + (1+k)^2\, s^2(\tau)]\, d\tau \leqq C \int_0^t [(r^2 + k^2)\, |s'(\tau)|^2 + (1 + r^2)\, |s''|^2]\, d\tau. \tag{3. 21}$$

C is independent of r, k, and T.

Proof. Let $\tau(\xi; x, t)$ denote the positive characteristic through (x, t), and $\tau_-(\xi; x, t)$ the negative characteristic; α and β the Riemann invariants. Since $\xi \to \alpha(\xi, \tau(\xi))$ and $\xi \to \beta(\xi, \tau_-(\xi))$ are constant, and $(\alpha + \beta)(L, t) = 0$, it follows that for $x, x' \in [0, L]$,

$$\begin{aligned} \left| \int_0^{u(x,t)} \sqrt{\sigma'(\tau)}\, d\tau - \int_0^{u(x',t)} \sqrt{\sigma'(\tau)}\, d\tau \right| &= |\beta(x, t) - \alpha(x, t) - (\beta(x', t) - \alpha(x', t))| \\ &= |\beta(L, \tau_-(L, x, t)) - \beta(L, \tau_-(L, x', t)) \\ &\quad - (\alpha(0, \tau(0; x, t)) - \alpha(0, \tau(0; x', t)))| \\ &\leqq |\alpha(0, \tilde{\tau}) - \alpha(0, \tilde{\tau}')| + |\alpha(0, \tau) - \alpha(0, \tau')| \end{aligned} \tag{3. 22}$$

where $\tau=\tau(0; x, t)$, $\tau'=\tau(0; x', t)$, $\tilde{\tau}=\tau(0; L, \tau_-(L, x, t))$, and $\tilde{\tau}'=\tau(0; L, \tau_-(L, x', t))$. From the definition of α,

$$|\alpha(0,\tau)-\alpha(0,\tau')| \leqq \frac{1}{2}|v(0,\tau)-v(0,\tau')| + \frac{1}{2}(\bar{\sigma}_1)^{1/2}|u(0,\tau)-u(0,\tau')|. \tag{3.23}$$

Hence from (3.22) and (3.23), we have

$$\begin{aligned}(\underline{\sigma}_1)^{1/2}|u(x,t)-u(x',t)| &\leqq \frac{1}{2}[|v(0,\tilde{\tau})-v(0,\tilde{\tau}')|+|v(0,\tau)-v(0,\tau')|] \\ &\quad +(\bar{\sigma}_1)^{1/2}[|u(0,\tilde{\tau})-u(0,\tilde{\tau}')|+|u(0,\tau)-u(0,\tau')|].\end{aligned} \tag{3.24}$$

Since $v(0, t)=s'(t)$, we find that

$$|v(0,\tau)-v(0,\tau')| \leqq (T^*)^{1/2}\left[\int_{t-T^*}^{t}|s''|^2\,d\tau\right]^{1/2},$$

and from the boundary condition $\sigma(u(0, t))=rs'+ks$, we see that

$$\begin{aligned}|u(0,\tau)-u(0,\tau')| &= |\sigma^{-1}(rs'(\tau)+ks(\tau))-\sigma^{-1}(rs'(\tau')+ks(\tau'))| \\ &\leqq (\underline{\sigma}_1)^{-1}(T^*)^{1/2}\left\{r\left[\int_{t-T^*}^{t}|s''|^2\,d\tau\right]^{1/2}+k\left[\int_{t-T^*}^{t}|s'|^2\,d\tau\right]^{1/2}\right\}.\end{aligned}$$

If we substitute these estimates into (3.24), we obtain

$$|u(x,t)-u(x',t)|^2 \leqq C\left\{(1+r)^2\int_{t-T^*}^{t}|s''|^2\,d\tau+k^2\int_{t-T^*}^{t}|s'|^2\,d\tau\right\}. \tag{3.25}$$

In (3.25) we intend to take $x=0$ and $x'=x_0$ where $x\to u(x, t)$ takes on its average value. From the differential equations (2.1) and the boundary conditions (2.2) we have

$$\frac{d}{dt}\left[\int_0^L u(x,t)\,dx+s(t)\right]=\int_0^L v_x(x,t)\,dt+s'(t)=0.$$

Hence the condition (1.8) implies that

$$\int_0^L u(x,t)\,dx+s(t)=0 \quad \text{for all } t.$$

For each t, let $x_0 = x_0(t)$ be the point where

$$Lu(x_0, t) = \int_0^L u(x, t)\, dx = -s(t). \tag{3.26}$$

Then by virtue of (2.2),

$$\sigma(u(0, t)) = rs'(t) - kLu(x_0, t)$$

or

$$\sigma(u(0, t)) + kLu(0, t) = rs'(t) + kL(u(0, t) - u(x_0, t)).$$

Hence

$$(\underline{\sigma}_1 + kL)\, |u(0, t)| \leqq r|s'(t)| + kL|u(0, t) - u(x_0, t)|$$

so that using (3.25) we have

$$|u(0, t)|^2 \leqq C \left\{ r^2 |s'(t)|^2 + (1+r)^2 \int_{t-T^*}^{t} |s''|^2\, d\tau + k^2 \int_{t-T^*}^{t} |s'|^2\, d\tau \right\}, \tag{3.27}$$

where C is independent of k and r.

From the boundary condition (2.2) and from (3.26) we deduce

$$(1+k)\, |s(t)| \leqq (\bar{\sigma}_1 + L)\, |u(0, t)| + r|s'(t)| + L|u(0, t) - u(x_0, t)|$$

so that $|u(0, t)|^2 + (1+k)^2\, |s(t)|^2$ is also bounded by the right side of (3.27), with a larger constant C, independent of r, k, and T. We integrate the resulting inequality to obtain

$$\begin{aligned} &\int_{T^*}^{t} (|u(0, \tau)|^2 + (1+k)^2\, |s(\tau)|^2)\, d\tau \\ &\quad \leqq C \left\{ r^2 \int_{T^*}^{t} |s'(\tau)|^2\, d\tau + (1+r)^2 \int_{T^*}^{t} \int_{\tau - T^*}^{\tau} |s''(\eta)|^2\, d\eta\, d\tau \right. \\ &\qquad \left. + k^2 \int_{T^*}^{t} \int_{\tau - T^*}^{\tau} |s'(\eta)|^2\, d\eta\, d\tau \right\} \\ &\quad \leqq C \int_0^t [(r^2 + k^2)\, |s'|^2 + (1+r)^2\, |s''|^2]\, d\eta. \end{aligned} \tag{3.28}$$

Finally, if we use the forward characteristics in (3.22) instead of the backward characteristics, we obtain in the same way the inequality

$$\int_0^{T^*} (|u(0, \tau)|^2 + (1+k)^2\, |s(\tau)|^2)\, d\tau \leqq C \int_0^{2T^*} [(r^2 + k^2)\, |s'|^2 + (1+r)^2\, |s''|^2]\, d\eta.$$

Addition of this inequality to (3.28) yields (3.21).

Proof of Theorem 3. 1. From the definition of $E(t)$ and Lemma 3. 3, we have

$$\int_0^t E(\tau)\,d\tau \leqq C\left\{\exp(a_1\bar{E}^{1/2})\sum_{i=0}^{2}\int_0^t (|D_t^i u(0,\tau)|^2+|D_t^i v(0,\tau)|^2)\,d\tau + k\int_0^t (|s|^2+|s'|^2+|s''|^2)\,d\tau\right\}. \tag{3. 29}$$

We wish to estimate the boundary values of $|D_t^i u|^2$ and $|D_t^i v|^2$ in terms of $|s'|^2$, $|s''|^2$, and $|s'''|^2$. The boundary condition $\sigma(u(0,t))=rs'(t)+ks(t)$ implies that

$$|u_t(0,t)| \leqq (\underline{\sigma}_1)^{-1}(r|s''(t)|+k|s'(t)|). \tag{3. 30}$$

Differentiating this boundary condition twice, we have

$$u_{tt}(0,t)=(\sigma'(u(0,t)))^{-1}[rs'''(t)+ks''(t)-\sigma''(u(0,t))\,u_t^2(0,t)].$$

We use Sobolev's inequality to estimate $u_t(0,t)$ and deduce that

$$|u_{tt}(0,t)| \leqq C[r|s'''(t)|+k|s''(t)|+E(t)]. \tag{3. 31}$$

Now use the fact that $v(0,t)=s'(t)$ and insert (3. 30) and (3. 31) into (3. 29). The latter becomes

$$\int_0^t E(\tau)\,d\tau \leqq C\exp(a_1\bar{E}^{1/2})\left\{\int_0^t (|u(0,\tau)|^2+k|s(\tau)|^2)\,d\tau + \int_0^t [(1+k+k^2)|s'|^2+(1+r^2+k+k^2)|s''|^2 + (1+r^2)|s'''|^2+E^2(\tau)]\,d\tau\right\}. \tag{3. 32}$$

Finally we use the estimate of Lemma 3. 4 to take care of the first integral of the right side of (3. 32). The proof of Theorem 3. 1 is complete.

4. Global existence

The "energy" is related to the supnorms as follows: There is a constant E^0 such that if $w=(u,v)$ is a C^2 solution of (2. 1)—(2. 2) with $E(t,w) \leqq E^0$, then

$$\sup_{0\leqq x\leqq L} |D^\alpha u(x,t)|,\quad |D^\alpha v(x,t)|,\quad s^{(j)}(t) \leqq C_0\,E(t,w)^{1/2}, \tag{4. 1}$$

for $|\alpha| \leqq 1$ and $j=0,1,2$, where C_0 depends on r and k.

The inequality for $D^\alpha v$ and $s^{(j)}$ follows directly from the definition of $E(t,w)$ and from the Sobolev inequality. Since $u_t=v_x$, (4. 1) is also valid for u_t. Integrating the second differential equation of (2. 1) and using (2. 2) we see that

$$\sigma(u(x,t))=rs'+ks+\int_0^x v_t(\xi,t)\,d\xi.$$

Hence $|\sigma(u(x,t))| \leqq C_1 E(t,w)^{1/2}$ where C_1 depends on r and k. Since $\sigma' > 0$ on I, there is a value E^0 such that $E(t,w) \leqq E^0$ implies that $\sup_{0 \leqq x \leqq L} |u(x,t)|$ satisfies (4. 1). Then a second appeal to the definition of $E(t,w)$ and the Sobolev inequality show that u_x also satisfies (4. 1).

To simplify the statement of the next theorem we shall assume $E^0 = 1$.

Theorem 4. 1. *Assume that the initial data $u^0, v^0 \in C^n([0,L])$ with $n \geqq 3$ satisfy the compatibility conditions*

$$r s_{j+1} + k s_j = \partial_t^{(j)} \sigma(u^0)(0), \qquad \partial_t^j v^0(L) = 0$$

for $j = 0, \ldots, n$. Here $s_0 = s^0$, and $s_{j+1} = \partial_t^j v^0(0)$, $\partial_t^{(j)} \sigma(u^0)(0)$, $\partial_t^{(j)} v^0(L)$ are determined from u^0 and v^0 via the differential equations (1. 1) *and* (1. 2). *In addition, assume that* (1. 8) *is satisfied*:

$$\int_0^L u^0(x)\,dx + s^0 = 0.$$

Then for $E(0)$ sufficiently small, the solution (u, v) of (2. 1), (2. 2) *exists in C^n for all $t \geqq 0$. Moreover, there are constants C and a such that*

$$E(t) \leqq C e^{-at} E(0).$$

Proof. By the local existence theorem the local C^n-solution w can be continued as long as $\sum_{|\alpha| \leqq 1} \|D^\alpha w(\cdot, t)\|_\infty$ remains bounded, and therefore, by (4. 1), as long as $E(t)$ remains bounded. Suppose that $E(0) \leqq 1/4$. Then the local C^n solution must satisfy $E(t) \leqq 1$ for some interval $[0, \delta]$. In this interval the differential inequality (2. 7) implies

$$\frac{d}{dt} E(t) \leqq 2 C_1^* E(t)^{3/2} \tag{4. 2}$$

hence

$$E(t)^{1/2} \leqq \frac{E(0)^{1/2}}{1 - t C_1^* E(0)^{1/2}} \leqq 2 E(0)^{1/2} \leqq 1 \tag{4. 3}$$

for $0 \leqq t \leqq T$, where $C_1^* = \frac{1}{2}\left(1 + \frac{r^2+1}{r}\right) C_1$ with the constant C_1 from (2. 7), and where

$$T = (2 C_1^* E(0)^{1/2})^{-1}$$

is a lower bound for the time of existence of the solution. This estimate shows that by taking $E(0)^{1/2}$ smaller if necessary, we can assume $T > 2T^*$, where $T^* = 2L(\underline{\sigma}_1^{-1/2})$ is the constant from Theorem 3. 1. Integration of the differential inequality (2. 7) and substitution of (3. 1) into the resulting inequality yields

$$E(t)+(K_1-K_2\sup_{0\leqq\tau\leqq t}E(\tau)^{1/2})\int_0^t E(\tau)\,d\tau\leqq E(0), \tag{4.4}$$

where

$$K_1=\frac{C_2 r}{C(r^2+k^2+1)\exp(a_1)},\quad K_2=(2C_1^*+C_2 r),$$

C, C_2, and a_1 being the constants of (2.7) and (3.1). We used that $\bar{E}=\sup_{0\leqq t\leqq T}E(t)\leqq 1$. Now

$$K_1-K_2\sup_{0\leqq\tau\leqq t}E(\tau)^{1/2}\geqq K_1-2K_2E(0)^{1/2}\geqq\frac{1}{2}K_1$$

for $E(0)\leqq K_1^2(16K_2^2)^{-1}$ by virtue of (4.3), whence, from (4.4),

$$E(t)+\frac{1}{2}K_1\int_0^t E(\tau)\,d\tau\leqq E(0) \tag{4.5}$$

for $2T^*\leqq t\leqq T$. This inequality implies $E(T)\leqq E(0)$. We may then repeat the estimates starting at T, and continue the solution for all $t\geqq 0$.

Finally we address the question of exponential decay. The mean value theorem and (4.5) yield the existence of a point $t_0\in[0,T]$ such that

$$\frac{1}{2}K_1TE(t_0)=\frac{1}{2}K_1\int_0^T E(\tau)\,d\tau\leqq E(0).$$

By taking $E(0)$ smaller if necessary we can assume $\frac{1}{2}K_1T\geqq 8$ so that

$$E(t_0)\leqq\frac{1}{8}E(0).$$

We integrate the inequality (4.2) from t_0 to T and deduce that $E(T)\leqq 4E(t_0)$ if $T-t_0\leqq(2C_1^*E^{1/2}(t_0))^{-1}$. However, this condition is satisfied because $E(t_0)\leqq E(0)$ whence $T-t_0\leqq T=(2C_1^*E^{1/2}(0))^{-1}\leqq(2C_1^*E^{1/2}(t_0))^{-1}$. Hence $E(T)\leqq\frac{1}{2}E(0)$. If we repeat this procedure we deduce that $E(nT)\leqq 2^{-n}E(0)$ for $n=1,2,3,\ldots$. Furthermore, by the choice of T, $E(t)\leqq 4E(nT)$, so that $E(t)\leqq 2^{2-n}E(0)$ for $nT\leqq t\leqq(n+1)T$. Thus

$$E(t)\leqq e^{(3-t/T)\ln 2}E(0)$$

where we have taken $n=[t/T]$, the greatest integer in t/T. The proof of Theorem 4.1 is complete.

5. Breakdown of solutions satisfying the second order boundary condition

In this section we prove that if the constant m in the boundary condition (1. 5) is positive, then for initial data which is small in an appropriate sense, a global smooth solution does not exist, contrary to the results of the last section. Instead, after finite time, the first derivatives of the solution become infinite. Our method of proof requires that the system (1. 1)—(1. 5) be truly nonlinear. We therefore must assume that $\sigma''(0)$ differs from zero which occurs in the gas dynamics case, and for definiteness we assume in this section that

$$\sigma''(0)<0. \tag{5. 1}$$

Our main result is stated in Theorem 5. 1 below in terms of the Riemann invariants

$$\alpha=\frac{1}{2}\left(v-\int_0^u \sqrt{\sigma'(\eta)}\,d\eta\right),\quad \beta=\frac{1}{2}\left(v+\int_0^u \sqrt{\sigma'(\eta)}\,d\eta\right).$$

First we introduce some definitions and notations. In the remainder of this paper we set

$$\|f\|=\sup_{0\leqq x\leqq L}|f(x)|.$$

Let $(u, v)\in C^2([0, L]\times[0, T))$ be a solution of the system (1. 1)—(1. 5), with $m, r, k>0$.

Definition. The number $T_{\max}=T_{\max}(u, v)>0$ is called maximal time of existence of (u, v), if (u, v) is a C^2-solution of (1. 1)—(1. 5) in $[0, L]\times[0, T_{\max})$, but cannot be extended to a C^2-solution in $[0, L]\times[0, T)$ for any $T>T_{\max}$.

Let $\gamma\mapsto\hat{u}(\gamma)$ be the inverse of the function

$$\gamma\mapsto\int_0^\gamma \sqrt{\sigma'(\eta)}\,d\eta,$$

and let

$$\hat{\sigma}(\gamma)=\sigma(\hat{u}(\gamma)),\quad c(\gamma)=\sqrt{\sigma'(\hat{u}(\gamma))},\quad q(\gamma)=\frac{c'(\gamma)}{c(\gamma)^{1/2}}=\frac{\sigma''(\hat{u}(\gamma))}{2[\sigma'(\hat{u}(\gamma))]^{3/2}}. \tag{5. 2}$$

Note that (5. 1) implies $q(0)<0$. Let

$$\alpha(x, 0)=\alpha^0(x),\quad \beta(x, 0)=\beta^0(x) \tag{5. 3}$$

be the initial data for α and β, and let

$$A=A(x, t)=c(\beta-\alpha)^{1/2}\alpha_x,\quad B=B(x, t)=c(\beta-\alpha)^{1/2}\beta_x. \tag{5. 4}$$

Moreover, let $\mu(u, v)$ be the diameter of $\operatorname{supp}(A(\cdot, 0), B(\cdot, 0))$, let $D=D(u, v)=\mu/m$, and let

$$\Delta(u, v)=\min_{0\leqq x\leqq L}\{A(x, 0), B(x, 0)\}. \tag{5. 5}$$

Theorem 5. 1. *To every $m_0>0$ there exists a constant $C=C(m_0)>0$ and to every $\delta>0$ there exist constants $D_0=D_0(m_0, \delta)$, $M=M(m_0, D_0)>0$ with the following property: Let (u, v) be a C^2-solution of (1. 1)—(1. 6) with $m \geqq m_0$ satisfying*

$$u^0(0)=v^0(0)=s^0=0, \tag{5. 6}$$

$$\delta=-\Delta(u, v)=-\min_{0\leqq x\leqq L}\{A(x, 0), B(x, 0)\}=\|A(\cdot, 0), B(\cdot, 0)\|, \tag{5. 7}$$

where the minimum is attained at some point $x_0 \in (0, L)$,

$$D(u, v)\leqq D_0, \tag{5. 8}$$

$$\|\alpha^0, \beta^0\|\leqq\frac{M}{1+T_1}\exp[-C(1+(1+T_1)^2)]. \tag{5. 9}$$

Here

$$T_1=T_1(\delta)=2T_0, \quad T_0=T_0(\delta)=-(\delta q(0))^{-1}. \tag{5. 10}$$

Then there exists a maximal time of existence $T_{\max}(u, v)\leqq T_1$ of (u, v) with

$$T_{\max}(u, v)\longrightarrow T_0(\delta)$$

for $\|\alpha^0, \beta^0\|\longrightarrow 0$ and $D(u, v)\longrightarrow 0$. Moreover, the solution satisfies

$$\|\alpha(\cdot, t), \beta(\cdot, t)\|\leqq\|\alpha^0, \beta^0\|\exp(C(1+t^2)), \tag{5. 11}$$

for all $0\leqq t<T_{\max}$, but

$$\lim_{t\nearrow T_{\max}}\|\alpha_x(\cdot, t), \beta_x(\cdot, t)\|=\infty.$$

To prove this theorem we need two lemmas, which we formulate first.

Lemma 5. 2. *To every $m_0>0$ there exist constants $C=C(m_0)>0$ and $M=M(m_0)$, $0<M\leqq 1$, such that for all $T\geqq 1$, and all solutions (u, v) of (1. 1)—(1. 5) with $m\geqq m_0$ satisfying (5. 6) and*

$$\|\alpha^0, \beta^0\|\leqq\frac{M}{\tilde{T}}\exp(-C(1+\tilde{T}^2)) \tag{5. 12}$$

we have

$$\sup_{\substack{0\leqq x\leqq L\\ 0\leqq t\leqq T}}\{|\alpha(x, t)|, |\beta(x, t)|\}\leqq\|\alpha^0, \beta^0\|\exp(C(1+T^2)) \tag{5. 13}$$

for all T, $0\leqq T<\min(\tilde{T}, T_{\max}(u, v))$.

The proof of Lemma 5. 2 is given in section 6. To state the second lemma, we need some definitions. Note that α and β satisfy

$$\alpha_t + c(\beta-\alpha)\alpha_x = 0,$$
$$\beta_t - c(\beta-\alpha)\beta_x = 0.$$

From these equations it easily follows that A and B defined in (5. 4) satisfy

$$\begin{aligned} A_t + c(\beta-\alpha)A_x &= q(\beta-\alpha)A^2, \\ B_t - c(\beta-\alpha)B_x &= q(\beta-\alpha)B^2. \end{aligned} \tag{5. 14}$$

Let the functions $\tau \mapsto x_\pm(\tau; x, t)$ be defined by

$$\frac{dx_\pm}{d\tau} = \pm c(\beta-\alpha)(x_\pm, \tau), \quad x_\pm(t; x, t) = x. \tag{5. 15}$$

Thus, $\tau \mapsto (x_\pm(\tau; x, t), \tau)$ are the characteristic curves through the point (x, t). We wish to follow A and B along reflected characteristics. For $0 \leqq x < L$ define the reflected characteristics $\tau \mapsto \Gamma_+(\tau, x)$ as follows:

$$\Gamma_+(\tau, x) = x_+(\tau; x, 0) \quad \text{for } 0 \leqq \tau \leqq \tau_1'$$

where $\tau_1' = \tau_{+,1}'(x)$ is the first positive time that $x_+(\tau_1'; x, 0) = L$;

$$\Gamma_+(\tau, x) = x_-(\tau; L, \tau_1') \quad \text{for } \tau_1' \leqq \tau \leqq \tau_1$$

where $\tau_1 = \tau_{+,1}(x) \geqq \tau_1'$ is the first time that $x_-(\tau_1; L, \tau_1') = 0$. In general, we will set

$$\begin{aligned} \Gamma_+(\tau, x) &= x_+(\tau; 0, \tau_j) \quad \text{for } \tau_j \leqq \tau \leqq \tau_{j+1}', \\ \Gamma_+(\tau, x) &= x_-(\tau; L, \tau_j') \quad \text{for } \tau_j' \leqq \tau \leqq \tau_j, \end{aligned} \tag{5. 16}$$

for $j = 1, 2, \ldots$. Also let $\tau_0 = \tau_0' = 0$. Finally we set

$$Z_+(\tau, x) = \begin{cases} A(\Gamma_+(\tau, x), \tau) & \text{for } \tau_j \leqq \tau \leqq \tau_{j+1}', \\ B(\Gamma_+(\tau, x), \tau) & \text{for } \tau_j' \leqq \tau \leqq \tau_j. \end{cases} \tag{5. 17}$$

The definition is consistent because the boundary condition (1. 3) implies $(\alpha+\beta)(L, t) = 0$, hence $A(L, t) = B(L, t)$. Analogously, for all x with $0 < x \leqq L$ we define the reflected characteristic $\Gamma_-(\tau, x)$ and the function $Z_-(\tau, x)$, where $\Gamma_-(\tau, x)$ starts as a negative characteristic at $(x, 0)$. If no confusion is possible we shall suppress the variable x and the + or − sign and write $\Gamma(\tau)$, $Z(\tau)$. From (5. 14)—(5. 17) we see that as long as $\Gamma(\tau)$ is not a boundary point, we have

$$\frac{d}{d\tau} Z(\tau) = q(\Gamma(\tau), \tau) Z^2(\tau), \tag{5. 18}$$

where we abbreviated $q((\beta-\alpha)(x,t))$ by $q(x,t)$. $Z(\tau)$ is continuous at times τ_j', but has jumps at the τ_j. Now we can state the second lemma:

Lemma 5.3. *There exist constants*

$$K=K(m_0)\geqq 1,\quad D_0=D_0(m_0)>0,\quad M=M(m_0,D_0)>0,$$

such that for all $\delta>0$, *all solutions* (u,v) *of* (1.1)—(1.5) *satisfying* (5.6)—(5.9), *and for all* $t<\min(T_1(\delta), T_{\max}(u,v))$ *we have*

$$(5.19)\qquad |Z(t,x)|\leqq\begin{cases}\dfrac{(1+K^{n^2}D_0)^n\,\|A(\cdot,0),B(\cdot,0)\|}{1+(1+K^{n^2}D_0)^n\,\|A(\cdot,0),B(\cdot,0)\|\int_0^t q(\Gamma(\eta,x),\eta)\,d\eta} \\ \qquad\qquad \text{if}\quad x\in\operatorname{supp}(A(\cdot,0),B(\cdot,0)) \\ \dfrac{(1+K^{n^2}D_0)^n K^{n^2}D_0\,\|A(\cdot,0),B(\cdot,0)\|}{1+(1+K^{n^2}D_0)^n\,\|A(\cdot,0),B(\cdot,0)\|\int_0^t q(\Gamma(\eta,x),\eta)\,d\eta} \\ \qquad\qquad \text{if}\quad x\notin\operatorname{supp}(A(\cdot,0),B(\cdot,0)).\end{cases}$$

Here n *is the largest integer with* $\tau_n(x)\leqq t$. *Moreover, if* D_0 *is chosen so small that* $K^{n^2}D_0<1$, *then*

$$(5.20)\qquad |Z(t,x_0)|\geqq\frac{(1-K^{n^2}D_0)^n\delta}{1+(1-K^{n^2}D_0)^n\delta\int_0^t q(\Gamma(\eta,x_0),\eta)\,d\eta}.$$

Here $x_0\in(0,L)$ *is the point where the minimum in* (5.7) *is attained, and* $Z=Z_+$ *if* $\delta=-A(x_0,0)$, $Z=Z_-$ *if* $\delta=-B(x_0,0)$.

This lemma is proved in section 7.

Proof of Theorem 5.1. The local existence theorem implies that the solution u, v of (1.1)—(1.5) can be continued as a C^2 solution as long as the first derivatives of u, v remain bounded. The differential equations (1.1), (1.2) show that u_t and v_t remain bounded as long as u_x and v_x, hence α_x and β_x, and therefore A, B remain bounded. From (5.17) we thus conclude that

$$(5.21)\qquad \limsup_{t\to t_0}\|Z_+(\cdot,t)\|=\infty\quad\text{or}\quad\limsup_{t\to t_0}\|Z_-(\cdot,t)\|=\infty$$

is equivalent to $t_0=T_{\max}$. Choose the constants D_0 and M small enough such that the assertions of Lemma 5.2 and 5.3 hold, and choose C as required in Lemma 5.2. Lemma 5.2 then implies that (5.11) is satisfied for all $t<\min(1+T_1(\delta), T_{\max}(u,v))$. (5.1), (5.2), and (5.10) imply

$$|q((\beta-\alpha)(x,t))-q(0)| \leqq C_1 \|\alpha^0, \beta^0\| \exp(C(1+t^2)) \leqq C_1 M(m_0),$$
$$|c((\beta-\alpha)(x,t))-c(0)| \leqq C_2 \|\alpha^0, \beta^0\| \exp(C(1+t^2)) \leqq C_2 M(m_0),$$

for all these t and for suitable constants $C_1, C_2 > 0$, hence

$$q((\beta-\alpha)(x,t)) \leqq q(0) + C_3 \|\alpha^0, \beta^0\| < 0, \tag{5.22}$$
$$c(0) - C_3 \|\alpha^0, \beta^0\| \leqq c((\beta-\alpha)(x,t)) \leqq c(0) + C_3 \|\alpha^0, \beta^0\|$$

with $C_3 = C_3(m_0, \delta) = (C_1 + C_2) \exp(C(2 + 2T_1(\delta) + T_1^2(\delta)))$.

Let K be the constant of Lemma 5.3, and let $d(t)$ be the denominator of the fraction in (5.20). Note that the number n in this fraction satisfies

$$n \geqq N(t) = \left[\frac{c(0) - C_3 \|\alpha^0, \beta^0\|}{2L} t \right],$$

where $[r]$ denotes the largest integer in r. Since $K \geqq 1$, we thus obtain from (5.22) that

$$d(t) \leqq Q(t) = 1 + (1 - K^{N(t)^2} D_0)^{N(t)} \delta t (q(0) + C_3 \|\alpha^0, \beta^0\|).$$

Now for $\|\alpha^0, \beta^0\| < (2C_3)^{-1} |q(0)|$ and for $T_1 = -2(\delta q(0))^{-1}$ we have

$$\delta T_1 (q(0) + C_3 \|\alpha^0, \beta^0\|) < -1,$$

and therefore also $Q(T_1) < 0$ if D_0 is chosen sufficiently small, hence $Q(T_+) = 0$ for a suitable number $T_+ < T_1$. We conclude that $d(t)$ cannot be bounded away from 0 in the interval $0 \leqq t < T_+$. (5.21) thus yields that $T_{\max} \leqq T_+$. Note that

$$T_+ \leqq \frac{-1}{(1 - K^{N(T_1)^2} D_0)^{N(T_1)} \delta (q(0) + C_3 \|\alpha^0, \beta^0\|)}.$$

To obtain the lower bound for $T_{\max}$ we now let $d_n(t)$ denote the denominator of the fractions in (5.19). Instead of (5.22) we now use the fact that

$$|q((\beta-\alpha)(x,t))| \leqq |q(0)| + C_3 \|\alpha^0, \beta^0\|.$$

For fixed $x \in [0, L]$, let n be largest integer such that $\tau_n(x) < T_{\max}$ and let

$$T_- = (1 + K^{n^2} D_0)^{-n} \delta^{-1} (|q(0)| + C_3 \|\alpha^0, \beta^0\|)^{-1}.$$

Then for $\tau_n \leqq t < T_-$ we have

$$d_n(t) > 1 - (1 + K^{n^2} D_0)^n \delta T_- (|q(0)| + C_3 \|\alpha^0, \beta^0\|) = 0.$$

Hence $T_- \leqq T_{\max}$. Clearly $T_\pm \to T_0(\delta) = -1/(\delta q(0))$ as D_0 and $\|\alpha^0, \beta^0\| \to 0$.

6. Proof of Lemma 5. 2

We first derive the boundary condition linking α and β on $x=0$. To this end we solve (1. 5) for $s(t)$ and use the hypotheses $s^0=0$ and $s'(0)=v^0(0)=0$ to obtain

$$s(t)=\int_0^t R(t-\tau)\,\sigma(u(0,\tau))\,d\tau, \tag{6. 1}$$

where $R(T)$ satisfies

$$mR''+rR'+kR=0, \quad R(0)=0, \quad R'(0)=\frac{1}{m}. \tag{6. 2}$$

Differentiating (6. 1) and using $s'=v=\alpha+\beta$ we conclude together with (5. 2) that

$$(\beta+\alpha)(0,t)=\int_0^t R_t(t-\tau)\,\hat{\sigma}(\beta-\alpha)(0,\tau)\,d\tau. \tag{6. 3}$$

Let $\bar{R}_1=\sup_{t\geqq 0}|R_t(t)|<\infty$.

Lemma 6. 1. *There is a constant $M\leqq 1$ such that for all $\tilde{T}\geqq 1$ and all T, $0\leqq T<\min(T_{\max},\tilde{T})$, if*

$$\sup_{0\leqq t\leqq T}|\beta(0,t)|\leqq\frac{M}{\tilde{T}}\exp(-2c(0)\bar{R}_1\tilde{T}), \tag{6. 4}$$

then

$$\sup_{0\leqq t\leqq T}|\alpha(0,t)|\leqq 5\exp(c(0)\bar{R}_1 T)\sup_{0\leqq t\leqq T}|\beta(0,t)|. \tag{6. 5}$$

M is independent of (α,β) and of the constant m in (1. 5) for all $m\geqq m_0$, but depends on $m_0>0$.

Proof. We set $f(t)=(\beta-\alpha)(0,t)$ and rewrite the integral equation (6. 3) as

$$f(t)=2\beta(0,t)-\int_0^t R_t(t-\tau)\,\hat{\sigma}(f(\tau))\,d\tau. \tag{6. 6}$$

To take advantage of the theory of linear Volterra equations, we expand $\hat{\sigma}(\gamma)$ about $\gamma=0$. Recall from (5. 2) that $\hat{\sigma}(0)=0$ and $\frac{d}{d\gamma}\hat{\sigma}(\gamma)=c(\gamma)$. Hence

$$\hat{\sigma}(\gamma)=c(0)\gamma+w(\gamma)\gamma \tag{6. 7}$$

where $w(\gamma)=0(\gamma)$ as $\gamma\to 0$,

$$|w(\gamma_1)-w(\gamma_2)|\leqq\omega|\gamma_1-\gamma_2| \tag{6. 8}$$

where $\omega > 0$ is a constant. Now substitute (6. 7) into (6. 6) and rearrange terms to arrive at

$$(I+V)f = 2\beta(0, t) - \int_0^t R_t(t-\tau)\, w(f(\tau))\, f(\tau)\, d\tau \tag{6. 9}$$

where

$$(Vf)(f) = c(0) \int_0^t R_t(t-\tau)\, f(\tau)\, d\tau. \tag{6. 10}$$

Let $C_0[0, T]$ be the space of continuous functions f in $[0, T]$ such that $f(0) = 0$ with the norm

$$\|f\|_T = \sup_{0 \leq t \leq T} |f(t)|.$$

It is well known from the theory of linear Volterra integral equations that $I+V$ is invertible in $C_0[0, T]$ with

$$\|(I+V)^{-1} g\|_T \leq e^{c(0)\bar{R}_1 T} \|g\|_T \tag{6. 11}$$

for all $g \in C_0[0, T]$. Hence if $f \in C_0[0, T]$ solves (6. 6), then f is a fixed point of the operator G defined by

$$Gg = 2(I+V)^{-1} \beta(0, t) - (I+V)^{-1} \int_0^t R_t(t-\tau)\, w(g)\, g\, d\tau. \tag{6. 12}$$

Using (6. 10) it is easy to show that for each $\beta(0, t) \in C_0[0, T]$, the fixed point is unique in $C_0[0, T]$.

Next we set

$$M = \min\left\{1, \frac{1}{8\omega \bar{R}_1}\right\} \tag{6. 13}$$

where ω was introduced in (6. 8) and we set

$$\mathscr{V}_M = \{g \in C_0[0, T] : \|g\|_T \leq \frac{4M}{\tilde{T}} \exp(-c(0)\bar{R}_1 \tilde{T})\}.$$

We shall show that the fixed point f lies in $\mathscr{V}_M$. By virtue of the estimates (6. 4), (6. 8), and (6. 11), we see that if $g \in \mathscr{V}_M$, then

$$\|Gg\|_T \leq \exp(c(0)\bar{R}_1 T)\, [2\|\beta(0, \cdot)\|_T + \omega \bar{R}_1 T \|g\|_T^2] \leq \frac{4M}{\tilde{T}} \exp(-c(0)\bar{R}_1 \tilde{T}). \tag{6. 14}$$

To show that G is a contraction on $\mathscr{V}_M$, we again use (6. 8) and (6. 11) to deduce that if $g_1, g_2 \in \mathscr{V}_M$, then

$$\begin{aligned}\|Gg_1 - Gg_2\|_T &\leqq \omega \bar{R}_1 T \exp(c(0)\bar{R}_1 T)(\|g_1\|_T + \|g_2\|_T)\|g_1 - g_2\|_T \\ &\leqq \theta \|g_1 - g_2\|_T,\end{aligned}$$

where $\theta < 1$ because $T < \tilde{T}$. Hence if β satisfies (6. 4), the unique fixed point f lies in $\mathscr{V}_M$ and from (6. 14) we have the estimate

$$\|f\|_T = \|Gf\|_T \leqq 2\exp(c(0)\bar{R}_1 T)\,\|\beta(0,\cdot)\|_T + \frac{1}{2}\|f\|_T$$

whence

$$\|f\|_T \leqq 4\exp(c(0)\bar{R}_1 T)\,\|\beta(0,\cdot)\|_T.$$

This means that when α and β solve (6. 3) and β satisfies (6. 4) we have

$$\|\alpha(0,t)\|_T \leqq \|f\|_T + \|\beta(0,\cdot)\|_T \leqq 5\exp(c(0)\bar{R}_1 T)\,\|\beta(0,t)\|_T. \tag{6. 15}$$

Lemma 6. 2. *There exists a constant $C>0$ with the following property. Let $\tilde{T} \geqq 1$ and suppose for some T with $0 \leqq T < \tilde{T}$, that* $\sup_{\substack{0\leqq x\leqq L\\ 0\leqq t\leqq T}} \{|\alpha(x,t)|, |\beta(x,t)|\} \leqq 1$. *Moreover, suppose that*

$$\|\alpha^0, \beta^0\| \leqq \frac{M}{\tilde{T}}\exp(-C(1+\tilde{T}^2)). \tag{6. 16}$$

Then

$$\begin{aligned}\sup_{\substack{0\leqq x\leqq L\\ 0\leqq t\leqq T}} \{|\alpha(x,t)|, |\beta(x,t)|\} &\leqq \|\alpha^0, \beta^0\|\exp(C(1+T^2)) \\ &\leqq \frac{M}{\tilde{T}}\exp(C(T^2-\tilde{T}^2)).\end{aligned} \tag{6. 17}$$

Here C is independent of (α, β) and of the constant m in (1. 5) for all $m \geqq m_0$, but depends on $m_0 > 0$. M is defined in (6. 13).

Proof. Consider the negative characteristic $x_-(\tau; 0, T)$ for $\tau \leqq T$. Continue this characteristic backward in time, reflecting into a positive characteristic at $x = L$, and again into a negative characteristic at $x = 0$. There are only a finite number of reflections with the boundary $x = 0$ before this backwards characteristics runs into the initial segment $\{0 \leqq x \leqq L, t = 0\}$. Let $0 < t_1 < t_2 < \ldots < t_n = T$ denote the reflection times with the boundary $x = 0$. We have the estimates $n \leqq \bar{c}T/(2L)$ and $t_k \leqq t_{k-1} + 2L/\underline{c}$ where

$$\bar{c} = \sup_{|\alpha|,|\beta|\leqq 1} c(\beta-\alpha), \quad \underline{c} = \inf_{|\alpha|,|\beta|\leqq 1} c(\beta-\alpha). \tag{6. 18}$$

Hence there is a constant C, independent of T, such that

$$5^n \exp(2c(0)\,\bar{R}_1(t_1 + \ldots + t_n)) \leqq \exp(C(1+T^2)). \tag{6.19}$$

Now suppose that $\|\alpha^0, \beta^0\| \leqq \frac{M}{\tilde{T}} \exp(-C(1+\tilde{T}^2))$. On $0 \leqq t \leqq t_1$, $\beta(0,t)$ is determined by the negative characteristics emanating from the initial segment

$$\{0 \leqq x \leqq L,\ t = 0\},$$

and by negative characteristics which are reflections at $x = L$ of positive characteristics emanating from the initial segment. Since β is constant on negative characteristics, α is constant on positive characteristics, and $\alpha = -\beta$ at $x = L$, we conclude that

$$\sup_{0 \leqq t \leqq t_1} |\beta(0,t)| \leqq \|\alpha^0, \beta^0\| \leqq \frac{M}{\tilde{T}} \exp(-2c(0)\,\bar{R}_1 t_1).$$

Since $\beta(0,t)|_{[0,t_1]}$ satisfies (6.4), we may apply Lemma 6.1 to deduce

$$\sup_{0 \leqq t \leqq t_1} |\alpha(0,t)| \leqq 5 \exp(c(0)\,\bar{R}_1 t_1)\, \|\alpha^0, \beta^0\|.$$

We claim that for $1 \leqq k \leqq n$,

$$\sup_{0 \leqq t \leqq t_k} |\beta(0,t)| \leqq 5^{k-1} \exp(c(0)\,\bar{R}_1(t_1 + \ldots + t_{k-1}))\, \|\alpha^0, \beta^0\| \tag{6.20}$$

and

$$\sup_{0 \leqq t \leqq t_k} |\alpha(0,t)| \leqq 5^k \exp(c(0)\,\bar{R}_1(t_1 + \ldots + t_k))\, \|\alpha^0, \beta^0\|. \tag{6.21}$$

These inequalities follow easily by induction when we note that for $2 \leqq k \leqq n$,

$$\sup_{[t_k, t_{k+1}]} |\beta(0,t)| = \sup_{[t_{k-1}, t_k]} |\alpha(0,t)|.$$

Assuming (6.20) and (6.21) hold, we see that

$$\begin{aligned}
\sup_{0 \leqq t \leqq t_{k+1}} |\beta(0,t)| &= \max\Big\{ \sup_{0 \leqq t \leqq t_k} |\beta(0,t)|,\ \sup_{t_k \leqq t \leqq t_{k+1}} |\beta(0,t)| \Big\} \\
&\leqq \max\Big\{ \sup_{0 \leqq t \leqq t_k} |\beta(0,t)|,\ \sup_{0 \leqq t \leqq t_k} |\alpha(0,t)| \Big\} \\
&\leqq 5^k \exp(c(0)\,\bar{R}_1(t_1 + \ldots + t_k))\, \|\alpha^0, \beta^0\| \\
&\leqq 5^k \exp(c(0)\,\bar{R}_1(t_1 + \ldots + t_k)) \frac{M}{\tilde{T}} \exp(-C(1+\tilde{T}^2)) \\
&\leqq \frac{M}{\tilde{T}} \exp(-2c(0)\,\bar{R}_1 t_{k+1})
\end{aligned}$$

where we have used (6. 19) in the last step. This means that $\beta(0, t)|_{[0,t_{k+1}]}$ satisfies (6. 4). We apply Lemma 6. 1 again to deduce (6. 21) with index $k+1$. It follows by virtue of (6. 19) that

$$\sup_{0\leqq t\leqq t_n}\{|\alpha(0, t)|, |\beta(0, t)|\}\leqq \|\alpha^0, \beta^0\| \exp(C(1+T^2)).$$

The assertion of the Lemma follows immediately because α is constant on positive characteristics and β is constant on negative characteristics.

Proof of Lemma 5. 2. Now if $\|\alpha^0, \beta^0\|$ satisfies (5. 12), then $\|\alpha^0, \beta^0\|<1$. Since (α, β) is continuous, there is some $\eta>0$ such that $|\alpha|, |\beta|\leqq 1$ on $[0, L]\times[0, \eta]$. Let $T_*=\sup\{T: |\alpha|, |\beta|\leqq 1 \text{ on } [0, L]\times[0, T]\}\geqq\eta$. We apply Lemma 6. 2 on $[0, L]\times[0, T_*]$ and deduce that $|\alpha|, |\beta|\leqq\frac{M}{\tilde{T}}\exp(C(T_*^2-\tilde{T}^2))$ on $[0, L]\times[0, T_*]$. Now $M\leqq 1$, $\tilde{T}\geqq 1$, so if $T_*<\min(T_{\max}, \tilde{T})$, then $|\alpha|, |\beta|<1$ on $[0, L]\times[0, T_*]$.

Since α and β are continuous, this implies that there is a larger time interval $[0, T_*+\varepsilon]$ on which $|\alpha|, |\beta|\leqq 1$ which contradicts the maximality of T_*. Hence we must have $T_*=\min\{T_{\max}, \tilde{T}\}$. This completes the proof of Lemma 5. 2.

7. Proof of Lemma 5. 3

Note that from (5. 12), (5. 13) and from $A(L, \tau)=B(L, \tau)$ it follows for $x\in[0, L]$ and for $0\leqq t<\tau_1(x)$ that

$$Z(t, x)=\frac{Z(0, x)}{1-Z(0, x)\int_0^t q(\Gamma(\eta, x), \eta)\,d\eta},$$

which immediately yields (5. 19) for these (x, t), since $q<0$, cf. (5. 1). We now prove that if (5. 19) is satisfied for all (x, t) with $t<\tau_{n+1}(x)$ then also for t with $\tau_{n+1}(x)<t<\tau_{n+2}(x)$. This proves (5. 19) by induction.

Note first that $Z(\tau_k(x)-, x)=B(0, \tau_k(x))$ for all k and all $x\in[0, L]$. From the induction hypothesis it thus follows that

$$|B(0, t)|\leqq\theta\frac{(1+K^{k^2}D_0)^k\,\|A(\cdot, 0), B(\cdot, 0)\|}{1+(1+K^{k^2}D_0)^k\,\|A(\cdot, 0), B(\cdot, 0)\|\int_0^t q(\Gamma(\eta, x), \eta)\,d\eta} \tag{7. 1}$$

for all $0\leqq k\leqq n$ and all t with $\tau_{+,k}(0)<t\leqq\tau_{+,k+1}(0)$. Here $\theta=1$ for $t\in G$ and $\theta=K^{k^2}D_0$ otherwise, where $G=G_+\cup G_-$, and $G_\pm$ is the set of all $\tau>0$ such that there exists $x\in\operatorname{supp}(A(\cdot, 0), B(\cdot, 0))$ with $\Gamma_\pm(\tau)=0$. Below we derive the boundary condition linking A and B on $x=0$, and show that

$$A(0,t)=B(0,t)+\int_0^t \kappa(t-\tau)\,B(0,\tau)\,d\tau, \tag{7.2}$$

where the kernel κ is bounded by

$$|\kappa(t-\tau)|\leqq 2\frac{N}{m}\exp\left(\frac{N}{m}(t-\tau)\right). \tag{7.3}$$

The constant N can be chosen independent of m for $m\geqq m_0>0$.

From Lemma 5.2 and from (5.2) it follows that if (5.9) is satisfied then we have $|c(\beta(x,t)-\alpha(x,t))-c(0)|\leqq\varepsilon$ for $t<\min(T_1, T_{\max}(u,v))$ with $\varepsilon=C_0M$, where $C_0>0$ is a suitable constant. Equation (5.15) thus implies

$$\operatorname{meas}(G\cap(\tau_{+,k-1}(0),\tau_{+,k}(0)))\leqq\frac{2}{c(0)}\mu(u,v)+\varepsilon C_1 k,$$

$$\left|\tau_{+,k}(0)-\frac{2L}{c(0)}k\right|\leqq\varepsilon C_2 k$$

for suitable constants C_1 and C_2. From these relations and from (7.1)—(7.3) we obtain for $\tau_{+,n}(0)<t<\tau_{+,n+1}(0)$

$$\begin{aligned}
|A(0,t)|&\leqq|B(0,t)|+\int_{[0,t]\setminus G}|\kappa(t-\tau)|\,|B(0,\tau)|\,d\tau\\
&\quad+\int_{[0,t]\cap G}|\kappa(t-\tau)|\,|B(0,\tau)|\,d\tau\\
&\leqq|B(0,t)|+2\frac{N}{m}\exp\left(\frac{N}{m}t\right)\left[tK^{n^2}D_0+\frac{2}{c(0)}(n+1)\mu+\varepsilon C_1\frac{1}{2}(n+1)(n+2)\right]\\
&\quad\cdot\frac{(1+K^{n^2}D_0)^n\,\|A(\cdot,0),B(\cdot,0)\|}{1+(1+K^{n^2}D_0)^n\,\|A(\cdot,0),B(\cdot,0)\|\int_0^t q(\Gamma(\eta,x),\eta)\,d\eta}\\
&\leqq|B(0,t)|+C_3^{n+1}K^{n^2}D_0\frac{(1+K^{n^2}D_0)^n\,\|A(\cdot,0),B(\cdot,0)\|}{1+(1+K^{n^2}D_0)^n\,\|A(\cdot,0),B(\cdot,0)\|\int_0^t q(\Gamma(\eta,x),\eta)\,d\eta}
\end{aligned}$$

if $M=M(m_0,D_0)$ is chosen such that $\varepsilon=C_0M\leqq D_0$. $C_3=C_3(m_0)>0$ is a suitable constant. Now we choose $K(m_0)=1+C_3(m_0)$, which implies

$$(1+C_3^{n+1})K^{n^2}\leqq K^{(n+1)^2},$$

and obtain after a second application of (7. 1)

$$(7.4)\qquad |A(0,t)| \leqq (\theta + C_3^{n+1} K^{n^2} D_0) \cdot \frac{(1+K^{n^2}D_0)^n \, \|A(\cdot,0), B(\cdot,0)\|}{1+(1+K^{(n+1)^2}D_0)^{n+1} \, \|A(\cdot,0), B(\cdot,0)\| \int_0^t q(\Gamma(\eta,x),\eta)\,d\eta}$$

$$\leqq \theta_1 \frac{(1+K^{(n+1)^2}D_0)^{n+1} \, \|A(\cdot,0), B(\cdot,0)\|}{1+(1+K^{(n+1)^2}D_0)^{n+1} \, \|A(\cdot,0), B(\cdot,0)\| \int_0^t q(\Gamma(\eta,x),\eta)\,d\eta},$$

where $\theta_1 = 1$ for $t \in G$, and $\theta_1 = K^{(n+1)^2} D_0$ otherwise. Note that

$$\tau_{+,n}(0) < \tau_{+,n+1}(x), \quad \tau_{-,n+1}(x) \leqq \tau_{+,n+1}(0)$$

for all $x \in [0, L]$. From (5. 17), (5. 18), from $A(L,t) = B(L,t)$, and from (7. 4) we thus obtain for all (x, t) with $\tau_{n+1}(x) < t < \min(T_1, T_{\max}, \tau_{n+2}(x))$

$$|Z(t,x)| = \left| \frac{A(0,\tau_{n+1}(x))}{1 - A(0,\tau_{n+1}(x)) \int_{\tau_{n+1}(x)}^t q(\Gamma(\eta,x),\eta)\,d\eta} \right|$$

$$\leqq \frac{\theta_1 (1+K^{(n+1)^2}D_0)^{n+1} \, \|A(\cdot,0), B(\cdot,0)\|}{1+(1+K^{(n+1)^2}D_0)^{n+1} \left[\|A(\cdot,0), B(\cdot,0)\| \int_0^{\tau_{n+1}(x)} q\,d\eta + \theta_1 \|A(\cdot,0), B(\cdot,0)\| \int_{\tau_{n+1}(x)}^t q\,d\eta \right]}$$

$$\leqq \theta_1 \frac{(1+K^{(n+1)^2}D_0)^{n+1} \, \|A(\cdot,0), B(\cdot,0)\|}{1+(1+K^{(n+1)^2}D_0)^{n+1} \, \|A(\cdot,0), B(\cdot,0)\| \int_0^t q\,d\eta},$$

provided D_0 is so small that $K^{(n+1)^2} D_0 \leqq 1$.

To complete the proof of (5. 19) it thus remains to prove (7. 2) and (7. 3). To this end we integrate by parts in (6. 3) and obtain

$$(\beta+\alpha)(0,t) = \int_0^t R_t(t-\tau)\, \hat{\sigma}(\beta-\alpha)(0,\tau)\,d\tau = \int_0^t R(t-\tau)\, c(\beta-\alpha)(\beta_\tau - \alpha_\tau)\,d\tau,$$

where we used the fact that $R(0) = \beta(0,0) = \alpha(0,0) = 0$. Differentiating with respect to t and using the equations $\alpha_t + c\alpha_x = 0$, $\beta_t - c\beta_x = 0$, we find that

$$c(\beta-\alpha)(\beta_x - \alpha_x)(0,t) = \int_0^t R_t(t-\tau)\, c^2(\beta-\alpha)(\beta_x + \alpha_x)\,d\tau.$$

In terms of A and B, this becomes

$$(B-A)(0,t) = V_1(B+A)(t),$$

where V_1 is the linear Volterra operator

$$(7.5) \qquad (V_1 f)(t) = c^{-1/2}(t) \int_0^t R_t(t-\tau)\, c^{3/2}(\tau)\, f(\tau)\, d\tau.$$

Here $c(t) = c(\beta - \alpha)(0, t)$. Hence considering these as functions of $C_0[0, T]$ we have

$$(7.6) \qquad A(0, t) = [(I+V_1)^{-1}(I-V_1)B](t) = \left[\sum_{k=0}^{\infty} (-V_1)^k (I-V_1)B\right](t) = [(I+V_2)B](t),$$

where

$$V_2 = 2\sum_{k=1}^{\infty} (-V_1)^k$$

is again a Volterra integral operator. We denote the kernel by κ and obtain (7.2). From (6.2) and (7.5) we see by some calculations that the kernel of V_1 is bounded by $\bar{c}^{3/2}\underline{c}^{-1/2} \sup|R_t| \leqq N/m$, where $\bar{c}, \underline{c}$ are defined as in (6.18), and where the constant N can be chosen independent of m for $m \geqq m_0 > 0$. It follows (see [7]) that the kernel κ of V_2 is bounded by

$$2\frac{N}{m} \exp\left(\frac{N}{m}(t-\tau)\right),$$

which proves (7.3).

The proof of (5.19) is complete. The estimate (5.20) is proved by analogous considerations, which we leave to the reader.

References

[1] *K. O. Friedrichs*, Nonlinear hyperbolic differential equations for functions of two independent variables, Amer. J. Math. **70** (1948), 555—588.

[2] *J. M. Greenberg* and *Li Ta-Tsien*, The effect of boundary damping for the quasilinear wave equation, J. Differential Eq. **52** (1984), 66—75.

[3] *P. D. Lax*, Development of singularities of solutions of nonlinear hyperbolic differential equations, J. Math. Phys. **5** (1964), 611—613.

[4] *Li Ta-tsien*, Global solutions to some free boundary value problems for quasilinear hyperbolic systems and applications, Proceedings of the Workshop on Nonlinear Hyperbolic Problems, St. Etienne 1986, Lecture Notes in Mathematics **1270**, New York-Heidelberg 1987.

[5] *Li Ta-tsien* and *Yu Wen-ci*, Boundary Value Problems for Quasilinear Hyperbolic Systems, Duke University Mathematics Series V, Durham, N.C., 1985.

[6] *A. Madja*, Compressible Fluid Flow and Systems of Conservation Laws in Several Space Variables, Applied Mathematical Sciences **53**, New York-Heidelberg 1984.

[7] *S. G. Mikhlin*, Integral Equations and their Applications to Certain Problems in Mathematical Physics and Technology, 2nd edition, New York 1984.

[8] *M. Slemrod*, Boundary feedback stabilization for a quasi-linear wave equation, Proc. Conf., Vorau/Styria 1982, Lecture notes in control and information sciences **54** (1983), 211—237.

Fachbereich Mathematik, Technische Hochschule Darmstadt, Schloßgartenstr. 7, D-6100 Darmstadt

Department of Mathematics, University of Maryland, College Park, MD 20742, U.S.A.

Eingegangen 27. April 1989

J. reine angew. Math. **406** (1990), 44—108

Journal für die reine und angewandte Mathematik

The number of subspaces occurring in the p-adic subspace theorem in diophantine approximation

By *Hans Peter Schlickewei* at Ulm

1. Introduction

Let α be a real or complex algebraic number of degree $d \geqq 2$. Roth's Theorem [10] says that given $\delta > 0$ there are only a finite number of rational approximations $\frac{x}{y}$ of α with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\delta}}. \tag{1. 1}$$

This was extended by Ridout [9] to include p-adic valuations.

Unfortunately the underlying method of Thue-Siegel-Roth is ineffective in the sense that it does not provide bounds for the *sizes* of x and y. However it does give explicit upper bounds for the *number* of such approximations. In fact in a paper by Davenport and Roth [3] it was shown that this number is under some bound which depends only upon d, δ and the height $H_0 = H_0(\alpha)$, the maximum modulus of the coefficients of the minimal defining polynomial of α over $\mathbb{Z}$. Bombieri and van der Poorten [1] and independently Luckhardt [6] using the modified proof of Roth's Theorem as presented by Esnault and Viehweg [4] obtained much better bounds.

Put $\mathbf{x} = (x, y)$, $L_1(\mathbf{x}) = y$, $L_2(\mathbf{x}) = \alpha y - x$. Then (1. 1) is equivalent to

$$|L_1(\mathbf{x})\, L_2(\mathbf{x})| < y^{-\delta}$$

and this is essentially the same as $|L_1(\mathbf{x})\, L_2(\mathbf{x})| < |\mathbf{x}|^{-\delta}$ where $|\mathbf{x}| = (x^2 + y^2)^{1/2}$. The Subspace Theorem treats the more general situation where we are given linearly independent linear forms $L_1, \ldots, L_n$ in n variables with algebraic coefficients. But we will include p-adic valuations as well.

Let $S=\{0, p_1, \ldots, p_s\}$ where $p_1, \ldots, p_s$ are s different rational primes. Write $|\ |_0$ for the ordinary absolute value of $\mathbb{Q}$ and for $j=1, \ldots, s$, $|\ |_j$ for the p_j-adic absolute value of $\mathbb{Q}$, normalized such that $|p_j|_j = p_j^{-1}$. For $j=0, \ldots, s$, we denote by $\mathbb{Q}_j$ the completion of $\mathbb{Q}$ with respect to $|\ |_j$ and by Ω_j the algebraic closure of $\mathbb{Q}_j$ (so that in particular $\mathbb{Q}_0=\mathbb{R}$, $\Omega_0=\mathbb{C}$). Each absolute value $|\ |_j$ has a unique extension to Ω_j which we denote again by $|\ |_j$. Let K be an algebraic number field of degree d. For each j let φ_j be an embedding of K over $\mathbb{Q}$ into Ω_j. Suppose that for each j $(0 \leqq j \leqq s)$ we are given linearly independent linear forms $L_1^{(j)}, \ldots, L_n^{(j)}$ in n variables with coefficients in $\varphi_j(K)$. Then the *Subspace Theorem* says that there is a finite number of proper subspaces of $\mathbb{Q}^n$ containing all rational integral solutions $\mathbf{x}=(x_1, \ldots, x_n) \neq \mathbf{0}$ of the inequality

$$\prod_{j=0}^{s} |L_1^{(j)}(\mathbf{x}) \cdots L_n^{(j)}(\mathbf{x})|_j < |\mathbf{x}|^{-\delta} \tag{1. 2}$$

where $\mathbf{x}=(x_1^2+\cdots+x_n^2)^{1/2}$.

The pioneering work of proving this result in the archimedean case is due to W. M. Schmidt [13], [14]. The general case including nonarchimedean valuations was treated by Schlickewei [11], [12]. Recently W. M. Schmidt [15] proved a more precise version of his Subspace Theorem. He gave an explicit upper bound for the number of subspaces needed in the Subspace Theorem. It is the purpose of this paper to generalize this result to include nonarchimedean valuations.

Theorem. *Let $S=\{0, p_1, \ldots, p_s\}$. Let K be an algebraic number field of degree d. For each j $(0 \leqq j \leqq s)$ let Ω_j and φ_j* be as above. Suppose that *$L_1^{(j)}, \ldots, L_n^{(j)}$ are linearly independent linear forms in n variables with coefficients in $\varphi_j(K)$. Consider the inequality*

$$\prod_{j=0}^{s} |L_1^{(j)}(\mathbf{x}) \cdots L_n^{(j)}(\mathbf{x})|_j < \left(\prod_{j=0}^{s} |\det(L_1^{(j)}, \ldots, L_n^{(j)})|_j \right) |\mathbf{x}|^{-\delta} \tag{1. 3}$$

where $0<\delta<1$ and $\det(L_1^{(j)}, \ldots, L_n^{(j)})$ denotes the determinant of the coefficient matrix of $L_1^{(j)}, \ldots, L_n^{(j)}$.

Then there are proper subspaces $T_1, \ldots, T_t$ of $\mathbb{Q}^n$ with

$$t=[(8(s+1)d!)^{2^{26n(s+1)^6\delta^{-2}}}] \tag{1. 4}$$

such that every rational integral solution $\mathbf{x}$ *of* (1. 3) *either lies in one of these subspaces, or has norm*

$$|\mathbf{x}| < \max\{(n!)^{8/\delta}, H(L_1^{(0)}), \ldots, H(L_n^{(0)}), \ldots, H(L_1^{(s)}), \ldots, H(L_n^{(s)})\} \tag{1. 5}$$

where the $H(L_i^{(j)})$ are heights which are defined below.

Schmidt's result [15] deals with the archimedean case, i.e. the case when $s=0$. He obtains the bound $[(2d)^{2^{26n\delta^{-2}}}]$. The reason why in (1. 4) we have $d!$ instead of d or some fixed power of d is based on the fact that $\mathbb{C}/\mathbb{R}$ is an extension of degree 2 with

basis 1, i, whereas in the nonarchimedean case the extensions $\Omega_j/\mathbb{Q}_j$ are far from being so well behaved. In section 2 we will see why this makes trouble in our context. On the other hand it will be shown there that in (1. 4) $d!$ may be replaced by the degree of the smallest normal extension of $\mathbb{Q}$ containing K.

We shall use the same definitions of heights as Schmidt [15]. In fact for a number field K let $M(K)$ be an indexing set for the absolute values of K. For $w \in M(K)$, the absolute value $|\lambda|_w$ where $\lambda \in K$ will be an extension of either the ordinary absolute value or a p-adic absolute value of $\mathbb{Q}$. Let d_w be the local degree of K_w over $\mathbb{Q}_w$, where K_w is the w-adic completion of K and $\mathbb{Q}_w$ the w-adic completion of $\mathbb{Q}$. Then we have the product formula

$$\prod_{w \in M(K)} |\lambda|_w^{d_w} = 1$$

for any $\lambda \neq 0$ in K. Let $M'(K)$ be a set of symbols v, such that to each $w \in M(K)$ there correspond d_w symbols $v \in M'(K)$, and for such v we put $|\lambda|_v = |\lambda|_w$. Then the product formula for K reads as

$$\prod_{v \in M'(K)} |\lambda|_v = 1.$$

Given $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in K^n$ and $v \in M'(K)$, we put

$$|\boldsymbol{\alpha}|_v = \begin{cases} (|\alpha_1|_v^2 + \cdots + |\alpha_n|_v^2)^{1/2} & \text{for } v \text{ archimedean,} \\ \max\{|\alpha_1|_v, \ldots, |\alpha_n|_v\} & \text{for } v \text{ nonarchimedean.} \end{cases}$$

For $\boldsymbol{\alpha} \neq \mathbf{0}$ we put

$$H_K(\boldsymbol{\alpha}) = \prod_{v \in M'(K)} |\boldsymbol{\alpha}|_v. \tag{1. 6}$$

In view of the product formula we have for $\lambda \in K$, $\lambda \neq 0$ the relation $H_K(\lambda\boldsymbol{\alpha}) = H_K(\boldsymbol{\alpha})$. Moreover we define the absolute height by

$$H(\boldsymbol{\alpha}) = H_K(\boldsymbol{\alpha})^{1/d}, \tag{1. 7}$$

where d is the degree of K. It is clear that $H(\boldsymbol{\alpha})$ does not depend on the particular field K. When $L = \alpha_1 X_1 + \cdots + \alpha_n X_n$ is a nonzero linear form with algebraic coefficients, we put

$$H(L) = H(\boldsymbol{\alpha}).$$

Now let H be any quantity with

$$H \geqq \max\{H(L_1^{(0)}), \ldots, H(L_n^{(0)}), \ldots, H(L_1^{(s)}), \ldots, H(L_n^{(s)})\}. \tag{1. 8}$$

Then (1. 5) may be replaced by

$$|\mathbf{x}| < \max\{(n!)^{8/\delta}, H\}. \tag{1. 9}$$

It is possible to estimate the number of subspaces containing all the solutions of (1. 3) and (1. 9). But here in contrariety to (1. 4) the bound depends also upon H. For details on this question the reader is referred to section 4.

Notice that our Theorem does not give a bound for the number of *solutions* of (1. 3). In fact, since in view of (1. 5) or (1. 9) our bound for the number of *subspaces* depends on H, there is a difficulty in principle to derive a bound for the number of solutions. For a more thorough discussion of this topic see Schmidt [15], section 1. However our Theorem may be applied to derive upper bounds for the number of solutions of norm form equations of the type $N(\alpha_1 x_1 + \cdots + \alpha_n x_n) = p_1^{z_1} \cdots p_s^{z_s}$ in integers $x_1, \ldots, x_n$, $z_1, \ldots, z_s$, i.e. the n-dimensional analogue of the Thue-Mahler equation. Moreover it allows us to give an explicit upper bound for the number of solutions of the S-unit equation. These questions are treated in forthcoming work by the author.

The method of proof of our Theorem is that of Schmidt [15] combined with results of [11]. However we will try to make the paper rather selfcontained and therefore we have sometimes to repeat arguments from [15] or [11].

2. Reduction to forms with coefficients in $\mathcal{Q}_j$

Let K be as above. Let p be a rational prime and define $\mathcal{Q}_p$ and Ω_p in the obvious way. Suppose K is embedded into Ω_p. Denote by K_p the completion of K with respect to $|\ |_p$ and write $d_p = [K_p : \mathcal{Q}_p]$.

Lemma 2. 1. *There exists a basis $\alpha_1, \ldots, \alpha_{d_p}$ of K_p over $\mathcal{Q}_p$ with the following properties.*

(i) $\alpha_1, \ldots, \alpha_{d_p} \in K$.

(ii) *For any $c \in K_p$ we have, writing*

$$c = c_1 \alpha_1 + \cdots + c_{d_p} \alpha_{d_p}$$

with $c_i \in \mathcal{Q}_p$ $(i = 1, \ldots, d_p)$,

$$|c|_p = \max_{1 \leqq i \leqq d_p} |c_i \alpha_i|_p. \tag{2. 1}$$

Proof. For any subfield F of K_p let $V(F)$ be the group of values assumed by the mapping $|\ |_p : F^* \to \mathbb{R}$, where $F^* = F \setminus \{0\}$. Let $e = [V(K_p) : V(\mathcal{Q}_p)]$ be the ramification index. It is well known that we have $V(K) = V(K_p)$. Hence we can choose elements $b_1, \ldots, b_e$ in K such that $|b_1|_p, \ldots, |b_e|_p$ represent the cosets mod $V(\mathcal{Q}_p)$ in $V(K_p)$.

For any subfield F of K_p write $\mathcal{O}(F)$ for the ring of integers of F, i.e.

$$\mathcal{O}(F)=\{x\in F \mid |x|_p\leqq 1\},$$

and $\mathfrak{m}(F)$ for the unique maximal ideal in $\mathcal{O}(F)$, i.e. $\mathfrak{m}(F)=\{x\in F \mid |x|_p<1\}$. Let

$$f=[\mathcal{O}(K_p)/\mathfrak{m}(K_p):\mathcal{O}(\mathbb{Q}_p)/\mathfrak{m}(\mathbb{Q}_p)]$$

be the residue class degree. Since $\mathcal{O}(K)/\mathfrak{m}(K)$ is isomorphic to $\mathcal{O}(K_p)/\mathfrak{m}(K_p)$ we can choose elements $a_1,\dots,a_f$ in $\mathcal{O}(K)$ whose images under the canonical homomorphism $\mathcal{O}(K_p)\to\mathcal{O}(K_p)/\mathfrak{m}(K_p)$ are a basis of $\mathcal{O}(K_p)/\mathfrak{m}(K_p)$ over $\mathcal{O}(\mathbb{Q}_p)/\mathfrak{m}(\mathbb{Q}_p)$. Now it is well-known that the elements a_ib_j $(i=1,\dots,f;\ j=1,\dots,e)$ form a basis of K_p over $\mathbb{Q}_p$ and our construction implies that this basis satisfies assertion (i) of the Lemma (cf. Weiss [16], Theorem 2-3-2).

We claim that our basis satisfies (ii) as well. Notice that the definition of the a_i implies

$$|a_i|_p=1 \quad \text{for} \quad i=1,\dots,f.$$

We prove first that given $c_1,\dots,c_f\in\mathbb{Q}_p$ we have

$$|c_1a_1+\cdots+c_fa_f|_p=\max_{1\leqq i\leqq f}|c_i|_p. \tag{2. 2}$$

In fact suppose that

$$|c_1|_p=\max_{1\leqq i\leqq f}|c_i|_p\neq 0.$$

Then we have to show that $|a_1+c_2'a_2+\cdots+c_f'a_f|_p=1$ where $c_i'=c_i/c_1$ $(i=2,\dots,f)$ and $c_i'\in\mathcal{O}(\mathbb{Q}_p)$. Clearly $|a_1+c_2'a_2+\cdots+c_f'a_f|_p\leqq 1$. But if $|a_1+c_2'a_2+\cdots+c_f'a_f|_p<1$ then writing $\bar{a}$ for the image of an element $a\in\mathcal{O}(K_p)$ under the residue class homomorphism we would have $\bar{1}\,\bar{a}_1+\bar{c}_2'\,\bar{a}_2+\cdots+\bar{c}_f'\,\bar{a}_f=\bar{0}$, which contradicts the choice of the a_i.

Now consider any $c\in K_p$. It may be written uniquely as

$$c=\sum_{j=1}^{e}\left(\sum_{i=1}^{f}c_{ij}a_i\right)b_j$$

with suitable elements $c_{ij}\in\mathbb{Q}_p$. We infer from (2. 2) that for each j

$$\left|\left(\sum_{i=1}^{f}c_{ij}a_i\right)b_j\right|_p=\max_{1\leqq i\leqq f}|c_{ij}b_j|_p=\max_{1\leqq i\leqq f}|c_{ij}a_ib_j|_p.$$

On the other hand since $|a_i|_p=1$ and $c_{ij}\in\mathbb{Q}_p$ $\left|\left(\sum_{i=1}^{f}c_{ij}a_i\right)b_j\right|_p$ represents the same coset mod $V(\mathbb{Q}_p)$ in $V(K_p)$ as $|b_j|_p$. In particular this implies that for any pair j, j' with $j\neq j'$ we have

$$\left|\left(\sum_{i=1}^{f} c_{ij} a_i\right) b_j\right|_p \neq \left|\left(\sum_{i=1}^{f} c_{ij'} a_i\right) b_{j'}\right|_p.$$

Thus

$$|c|_p = \left|\sum_{j=1}^{e}\left(\sum_{i=1}^{f} c_{ij} a_i\right) b_j\right|_p = \max_{1\leqq j\leqq e}\left|\left(\sum_{i=1}^{f} c_{ij} a_i\right) b_j\right|_p$$
$$= \max_{\substack{1\leqq j\leqq e\\ 1\leqq i\leqq f}} |c_{ij} a_i b_j|_p,$$

and this is the assertion in (2. 1).

Lemma 2. 2. *Let L be a linear form with coefficients in K. Let $\alpha_1, \ldots, \alpha_{d_p}$ be a basis of K_p over $\mathbb{Q}_p$ as in Lemma 2. 1. If we write $L = \alpha_1 L_1 + \cdots + \alpha_{d_p} L_{d_p}$ with linear forms L_i $(i = 1, \ldots, d_p)$ with coefficients in $\mathbb{Q}_p$, then the L_i have the following properties.*

(i) *The coefficients of the L_i lie in the smallest normal extension of $\mathbb{Q}$ containing K, hence in a number field of degree say $\tilde{d} \leqq d!$.*

(ii) *For each i $(1 \leqq i \leqq d_p)$ we have*

$$H(L_i) \leqq \tilde{d} H(L)^{\tilde{d}}. \tag{2. 3}$$

Proof. As $[K_p : \mathbb{Q}_p] = d_p$ there are d_p isomorphic embeddings $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_{d_p}$ of K_p over $\mathbb{Q}_p$ into Ω_p. From

$$\sigma_i(\alpha_1 L_1 + \cdots + \alpha_{d_p} L_{d_p}) = \sigma_i(\alpha_1) L_1 + \cdots + \sigma_i(\alpha_{d_p}) L_{d_p} = \sigma_i(L)$$

we get the system of equations

$$\begin{aligned} \sigma_1(\alpha_1) L_1 + \cdots + \sigma_1(\alpha_{d_p}) L_{d_p} &= \sigma_1(L) \\ \vdots \qquad\qquad\quad & \vdots \qquad\quad \vdots \\ \sigma_{d_p}(\alpha_1) L_1 + \cdots + \sigma_{d_p}(\alpha_{d_p}) L_{d_p} &= \sigma_{d_p}(L). \end{aligned} \tag{2. 4}$$

Since $\alpha_1, \ldots, \alpha_{d_p}$ lie in K and since the restrictions of the σ_i to K are embeddings of K over $\mathbb{Q}$ into Ω_p we infer from (2. 4) that the coefficients of L_i lie in the compositum $\sigma_1(K) \cdots \sigma_{d_p}(K)$ and (i) follows.

As for (ii), let $\tilde{K}$ be the smallest normal extension of $\mathbb{Q}$ containing K, let $K' = \sigma_1(K) \cdots \sigma_{d_p}(K)$ and K'_p be the completion of K' with respect to $|\ |_p$, i.e. $K'_p = \sigma_1(K_p) \cdots \sigma_{d_p}(K_p)$. Then $[\tilde{K} : \mathbb{Q}] = \tilde{d} \leqq d!$ and $K' \subseteq \tilde{K}$. Moreover putting $[K'_p : \mathbb{Q}_p] = l$ then we have $l \leqq \tilde{d} \leqq d!$.

Extend the basis $\alpha_1, \ldots, \alpha_{d_p}$ of K_p to a basis $\alpha_1, \ldots, \alpha_{d_p}, \alpha_{d_p+1}, \ldots, \alpha_l$ of K'_p with elements $\alpha_i \in K'$. Let G be the Galois group of K'_p over $\mathbb{Q}_p$. Denote its elements by $\sigma_1, \ldots, \sigma_{d_p}, \sigma_{d_p+1}, \ldots, \sigma_l$ where the embeddings $\sigma_1, \ldots, \sigma_{d_p}$ of K_p into Ω_p are extended to K'_p. Then in analogy with (2. 4) we have

(2. 5)

$$\begin{array}{ccccccccc}
\sigma_1(\alpha_1)L_1 & +\cdots+ & \sigma_1(\alpha_{d_p})L_{d_p} & + & \sigma_1(\alpha_{d_p+1})L_{d_p+1} & +\cdots+ & \sigma_1(\alpha_l)L_l & = & \sigma_1(L) \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
\sigma_{d_p}(\alpha_1)L_1 & +\cdots+ & \sigma_{d_p}(\alpha_{d_p})L_{d_p} & + & \sigma_{d_p}(\alpha_{d_p+1})L_{d_p+1} & +\cdots+ & \sigma_{d_p}(\alpha_l)L_l & = & \sigma_{d_p}(L) \\
\sigma_{d_p+1}(\alpha_1)L_1 & +\cdots+ & \sigma_{d_p+1}(\alpha_{d_p})L_{d_p} & + & \sigma_{d_p+1}(\alpha_{d_p+1})L_{d_p+1} & +\cdots+ & \sigma_{d_p+1}(\alpha_l)L_l & = & \sigma_{d_p+1}(L) \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
\sigma_l(\alpha_l)L_l & +\cdots+ & \sigma_l(\alpha_{d_p})L_{d_p} & + & \sigma_l(\alpha_{d_p+1})L_{d_p+1} & +\cdots+ & \sigma_l(\alpha_l)L_l & = & \sigma_l(L)
\end{array}$$

where $L_{d_p+1} \equiv \cdots \equiv L_l \equiv 0$.

By symmetry it suffices to show (2. 3) for L_1. Let $\Delta = \det(\sigma_i(\alpha_j))_{1 \leqq i,\, j \leqq l}$ and denote by A_{i1} the cofactor of $\sigma_i(\alpha_1)$ in the matrix $(\sigma_i(\alpha_j))_{1 \leqq i,\, j \leqq l}$. Since $\sigma_i(G \setminus \{\sigma_1\}) = G \setminus \{\sigma_i\}$ we see that $A_{i1} = \sigma_i(A_{11})$ and therefore (2. 5) implies

$$L_1 = \frac{1}{\Delta}(\pm\sigma_1(A_{11}L) \pm \cdots \pm \sigma_l(A_{11}L)). \tag{2. 6}$$

As $H_{K'}(\lambda L) = H_{K'}(L)$ for any $\lambda \neq 0$ in K' we may suppose that $A_{11}L$ has some coefficient equal to 1. Now by (2. 6)

$$\begin{aligned}
H_{K'}(L_1) &= H_{K'}\left(\frac{1}{\Delta}(\pm\sigma_1(A_{11}L) \pm \cdots \pm \sigma_l(A_{11}L))\right) \\
&= H_{K'}(\pm\sigma_1(A_{11}L) \pm \cdots \pm \sigma_l(A_{11}L)) \\
&= \prod_{v \in M'(K')} |\pm\sigma_1(A_{11}L) \pm \cdots \pm \sigma_l(A_{11}L)|_v .
\end{aligned}$$

Since $A_{11}L$ has some coefficient equal to 1, we have $|\sigma_i(A_{11}L)|_v \geqq 1$ for each i $(1 \leqq i \leqq l)$ and for each $v \in M'(K')$. Therefore

$$|\pm\sigma_1(A_{11}L) \pm \cdots \pm \sigma_l(A_{11}L)|_v \leqq \max_{1 \leqq i \leqq l} |\sigma_i(A_{11}L)|_v \leqq |\sigma_1(A_{11}L)|_v \cdots |\sigma_l(A_{11}L)|_v$$

if v is nonarchimedean, and

$$|\pm\sigma_1(A_{11}L) \pm \cdots \pm \sigma_l(A_{11}L)|_v \leqq l \max_{1 \leqq i \leqq l} |\sigma_i(A_{11}L)|_v \leqq l\,|\sigma_1(A_{11}L)|_v \cdots |\sigma_l(A_{11}L)|_v$$

if v is archimedean. So we get putting $d' = [K' : \mathbb{Q}]$

$$\begin{aligned}
H_{K'}(L_1) &\leqq l^{d'} \prod_{v \in M'(K')} (|\sigma_1(A_{11}L)|_v \cdots |\sigma_l(A_{11}L)|_v) \\
&= l^{d'} H_{K'}(\sigma_1(A_{11}L)) \cdots H_{K'}(\sigma_l(A_{11}L)) \\
&= l^{d'} H_{K'}(\sigma_1(L)) \cdots H_{K'}(\sigma_l(L)) = l^{d'} H_{K'}(L)^l .
\end{aligned}$$

Thus $H(L_1) \leqq l H(L)^l$ and since $l \leqq \tilde{d}$ we obtain (2. 3).

Proposition A. *For each j $(0 \leqq j \leqq s)$ let $L_1^{(j)}, \ldots, L_n^{(j)}$ be linearly independent linear forms with coefficients in $\varphi_j(K) \cap \mathcal{Q}_j$. Let $[K : \mathcal{Q}] = d$. Then the solutions of* (1. 3) *with*

$$|\mathbf{x}| \geqq \max\left\{(n!)^{4/\delta}, \frac{1}{2} H^{1/d}\right\}, \tag{2. 6}$$

where H satisfies (1. 8), *lie in at most t_0 subspaces with*

$$t_0 = (4(s+1)d)^{2^{25n}(s+1)^6 \delta^{-2}}.$$

We proceed to show that Proposition A implies the Theorem. For this purpose we have to make a transition to forms with coefficients in $\mathcal{Q}_j$ $(j = 0, \ldots, s)$.

The forms $L_1^{(0)}, \ldots, L_n^{(0)}$ are treated as in Schmidt [15], section 2. It is shown there that with a suitable choice of the real or imaginary parts of the forms $L_k^{(0)}$ say $L_1'^{(0)}, \ldots, L_n'^{(0)}$ (1. 3) implies

$$\begin{aligned} |L_1'^{(0)}(\mathbf{x}) \cdots L_n'^{(0)}(\mathbf{x})|_0 \prod_{j=1}^{s} |L_1^{(j)}(\mathbf{x}) \cdots L_n^{(j)}(\mathbf{x})|_j \\ < 2^n |\det(L_1'^{(0)}, \ldots, L_n'^{(0)})|_0 \prod_{j=1}^{s} |\det(L_1^{(j)}, \ldots, L_n^{(j)})|_j \, |\mathbf{x}|^{-\delta}. \end{aligned} \tag{2. 7}$$

Here $L_k'^{(0)}$, being the real or imaginary part of $L_k^{(0)}$, has coefficients in the auxiliary field $\varphi_0(K)\,\overline{\varphi_0(K)}\,(i)$, where $\overline{\varphi_0(K)}$ is obtained from $\varphi_0(K)$ by complex conjugation.

To treat the nonarchimedean absolute values in a similar way, we have to pay a much higher price. In fact the degree of the auxiliary field in this case may be bounded only by $d!$. Suppose now that j with $1 \leqq j \leqq s$ is fixed. Let K_j be the completion of $\varphi_j(K)$ and let $\alpha_1, \ldots, \alpha_{d_j}$ be a basis of K_j over $\mathcal{Q}_j$ with $\alpha_1, \ldots, \alpha_{d_j} \in \varphi_j(K)$ as in Lemma 2. 1. (Here for simplicity we have put $K_{p_j} = K_j$.) There are d_j isomorphic embeddings of K_j into Ω_j say $\varphi_j^{(1)}(K), \ldots, \varphi_j^{(d_j)}(K)$. Write $L_n^{(j)} = \alpha_1 L_{n1}^{(j)} + \cdots + \alpha_{d_j} L_{nd_j}^{(j)}$, with linear forms $L_{ni}^{(j)}$ having coefficients in $\mathcal{Q}_j$. Moreover by Lemma 2. 2 the coefficients of $L_{ni}^{(j)}$ lie in $\tilde{K}$, the smallest normal extension of $\mathcal{Q}$ containing K. In fact they lie in $\varphi_j^{(1)}(K) \cdots \varphi_j^{(d_j)}(K)$, as was shown in the proof of Lemma 2. 2. In view of Lemma 2. 1 we have

$$\max_{1 \leqq i \leqq d_j} |\alpha_i L_{ni}^{(j)}(\mathbf{x})|_j = |L_n^{(j)}(\mathbf{x})|_j.$$

On the other hand we notice that

$$|\det(L_1^{(j)}, \ldots, L_n^{(j)})|_j \leqq \max_{1 \leqq i \leqq d_j} |\det(L_1^{(j)}, \ldots, L_{n-1}^{(j)}, \alpha_i L_{ni}^{(j)}|.$$

Assume without loss of generality that $i = 1$ is a subscript where this maximum is attained. Then replacing, the term $|L_1^{(j)}(\mathbf{x}) \cdots L_n^{(j)}(\mathbf{x})|_j$ on the left hand side of (1. 3) by $|L_1^{(j)}(\mathbf{x}) \cdots L_{n-1}^{(j)}(\mathbf{x})\, \alpha_1 L_{n1}^{(j)}(\mathbf{x})|_j$ and $|\det(L_1^{(j)}, \ldots, L_n^{(j)})|_j$ on the right hand side of (1. 3) by $|\det(L_1^{(j)}, \ldots, L_{n-1}^{(j)}, \alpha_1 L_{n1}^{(j)})|_j$ and cancelling α_1 on both sides, we see that (1. 3) implies

$$\left(\prod_{\substack{i=0\\ i\neq j}}^{s} |L_1^{(i)}(\mathbf{x})\cdots L_n^{(i)}(\mathbf{x})|_i\right) |L_1^{(j)}(\mathbf{x})\cdots L_{n-1}^{(j)}(\mathbf{x})\, L_{n1}^{(j)}(\mathbf{x})|_j$$

$$< \left(\prod_{\substack{i=0\\ i\neq j}}^{s} |\det(L_1^{(i)},\ldots,L_n^{(i)})|_j\right) |\det(L_1^{(j)},\ldots,L_{n-1}^{(j)},L_{n1}^{(j)})|_j\, |\mathbf{x}|^{-\delta}.$$

In a similar manner we may replace for each i $(1\leqq i\leqq n)$ and for each j $(0\leqq j\leqq s)$ the forms $L_i^{(j)}$ by forms $L_i'^{(j)}$ with coefficients in $\mathfrak{Q}_j$. Taking into consideration the results of [15], section 2, for the archimedean absolute value we finally obtain (cancelling the factor 2^n in (2. 7) with $|\mathbf{x}|^{-\delta/2}$)

$$\prod_{j=0}^{s} |L_1'^{(j)}(\mathbf{x})\cdots L_n'^{(j)}(\mathbf{x})|_j < \left(\prod_{j=0}^{s} |\det(L_1'^{(j)},\ldots,L_n'^{(j)})|_j\right) |\mathbf{x}|^{-\delta/2}.$$

Let us study again the location of the coefficients of our new forms $L_i'^{(j)}$. We know already that $L_i'^{(j)}$ has coefficients in $\mathfrak{Q}_j$. We claim that moreover its coefficients lie in $\tilde{K}(i)$. In fact the embeddings φ_j of K into Ω_j admit a prolongation to $\tilde{K}(i)$ which we denote again by φ_j $(j=0,\ldots,s)$. But $\varphi_0(\tilde{K}(i))$ contains $\varphi_0(K)$ $\overline{\varphi_0(K)}$ (i) and for $1\leqq j\leqq s$ $\varphi_j(\tilde{K}(i))$ contains $\varphi_j^{(1)}(K)\cdots\varphi_j^{(d_j)}(K)$. Thus our new forms $L_i'^{(j)}$ have coefficients in $\varphi_j(\tilde{K}(i))\cap\mathfrak{Q}_j$ $(j=0,\ldots,s)$. Put $[\tilde{K}(i):\mathbb{Q}]=d^*$. Then we have $d^*\leqq 2\tilde{d}\leqq 2(d!)$.

We apply Proposition A with $L_1^{(0)},\ldots,L_n^{(s)}$, K, d, δ replaced by $L_1'^{(0)},\ldots,L_n'^{(s)}$, $\tilde{K}(i)$, d^*, $\delta/2$ respectively. Let

$$H'=\max\{H(L_1'^{(0)}),\ldots,H(L_n'^{(0)}),\ldots,H(L_1'^{(s)}),\ldots,H(L_n'^{(s)})\}.$$

Combining (2. 3) with the estimate for the quantities $H(L_i'^{(0)})\leqq 2H^2(L_i^{(0)})$ from [15] we obtain

$$H'\leqq d^*H^{d^*}.$$

The points $\mathbf{x}$ violating (1. 9) satisfy

$$|\mathbf{x}|\geqq\max\{(n!)^{8/\delta},H\}\geqq\max\left\{(n!)^{4/(\delta/2)},\frac{1}{2}H'^{1/d^*}\right\}.$$

Now Proposition A says that the integer points $\mathbf{x}$ with (1. 3) but not (1. 9) lie in not more than

$$[(4(s+1)d^*)^{2^{25n(s+1)^6(\delta/2)^{-2}}}]\leqq[(4(s+1)\,2(d!))^{2^{26n(s+1)^6\delta^{-2}}}]=t$$

subspaces.

3. The gap principle

Lemma 3. 1. *For each j with $0 \leqq j \leqq s$ let $L_1^{(j)}, \ldots, L_n^{(j)}$ be linearly independent linear forms in $n \geqq 2$ variables with coefficients in $\mathbb{Q}_j$. Suppose that*

$$(n!)^4 \leqq P \leqq B \tag{3. 1}$$

and put $Q = (\log B)/(\log P)$. Then the points $\mathbf{x} \in \mathbb{Z}^n$ in the ball

$$|\mathbf{x}| \leqq B \tag{3. 2}$$

satisfying

$$\prod_{j=0}^{s} |L_1^{(j)}(\mathbf{x}) \cdots L_n^{(j)}(\mathbf{x})|_j < \left(\prod_{j=0}^{s} |\det(L_1^{(j)}, \ldots, L_n^{(j)})|_j \right) P^{-1} \tag{3. 3}$$

lie in the union of not more than

$$(3n^3(s+1)Q)^{n(s+1)-1}$$

proper rational subspaces.

Proof. It is shown in section 3 of [15] that *it will be enough to prove that for forms $L_1^{(0)}, \ldots, L_n^{(0)}$ whose coefficient vectors are an orthonormal system, the points in the ball* (3. 2) *with*

$$\prod_{j=0}^{s} |L_1^{(j)}(\mathbf{x}) \cdots L_n^{(j)}(\mathbf{x})|_j < \left(\prod_{j=0}^{s} |\det(L_1^{(j)}, \ldots, L_n^{(j)})|_j \right) n!\, P^{-1} \tag{3. 4}$$

lie in not more than $(n!)^{-1}Z$ subspaces with $Z = (3n^3(s+1)Q)^{n(s+1)-1}$. Notice that if $L_1^{(0)}, \ldots, L_n^{(0)}$ is an orthonormal system, then we have

$$|\det(L_1^{(0)}, \ldots, L_n^{(0)})|_0 = 1 \text{ and in view of (3. 2)} \tag{3. 5}$$

$$|L_i^{(0)}(\mathbf{x})|_0 \leqq B. \tag{3. 6}$$

Our next goal is to reduce the problem to a situation where for each j $(1 \leqq j \leqq s)$ the forms $L_1^{(j)}, \ldots, L_n^{(j)}$ are of the shape

$$\begin{cases} L_1^{(j)} = X_1, \\ L_2^{(j)} = \alpha_{21}^{(j)} X_1 + X_2, \\ \quad \vdots \quad \vdots \qquad \cdot \qquad \cdot \\ L_n^{(j)} = \alpha_{n1}^{(j)} X_1 + \alpha_{n2}^{(j)} X_2 + \cdots + \alpha_{n,n-1}^{(j)} X_{n-1} + X_n \end{cases} \tag{3. 7}$$

with coefficients $\alpha_{ik}^{(j)} \in \mathbb{Z}_j = \{x \in \mathbb{Q}_j \mid |x|_j \leqq 1\}$. So fix any j with $1 \leqq j \leqq s$. (3.4) is invariant under replacing $L_i^{(j)}$ by $\lambda_i L_i^{(j)}$ $(i = 1, \ldots, n)$ with nonzero λ_i in $\mathbb{Q}_j$. Therefore we may suppose that $L_i^{(j)}(\mathbf{X}) = \alpha_{i1}^{(j)} X_1 + \cdots + \alpha_{in}^{(j)} X_n = \boldsymbol{\alpha}_i^{(j)} \mathbf{X}$ has coefficient vector $\boldsymbol{\alpha}_i^{(j)}$ in $\mathbb{Z}_j^{\,n}$ and that moreover for any i $(1 \leqq i \leqq n)$ there exists k with $\alpha_{ik}^{(j)} = 1$. By symmetry it will suffice to consider solutions of (3.2), (3.4) with

$$|L_n^{(j)}(\mathbf{x})|_j = \min\{|L_1^{(j)}(\mathbf{x})|_j, \ldots, |L_n^{(j)}(\mathbf{x})|_j\} \tag{3.8}$$

and to prove that they are contained in the union of not more than $n^{-1}(n!)^{-1}Z$ subspaces.

Suppose for simplicity of notation that we have $\alpha_{nn}^{(j)} = 1$. Define forms

$$L_1'^{(j)}(\mathbf{X}) = L_1^{(j)}(\mathbf{X}) - \alpha_{1n}^{(j)} L_n^{(j)}(\mathbf{X}), \ldots, L_{n-1}'^{(j)}(\mathbf{X}) = L_{n-1}^{(j)}(\mathbf{X}) - \alpha_{n-1,n}^{(j)} L_n^{(j)}(\mathbf{X}).$$

Here $\det(L_1'^{(j)}, \ldots, L_{n-1}'^{(j)}, L_n^{(j)}) = \det(L_1^{(j)}, \ldots, L_{n-1}^{(j)}, L_n^{(j)})$.

Moreover for $i = 1, \ldots, n-1$ we have

$$\begin{aligned} |L_i'^{(j)}(\mathbf{x})|_j = |L_i^{(j)}(\mathbf{x}) - \alpha_{in}^{(j)} L_n^{(j)}(\mathbf{x})|_j &\leqq \max\{|L_i^{(j)}(\mathbf{x})|_j, |\alpha_{in}^{(j)}|_j \cdot |L_n^{(j)}(\mathbf{x})|_j\} \\ &\leqq \max\{|L_i^{(j)}(\mathbf{x})|_j, |L_n^{(j)}(\mathbf{x})|_j\} \leqq |L_i^{(j)}(\mathbf{x})|_j \end{aligned}$$

by (3.8) and since $\alpha_{in}^{(j)} \in \mathbb{Z}_j$. Notice that the forms

$$L_i'^{(j)}(\mathbf{X}) = \alpha_{i1}'^{(j)} X_1 + \cdots + \alpha_{i,n-1}'^{(j)} X_{n-1} + \alpha_{in}'^{(j)} X_n$$

have $\alpha_{in}'^{(j)} = 0$. Thus we see that *it will suffice to show that when* $L_1^{(j)}, \ldots, L_n^{(j)}$ *have coefficients in* $\mathbb{Z}_j$ *such that* $\alpha_{nn}^{(j)} = 1$ *and for* $i = 1, \ldots, n-1$ $\alpha_{in}^{(j)} = 0$, *then the points* $\mathbf{x}$ *with* (3.2), (3.4) *lie in at most* $n^{-1}(n!)^{-1}Z$ *subspaces.* Starting with the new forms $L_1^{(j)}, \ldots, L_{n-1}^{(j)}, L_n^{(j)}$ we repeat the procedure. Again we may multiply $L_1^{(j)}, \ldots, L_{n-1}^{(j)}$ with suitable nonzero factors in $\mathbb{Q}_j$ to ensure that they have coefficients in $\mathbb{Z}_j$ and such that moreover for each i $(1 \leqq i \leqq n-1)$ there exists k $(1 \leqq k \leqq n-1)$ with $\alpha_{ik}^{(j)} = 1$, whereas $\alpha_{in}^{(j)} = 0$ $(i = 1, \ldots, n-1)$. It will suffice to show that the solutions of (3.2), (3.4), (3.8) and

$$|L_{n-1}^{(j)}(\mathbf{x})|_j = \min\{|L_1^{(j)}(\mathbf{x})|_j, \ldots, |L_{n-1}^{(j)}(\mathbf{x})|_j\}$$

lie in at most $(n-1)^{-1} n^{-1}(n!)^{-1}Z$ subspaces. Suppose for simplicity that $\alpha_{n-1,n-1}^{(j)} = 1$ and put $L_i'^{(j)}(\mathbf{X}) = L_i^{(j)}(\mathbf{X}) - \alpha_{i,n-1}^{(j)} L_{n-1}^{(j)}(\mathbf{X})$ $(i = 1, \ldots, n-2)$. Then again $|L_i'^{(j)}(\mathbf{x})|_j \leqq |L_i^{(j)}(\mathbf{x})|_j$ $(i = 1, \ldots, n-2)$. Denoting the new forms again by $L_1^{(j)}, \ldots, L_n^{(j)}$ we see: *It will suffice to show that when* $L_1^{(j)}, \ldots, L_{n-2}^{(j)}, L_{n-1}^{(j)}, L_n^{(j)}$ *have coefficients in* $\mathbb{Z}_j$, *when*

$$L_i^{(j)} = \alpha_{i1}^{(j)} X_1 + \cdots + \alpha_{i,n-2}^{(j)} X_{n-2}$$

for $i = 1, \ldots, n-2$, *whereas* $L_{n-1}^{(j)} = \alpha_{n-1,1}^{(j)} X_1 + \cdots + \alpha_{n-1,n-2}^{(j)} X_{n-2} + X_{n-1}$ *and*

$$L_n^{(j)} = \alpha_{n1}^{(j)} X_1 + \cdots + \alpha_{n,n-1}^{(j)} X_{n-1} + X_n$$

then the solutions of (3. 2), (3. 4) *lie in at most* $(n-1)^{-1}\, n^{-1}(n!)^{-1} Z$ *subspaces.* Continuing in this way and applying our procedure for each j $(1 \leqq j \leqq s)$ we finally see that *it will be enough to show that for an orthonormal system* $L_1^{(0)}, \ldots, L_n^{(0)}$ *and for forms* $L_1^{(j)}, \ldots, L_n^{(j)}$ *of the shape* (3. 7) *and with coefficients in* $\mathbb{Z}_j$ $(j=1, \ldots, s)$ *the rational integral solutions of*

$$|\mathbf{x}| \leqq B \quad \text{and} \quad \prod_{j=0}^{s} |L_1^{(j)}(\mathbf{x}) \cdots L_n^{(j)}(\mathbf{x})|_j < n!\, P^{-1} \tag{3. 9}$$

lie in not more than $(n!)^{-(s+1)} Z$ *subspaces.*

Now points $\mathbf{x}$ with (3. 2) satisfy (3. 6) and moreover (since for $1 \leqq j \leqq s$ $L_i^{(j)}$ has coefficients in $\mathbb{Z}_j$) for $\mathbf{x} \in \mathbb{Z}^n$ we have

$$|L_i^{(j)}(\mathbf{x})|_j \leqq 1 \qquad (i=1, \ldots, n;\ j=1, \ldots, s). \tag{3. 10}$$

Put $C = (P/(n!)^2)^{1/(n(s+1)-1)}$. Then (3. 9) may be rewritten as

$$\prod_{j=0}^{s} |L_1^{(j)}(\mathbf{x}) \cdots L_n^{(j)}(\mathbf{x})|_j < \frac{1}{n!\, C^{n(s+1)-1}}. \tag{3. 11}$$

Write $R = (\log(n!\, B^n))/\log C$. Given i with $1 \leqq i \leqq n-1$ let $M(i, 0)$ be the set of solutions of (3. 9) satisfying

$$|L_i^{(0)}(\mathbf{x})|_0 < BC^{-R} = \frac{1}{n!}\, B^{1-n}. \tag{3. 12}$$

Given a pair (i, j) with $1 \leqq i \leqq n$, $1 \leqq j \leqq s$ let $M(i, j)$ be the set of solutions with

$$|L_i^{(j)}(\mathbf{x})|_j < C^{-R} = \frac{1}{n!}\, B^{-n}. \tag{3. 13}$$

If $\mathbf{x}$ is a solution of (3. 9) which does not lie in the union of

$$M(1, 0), \ldots, M(n-1, 0),\ M(1, 1), \ldots, M(n, 1), \ldots, M(1, s), \ldots, M(n, s)$$

then by (3. 6) and (3. 10) there exist integers $q_{10}, \ldots, q_{n-1,0}, q_{11}, \cdots, q_{n1}, \cdots, q_{1s}, \cdots, q_{ns}$ with $0 \leqq q_{ij} \leqq R$ such that

$$C^{-q_{i0}-1} B < |L_i^{(0)}(\mathbf{x})|_0 \leqq C^{-q_{i0}} B \qquad (i=1, \ldots, n-1) \tag{3. 14}$$

and

$$C^{-q_{ij}-1} < |L_i^{(j)}(\mathbf{x})|_j \leqq C^{-q_{ij}} \qquad (i=1, \ldots, n;\ j=1, \ldots, s) \tag{3. 15}$$

hold true. For an $(n(s+1)-1)$-tuple $\mathbf{q} = (q_{10}, \ldots, q_{n-1,0}, q_{11}, \cdots, q_{ns})$ let $M(\mathbf{q})$ be the set of solutions of (3. 9) satisfying (3. 14) and (3. 15). We are going to show that for each of the sets $M(i, 0)$, $M(i, j)$, $M(\mathbf{q})$ there exists a proper rational subspace S_{i0}, S_{ij}, $S_{\mathbf{q}}$ respectively such that $M(i, 0) \subset S_{i0}$, $M(i, j) \subset S_{ij}$, $M(\mathbf{q}) \subset S_{\mathbf{q}}$.

In fact let $\mathbf{x}_1, \ldots, \mathbf{x}_n$ be a family of n points in $M(i, 0)$ whose rank r is maximal among all families with elements in $M(i, 0)$. Then, since

$$|\det(L_1^{(j)}, \ldots, L_n^{(j)})|_j = 1 \qquad (j = 0, \ldots, s)$$

and by (3. 6), (3. 10), (3. 12) we have

$$(3.16) \qquad \prod_{j=0}^{s} |\det(\mathbf{x}_1, \ldots, \mathbf{x}_n)|_j = \prod_{j=0}^{s} |\det(L_i^{(j)}(\mathbf{x}_k))_{(i,k)}|_j < n!\, B^{n-1} \frac{1}{n!} B^{1-n} = 1.$$

But $\prod_{j=0}^{s} |\det(\mathbf{x}_1, \ldots, \mathbf{x}_n)|_j$ is an integer. Hence $\det(\mathbf{x}_1, \ldots, \mathbf{x}_n) = 0$ and $\mathbf{x}_1, \ldots, \mathbf{x}_n$ have rank $r \leqq n-1$. Therefore there exists a subfamily say $\mathbf{x}_1, \ldots, \mathbf{x}_{n-1}$ whose rank is r as well. Now if $\mathbf{x}$ is any point in $M(i, 0)$ then by the maximality of r we infer

$$\operatorname{rank}\{\mathbf{x}_1, \ldots, \mathbf{x}_{n-1}, \mathbf{x}\} = r.$$

So $\mathbf{x}$ lies in the subspace S_{i0} generated by $\mathbf{x}_1, \ldots, \mathbf{x}_{n-1}$.

If instead of $M(i, 0)$ we study $M(i, j)$ for some $j > 0$ we get again (3. 16) using (3. 6), (3. 10), (3. 13) and thus we find a proper subspace S_{ij} with $M(i, j) \subset S_{ij}$. Now suppose that for some $\mathbf{q}$ we have solutions $\mathbf{x} \in M(\mathbf{q})$. Then we infer from (3. 11), (3. 14), (3. 15) that

$$|L_n^{(0)}(\mathbf{x})|_0 < \frac{1}{n!} B^{1-n} C^{q_{10} + \cdots + q_{n-1,0} + q_{11} + \cdots + q_{ns}}.$$

Therefore if $\mathbf{x}_1, \ldots, \mathbf{x}_n$ are any n solutions in $M(\mathbf{q})$ we have

$$\prod_{j=0}^{s} |\det(\mathbf{x}_1, \ldots, \mathbf{x}_n)|_j = \prod_{j=0}^{s} |\det(L_i^{(j)}(\mathbf{x}_k))_{(i,k)}|_j < n! \left(\prod_{i=1}^{n-1} BC^{-q_{i0}} \right) \frac{1}{n!} B^{1-n}$$
$$\times C^{q_{10} + \cdots + q_{n-1,0} + q_{11} + \cdots + q_{ns}} C^{-q_{11} - \cdots - q_{ns}} = 1,$$

and again there exists a proper subspace $S_{\mathbf{q}}$ containing $M(\mathbf{q})$.

The total number of our subspaces S_{i0}, S_{ij}, $S_{\mathbf{q}}$ is

$$\leqq n(s+1) - 1 + (R+1)^{n(s+1)-1}.$$

Now by (3. 1) we have $C \geqq P^{1/2(n(s+1)-1)}$ and $n!\, B^n \leqq B^{(4n+1)/4}$, so that

$$R \leqq (\log(B^{(4n+1)/4}))/(\log(P^{1/2(n(s+1)-1)})) = \frac{(4n+1)(n(s+1)-1)}{2} Q.$$

Thus the number of subspaces is

$$\leqq n(s+1)-1+\left(\left(2n^2(s+1)-2n+\frac{n}{2}(s+1)+\frac{1}{2}\right)\cdot Q\right)^{n(s+1)-1} \leqq \left(\frac{5}{2}n^2(s+1)Q\right)^{n(s+1)-1}.$$

Since

$$\left(\frac{5}{2}n^2(s+1)Q\right)^{n(s+1)-1} \leqq (n!)^{-(s+1)}Z = (n!)^{-(s+1)}(3n^3(s+1)Q)^{n(s+1)},$$

the assertion follows.

Lemma 3. 2. *Suppose that* $0<\delta<1$ *and* $n\geqq 2$. *Let* $(n!)^{4/\delta}\leqq A<B$. *Then the integral points* $\mathbf{x}$ *in* $A<|\mathbf{x}|\leqq B$ *with*

$$\prod_{j=0}^{s}|L_1^{(j)}(\mathbf{x})\cdots L_n^{(j)}(\mathbf{x})|_j<\left(\prod_{j=0}^{s}|\det(L_1^{(j)},\ldots,L_n^{(j)})|_j\right)|\mathbf{x}|^{-\delta} \tag{3. 17}$$

lie in

$$<(3n^3(s+1)e\delta^{-1})^{n(s+1)-1}\left(1+\log\frac{\log B}{\log A}\right)$$

proper subspaces.

Proof. Let us first consider the case when $B=A^e$. The solutions of (3. 17) then have

$$\prod_{j=0}^{s}|L_1^{(j)}(\mathbf{x})\cdots L_n^{(j)}(\mathbf{x})|_j<\left(\prod_{j=0}^{s}|\det(L_1^{(j)},\ldots,L_n^{(j)})|_j\right)P^{-1} \tag{3. 18}$$

with $P=A^{\delta}\geqq(n!)^4$. By Lemma 3. 1 the integral points $\mathbf{x}$ with (3. 18) and $|\mathbf{x}|\leqq B$ lie in

$$<\left(3n^3(s+1)\frac{\log B}{\log P}\right)^{n(s+1)-1}=\left(3n^3(s+1)\frac{e}{\delta}\right)^{n(s+1)-1}$$

subspaces. On the other hand the interval $A<\xi\leqq B$ is contained in the union of the intervals $A^{e^{\nu}}<\xi\leqq A^{e^{\nu+1}}$ with $0\leqq\nu\leqq\log\frac{\log B}{\log A}$. The number of these intervals is

$$\leqq 1+\log\frac{\log B}{\log A},$$

and the Lemma follows.

4. A further reduction

Let $L(\mathbf{X}) = \alpha_1 X_1 + \cdots + \alpha_n X_n$ be a linear form with coefficients in a number field K. For any $v \in M'(K)$ we put $|L|_v = |\boldsymbol{\alpha}|_v$, where $\boldsymbol{\alpha}$ is the coefficient vector of L and $|\boldsymbol{\alpha}|_v$ is defined in section 1.

Proposition B. *Let K be a number field of degree d. For each j $(0 \leqq j \leqq s)$ let $L_1^{(j)}, \ldots, L_n^{(j)}$ be linearly independent linear forms with coefficients in $\varphi_j(K) \cap \mathfrak{Q}_j$. Then the integral points $\mathbf{x}$ with*

$$\prod_{j=0}^{s} |L_1^{(j)}(\mathbf{x}) \cdots L_n^{(j)}(\mathbf{x})|_j < \left(\prod_{j=0}^{s} |L_1^{(j)}|_j \cdots |L_n^{(j)}|_j \right) |\mathbf{x}|^{-\delta} \tag{4. 1}$$

having

$$|\mathbf{x}| > (2H)^{e^{t_1}}, \tag{4. 2}$$

where $0 < \delta < 1$, H is a quantity satisfying (1. 8), *and where*

$$t_1 = (2(s+1)d)^{2^{25n}(s+1)^6 \delta^{-2}} \tag{4. 3}$$

lie in the union of at most t_1 proper subspaces.

We claim that Proposition B implies Proposition A. Notice that (1. 3) implies (4. 1). We still have to study solutions of (1. 3) with $A < |\mathbf{x}| \leqq B$, where

$$A = \max \left\{ (n!)^{4/\delta}, \frac{1}{2} H^{1/d} \right\}$$

and $B = (2H)^{e^{t_1}}$. Notice that

$$A \geqq \left((n!)^{4/\delta} \cdot \frac{1}{2} H^{1/d} \right)^{1/2} > (2H)^{1/2d},$$

whence $\dfrac{\log B}{\log A} < 2de^{t_1} < e^{(3/2)t_1}$ and $1 + \log \dfrac{\log B}{\log A} < 1 + \dfrac{3}{2} t_1 < 2t_1$. So if $B > A$, we infer from Lemma 3. 2 that the solutions under consideration are contained in the union of

$$< 2t_1 (3en^3(s+1)\delta^{-1})^{n(s+1)} < 2^{8n^2(s+1)^2\delta^{-1}} t_1$$

subspaces. Combining this with Proposition B we see, that the integer points with (1. 3) and (2. 6) lie in the union of not more than

$$t_1 + 2^{8n^2(s+1)^2\delta^{-1}} t_1 \leqq t_0$$

subspaces and Proposition A follows.

The remainder of the paper deals with the proof of Proposition B. At several places in the proof it will be useful to take forms into consideration whose coefficients do not necessarily lie in K but which are proportional to forms with coefficients in K (with an algebraic factor). Such forms will be said to be defined over K. Similarly if $\boldsymbol{\beta}$ is a vector with $\boldsymbol{\beta}=\lambda\boldsymbol{\alpha}$ for some vector $\boldsymbol{\alpha}\in K^n$ and an algebraic number $\lambda\neq 0$ we will say that $\boldsymbol{\beta}$ is defined over K. Notice that this definition implies that $H(\boldsymbol{\beta})=H(\boldsymbol{\alpha})$. Thus in particular if M is a linear form which is defined over K and if $M=\lambda L$, where L has coefficients in K and where $\lambda\neq 0$ is algebraic, we have $H(M)=H(L)$. Moreover if L has coefficients in K we denote its image in $\varphi_j(K)$ by $L^{(j)}$, where φ_j is the embedding of K into Ω_j described in section 1. Then $M^{(0)}=|L^{(0)}|_0^{-1}L^{(0)}$ is defined over K and is normalized in the sense that $|M^{(0)}|_0=1$. Moreover it is clear that for j with $1\leqq j\leqq s$ $M^{(j)}=|L^{(j)}|_j L^{(j)}$ is defined over K and has $|M^{(j)}|_j=1$. We will then say that $M^{(j)}$ is normalized with respect to $|\ |_j$ or simply that it is normalized.

With this notation (4. 1) becomes

$$\prod_{j=0}^{s}|M_1^{(j)}(\mathbf{x})\cdots M_n^{(j)}(\mathbf{x})|_j<|\mathbf{x}|^{-\delta}. \tag{4. 4}$$

We will write $M_i^{(j)}(\mathbf{X})=\boldsymbol{\beta}_i^{(j)}\mathbf{X}=\beta_{i1}^{(j)}X_1+\cdots+\beta_{in}^{(j)}X_n$, where $|\boldsymbol{\beta}_i^{(j)}|_j=1$ and

$$H(\boldsymbol{\beta}_i^{(j)})=H(M^{(j)})\qquad (i=1,\ldots,n;\ j=0,\ldots,s).$$

So (1. 8) is the same as

$$H\geqq\max\{H(\boldsymbol{\beta}_1^{(0)}),\ldots,H(\boldsymbol{\beta}_n^{(0)}),\ldots,H(\boldsymbol{\beta}_1^{(s)}),\ldots,H(\boldsymbol{\beta}_n^{(s)})\} \tag{4. 5}$$

and (4. 4) becomes

$$\prod_{j=0}^{s}|(\boldsymbol{\beta}_1^{(j)}\mathbf{x})\cdots(\boldsymbol{\beta}_n^{(j)}\mathbf{x})|_j<|\mathbf{x}|^{-\delta}. \tag{4. 6}$$

5. Lemmata on heights

In the sequel we shall use several times exterior products. For details the reader is referred to [14], p. 102ff., or to [5]. In fact the material of this section is very similar to section 5 in [15]. For the convenience of the reader we shall however present in some cases the proofs.

When $\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_k$ lie in K^n with $1\leqq k\leqq n$, then the exterior product $\boldsymbol{\alpha}_1\wedge\cdots\wedge\boldsymbol{\alpha}_k$ lies in K^l with $l=\binom{n}{k}$. In particular $\boldsymbol{\alpha}_1\wedge\cdots\wedge\boldsymbol{\alpha}_{n-1}$ lies in K^n and it is orthogonal to each of $\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_{n-1}$ with respect to the standard inner product.

Lemma 5. 1. *Let $\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_k$ be linearly independent vectors defined over K. Then*

$$\boldsymbol{\gamma}=\boldsymbol{\alpha}_1\wedge\cdots\wedge\boldsymbol{\alpha}_k$$

has

$$H(\boldsymbol{\gamma})\leqq H(\boldsymbol{\alpha}_1)\cdots H(\boldsymbol{\alpha}_k). \tag{5. 1}$$

This is Lemma 5. 1 of [15].

If $\mathfrak{a}$ is defined over a number field K then in particular $\mathfrak{a}$ has components in a finite extension say F of K. Given $v \in M'(K)$ we fix any extension of v to F and we denote it again by v.

Lemma 5. 2. *Suppose K has degree d. Again let $\gamma = \mathfrak{a}_1 \wedge \cdots \wedge \mathfrak{a}_k$ where $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ are linearly independent and defined over K. Then for $v \in M'(K)$*

$$|\gamma|_v \, H(\gamma)^{-d} \geqq |\mathfrak{a}_1|_v \cdots |\mathfrak{a}_k|_v \, (H(\mathfrak{a}_1) \cdots H(\mathfrak{a}_k))^{-d}. \tag{5. 2}$$

In particular in the case $k = n$ we have

$$|\det(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)|_v \geqq |\mathfrak{a}_1|_v \cdots |\mathfrak{a}_n|_v \, (H(\mathfrak{a}_1) \cdots H(\mathfrak{a}_n))^{-d}. \tag{5. 3}$$

This is mutatis mutandis Lemma 5. 2 of [15].

Lemma 5. 3. *Let K be a number field of degree d and $v \in M'(K)$. Suppose $\mathfrak{a}$ is defined over K. Let $\mathbf{g}$ be a point with rational integral components and with $\mathfrak{a}\mathbf{g} \neq 0$. Then we have*

$$|\mathfrak{a}\mathbf{g}|_v \geqq |\mathfrak{a}|_v \, H(\mathfrak{a})^{-d} \, |\mathbf{g}|^{1-d} \quad \text{if } v \text{ is archimedean} \tag{5. 4}$$

and

$$|\mathfrak{a}\mathbf{g}|_v \geqq |\mathfrak{a}|_v \, H(\mathfrak{a})^{-d} \, |\mathbf{g}|^{-d} \quad \text{if } v \text{ is nonarchimedean.} \tag{5. 5}$$

Proof. Since our inequalities are invariant if we multiply $\mathfrak{a}$ by some nonzero algebraic factor, we may suppose that $\mathfrak{a}$ has components in K. Since $\mathbf{g}$ is integral we have for any $w \in M'(K)$

$$|\mathfrak{a}\mathbf{g}|_w \leqq |\mathfrak{a}|_w \, |\mathbf{g}|_w \quad \text{if } w \text{ is archimedean} \tag{5. 6}$$

and

$$|\mathfrak{a}\mathbf{g}|_w \leqq |\mathfrak{a}|_w \quad \text{if } w \text{ is nonarchimedean.} \tag{5. 7}$$

Now by the product formula for K we get for $v \in M'(K)$

$$1 = \prod_{w \in M'(K)} |\mathfrak{a}\mathbf{g}|_w = |\mathfrak{a}\mathbf{g}|_v \prod_{w \neq v} |\mathfrak{a}\mathbf{g}|_w. \tag{5. 8}$$

As there are precisely d archimedean elements $w \in M'(K)$, we obtain combining (5. 6), (5. 7), (5. 8) for archimedean v

$$1 \leqq |\mathfrak{a}\mathbf{g}|_v \, |\mathbf{g}|^{d-1} \, |\mathfrak{a}|_v^{-1} \prod_{w \in M'(K)} |\mathfrak{a}|_w = |\mathfrak{a}\mathbf{g}|_v \, |\mathfrak{a}|_v^{-1} \, H(\mathfrak{a})^d \, |\mathbf{g}|^{d-1}$$

whereas for nonarchimedean v we get

$$1 \leqq |\mathfrak{a}\mathbf{g}|_v \, |\mathbf{g}|^d \, |\mathfrak{a}|_v^{-1} \prod_{w \in M'(K)} |\mathfrak{a}|_w = |\mathfrak{a}\mathbf{g}|_v \, |\mathfrak{a}|_v^{-1} \, H(\mathfrak{a})^d \, |\mathbf{g}|^d.$$

For $j=0,\dots,s$ let $|\ |_j$ be the absolute value as defined in section 1. Remember that for $1\leqq j\leqq s$ $|\ |_j$ is the p_j-adic valuation.

Lemma 5. 4. *Let K be as above. For $j=0,\dots,s$ let $\alpha_1^{(j)},\dots,\alpha_{n-1}^{(j)}$ be linearly independent vectors in Ω_j^n and defined over K. Put $\gamma^{(j)}=\alpha_1^{(j)}\wedge\cdots\wedge\alpha_{n-1}^{(j)}$ $(j=0,\dots,s)$. Let $\mathbf{g}$ be a point with rational components whose denominators are only composed by $p_1,\dots,p_s$. Assume that we have*

$$\prod_{j=0}^{s}|\gamma^{(j)}\mathbf{g}|_j\neq 0.$$

Then

$$\prod_{j=0}^{s}|\gamma^{(j)}\mathbf{g}|_j\geqq\prod_{j=0}^{s}\left(|\alpha_1^{(j)}|_j\cdots|\alpha_{n-1}^{(j)}|_j\,H(\alpha_1^{(j)})^{-d}\cdots H(\alpha_{n-1}^{(j)})^{-d}\,|\mathbf{g}|_j^{-d(s+1)+1}\right). \tag{5. 6}$$

Proof. If $\alpha_i^{(j)}$ is multiplied by a factor $\lambda_i^{(j)}\neq 0$ $(i=1,\dots,n-1)$, then $\gamma^{(j)}$ is multiplied by $\lambda_1^{(j)}\cdots\lambda_{n-1}^{(j)}$. Thus we may suppose that $\alpha_i^{(j)}$ has components in K (more precisely in $\varphi_j(K)$). We have $\gamma^{(j)}\mathbf{g}=\det(\alpha_1^{(j)},\dots,\alpha_{n-1}^{(j)},\mathbf{g})$, hence for each $w\in M'(K)$

$$|\gamma^{(j)}\mathbf{g}|_w\leqq|\alpha_1^{(j)}|_w\cdots|\alpha_{n-1}^{(j)}|_w\,|\mathbf{g}|_w.$$

The hypothesis about $\mathbf{g}$ implies that $|\mathbf{g}|_w\leqq 1$ for any nonarchimedean $w\in M'(K)$ which is not an extension of one of the absolute values $|\ |_j$ of $\mathbb{Q}$ for $1\leqq j\leqq s$.

For any j_0 with $0\leqq j_0\leqq s$ we have by the product formula

$$\begin{aligned}1&=\prod_{w\in M'(K)}|\gamma^{(j_0)}\mathbf{g}|_w=|\gamma^{(j_0)}\mathbf{g}|_{j_0}\prod_{w\neq j_0}|\gamma^{(j_0)}\mathbf{g}|_w\\&\leqq|\gamma^{(j_0)}\mathbf{g}|_{j_0}\prod_{w\neq j_0}\left(|\alpha_1^{(j_0)}|_w\cdots|\alpha_{n-1}^{(j_0)}|_w\,|\mathbf{g}|_w\right).\end{aligned}$$

Now any absolute value of $\mathbb{Q}$ has precisely d extensions in $M'(K)$. Applying this for $|\ |_0,\dots,|\ |_s$ we obtain

$$\begin{aligned}1&\leqq|\gamma^{(j_0)}\mathbf{g}|_{j_0}\,|\mathbf{g}|_{j_0}^{d-1}\left(\prod_{\substack{j=0\\ j\neq j_0}}^{s}|\mathbf{g}|_j^d\right)(|\alpha_1^{(j_0)}|_{j_0}\cdots|\alpha_{n-1}^{(j_0)}|_{j_0})^{-1}\prod_{w\in M'(K)}(|\alpha_1^{(j_0)}|_w\cdots|\alpha_{n-1}^{(j_0)}|_w)\\&=|\gamma^{(j_0)}\mathbf{g}|_{j_0}\,|\mathbf{g}|_{j_0}^{-1}\left(\prod_{j=0}^{s}|\mathbf{g}|_j^d\right)(|\alpha_1^{(j_0)}|_{j_0}\cdots|\alpha_{n-1}^{(j_0)}|_{j_0})^{-1}\,(H(\alpha_1^{(j_0)})\cdots H(\alpha_{n-1}^{(j_0)}))^d.\end{aligned}$$

Taking the product over $j_0=0,\dots,s$ we get the assertion.

Lemma 5. 5. *Let K be a number field of degree d. Suppose $v \in M'(K)$ and let $L_1, \dots, L_n$ be linearly independent forms in n variables defined over K. Then the variables X_i may be uniquely expressed as linear combinations*

$$X_i = \gamma_{i1} L_1 + \cdots + \gamma_{in} L_n \quad (i = 1, \dots, n),$$

and here

$$|\gamma_{ij}|_v \, |L_j|_v \leqq (H(L_1) \cdots H(L_n))^d \quad (1 \leqq i, j \leqq n). \tag{5. 10}$$

This is Lemma 5. 6 of [15].

Lemma 5. 6. *Let $\gamma_1, \dots, \gamma_k$ be vectors in K^n. Suppose that there is an $\mathbf{h} \neq \mathbf{0}$ in $\mathbb{Q}^n$ with*

$$\gamma_i \mathbf{h} = 0 \quad (i = 1, \dots, k). \tag{5. 11}$$

Then there is an $\mathbf{h} \neq \mathbf{0}$ in $\mathbb{Z}^n$ with (5. 11) *and with*

$$|\mathbf{h}| \leqq H_1^{n-1}$$

where $H_1 = \max\{H(\gamma_1), \dots, H(\gamma_k)\}$.

This is Lemma 5. 9 of [15].

6. Lattices

Let $C = (c_{ij})$ be an $(n \times n)$-matrix with integral entries. Moreover let m be a natural number. We shall study the congruence

$$C\mathbf{x} \equiv \mathbf{0} \bmod m$$

that is

$$c_{i1} x_1 + c_{i2} x_2 + \cdots + c_{in} x_n \equiv 0 \bmod m \quad (i = 1, \dots, n). \tag{6. 1}$$

A classical result in linear algebra says that there are unimodular integral $(n \times n)$-matrices S_1 and S_2 such that

$$S_1 C S_2 = \begin{pmatrix} c_1 & & & 0 \\ & c_2 & & \\ & & \ddots & \\ 0 & & & c_n \end{pmatrix}. \tag{6. 2}$$

Lemma 6. 1. *The set of integral solutions* $\mathbf{x}$ *of the system of congruences* (6. 1) *is a sublattice* Λ_m *of* $\mathbb{Z}^n$ *of determinant*

$$\det \Lambda_m = \prod_{i=1}^{n} \frac{m}{(m, c_i)}. \tag{6. 3}$$

Proof. Only (6. 3) has to be shown. The system (6. 1) may be written as

$$C\mathbf{x} = m\mathbf{z} \tag{6. 4}$$

where $\mathbf{z}$ is in $\mathbb{Z}^n$. Let S_1, S_2 be unimodular matrices as in (6. 2). Put

$$\mathbf{y} = S_2^{-1}\mathbf{x}, \quad S_1\mathbf{z} = \mathbf{z}'. \tag{6. 5}$$

Then (6. 4) is equivalent to $S_1 C S_2 \mathbf{y} = m\mathbf{z}'$ that is (using (6. 2))

$$c_i y_i = m z_i' \quad (i = 1, \ldots, n). \tag{6. 6}$$

The integral solutions y_i, z_i' of (6. 6) are of the shape

$$y_i = \frac{m}{(m, c_i)} \xi_i, \quad z_i' = \frac{c_i}{(m, c_i)} \xi_i,$$

where ξ_i is an integral parameter. But this implies that the points $\mathbf{y}$ in (6. 6) form a sublattice of $\mathbb{Z}^n$ of determinant $\prod_{i=1}^{n} \frac{m}{(m, c_i)}$. Since S_2 is unimodular, we infer from (6. 5) that the same holds true for the solutions $\mathbf{x}$ of (6. 1).

Let p be a prime and let $\mathbb{Z}(p)$ be the set of rational numbers $r = \frac{u}{v}$ with v a power of p.

Lemma 6. 2. *Let* $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ *be linearly independent vectors in* $\mathbb{Q}_p^n$. *Then the set of solutions* $\mathbf{x}$ *with components in* $\mathbb{Z}(p)$ *of the simultaneous inequalities*

$$|\boldsymbol{\beta}_i \mathbf{x}|_p \leqq 1 \quad (i = 1, \ldots, n) \tag{6. 7}$$

is a lattice Λ_p *in* $\mathbb{Z}(p)^n$ *having*

$$\det \Lambda_p = |\det(\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n)|_p.$$

Proof. Write $\boldsymbol{\beta}_i = (\beta_{i1}, \ldots, \beta_{in})$. Let B be the matrix with rows $\boldsymbol{\beta}_i$. Define ϑ by

$$\max_{1 \leqq i \leqq n} |\boldsymbol{\beta}_i|_p = p^{\vartheta} \tag{6. 8}$$

and γ by

$$|\det B|_p = p^{\gamma}. \tag{6. 9}$$

Moreover put

$$\boldsymbol{\beta}_i' = p^{\vartheta}\boldsymbol{\beta}_i \quad (1 \leqq i \leqq n). \tag{6. 10}$$

Then the matrix B' with rows $\boldsymbol{\beta}_i'$ has

$$|\det B'|_p = p^{-n\vartheta+\gamma} \tag{6. 11}$$

and by (6. 8), (6. 10) the entries of B' are p-adic integers.

Now any solution $\mathbf{x} \in \mathbb{Q}_p^n$ of (6. 7) satisfies $B\mathbf{x} = \mathbf{z}$, where the components of $\mathbf{z}$ are suitable p-adic integers. Thus $\mathbf{x} = B^{-1}\mathbf{z}$, and using Cramer's rule as well as (6. 8) and (6. 9) we obtain for any solution $\mathbf{x}$ of (6. 7)

$$|\mathbf{x}|_p \leqq p^{(n-1)\vartheta-\gamma}. \tag{6. 12}$$

Since we ask for solutions in $\mathbb{Z}(p)^n$, (6. 12) implies that

$$p^{(n-1)\vartheta-\gamma}\mathbf{x} = \mathbf{y} \in \mathbb{Z}^n. \tag{6. 13}$$

Now by (6. 7), (6. 10), (6. 13) we have to look for the integral solutions $\mathbf{y}$ of

$$|\boldsymbol{\beta}_i'\mathbf{y}|_p \leqq p^{-n\vartheta+\gamma} \quad (i = 1, \ldots, n). \tag{6. 14}$$

Let $\boldsymbol{\beta}_i''$ be a vector with rational integral components satisfying

$$\boldsymbol{\beta}_i'' \equiv \boldsymbol{\beta}_i' \bmod p^{n\vartheta-\gamma+1} \quad (i = 1, \ldots, n).$$

Denote by B'' the corresponding matrix. Then we have $\det B'' \equiv \det B' \bmod p^{n\vartheta-\gamma+1}$ and thus by (6. 11)

$$|\det B''|_p = p^{-n\vartheta+\gamma}. \tag{6. 15}$$

Moreover (6. 14) is equivalent to

$$\boldsymbol{\beta}_i''\mathbf{y} \equiv \mathbf{0} \bmod p^{n\vartheta-\gamma} \quad (i = 1, \ldots, n). \tag{6. 16}$$

We may apply Lemma 6. 1 to (6. 16). Let $c_1, \ldots, c_n$ be the invariants of B''. According to Lemma 6. 1 the integral solutions $\mathbf{y}$ of (6. 16) form a sublattice Λ' of $\mathbb{Z}^n$ with

$$\det \Lambda' = \frac{p^{n(n\vartheta-\gamma)}}{(p^{n\vartheta-\gamma}, c_1)\cdots(p^{n\vartheta-\gamma}, c_n)}. \tag{6. 17}$$

But (6. 15) implies $c_1 \cdots c_n = p^{n\vartheta-\gamma}c$ with an integer c which is not divisible by p. Therefore (6. 17) yields

$$\det \Lambda' = p^{(n-1)(n\vartheta-\gamma)}. \tag{6. 18}$$

By (6. 13) the lattice Λ_p consisting of the solutions $\mathbf{x}$ of (6. 7) satisfies

$$\det \Lambda_p = p^{n(\gamma-(n-1)\vartheta)} \det \Lambda',$$

and the assertion of Lemma 6. 2 follows from (6. 18) and (6. 9).

We now assume that $p_1, \ldots, p_s$ are s different primes and that for each j $(1 \leqq j \leqq s)$ we are given n linearly independent vectors $\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)}$ in $\mathbb{Q}_j^n$. We want to study the simultaneous inequalities

$$|\boldsymbol{\beta}_i^{(j)}\mathbf{x}|_j \leqq 1 \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s). \tag{6. 19}$$

For each j $(1 \leqq j \leqq s)$ put $B_j = |\det(\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)})|_j$. Define ϑ_j and γ_j in analogy with (6. 8), (6. 9) by $\max\limits_{1 \leqq i \leqq n} |\boldsymbol{\beta}_i^{(j)}|_j = p_j^{\vartheta_j}$ and

$$B_j = p_j^{\gamma_j} \qquad (1 \leqq j \leqq s). \tag{6. 20}$$

Let $\mathbb{Z}(p_1, \ldots, p_s)$ be the ring of rational numbers $r = \dfrac{u}{v}$ with v being a product of powers of the p_j. Moreover define R as the subring of $\mathbb{Z}(p_1, \ldots, p_s)$ with

$$R = \{r \in \mathbb{Z}(p_1, \ldots, p_s) \mid |r|_j \leqq p_j^{(n-1)\vartheta_j - \gamma_j}\ (1 \leqq j \leqq s)\}. \tag{6. 21}$$

We infer from (6. 12) that the solutions $\mathbf{x}$ of (6. 19) with components in $\mathbb{Z}(p_1, \ldots, p_s)$ lie in R^n.

Lemma 6. 3. *The solutions* $\mathbf{x}$ *with components in* $\mathbb{Z}(p_1, \ldots, p_s)$ *of the system of inequalities* (6. 19) *form a lattice* Λ *with*

$$\det \Lambda = \prod_{j=1}^{s} B_j. \tag{6. 22}$$

Proof. Let j with $1 \leqq j \leqq s$ be fixed. Using Lemma 6. 2 and (6. 21) we see that the set of $\mathbf{x}$ solving (6. 19) for this particular j form a sublattice Λ_j of R^n of index $p_j^{(n-1)(n\vartheta_j-\gamma_j)}$. Now $\Lambda=\Lambda_1\cap\cdots\cap\Lambda_s$, and since $R^n/\Lambda_1\oplus\cdots\oplus R^n/\Lambda_s$ is isomorphic to $R^n/\Lambda_1\cap\cdots\cap\Lambda_s$ we conclude that Λ has index $\prod_{j=1}^{s} p_j^{(n-1)(n\vartheta_j-\gamma_j)}$ in R^n. On the other hand (6. 21) implies that $\det R^n=\prod_{j=1}^{s} p_j^{n(\gamma_j-(n-1)\vartheta_j)}$. Since $\det\Lambda=\operatorname{ind}\Lambda\det R^n$, the assertion follows from (6. 21).

In the remainder of the paper, when we speak about the lattice defined by inequalities (6. 19), we shall always mean the sublattice Λ of R^n defined by (6. 19). So let Λ be defined by (6. 19). Let $\mathbf{h}_1,\ldots,\mathbf{h}_n$ be a basis of Λ. Let $1\leqq k\leqq n$ and $\sigma\in C(n,k)$, where $C(n,k)$ is the set of k-tuples $\{1\leqq i_1<i_2<\cdots<i_k\leqq n\}$. Put $l=\binom{n}{k}$ and for $\sigma=\{i_1<\cdots<i_k\}$ define $\mathbf{H}_\sigma\in\mathbb{R}^l$ by $\mathbf{H}_\sigma=\mathbf{h}_{i_1}\wedge\cdots\wedge\mathbf{h}_{i_k}$. Write $\Lambda^{(k)}$ for the lattice generated by the points $\mathbf{H}_\sigma$ with $\sigma\in C(n,k)$. We call $\Lambda^{(k)}$ the k-th compound of Λ. For the determinant of the k-th compound we know that $\det\Lambda^{(k)}=(\det\Lambda)^{lk/n}$ hence by (6. 22)

$$\det\Lambda^{(k)}=\prod_{j=1}^{s} B_j^{lk/n}. \tag{6. 23}$$

On the other hand we define for j with $1\leqq j\leqq s$ and for $\sigma\in C(n,k)$ $\boldsymbol{\beta}_\sigma^{(j)}$ by

$$\boldsymbol{\beta}_\sigma^{(j)}=\boldsymbol{\beta}_{i_1}^{(j)}\wedge\boldsymbol{\beta}_{i_2}^{(j)}\wedge\cdots\wedge\boldsymbol{\beta}_{i_k}^{(j)}.$$

The inequalities

$$|\boldsymbol{\beta}_\sigma^{(j)}\mathbf{x}^{(k)}|_j\leqq 1,\qquad \sigma\in C(n,k),\ j=1,\ldots,s, \tag{6. 24}$$

where $\mathbf{x}^{(k)}$ stands for a vector in $\mathbb{Q}^l$ define a lattice in $\mathbb{R}^l$. Since

$$\det\left((\boldsymbol{\beta}_\sigma^{(j)})_{\sigma\in C(n,k)}\right)=\det(\boldsymbol{\beta}_1^{(j)},\ldots,\boldsymbol{\beta}_n^{(j)})^{lk/n},$$

and in view of Lemma 6. 3 the determinant of the lattice (6. 24) equals

$$\prod_{j=1}^{s} B_j^{lk/n}. \tag{6. 25}$$

Lemma 6. 4. *The lattice defined by* (6. 24) *is the* k-th *compound of the lattice* Λ *defined in* (6. 19).

Proof. By (6. 23) and (6. 25) the lattice (6. 24) and $\Lambda^{(k)}$ have the same determinant. Thus it suffices to show that the basis vectors $\mathbf{H}_\sigma$ ($\sigma\in C(n,k)$) of $\Lambda^{(k)}$ satisfy (6. 24). Let $\sigma=\{i_1<\cdots<i_k\}$ and $\tau=\{j_1<\cdots<j_k\}$ be in $C(n,k)$. Then

$$|\boldsymbol{\beta}_\sigma^{(j)}\mathbf{H}_\tau|_j = |(\boldsymbol{\beta}_{i_1}^{(j)} \wedge \cdots \wedge \boldsymbol{\beta}_{i_k}^{(j)})\,(\mathbf{h}_{j_1} \wedge \cdots \wedge \mathbf{h}_{j_k})|_j$$

$$= \begin{vmatrix} \boldsymbol{\beta}_{i_1}^{(j)}\mathbf{h}_{j_1} & \boldsymbol{\beta}_{i_1}^{(j)}\mathbf{h}_{j_k} \\ \boldsymbol{\beta}_{i_k}^{(j)}\mathbf{h}_{j_1} & \boldsymbol{\beta}_{i_k}^{(j)}\mathbf{h}_{j_k} \end{vmatrix}_j \leqq \max_\varphi \prod_{\kappa=1}^{k} |\boldsymbol{\beta}_{i_\kappa}^{(j)}\mathbf{h}_{j_{\varphi(\kappa)}}|_j$$

where φ runs through the permutations of $\{1, 2, \ldots, k\}$. Since the vectors $\mathbf{h}_j$ lie in Λ, they satisfy (6. 19) and therefore the last expression is $\leqq 1$. The Lemma follows.

The $(n-1)$-st compound $\Lambda^{(n-1)}$ of Λ is closely related to the polar lattice Λ^* of Λ. Λ^* may be defined as $\Lambda^* = \{\mathbf{x} \mid \forall \mathbf{a} \in \Lambda\ \mathbf{x}\mathbf{a} \in \mathbb{Z}\}$. Let $\mathbf{h}_1^*, \ldots, \mathbf{h}_n^*$ be dual to the basis $\mathbf{h}_1, \ldots, \mathbf{h}_n$ of Λ, i.e. $\mathbf{h}_i\mathbf{h}_j^* = \delta_{ij}$ (= Kronecker's symbol). Then $\mathbf{h}_1^*, \ldots, \mathbf{h}_n^*$ is a basis of Λ^* and consequently we have

$$\det \Lambda^* = (\det \Lambda)^{-1}. \tag{6. 26}$$

Let $\boldsymbol{\beta}_1^{(j)*}, \ldots, \boldsymbol{\beta}_n^{(j)*}$ be dual to $\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)}$, i.e. $\boldsymbol{\beta}_i^{(j)}\boldsymbol{\beta}_k^{(j)*} = \delta_{ik}$. The inequalities

$$|\boldsymbol{\beta}_i^{(j)*}\mathbf{x}|_j \leqq 1 \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s) \tag{6. 27}$$

define a lattice Λ_*.

Lemma 6. 5. *The lattice Λ_* defined by* (6. 27) *is the polar lattice Λ^* of Λ. Moreover we have*

$$(\det \Lambda) \cdot \Lambda^* = \Lambda^{(n-1)}.$$

Proof. We first show the last assertion. Put

$$\hat{\mathbf{h}}_k = \mathbf{h}_1 \wedge \cdots \wedge \mathbf{h}_{k-1} \wedge \mathbf{h}_{k+1} \wedge \cdots \wedge \mathbf{h}_n.$$

Then

$$\mathbf{h}_i\hat{\mathbf{h}}_k = \pm\,\delta_{ik} \det(\mathbf{h}_1, \ldots, \mathbf{h}_n) = \pm\,\delta_{ik} \det \Lambda.$$

Therefore

$$\hat{\mathbf{h}}_k = \pm (\det \Lambda)\mathbf{h}_k^*. \tag{6. 28}$$

Since $\hat{\mathbf{h}}_1, \ldots, \hat{\mathbf{h}}_n$ is a basis of $\Lambda^{(n-1)}$ and $\mathbf{h}_1^*, \ldots, \mathbf{h}_n^*$ is a basis of Λ^*, the last assertion follows.

Define $\hat{\boldsymbol{\beta}}_1^{(j)}, \ldots, \hat{\boldsymbol{\beta}}_n^{(j)}$ in analogy with $\hat{\mathbf{h}}_1, \ldots, \hat{\mathbf{h}}_n$. Then we obtain in a similar way as above

$$\hat{\boldsymbol{\beta}}_i^{(j)} = \pm \det(\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)})\,\boldsymbol{\beta}_i^{(j)*}. \tag{6. 29}$$

We infer from Lemma 6. 4 that

$$|\hat{\boldsymbol{\beta}}_i^{(j)}\hat{\mathbf{h}}_k|_j \leqq 1 \qquad (1 \leqq i \leqq n;\ 1 \leqq k \leqq n;\ 1 \leqq j \leqq s). \tag{6. 30}$$

On the other hand (6. 22) implies that

$$|\det \Lambda|_j = B_j^{-1}. \tag{6. 31}$$

Combining (6. 28)—(6. 31) we conclude that $|\boldsymbol{\beta}_i^{(j)*}\mathbf{h}_k|_j \leqq 1$ $(1 \leqq i \leqq n;\ 1 \leqq k \leqq n;\ 1 \leqq j \leqq s)$. Therefore $\Lambda^* \subset \Lambda_*$.

But $\det \Lambda_* = \prod_{j=1}^{s} B_j^{-1}$ by (6. 27) and Lemma 6. 3. However by (6. 26) and by Lemma 6. 3 the last expression equals $\det \Lambda^*$. Thus $\Lambda_* = \Lambda^*$.

Again let for each j $(1 \leqq j \leqq s)$ $\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)}$ be linearly independent vectors in $\mathbb{Q}_j^n$. Suppose that we are given real numbers c_{ij} $(1 \leqq i \leqq n;\ 1 \leqq j \leqq s)$. Let $Q > 1$. Define the lattice $\Lambda(Q)$ by the inequalities

$$|\boldsymbol{\beta}_i^{(j)}\mathbf{x}|_j \leqq Q^{c_{ij}} \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s). \tag{6. 32}$$

Let f_{ij} be integers with

$$p_j^{-f_{ij}} \leqq Q^{c_{ij}} < p_j^{-f_{ij}+1} \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s). \tag{6. 33}$$

Lemma 6. 6. *The determinant of the lattice $\Lambda(Q)$ defined in* (6. 32) *satisfies*

$$\det \Lambda(Q) \geqq \left(\prod_{j=1}^{s} B_j \right) Q^{-\sum_{j=1}^{s} \sum_{i=1}^{n} c_{ij}}. \tag{6. 34}$$

Proof. Since the absolute value $|\ |_j$ maps $\mathbb{Q}_j^*$ onto the integral powers of p_j, the inequalities (6. 32) are in view of (6. 33) equivalent to

$$|\boldsymbol{\beta}_i^{(j)}\mathbf{x}|_j \leqq p_j^{-f_{ij}} \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s);$$

hence they are equivalent to

$$|p_j^{-f_{ij}}\boldsymbol{\beta}_i^{(j)}\mathbf{x}|_j \leqq 1 \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s). \tag{6. 35}$$

But $|\det(p_j^{-f_{1j}}\boldsymbol{\beta}_1^{(j)}, \ldots, p_j^{-f_{nj}}\boldsymbol{\beta}_n^{(j)})|_j = p_j^{f_{1j}+\cdots+f_{nj}} |\det(\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)})|_j = p_j^{f_{1j}+\cdots+f_{nj}} B_j$.

Therefore we get combining Lemma 6. 3 and (6. 33)

$$\det \Lambda(Q) = \prod_{j=1}^{s} (p_j^{f_{1j}+\cdots+f_{nj}} B_j) \geqq \prod_{j=1}^{s} (B_j Q^{-c_{1j}-\cdots-c_{nj}})$$

as asserted.

Lemma 6. 7. *Suppose that the vectors* $\boldsymbol{\beta}_i^{(j)}$ *are normalized, i.e. that*

$$|\boldsymbol{\beta}_i^{(j)}|_j = 1 \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s).$$

Let $c_{11}, \ldots, c_{n1}, \ldots, c_{1s}, \ldots, c_{ns}$ *be real numbers and let* $\Lambda(Q)$ *be the lattice defined by* (6. 32). *Let* $\Lambda^*(Q)$ *be the lattice which is polar to* $\Lambda(Q)$. *Given* $\mathbf{h} \in \mathbb{Z}^n$, $\mathbf{h} \neq \mathbf{0}$, *define for* $j = 1, \ldots, s$ $\tilde{c}_j = \tilde{c}_j(\mathbf{h})$ *by* $\tilde{c}_j = \max_{1 \leqq i \leqq n} \{c_{ij} | \boldsymbol{\beta}_i^{(j)*} \mathbf{h} \neq 0\}$. *Then there exists a rational number* r *with*

$$0 < r \leqq \prod_{j=1}^{s} (B_j^{-1} Q^{\tilde{c}_j})$$

such that $r\mathbf{h} \in \Lambda^*(Q)$.

Proof. Let the integers f_{ij} be defined by (6. 33). Then $\Lambda(Q)$ may be defined by (6. 35). In view of Lemma 6. 5 $\Lambda^*(Q)$ is given by

$$|p_j^{f_{ij}} \boldsymbol{\beta}_i^{(j)*} \mathbf{x}|_j \leqq 1 \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s). \tag{6. 36}$$

Remember that $B_j = |\det(\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)})|_j$. Since the $\boldsymbol{\beta}_i^{(j)}$ are normalized, we have

$$|\boldsymbol{\beta}_i^{(j)*}|_j \leqq B_j^{-1} \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s).$$

Put

$$f_j = \min_{1 \leqq i \leqq n} \{f_{ij} | \boldsymbol{\beta}_i^{(j)*} \mathbf{h} \neq 0\} \quad \text{and} \quad r = \prod_{j=1}^{s} B_j^{-1} p_j^{-f_j}.$$

Then the point $r\mathbf{h}$ satisfies

$$|p_j^{f_{ij}} \boldsymbol{\beta}_i^{(j)*} r\mathbf{h}|_j \leqq |p_j^{f_{ij}} \boldsymbol{\beta}_i^{(j)*}|_j \, |r\mathbf{h}|_j \leqq p_j^{-f_{ij}} B_j^{-1} B_j p_j^{f_j} \leqq 1$$

for each pair (i, j) $(1 \leqq i \leqq n;\ 1 \leqq j \leqq s)$ such that $\boldsymbol{\beta}_i^{(j)*} \mathbf{h} \neq 0$. But if $\boldsymbol{\beta}_i^{(j)*} \mathbf{h} = 0$ then we have naturally $|p_j^{f_{ij}} \boldsymbol{\beta}_i^{(j)*} r\mathbf{h}|_j \leqq 1$. Thus $r\mathbf{h}$ satisfies (6. 36) and therefore $r\mathbf{h} \in \Lambda^*(Q)$. Our definition of f_j and $\tilde{c}_j$ in conjunction with (6. 33) yields $p_j^{-f_j} \leqq Q^{\tilde{c}_j}$ and the Lemma follows.

Let $f_{11} \geqq 0, \ldots, f_{ns} \geqq 0$ be integers. Define the lattice $\Lambda(\mathbf{f}) = \Lambda(f_{11}, \ldots, f_{ns})$ by

$$|\boldsymbol{\beta}_i^{(j)} \mathbf{x}|_j \leqq p_j^{-f_{ij}} \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s). \tag{6. 37}$$

Lemma 6. 8. *Suppose that for* $j = 1, \ldots, s$ *the vectors* $\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)}$ *are normalized. Then any point* $\mathbf{x} \in \Lambda(\mathbf{f})$, $\mathbf{x} \neq \mathbf{0}$ *has*

$$|\mathbf{x}| \geqq \prod_{j=1}^{s} B_j.$$

Proof. The solutions $\mathbf{x}$ of (6. 37) certainly satisfy

$$|\boldsymbol{\beta}_i^{(j)}\mathbf{x}|_j \leqq 1 \qquad (i=1,\ldots,n;\ j=1,\ldots,s). \tag{6. 38}$$

It was shown in the proof of Lemma 6. 2 in (6. 12) that any $\mathbf{x}$ with (6. 38) and with $\mathbf{x} \in \mathbb{Z}(p_1,\ldots,p_s)^n$ has

$$|\mathbf{x}|_j \leqq (\max_{1\leqq i\leqq n} |\boldsymbol{\beta}_i^{(j)}|_j)^{n-1} B_j^{-1} = B_j^{-1} \qquad (j=1,\ldots,s). \tag{6. 39}$$

But for $\mathbf{x} \in \mathbb{Z}(p_1,\ldots,p_s)^n$, $\mathbf{x} \neq \mathbf{0}$ (6. 39) implies $|\mathbf{x}| \geqq \prod_{j=1}^{s} B_j$.

7. Geometry of numbers

Let $\boldsymbol{\beta}_1^{(0)},\ldots,\boldsymbol{\beta}_n^{(0)}$ be linearly independent vectors in $\mathbb{R}^n$. Suppose that we have

$$|\det(\boldsymbol{\beta}_1^{(0)},\ldots,\boldsymbol{\beta}_n^{(0)})|_0 = B_0.$$

The inequalities

$$|\boldsymbol{\beta}_i^{(0)}\mathbf{x}|_0 \leqq 1 \qquad (i=1,\ldots,n) \tag{7. 1}$$

define a parallelepiped Π of volume $2^n B_0^{-1}$ in $\mathbb{R}^n$. Let Λ be a lattice in $\mathbb{R}^n$ of determinant $\det\Lambda$. Moreover let $\lambda_1,\ldots,\lambda_n$ be the successive minima of Π with respect to Λ, that is λ_j is the least number λ such that there are j linearly independent points of Λ in $\lambda\Pi$. We have according to Minkowski (cf. Cassels [2], Theorem V on p. 218)

$$\frac{1}{n!} B_0 \det\Lambda \leqq \lambda_1 \cdots \lambda_n \leqq B_0 \det\Lambda. \tag{7. 2}$$

Fix linearly independent lattice points $\mathbf{g}_1,\ldots,\mathbf{g}_n$ with

$$\mathbf{g}_j \in \lambda_j \Pi \qquad (j=1,\ldots,n). \tag{7. 3}$$

Then $|\det(\mathbf{g}_1,\ldots,\mathbf{g}_n)| = I \det\Lambda$, where I is the index of the lattice generated by $\mathbf{g}_1,\ldots,\mathbf{g}_n$ in Λ, and we have

$$1 \leqq I \leqq n!. \tag{7. 4}$$

(See Cassels [2], Corollary on p. 219).

Lemma 7. 1 (Davenport's Lemma). *Let $\varrho_1, \ldots, \varrho_n$ be reals with*

$$\varrho_1 \geqq \varrho_2 \geqq \cdots \geqq \varrho_n > 0, \tag{7. 5}$$

$$\varrho_1 \lambda_1 \leqq \varrho_2 \lambda_2 \leqq \cdots \leqq \varrho_n \lambda_n, \tag{7. 6}$$

$$\varrho_1 \cdots \varrho_n = 1. \tag{7. 7}$$

Then there is a permutation of $\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)}$, say $\boldsymbol{\beta}_1^{(0)'}, \ldots, \boldsymbol{\beta}_n^{(0)'}$ such that the parallelepiped Π' defined by

$$|\varrho_i \boldsymbol{\beta}_i^{(0)'} \mathbf{x}|_0 \leqq 1 \qquad (i = 1, \ldots, n)$$

has successive minima $\lambda_1', \ldots, \lambda_n'$ with respect to Λ satisfying

$$2^{-n} \varrho_i \lambda_i \leqq \lambda_i' \leqq 4^{n^2} \varrho_i \lambda_i \qquad (i = 1, \ldots, n). \tag{7. 8}$$

Moreover, every point $\mathbf{x}$ in Λ not in the subspace S_{i-1} spanned by $\mathbf{g}_1, \ldots, \mathbf{g}_{i-1}$, where $\mathbf{g}_1, \ldots, \mathbf{g}_n$ are as in (7. 3), *has*

$$\max \{|\varrho_1 \boldsymbol{\beta}_1^{(0)'} \mathbf{x}|_0, \ldots, |\varrho_n \boldsymbol{\beta}_n^{(0)'} \mathbf{x}|_0\} \geqq 2^{-n} \varrho_i \lambda_i. \tag{7. 9}$$

Proof (cf. Schmidt [14], section IV, Theorem 3A). For $\mathbf{x} \in \mathbb{R}^n$ put

$$N(\mathbf{x}) = \max \{|\boldsymbol{\beta}_1^{(0)} \mathbf{x}|_0, \ldots, |\boldsymbol{\beta}_n^{(0)} \mathbf{x}|_0\}.$$

The points $\mathbf{g}_1, \ldots, \mathbf{g}_n$ satisfy $N(\mathbf{g}_j) = \lambda_j$ $(j = 1, \ldots, n)$ and any point $\mathbf{x} \in \Lambda$, $\mathbf{x} \notin S_{j-1}$ has

$$N(\mathbf{x}) \geqq \lambda_j. \tag{7. 10}$$

If $\mathbf{x}$ lies in S_i, the point $(\boldsymbol{\beta}_1^{(0)} \mathbf{x}, \ldots, \boldsymbol{\beta}_n^{(0)} \mathbf{x})$ satisfies $n - i$ independent linear equations. In particular we have for $\mathbf{x} \in S_{n-1}$

$$a_1 \boldsymbol{\beta}_1^{(0)} \mathbf{x} + \cdots + a_n \boldsymbol{\beta}_n^{(0)} \mathbf{x} = 0 \tag{7. 11}$$

with certain fixed coefficients $a_1, \ldots, a_n$ not all equal to zero. After a suitable permutation we may suppose that

$$|a_n|_0 = \max \{|a_1|_0, \ldots, |a_n|_0\}. \tag{7. 12}$$

But then (7. 11) implies

$$\boldsymbol{\beta}_n^{(0)} \mathbf{x} = -\frac{a_1}{a_n} \boldsymbol{\beta}_1^{(0)} \mathbf{x} - \cdots - \frac{a_{n-1}}{a_n} \boldsymbol{\beta}_{n-1}^{(0)} \mathbf{x} \quad \text{for} \quad \mathbf{x} \in S_{n-1},$$

and using (7. 12) we obtain

$$|\boldsymbol{\beta}_n^{(0)}\mathbf{x}|_0 \leqq |\boldsymbol{\beta}_1^{(0)}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_{n-1}^{(0)}\mathbf{x}|_0$$

which in turn yields

$$|\boldsymbol{\beta}_1^{(0)}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_{n-1}^{(0)}\mathbf{x}|_0 \geqq \frac{1}{2}(|\boldsymbol{\beta}_1^{(0)}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_n^{(0)}\mathbf{x}|_0) \quad \text{for} \quad \mathbf{x} \in S_{n-1}. \tag{7. 13}$$

If $\mathbf{x}$ lies in S_{n-2} it satisfies (7. 11) and moreover a second relation which is independent of (7. 11). In particular this relation may be written as

$$b_1\boldsymbol{\beta}_1^{(0)}\mathbf{x} + \cdots + b_{n-1}\boldsymbol{\beta}_{n-1}^{(0)}\mathbf{x} = 0. \tag{7. 14}$$

Again after a permutation we may suppose that

$$|b_{n-1}|_0 = \max\{|b_1|_0, \ldots, |b_{n-1}|_0\}, \tag{7. 15}$$

which yields similarly as above

$$|\boldsymbol{\beta}_{n-1}^{(0)}\mathbf{x}|_0 \leqq |\boldsymbol{\beta}_1^{(0)}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_{n-2}^{(0)}\mathbf{x}|_0 \quad \text{for} \quad \mathbf{x} \in S_{n-2}$$

and thus by (7. 13)

$$\begin{aligned} |\boldsymbol{\beta}_1^{(0)}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_{n-2}^{(0)}\mathbf{x}|_0 &\geqq \frac{1}{2}(|\boldsymbol{\beta}_1^{(0)}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_{n-1}^{(0)}\mathbf{x}|_0) \\ &\geqq 2^{-2}(|\boldsymbol{\beta}_1^{(0)}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_n^{(0)}\mathbf{x}|_0) \quad \text{for} \quad \mathbf{x} \in S_{n-2}. \end{aligned} \tag{7. 16}$$

Continuing in this way we obtain for any j with $1 \leqq j \leqq n$ inequalities like (7. 13), (7. 16). Conditions (7. 12), (7. 15) etc. finally lead to a permutation $\boldsymbol{\beta}_1^{(0)'}, \ldots, \boldsymbol{\beta}_n^{(0)'}$ of $\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)}$. We get

$$|\boldsymbol{\beta}_1^{(0)'}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_{n-j}^{(0)'}\mathbf{x}|_0 \geqq 2^{-j}(|\boldsymbol{\beta}_1^{(0)'}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_n^{(0)'}\mathbf{x}|_0) \tag{7. 17}$$

for any j $(1 \leqq j \leqq n)$ and for any $\mathbf{x} \in S_{n-j}$.

Now suppose that $\mathbf{x} \in \Lambda \backslash S_{i-1}$. Then there exists j with $1 \leqq j \leqq n$ such that $\mathbf{x} \in S_j$, $\mathbf{x} \notin S_{j-1}$. Since $\mathbf{x} \in S_j$, we infer from (7. 17) and (7. 5)

$$\begin{aligned} \max\{|\varrho_1\boldsymbol{\beta}_1^{(0)'}\mathbf{x}|_0, \ldots, |\varrho_n\boldsymbol{\beta}_n^{(0)'}\mathbf{x}|_0\} &\geqq \max\{|\varrho_1\boldsymbol{\beta}_1^{(0)'}\mathbf{x}|_0, \ldots, |\varrho_j\boldsymbol{\beta}_j^{(0)'}\mathbf{x}|_0\} \\ &\geqq \varrho_j \max\{|\boldsymbol{\beta}_1^{(0)'}\mathbf{x}|_0, \ldots, |\boldsymbol{\beta}_j^{(0)'}\mathbf{x}|_0\} \geqq \frac{\varrho_j}{j}(|\boldsymbol{\beta}_1^{(0)'}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_j^{(0)'}\mathbf{x}|_0) \\ &\geqq \frac{2^{j-n}}{j}\varrho_j(|\boldsymbol{\beta}_1^{(0)'}\mathbf{x}|_0 + \cdots + |\boldsymbol{\beta}_n^{(0)'}\mathbf{x}|_0) \geqq 2^{-n}\varrho_j N(\mathbf{x}). \end{aligned}$$

The definition of j implies that we have $\mathbf{x} \in \Lambda \backslash S_{j-1}$. Thus by (7. 10) we see that $N(\mathbf{x}) \geqq \lambda_j$. Therefore we obtain for any $\mathbf{x} \in \Lambda \backslash S_{i-1}$

$$\max\{|\varrho_1 \boldsymbol{\beta}_1^{(0)'} \mathbf{x}|_0, \ldots, |\varrho_n \boldsymbol{\beta}_n^{(0)'} \mathbf{x}|_0\} \geqq 2^{-n} \varrho_j N(\mathbf{x}) \geqq 2^{-n} \varrho_j \lambda_j \geqq 2^{-n} \varrho_i \lambda_i, \tag{7. 18}$$

the last inequality since $j \geqq i$ and by (7. 6). Notice that (7. 18) is exactly the assertion in (7. 9). Moreover it implies

$$\lambda_i' \geqq 2^{-n} \varrho_i \lambda_i, \tag{7. 19}$$

which is the left hand side of (7. 8).

As for the right hand side of (7. 8), we get using (7. 7)

$$|\det(\varrho_1 \boldsymbol{\beta}_1^{(0)'}, \ldots, \varrho_n \boldsymbol{\beta}_n^{(0)'})|_0 = |\det(\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)})|_0 = B_0.$$

According to (7. 2) we have

$$\frac{1}{n!} B_0 \det \Lambda \leqq \lambda_1 \cdots \lambda_n \leqq B_0 \det \Lambda$$

and

$$\frac{1}{n!} B_0 \det \Lambda \leqq \lambda_1' \cdots \lambda_n' \leqq B_0 \det \Lambda.$$

Thus (7. 19) yields

$$\begin{aligned} \lambda_i' &\leqq \frac{\det \Lambda \cdot B_0}{\lambda_1' \cdots \lambda_{i-1}' \lambda_{i+1}' \cdots \lambda_n'} \leqq \frac{\det \Lambda \cdot B_0}{2^{-n(n-1)} \varrho_1 \lambda_1 \cdots \varrho_{i-1} \lambda_{i-1} \varrho_{i+1} \lambda_{i+1} \cdots \varrho_n \lambda_n} \\ &= 2^{n(n-1)} \varrho_i \frac{\det \Lambda \cdot B_0}{\lambda_1 \cdots \lambda_{i-1} \lambda_{i+1} \cdots \lambda_n} \leqq 2^{n(n-1)} \varrho_i \frac{\det \Lambda \cdot B_0}{(n!)^{-1} B_0 \det \Lambda} \lambda_i \\ &= 2^{n(n-1)} n! \varrho_i \lambda_i < 4^{n^2} \varrho_i \lambda_i, \end{aligned}$$

and (7. 8) follows.

Let $\boldsymbol{\beta}_1^{(0)*}, \ldots, \boldsymbol{\beta}_n^{(0)*}$ be the reciprocal basis with respect to $\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)}$, which means that $\boldsymbol{\beta}_i^{(0)*}$ is the vector with $\boldsymbol{\beta}_i^{(0)*} \boldsymbol{\beta}_k^{(0)} = \delta_{ik}$, the Kronecker symbol $(1 \leqq i, k \leqq n)$. The parallelepiped Π^*

$$|\boldsymbol{\beta}_i^{(0)*} \mathbf{x}|_0 \leqq 1 \qquad (i = 1, \ldots, n) \tag{7. 20}$$

is the reciprocal parallelepiped to the one defined in (7. 1). Denote the successive minima of Π^* with respect to Λ^*, the lattice which is polar to Λ, by $\lambda_1^*, \ldots, \lambda_n^*$.

Again let $\mathbf{g}_1, \ldots, \mathbf{g}_n$ be the points in (7. 3), and let $\mathbf{g}_1^*, \ldots, \mathbf{g}_n^*$ be the reciprocal basis. We put

$$\hat{\mathbf{g}}_k = \frac{1}{\det \Lambda} (\mathbf{g}_1 \wedge \cdots \wedge \mathbf{g}_{k-1} \wedge \mathbf{g}_{k+1} \wedge \cdots \wedge \mathbf{g}_n) \quad (k = 1, \ldots, n). \tag{7. 21}$$

Then we have $\mathbf{g}_i \hat{\mathbf{g}}_k = \pm \delta_{ik} \frac{1}{\det \Lambda} \det(\mathbf{g}_1, \ldots, \mathbf{g}_n) = \pm \delta_{ik} \cdot I \in \mathbb{Z}$, where I is as in (7. 4). Therefore $\hat{\mathbf{g}}_k$ lies in Λ^* and we obtain

$$\hat{\mathbf{g}}_k = \pm I \mathbf{g}_k^* \quad (1 \leqq k \leqq n). \tag{7. 22}$$

Lemma 7. 2 (Mahler [7]). *We have*

$$n^{-1} \leqq \lambda_i^* \lambda_{n+1-i} \leqq (n-1)! \quad (1 \leqq i \leqq n) \tag{7. 23}$$

and

$$|\boldsymbol{\beta}_i^{(0)} \hat{\mathbf{g}}_j|_0 \leqq (n-1)! \lambda_j^{-1} \quad (1 \leqq i, j \leqq n). \tag{7. 24}$$

Proof. Using linearity we get the identity $\sum_{i=1}^{n} (\boldsymbol{\beta}_i^{(0)} \mathbf{x})(\boldsymbol{\beta}_i^{(0)*} \mathbf{y}) = \mathbf{x}\mathbf{y}$. In particular this implies $\sum_{i=1}^{n} (\boldsymbol{\beta}_i^{(0)} \mathbf{g}_k)(\boldsymbol{\beta}_i^{(0)*} \mathbf{g}_j^*) = \mathbf{g}_k \mathbf{g}_j^* = \delta_{kj}$ $(1 \leqq k, j \leqq n)$. It follows that

$$\boldsymbol{\beta}_i^{(0)*} \mathbf{g}_j^* = \frac{A_{ij}}{\det A} \quad (1 \leqq i, j \leqq n),$$

where A is the matrix with entries $\boldsymbol{\beta}_i^{(0)} \mathbf{g}_m$ $(1 \leqq l, m \leqq n)$, and where A_{ij} is the cofactor of $\boldsymbol{\beta}_i^{(0)} \mathbf{g}_j$ in this matrix. It is clear that

$$|\det A|_0 = |\det(\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)})|_0 \, |\det(\mathbf{g}_1, \ldots, \mathbf{g}_n)|_0 = B_0 I \det \Lambda.$$

To estimate A_{ij} we observe that $\mathbf{g}_j \in \lambda_j \Pi \cap \Lambda$ implies that $|\boldsymbol{\beta}_i^{(0)} \mathbf{g}_j|_0 \leqq \lambda_j$, whence

$$|A_{ij}|_0 \leqq (n-1)! \lambda_1 \cdots \lambda_{j-1} \lambda_{j+1} \cdots \lambda_n.$$

Thus we obtain

$$|\boldsymbol{\beta}_i^{(0)*} \mathbf{g}_j^*|_0 \leqq (n-1)! \lambda_1 \cdots \lambda_n \lambda_j^{-1} B_0^{-1} I^{-1} (\det \Lambda)^{-1}$$

and using (7. 2), (7. 22) we infer that

$$|\boldsymbol{\beta}_i^{(0)*} (I \mathbf{g}_j^*)|_0 = |\boldsymbol{\beta}_i^{(0)*} \hat{\mathbf{g}}_j|_0 \leqq (n-1)! \lambda_j^{-1}$$

and (7. 24) is shown. But (7. 24) yields

$$\lambda_{n-j+1}^* \leqq (n-1)! \lambda_j^{-1}.$$

Therefore the right hand inequality in (7. 23) follows.

Put

$$F(\mathbf{x}) = \max_i |\boldsymbol{\beta}_i^{(0)}\mathbf{x}|_0, \quad F^*(\mathbf{x}) = \max_i |\boldsymbol{\beta}_i^{(0)*}\mathbf{x}|_0, \quad \bar{F}(\mathbf{x}) = \sum_{i=1}^{n} |\boldsymbol{\beta}_i^{(0)}\mathbf{x}|_0.$$

Then F and $\bar{F}$ are distance functions which are polar to each other (Cassels [2], VIII. 5). Thus if $\bar{\lambda}_1, \ldots, \bar{\lambda}_n$ are the successive minima of the set of $\mathbf{x}$ with $\bar{F}(\mathbf{x}) \leqq 1$ with respect to the lattice Λ^* we have $\bar{\lambda}_i \lambda_{n+1-i} \geqq 1$ $(i = 1, \ldots, n)$. But $\bar{F}(\mathbf{x}) \leqq nF^*(\mathbf{x})$ and since $\lambda_1^*, \ldots, \lambda_n^*$ are the successive minima of the set of $\mathbf{x}$ with $F^*(\mathbf{x}) \leqq 1$ with respect to Λ^*, we have

$$\bar{\lambda}_i \leqq n\lambda_i^*.$$

This implies the first inequality in (7. 23).

Now suppose that $1 < k \leqq n$ and put $l = \binom{n}{k}$. As in section 6 let $C(n, k)$ be the set of k-tuples $\sigma = \{i_1 < \cdots < i_k\}$ of integers i in $1 \leqq i \leqq n$. $C(n, k)$ has cardinality l. If $\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)}$ are a basis of $\mathbb{R}^n$ with $|\det(\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)})|_0 = B_0$, put

$$\boldsymbol{\beta}_\sigma^{(0)} = \boldsymbol{\beta}_{i_1}^{(0)} \wedge \cdots \wedge \boldsymbol{\beta}_{i_k}^{(0)} \quad (\sigma \in C(n, k)). \tag{7. 25}$$

The vectors $\boldsymbol{\beta}_\sigma^{(0)}$ with $\sigma \in C(n, k)$ are a basis of $\mathbb{R}^l$ and the determinant of this basis is of modulus $B_0^{lk/n}$. The inequalities

$$|\boldsymbol{\beta}_\sigma^{(0)}\mathbf{x}^{(k)}|_0 \leqq 1 \quad (\sigma \in C(n, k)) \tag{7. 26}$$

where $\mathbf{x}^{(k)}$ stands for a vector in $\mathbb{R}^l$ define a parallelepiped $\Pi^{(k)}$ in $\mathbb{R}^l$ of volume $2^l B_0^{-lk/n}$ called the k-th pseudocompound of Π. Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of Π with respect to the lattice Λ, and for $\varrho \in C(n, k)$ put

$$\lambda_\varrho = \prod_{i \in \varrho} \lambda_i.$$

There is an ordering $\varrho_1, \ldots, \varrho_l$ of the elements of $C(n, k)$ such that $\lambda_{\varrho_1} \leqq \cdots \leqq \lambda_{\varrho_l}$. Let $\mathbf{g}_1, \ldots, \mathbf{g}_n$ be independent points with $\mathbf{g}_j \in \lambda_j \Pi \cap \Lambda$ i.e. $\mathbf{g}_j \in \Lambda$ and

$$|\boldsymbol{\beta}_i^{(0)}\mathbf{g}_j|_0 \leqq \lambda_j \quad (1 \leqq i, j \leqq n). \tag{7. 27}$$

Let $v_1, \ldots, v_l$ be the successive minima of the k-th pseudocompound $\Pi^{(k)}$ of Π with respect to the k-th compound $\Lambda^{(k)}$ of the lattice Λ.

Lemma 7. 3 (Mahler [8]). *The successive minima of $\Pi^{(k)}$ with respect to $\Lambda^{(k)}$ have*

$$(l!)^{-1}(k!)^{-(l-1)}\lambda_{\varrho_i} \leqq v_i \leqq k!\,\lambda_{\varrho_i} \quad (i = 1, \ldots, l). \tag{7. 28}$$

Proof. For $\varrho = \{j_1 < \cdots < j_k\} \in C(n, k)$ put $\mathbf{G}_\varrho = \mathbf{g}_{j_1} \wedge \cdots \wedge \mathbf{g}_{j_k}$. Then $\mathbf{G}_\varrho$ lies in $\Lambda^{(k)}$. Using Laplace's identity and (7. 27) we see that

$$|\boldsymbol{\beta}_\sigma^{(0)} \mathbf{G}_\varrho|_0 \leqq k! \lambda_\varrho \qquad (\sigma, \varrho \in C(n, k)) \tag{7. 29}$$

and the right hand side of (7. 28) follows. On the other hand (7. 2) implies

$$((n!)^{-1} B_0 \det \Lambda)^{lk/n} \leqq \lambda_{\varrho_1} \cdots \lambda_{\varrho_l} \leqq (B_0 \det \Lambda)^{lk/n}.$$

The analogue of (7. 2) for $\Pi^{(k)}$ and $\Lambda^{(k)}$ is

$$(l!)^{-1} B_0^{lk/n} (\det \Lambda)^{lk/n} \leqq v_1 \cdots v_l \leqq B_0^{lk/n} (\det \Lambda)^{lk/n}.$$

Thus we obtain

$$(l!)^{-1} \leqq \prod_{i=1}^{l} (v_i / \lambda_{\varrho_i}) \leqq (n!)^{lk/n},$$

and the upper bound in (7. 28) implies the lower bound.

Lemma 7. 4. *Define the points* $\mathbf{G}_\varrho$ *and* $\varrho_1, \ldots, \varrho_l$ *as above. Once the span of* $\mathbf{G}_{\varrho_1}, \ldots, \mathbf{G}_{\varrho_{l-1}}$ *in* $\mathbb{R}^l$ *is determined, the span of* $\mathbf{g}_1, \ldots, \mathbf{g}_{n-k}$ *in* $\mathbb{R}^n$ *is determined.*

This is Lemma 6. 4 of Schmidt [15].

8. Geometry of numbers continued

Again $\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)}$ will be linearly independent vectors in $\mathbb{R}^n$ with determinant of modulus B_0. Moreover for the s primes $p_1, \ldots, p_s$ we consider linearly independent vectors $\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)}$ in $\mathbb{Q}_j^n$ with $|\det(\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)})|_j = B_j$ $(1 \leqq j \leqq s)$. We will make the additional assumption that for all j $(0 \leqq j \leqq s)$ $\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)}$ are normalized, i.e. that

$$|\boldsymbol{\beta}_1^{(j)}|_j = \cdots = |\boldsymbol{\beta}_n^{(j)}|_j = 1.$$

Throughout $c_{1j}, \ldots, c_{nj}$ $(j = 0, \ldots, s)$ will be reals with $|c_{ij}| \leqq 1$ $(1 \leqq i \leqq n;\ 0 \leqq j \leqq s)$ and with

$$\sum_{j=0}^{s} \sum_{i=1}^{n} c_{ij} = 0. \tag{8. 1}$$

Given $Q > 0$ let $\Pi = \Pi(Q)$ be the parallelepiped

$$|\boldsymbol{\beta}_i^{(0)} \mathbf{x}|_0 \leqq Q^{c_{i0}} \qquad (i = 1,, \ldots, n) \tag{8. 2}$$

and $\Lambda = \Lambda(Q)$ be the lattice

$$|\boldsymbol{\beta}_i^{(j)} \mathbf{x}|_j \leqq Q^{c_{ij}} \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s). \tag{8. 3}$$

The inequalities (8. 2) are equivalent with $|\boldsymbol{\beta}_i^{(0)\prime}\mathbf{x}|_0 \leqq 1$, where $\boldsymbol{\beta}_i^{(0)\prime} = Q^{-c_{i0}}\boldsymbol{\beta}_i^{(0)}$. Therefore and in view of the last part of section 6 the theory developed in section 7 applies.

We define minima $\lambda = \lambda(Q)$ of $\Pi(Q)$ with respect to $\Lambda(Q)$. Again we have points $\mathbf{g}_1 = \mathbf{g}_1(Q), \ldots, \mathbf{g}_n = \mathbf{g}_n(Q)$ with (7. 3). The reciprocal parallelepiped $\Pi^* = \Pi^*(Q)$ is given by

$$|\boldsymbol{\beta}_i^{(0)*}\mathbf{x}|_0 \leqq Q^{-c_{i0}}.$$

We have seen in (7. 22) that the point

$$\hat{\mathbf{g}}_n = (\det \Lambda)^{-1}\,(\mathbf{g}_1 \wedge \cdots \wedge \mathbf{g}_{n-1})$$

lies in Λ^* and that we have $\hat{\mathbf{g}}_n = \pm I\mathbf{g}_n^*$ where I is the index of the lattice generated by $\mathbf{g}_1, \ldots, \mathbf{g}_n$ in Λ. Since by definition (cf. section 6) Λ is a subset of $\mathbb{Z}(p_1, \ldots, p_s)^n$ it is clear that the point $G\hat{\mathbf{g}}_n$ with

$$G = \prod_{j=1}^{s} |\hat{\mathbf{g}}_n|_j \tag{8. 4}$$

lies in $\mathbb{Z}^n$.

Lemma 8. 1. *The point $G\hat{\mathbf{g}}_n$ with G defined by* (8. 4) *has*

$$|G\hat{\mathbf{g}}_n|_0 \leqq n!\left(\prod_{j=0}^{s} B_j^{-1}\right)\lambda_1 \cdots \lambda_{n-1} Q^{s+1}. \tag{8. 5}$$

Proof. For each j $(0 \leqq j \leqq s)$ write $\hat{\boldsymbol{\beta}}_i^{(j)} = \boldsymbol{\beta}_1^{(j)} \wedge \cdots \wedge \boldsymbol{\beta}_{i-1}^{(j)} \wedge \boldsymbol{\beta}_{i+1}^{(j)} \wedge \cdots \wedge \boldsymbol{\beta}_n^{(j)}$ so that we obtain in analogy with (7. 21) and (7. 22)

$$\hat{\boldsymbol{\beta}}_i^{(j)} = \pm \det(\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)})\,\boldsymbol{\beta}_i^{(j)*} \qquad (i = 1, \ldots, n;\ j = 0, \ldots, s).$$

By Laplace's identity we have

$$|\hat{\boldsymbol{\beta}}_i^{(0)}\hat{\mathbf{g}}_n|_0 \leqq \det \Lambda)^{-1}\,(n-1)!\,\lambda_1 \cdots \lambda_{n-1} Q^{c_{10}+\cdots+c_{i-1,0}+c_{i+1,0}+\cdots+c_{n0}} \tag{8. 6}$$

and therefore

(8. 7)

$$|\boldsymbol{\beta}_i^{(0)*}\hat{\mathbf{g}}_n|_0 \leqq B_0^{-1}(\det \Lambda)^{-1}\,(n-1)!\,\lambda_1 \cdots \lambda_{n-1} Q^{c_{10}+\cdots+c_{i-1,0}+c_{i+1,0}+\cdots+c_{n0}} \qquad (i = 1, \ldots, n).$$

If we write $\hat{\mathbf{g}}_n$ as $\hat{\mathbf{g}}_n = u_1^{(0)}\boldsymbol{\beta}_1^{(0)} + \cdots + u_n^{(0)}\boldsymbol{\beta}_n^{(0)}$, this says that

$$|u_i^{(0)}|_0 \leqq B_0^{-1}(\det \Lambda)^{-1}\,(n-1)!\,\lambda_1 \cdots \lambda_{n-1} Q^{c_{10}+\cdots+c_{i-1,0}+c_{i+1,0}+\cdots+c_{n0}}$$

and since the $\boldsymbol{\beta}_i^{(0)}$ are normalized we get

$$|\hat{\mathbf{g}}_n|_0 \leqq n!\,B_0^{-1}(\det \Lambda)^{-1}\,\lambda_1 \cdots \lambda_{n-1} Q^{\max_i (c_{10}+\cdots+c_{i-1,0}+c_{i+1,0}+\cdots+c_{n0})}. \tag{8. 8}$$

Similarly we obtain for j with $1 \leqq j \leqq s$

$$|\hat{\boldsymbol{\beta}}_i^{(j)} \hat{\mathbf{g}}_n|_j \leqq |\det \Lambda|_j^{-1} Q^{c_{1j}+\cdots+c_{i-1,j}+c_{i+1,j}+\cdots+c_{nj}} \quad (1 \leqq i \leqq n) \tag{8. 9}$$

hence

$$|\boldsymbol{\beta}_i^{(j)*} \hat{\mathbf{g}}_n|_j \leqq B_j^{-1} |\det \Lambda|_j^{-1} Q^{c_{1j}+\cdots+c_{i-1,j}+c_{i+1,j}+\cdots+c_{nj}} \quad (1 \leqq i \leqq n). \tag{8. 10}$$

Finally writing $\hat{\mathbf{g}}_n$ as $u_1^{(j)} \boldsymbol{\beta}_1^{(j)} + \cdots + u_n^{(j)} \boldsymbol{\beta}_n^{(j)}$ we infer from (8. 10) that

$$|\hat{\mathbf{g}}_n|_j \leqq B_j^{-1} |\det \Lambda|_j^{-1} Q^{\max_i (c_{1j}+\cdots+c_{i-1,j}+c_{i+1,j}+\cdots+c_{nj})}. \tag{8. 11}$$

Notice that $\prod_{j=0}^{s} |\det \Lambda|_j = 1$. Moreover (8. 1) implies

$$\sum_{j=0}^{s} \max_i (c_{1j} + \cdots + c_{i-1,j} + c_{i+1,j} + \cdots + c_{nj}) \leqq s+1.$$

Combining this with (8. 8) and (8. 11) we get

$$|G\hat{\mathbf{g}}_n|_0 \leqq n! \left(\prod_{j=0}^{s} B_j^{-1} \right) \lambda_1 \cdots \lambda_{n-1} Q^{s+1}.$$

We now apply Lemma 5. 2 to (8. 5). If $\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)}$ are independent and normalized and if they are defined over K, we have

$$1 \geqq B_j = |\det(\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)})|_j \geqq (H(\boldsymbol{\beta}_1^{(j)}) \cdots H(\boldsymbol{\beta}_n^{(j)}))^{-d} \quad (j = 0, \ldots, s). \tag{8. 12}$$

Therefore if H is a quantity satisfying (4. 5), then

$$|G\hat{\mathbf{g}}_n|_0 \leqq n!\, \lambda_1 \cdots \lambda_{n-1} H^{n(s+1)d} Q^{s+1}. \tag{8. 13}$$

Lemma 8. 2. *Let $\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)}; \ldots; \boldsymbol{\beta}_1^{(s)}, \ldots, \boldsymbol{\beta}_n^{(s)}$ be $s+1$ sets of linearly independent vectors such that $\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)}$ are normalized with respect to $|\ |_j$ $(0 \leqq j \leqq s)$ and defined over K. Let $\Pi(Q)$ and $\Lambda(Q)$ be given by* (8. 2), (8. 3) *and let $\mathbf{g}_1, \ldots, \mathbf{g}_n$ as well as $\hat{\mathbf{g}}_n$ be as above. Suppose G is defined as in* (8. 4). *Then for each $(s+1)$-tuple of subscripts $(i_0, i_1, \ldots, i_s)$ with*

$$\prod_{j=0}^{s} |\boldsymbol{\beta}_{i_j}^{(j)*} \hat{\mathbf{g}}_n|_j \neq 0 \tag{8. 14}$$

we have

$$|G\hat{\mathbf{g}}_n|_0 > (n!)^{-1} H^{-n} ((\lambda_1 \cdots \lambda_{n-1})^{-1} Q^{c_{i_0 0}+c_{i_1 1}+\cdots+c_{i_s s}})^{\frac{1}{d(s+1)}}. \tag{8. 15}$$

Proof. Let $(i_0, \dots, i_s)$ be an $(s+1)$-tuple for which (8. 14) holds true. We apply Lemma 5. 4 with $\gamma^{(j)} = \hat{\mathfrak{B}}_{i_j}^{(j)} = \mathfrak{B}_1^{(j)} \wedge \cdots \wedge \mathfrak{B}_{i_j-1}^{(j)} \wedge \mathfrak{B}_{i_j+1}^{(j)} \wedge \cdots \wedge \mathfrak{B}_n^{(j)}$. Since the $\mathfrak{B}_i^{(j)}$ are normalized, (5. 9) says that

$$\prod_{j=0}^{s} |\hat{\mathfrak{B}}_{i_j}^{(j)} \hat{\mathfrak{g}}_n|_j \geqq \prod_{j=0}^{s} (H(\mathfrak{B}_1^{(j)}) \cdots H(\mathfrak{B}_{i_j-1}^{(j)}) H(\mathfrak{B}_{i_j+1}^{(j)}) \cdots H(\mathfrak{B}_n^{(j)}))^{-d} |\hat{\mathfrak{g}}_n|_j^{-d(s+1)+1}. \tag{8. 16}$$

On the other hand we have (8. 6) and (8. 9). Together with (8. 1) they imply

$$\prod_{j=0}^{s} |\hat{\mathfrak{B}}_{i_j}^{(j)} \hat{\mathfrak{g}}_n|_j \leqq (n-1)!\, \lambda_1 \cdots \lambda_{n-1} Q^{-c_{i_0 0} - c_{i_1 1} - \cdots + c_{i_s s}}. \tag{8. 17}$$

Combination of (8. 16) and (8. 17) yields

$$\begin{aligned} \prod_{j=0}^{s} |\hat{\mathfrak{g}}_n|_j^{d(s+1)} &\geqq \prod_{j=0}^{s} |\hat{\mathfrak{g}}_n|_j^{d(s+1)-1} \\ &\geqq (n!) H^{-nd(s+1)} (\lambda_1 \cdots \lambda_{n-1})^{-1} Q^{c_{i_0 0} + c_{i_1 1} + \cdots + c_{i_s s}}. \end{aligned} \tag{8. 18}$$

Remember the definition of G in (8. 4). Thus (8. 15) follows from (8. 18).

There is a linear form $V = V(\mathbf{X}) = v_1 X_1 + \cdots + v_n X_n$ with coprime integral coefficients vanishing on $\mathfrak{g}_1, \dots, \mathfrak{g}_n$. This form is unique up to a factor ± 1. Write

$$\lceil V \rceil = \max(|v_1|_0, \dots, |v_n|_0) = \lceil \mathbf{v} \rceil.$$

We also write

$$q = n - 1 \tag{8. 19}$$

and we denote by $\mathfrak{S}$ the set of $(s+1)$-tuples of subscripts $(i_0, i_1, \dots, i_s)$ with

$$c_{i_0 0} + c_{i_1 1} + \cdots + c_{i_s s} > 0.$$

Lemma 8. 3. *Suppose* $\delta > 0$,

$$\lambda_q = \lambda_q(Q) \leqq Q^{-\delta} \tag{8. 20}$$

and

$$Q^{q\delta} > (n!)^{6d(s+1)} H^{2nd(s+1)}. \tag{8. 21}$$

Suppose there is an $(i_0, i_1, \dots, i_s) \in \mathfrak{S}$ *with* $\prod_{j=0}^{s} |\mathfrak{B}_{i_j}^{(j)*} \hat{\mathfrak{g}}_n|_j \neq 0$, *i.e. with* (8. 14). *Then*

$$Q^{\frac{q\delta}{2d(s+1)}} < \lceil V \rceil < Q^{s+1}. \tag{8. 22}$$

Proof. Clearly $\hat{\mathbf{g}}_n$ is a multiple of the coefficient vector $\mathbf{v}$ of V. Now $G\hat{\mathbf{g}}_n$ with G as in (8. 4) is an integral vector. Thus there is an integer m such that $G\hat{\mathbf{g}}_n = m\mathbf{v}$.

It follows moreover from (8. 4) that the greatest common divisor of the components of $G\hat{\mathbf{g}}_n$ is not divisible by any of $p_1, \dots, p_s$. On the other hand by (7. 22) we have $|\mathbf{g}_n \hat{\mathbf{g}}_n| = I$, the index of the lattice generated by $\mathbf{g}_1, \dots, \mathbf{g}_n$ in Λ. Therefore, in view of (7. 4) we may infer that the g.c.d. of the components of $G\hat{\mathbf{g}}_n$ is $\leqq n!$, so that $1 \leqq m \leqq n!$. Now (8. 13), (8. 20) yield

$$\overline{|V|} = \overline{|\mathbf{v}|} \leqq |G\hat{\mathbf{g}}_n|_0 \leqq n!\, H^{n(s+1)d} Q^{-q\delta} Q^{s+1}$$

and the right hand side of (8. 22) follows from (8. 21).

As for an estimate in the opposite direction, Lemma 8. 2 with

$$c_{i_0 0} + c_{i_1 1} + \cdots + c_{i_s s} > 0$$

implies

$$\overline{|V|} = \overline{|\mathbf{v}|} \geqq \frac{1}{n} |\mathbf{v}|_0 \geqq (n!)^{-2} |G\hat{\mathbf{g}}_n|_0 > (n!)^{-3} H^{-n} Q^{\frac{q\delta}{d(s+1)}} > Q^{\frac{q\delta}{2d(s+1)}}$$

by (8. 21) and this is the left hand side of (8. 22).

Lemma 8. 4. *Again let $\Pi = \Pi(Q)$ be the parallelepiped* (8. 2), *where $\boldsymbol{\beta}_1^{(0)}, \dots, \boldsymbol{\beta}_n^{(0)}$ in $\mathbb{R}^n$ are normalized and have $|\det(\boldsymbol{\beta}_1^{(0)}, \dots, \boldsymbol{\beta}_n^{(0)})|_0 = B_0$. Moreover let $\Lambda = \Lambda(Q)$ be the lattice* (8. 3), *where for each j $(1 \leqq j \leqq s)$ $\boldsymbol{\beta}_1^{(j)}, \dots, \boldsymbol{\beta}_n^{(j)}$ in $\mathbb{Q}_j^n$ are normalized and have*

$$|\det(\boldsymbol{\beta}_1^{(j)}, \dots, \boldsymbol{\beta}_n^{(j)})|_j = B_j.$$

Suppose that

$$n! \left(\prod_{j=0}^{s} B_j^{-1} \right) \lambda_q^n < 1 \tag{8. 23}$$

and that there is an integral point $\mathbf{h} \neq \mathbf{0}$ with

$$\prod_{j=0}^{s} |\boldsymbol{\beta}_{i_j}^{(j)*} \mathbf{h}|_j = 0 \quad \textit{for every} \quad (i_0, \dots, i_s) \quad \textit{with} \tag{8. 24}$$

$$n \left(\prod_{j=0}^{s} B_j^{-1} Q^{c_{ij}} \right) |\mathbf{h}|_0 \lambda_q \geqq 1.$$

Then

$$\mathbf{g}_i \mathbf{h} = 0 \quad \text{for} \quad i = 1, 2, \dots, q. \tag{8. 25}$$

Proof. For $j=1, \ldots, s$ we define sets $C_j \subset \{1, \ldots, n\}$ as

$$C_j = \{i \mid \boldsymbol{\beta}_i^{(j)*} \mathbf{h} \neq 0\}.$$

Since $\boldsymbol{\beta}_1^{(j)*}, \ldots, \boldsymbol{\beta}_n^{(j)*}$ are linearly independent, we have $C_j \neq \emptyset$. Let

$$\tilde{c}_j = \max_{i \in C_j} c_{ij}$$

and suppose $i(j) \in C_j$ is a subscript with $c_{i(j),j} = \tilde{c}_j$. By Lemma 6. 7 there exists a rational number $r \neq 0$ having

$$0 < r \leqq \prod_{j=1}^{s} (B_j^{-1} Q^{\tilde{c}_j}) \tag{8. 26}$$

such that $r\mathbf{h} = \tilde{\mathbf{h}}$, say, lies in Λ^*.

Now the inequality (7. 23) holds true for the pair Π, Λ and the reciprocal pair Π^*, Λ^*. In particular for i with

$$n \left(\prod_{j=0}^{s} B_j^{-1} \right) |\mathbf{h}|_0 \lambda_q Q^{c_{i0} + \tilde{c}_1 + \cdots + \tilde{c}_s} < 1$$

we infer

$$\lambda_2^* \geqq n^{-1} \lambda_{n-1}^{-1} = n^{-1} \lambda_q^{-1} \geqq |\mathbf{h}|_0 \left(\prod_{j=0}^{s} B_j^{-1} \right) Q^{c_{i0} + \tilde{c}_1 + \cdots + \tilde{c}_s}.$$

Since $\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)}$ are normalized, we have $|\boldsymbol{\beta}_i^{(0)*}|_0 \leqq B_0^{-1}$ and thus we obtain by (8. 26)

$$|\boldsymbol{\beta}_i^{(0)*} \tilde{\mathbf{h}}|_0 \leqq B_0^{-1} |r|_0 \, |\mathbf{h}|_0 \leqq B_0^{-1} \left(\prod_{j=0}^{s} B_j^{-1} Q^{\tilde{c}_j} \right) |\mathbf{h}|_0 < \lambda_2^* Q^{-c_{i0}} \tag{8. 27}$$

for such i.

If however i is a subscript with $n \left(\prod_{j=0}^{s} B_j^{-1} \right) |\mathbf{h}|_0 Q^{c_{i0} + \tilde{c}_1 + \cdots + \tilde{c}_s} \geqq 1$, then by (8. 24) we get

$$|\boldsymbol{\beta}_i^{(0)*} \mathbf{h}|_0 \prod_{j=1}^{s} |\boldsymbol{\beta}_{i(j)}^{(j)*} \mathbf{h}|_j = 0.$$

However the definition of the sets C_j says that

$$\prod_{j=1}^{s} |\boldsymbol{\beta}_{i(j)}^{(j)*} \mathbf{h}|_j \neq 0.$$

Thus (8. 24) even implies $|\boldsymbol{\beta}_i^{(0)*} \mathbf{h}|_0 = 0$ and therefore also

$$|\boldsymbol{\beta}_i^{(0)*} \tilde{\mathbf{h}}|_0 = 0. \tag{8. 28}$$

Combining (8. 27) and (8. 28) we see that the point $\tilde{\mathbf{h}} \neq \mathbf{0}$ lies in Λ^* as well as in the interior of $\lambda_2^* \Pi^*$.

On the other hand using $1 \leqq n \lambda_2^* \lambda_{n-1}$ and (8. 7), we obtain for the point $\hat{\mathbf{g}}_n \in \Lambda^*$ in (7. 21)

$$|\boldsymbol{\beta}_i^{(0)*} \hat{\mathbf{g}}_n|_0 \leqq n! \, B_0^{-1} (\det \Lambda)^{-1} \lambda_1 \cdots \lambda_{n-2} \lambda_{n-1}^2 \lambda_2^* Q^{c_{10}+\cdots+c_{i-1,0}+c_{i+1,0}+\cdots+c_{n0}}.$$

We infer from Lemma 6. 6 and (8. 1) that

$$(\det \Lambda)^{-1} Q^{c_{10}+\cdots+c_{i-1,0}+c_{i+1,0}+\cdots+c_{n0}} \leqq Q^{-c_{i0}} \prod_{j=1}^{s} B_j^{-1}.$$

Thus by (8. 23) we get

$$|\boldsymbol{\beta}_i^{(0)*} \hat{\mathbf{g}}_n|_0 \leqq n! \left(\prod_{j=0}^{s} B_j^{-1} \right) \lambda_q^n \lambda_2^* Q^{-c_{i0}} < \lambda_2^* Q^{-c_{i0}} \qquad (i = 1, \ldots, n).$$

Hence $\hat{\mathbf{g}}_n$ also lies in the interior of $\lambda_2^* \Pi^*$. Since any two nonzero points of the lattice Λ^* lying in the interior of $\lambda_2^* \Pi^*$ are proportional, it follows that $\tilde{\mathbf{h}}$ and $\hat{\mathbf{g}}_n$ and therefore also $\mathbf{h}$ and $\hat{\mathbf{g}}_n$ are proportional. As $\hat{\mathbf{g}}_n$ is orthogonal to $\mathbf{g}_1, \ldots, \mathbf{g}_{n-1}$, the same holds true for $\mathbf{h}$ and (8. 25) follows.

Lemma 8. 5. *Let* $\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)}, \ldots, \boldsymbol{\beta}_1^{(s)}, \ldots, \boldsymbol{\beta}_n^{(s)}$ *be as in the preceding Lemma. In addition suppose that they are defined over K. Assume that there is an integral point* $\mathbf{h} \neq \mathbf{0}$ *with*

$$\prod_{j=0}^{s} |\boldsymbol{\beta}_{i_j}^{(j)*} \mathbf{h}|_j = 0 \quad \textit{for every} \quad (i_0, i_1, \ldots, i_s) \in \mathfrak{S}. \tag{8. 29}$$

In fact, let $\mathbf{h}$ *be a point with this property having smallest possible norm* $|\mathbf{h}|_0$. *Suppose that* (8. 20) *holds, i.e. that* $\lambda_q \leqq Q^{-\delta}$ *with* $\delta > 0$ *and that*

$$Q^{\delta} > n! \, H^{n(d(s+1)+n-1)}. \tag{8. 30}$$

Then (8. 25) *holds true, i.e.* $\mathbf{g}_1 \mathbf{h} = \cdots = \mathbf{g}_q \mathbf{h} = 0$.

Proof. It suffices to check the conditions (8. 23), (8. 24) of Lemma 8. 4. As for (8. 23) we obtain with (8. 12)

$$n! \left(\prod_{j=0}^{s} B_j^{-1} \right) \lambda_q^n < n! \, H^{nd(s+1)} Q^{-\delta}$$

and by (8. 30) this is < 1.

Now if there is an integral point $\mathbf{h} \neq \mathbf{0}$ with (8. 29), we may apply Lemma 5. 6 to a maximal linearly independent subset of the set of vectors $\boldsymbol{\beta}_{i_j}^{(j)}$ where i_j runs through the projection of $\mathfrak{S}$ onto the j-th coordinate and where j runs through $\{0, \ldots, s\}$. By Lemma 5. 6 we find an $\mathbf{h}$ with

$$|\mathbf{h}|_0 \leqq \max H(\boldsymbol{\beta}_{i_j}^{(j)*})^{n-1} = \max H(\hat{\boldsymbol{\beta}}_{i_j}^{(j)})^{n-1},$$

where the maximum is over j with $0 \leqq j \leqq s$ and over all possible values of i_j. This maximum is $\leqq \max_{i,j} H(\hat{\boldsymbol{\beta}}_i^{(j)})^{n-1}$. Finally, using Lemma 5. 1 we see that a minimal $\mathbf{h}$ satisfies

$$|\mathbf{h}|_0 \leqq H^{n^2-n}.$$

Therefore, if $(i_0, i_1, \ldots, i_s)$ is such that

$$n\left(\prod_{j=0}^{s} B_j^{-1}\right)|\mathbf{h}|_0 \lambda_q Q^{c_{i_0 0}+c_{i_1 1}+\cdots+c_{i_s s}} \geqq 1$$

then

$$n H^{n(d(s+1)+n-1)} Q^{-\delta} Q^{c_{i_0 0}+c_{i_1 1}+\cdots+c_{i_s s}} \geqq 1,$$

so that $Q^{c_{i_0 0}+c_{i_1 1}+\cdots+c_{i_s s}} > 1$ by (8. 30). We may conclude that $(i_0, i_1, \ldots, i_s) \in \mathfrak{S}$ and hence that we have (8. 29).

Thus (8. 24) is satisfied as well.

Lemma 8. 6. *Again let for $j = 0, \ldots, s$ the vectors $\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)}$ be normalized, independent, and defined over K. Let $\Pi(Q)$ and $\Lambda(Q)$ be given by* (8. 2) *and* (8. 3) *respectively, and let $S(Q)$ be the subspace spanned by $\mathbf{g}_1, \ldots, \mathbf{g}_q$. Suppose that*

$$0 < \delta < 1.$$

Then the values of Q with $\lambda_q = \lambda_q(Q) \leqq Q^{-\delta}$, and lying in an interval

(8. 31) $$Q_0 < Q \leqq Q_0^E,$$

where $E > 1$ and

(8. 32) $$Q_0^{n\delta/2} > n!\, H^{nd(s+1)}$$

give rise to not more than

$$1 + 4(s+1)\delta^{-1} \log E$$

distinct subspaces $S(Q)$.

Proof. The argument is similar to the one used in section 3. Consider an interval of the type

$$Q_0 < Q \leqq Q_0^{1+\frac{\delta}{2(s+1)}} \tag{8. 33}$$

with (8. 32). Let $Q_1, \ldots, Q_n$ be any values of Q in (8. 33) with $\lambda_q(Q) \leqq Q^{-\delta}$. For $1 \leqq k \leqq n$ let $\mathbf{h}_k$ be one of the points $\mathbf{g}_1(Q_k), \ldots, \mathbf{g}_q(Q_k)$. Then

$$|\boldsymbol{\beta}_i^{(0)} \mathbf{h}_k|_0 \leqq \lambda_q(Q_k) Q_k^{c_{i0}} \leqq Q_k^{c_{i0}-\delta} \qquad (i \leqq i,\ k \leqq n)$$

and

$$|\boldsymbol{\beta}_i^{(j)} \mathbf{h}_k|_j \leqq Q_k^{c_{ij}} \qquad (1 \leqq i,\ k \leqq n;\ 1 \leqq j \leqq s).$$

We have

$$\prod_{j=0}^{s} |\det(\mathbf{h}_1, \ldots, \mathbf{h}_n)|_j = \prod_{j=0}^{s} (B_j^{-1} |\det(\boldsymbol{\beta}_i^{(j)} \mathbf{h}_k)|_j)$$

$$\leqq n! \left(\prod_{j=0}^{s} B_j^{-1} \right) \max_{k_1, \ldots, k_n} (Q_{k_1}^{c_{10}-\delta} \cdots Q_{k_n}^{c_{n0}-\delta}) \prod_{j=1}^{s} \max_{k_1, \ldots, k_n} (Q_{k_1}^{c_{1j}} \cdots Q_{k_n}^{c_{nj}}),$$

where the maximum is over permutations $k_1, \ldots, k_n$ of $1, \ldots, n$. Now for $c < 0$ we have

$$Q_k^c \leqq Q_0^c \qquad (1 \leqq k \leqq n),$$

whereas for $c \geqq 0$ we have

$$Q_k^c \leqq Q_0^{c\left(1+\frac{\delta}{2(s+1)}\right)} \qquad (1 \leqq k \leqq n).$$

We thus obtain using (8. 1)

$$\prod_{j=0}^{s} |\det(\mathbf{h}_1, \ldots, \mathbf{h}_n)|_j \leqq n! \left(\prod_{j=0}^{s} B_j^{-1} \right) Q_0^{-n\delta + \frac{\delta}{2(s+1)}(\Sigma_0 + \Sigma_1)},$$

where $\sum_0$ is the sum of $c_{i0} - \delta$ over i with $c_{i0} - \delta \geqq 0$ and $\sum_1$ is the sum of c_{ij} over i and j $(1 \leqq j \leqq s)$ with $c_{ij} \geqq 0$, so that $\sum_0 + \sum_1 < n(s+1)$. Thus

$$\prod_{j=0}^{s} |\det(\mathbf{h}_1, \ldots, \mathbf{h}_n)|_j \leqq n! \left(\prod_{j=0}^{s} B_j^{-1} \right) Q_0^{-n\delta/2} \leqq n!\, H^{nd(s+1)} Q_0^{-n\delta/2} < 1$$

by (8. 32). Since the $\mathbf{h}_k$ have components in $\mathbb{Z}(p_1, \ldots, p_s)$, we see that

$$\prod_{j=0}^{s} |\det(\mathbf{h}_1, \ldots, \mathbf{h}_n)|_j$$

is an integer.

We may conclude that $\det(\mathbf{h}_1, \ldots, \mathbf{h}_n) = 0$, so that $\mathbf{h}_1, \ldots, \mathbf{h}_n$ are linearly dependent. In fact, any vectors $\mathbf{h}_1, \ldots, \mathbf{h}_n$ with $\mathbf{h}_i \in S(Q_i)$ are linearly dependent. Therefore $S(Q_1) = \cdots = S(Q_n)$, and for Q in (8. 33) with (8. 20), the subspace $S(Q)$ is always the same.

The given interval (8. 31) is contained in the union of not more than

$$1 + \frac{\log E}{\log\left(1 + \dfrac{\delta}{2(s+1)}\right)} < 1 + 4(s+1)\delta^{-1} \log E$$

intervals of the type (8. 33).

9. The index

We denote the ring of polynomials

$$P = P(X_{11}, \ldots, X_{1n}; \ldots; X_{m1}, \ldots, X_{mn})$$

in nm variables and with rational integral coefficients by $\mathscr{R}$. Given an m-tuple

$$\mathbf{r} = (r_1, \ldots, r_m)$$

of natural numbers, $\mathscr{R}'$ will denote the set of polynomials in $\mathscr{R}$ which are homogeneous of degree r_h in the block of variables $X_{h1}, \ldots, X_{hn}$ $(1 \leqq h \leqq m)$. The symbol $\mathscr{I}$ will denote nm-tuples of nonnegative integers

$$\mathscr{I} = (i_{11}, \ldots, i_{1n}; \ldots; i_{m1}, \ldots, i_{mn}),$$

and we will use the notation

$$(\mathscr{I}/r) = \sum_{h=1}^{m} \frac{i_{h_1} + \cdots + i_{h_n}}{r_h}.$$

We put

$$P^{\mathscr{I}} = \frac{1}{i_{11}! \cdots i_{mn}!} \frac{\partial^{i_{11} + \cdots + i_{mn}}}{\partial X_{11}^{i_{11}} \cdots \partial X_{mn}^{i_{mn}}} P.$$

If P lies in $\mathscr{R}$ then also $P^{\mathscr{I}}$ lies in $\mathscr{R}$. With $\lceil\,\rceil_j$ denoting the maximum modulus with respect to $|\ |_j$ of the coefficients of a polynomial $(0 \leqq j \leqq s)$, we have for $P \in \mathscr{R}'$

$$\lceil P^{\mathscr{I}} \rceil_0 \leqq 2^r \lceil P \rceil_0 \quad \text{and} \quad \lceil P^{\mathscr{I}} \rceil_j \leqq \lceil P \rceil_j \quad (1 \leqq j \leqq s) \tag{9. 1}$$

where

$$r = r_1 + \cdots + r_m. \tag{9. 2}$$

Let $L_1, \ldots, L_m$ be nonzero linear forms, where L_h is a form in the variables $X_{h1}, \ldots, X_{hn}$ with coefficients in a complete field F containing $\mathbb{Q}$, so that

$$L_h = \alpha_{h1} X_{h1} + \cdots + \alpha_{hn} X_{hn} \qquad (h = 1, \ldots, m).$$

Let T be the subspace of F^{nm} defined by $L_1 = \cdots = L_m = 0$. In view of Schmidt [14], VI, Lemmata 4B, 4C, the *index* of a polynomial $P \in \mathscr{R}$ with respect to $(L_1, \ldots, L_m; \mathbf{r})$ may be defined as follows. *When* $P \equiv 0$, *set* $\operatorname{Ind} P = \infty$. *When* $P \not\equiv 0$, *the index is the least value of* c *such that there is an* $\mathscr{I}$ *with* $(\mathscr{I}/\mathbf{r}) = c$, *such that* $P^{\mathscr{I}}$ *is not identically zero on* T. *Furthermore, if* $\alpha_{h1} \neq 0$ *for* $h = 1, \ldots, m$, *then there is an*

$$\mathscr{I} = (i_1, 0, \ldots, 0; \ldots; i_m, 0, \ldots, 0) \tag{9.3}$$

with $(\mathscr{I}/\mathbf{r}) = \operatorname{Ind} P$ *and* $P^{\mathscr{I}}$ *not identically zero on* T.

We now quote a version of Roth's Lemma from Schmidt [14], VI, Theorem 10B.

Lemma 9.1 (Roth's Lemma). *Suppose that* $0 < \vartheta < 1/12$, *that* m *is a positive integer, and let*

$$\omega = 24 \cdot 2^{-m} \left(\frac{\vartheta}{12}\right)^{2^{m-1}}. \tag{9.4}$$

Let $r_1, \ldots, r_m$ *be natural numbers with*

$$\omega r_h \geqq r_{h+1} \qquad (1 \leqq h \leqq m-1). \tag{9.5}$$

Let $V_1, \ldots, V_m$ *be nonzero linear forms in* n *variables with coprime rational integral coefficients, where* V_h *is a polynomial in* $X_{h1}, \ldots, X_{hn}$. *Suppose that* $0 < \Gamma \leqq q = n-1$, *and that*

$$\lceil V_h \rceil_0^{r_h} \geqq \lceil V_1 \rceil_0^{r_1 \Gamma} \qquad (2 \leqq h \leqq m), \tag{9.6}$$

$$\lceil V_h \rceil_0^{\omega \Gamma} \geqq 2^{3mq^2} \qquad (1 \leqq h \leqq m). \tag{9.7}$$

Let $P \in \mathscr{R}'$ *be nonzero, and with*

$$\lceil P \rceil_0^{q^2} \leqq \lceil V_1 \rceil_0^{\omega r_1 \Gamma}. \tag{9.8}$$

Then the index of P *with respect to* $(V_1, \ldots, V_m; \mathbf{r})$ *is* $\leqq \vartheta$.

Given a linear form $L = \alpha_1 X_1 + \cdots + \alpha_n X_n$, we make m forms out of it by setting

$$L_{[h]} = \alpha_1 X_{h1} + \cdots + \alpha_n X_{hn} \qquad (h = 1, \ldots, m).$$

The *index with respect to* $(L; \mathbf{r})$ is then defined as the index with respect to $(L_{[1]}, \ldots, L_{[m]}; \mathbf{r})$.

Lemma 9.2 (Index Theorem). *Suppose $L_1, \dots, L_w$ are nonzero linear forms with coefficients in a number field of degree d. Suppose*

$$H(L_i) \leqq H \qquad (i = 1, \dots, w). \tag{9.9}$$

Suppose that $\varepsilon > 0$ and

$$m > 4\varepsilon^{-2} \log(2wd). \tag{9.10}$$

Then given $\mathbf{r} = (r_1, \dots, r_m)$, there exists a nonzero polynomial $P \in \mathscr{R}'$ with

(i) $\operatorname{Ind} P \geqq \left(\frac{1}{n} - \varepsilon\right) m$ *with respect to* $(L_i; \mathbf{r})$ $(i = 1, \dots, w)$,

(ii) $\lceil P \rceil_0 < 2^{mn}(3n^{1/2}H)^r$ *and* $\lceil P \rceil_j \leqq 1$ $(j = 1, \dots, s)$.

This is the Index Theorem of section 9 in Schmidt [15]. The additional requirement $\lceil P \rceil_j \leqq 1$ $(j = 1, \dots, s)$ is automatically satisfied, since P has rational integral coefficients.

Let K be a number field of degree d. For each j $(0 \leqq j \leqq s)$ let φ_j be an embedding of K over $\mathbb{Q}$ into Ω_j, the algebraic closure of $\mathbb{Q}_j$. Let $L_1^{(j)}, \dots, L_n^{(j)}$ be linearly independent linear forms with coefficients in $\varphi_j(K) \cap \mathbb{Q}_j$ and let $M_1^{(j)}, \dots, M_n^{(j)}$ be their normalizations, i.e.

$$M_i^{(0)} = |L_i^{(0)}|_0^{-1} L_i^{(0)} \qquad (i = 1, \dots, n),$$
$$M_i^{(j)} = |L_i^{(j)}|_j L_i^{(j)} \qquad (i = 1, \dots, n;\ j = 1, \dots, s).$$

(Notice that here the second part of our definition makes sense, since for $j \geqq 1$ $|L_i^{(j)}|_j$ is a rational number.) For each j $(0 \leqq j \leqq s)$ we may write $X_1, \dots, X_n$ as linear combinations of $M_1^{(j)}, \dots, M_n^{(j)}$, and $X_{h1}, \dots, X_{hn}$ as linear combinations of

$$M_{1[h]}^{(j)}, \dots, M_{n[h]}^{(j)} \qquad (h = 1, \dots, m).$$

Now, if (9.10) holds with $w = n(s+1)$, let P be the polynomial of the Index Theorem. Given an nm-tuple $\mathscr{J}$, we may write $P^{\mathscr{J}}$ as

$$P^{\mathscr{J}} = \sum_{j_{11}, \dots, j_{mn}} d_j^{\mathscr{J}}(j_{11}, \dots, j_{mn}) M_{1[1]}^{(j)^{j_{11}}} \cdots M_{n[1]}^{(j)^{j_{1n}}} \cdots M_{1[m]}^{(j)^{j_{m1}}} \cdots M_{n[m]}^{(j)^{j_{mn}}} \tag{9.11}$$

for each j with $0 \leqq j \leqq s$. Here the summation may be restricted to

$$j_{h1} + \cdots + j_{hn} \leqq r_h \qquad (h = 1, \dots, m).$$

Lemma 9. 3 (Polynomial Theorem). (i) *When* $(\mathscr{I}/\mathbf{r}) \leqq 2\varepsilon m$, *then we have for each* j $(0 \leqq j \leqq s)$ $d_j^{\mathscr{I}}(j_{11}, \ldots, j_{mn}) = 0$ *unless*

$$\left| \left(\sum_{h=1}^{m} \frac{j_{hk}}{r_h} \right) - \frac{m}{n} \right| < 3nm\varepsilon \qquad (1 \leqq k \leqq n).$$

(ii) *As for the modulus of the coefficients of* $P^{\mathscr{I}}$ *we have*

$$|d_0^{\mathscr{I}}(j_{11}, \ldots, j_{mn})|_0 < 2^{mn}(6n^{3/2}H^{nd+1})^r$$

and

$$|d_j^{\mathscr{I}}(j_{11}, \ldots, j_{mn})|_j \leqq H^{ndr} \qquad (1 \leqq j \leqq s).$$

Proof. (i) and the first part of (ii) are identical with the Polynomial Theorem in Schmidt [15], section 9. So let us study the second assertion in (ii). If we write

$$X_i = \eta_{i1}^{(j)} M_1^{(j)} + \cdots + \eta_{in}^{(j)} M_n^{(j)}$$

then we have by Lemma 5. 5

$$|\eta_{ik}^{(j)}|_j \leqq H^{nd}.$$

The monomial $X_{11}^{j_{11}} \cdots X_{mn}^{j_{mn}}$ may be written as

$$X_{11}^{j_{11}} \cdots X_{mn}^{j_{mn}} = \left(\sum_{k=1}^{n} \eta_{1k}^{(j)} M_{k[1]}^{(j)} \right)^{j_{11}} \cdots \left(\sum_{k=1}^{n} \eta_{nk}^{(j)} M_{k[m]}^{(j)} \right)^{j_{mn}}$$

and this is a polynomial in the forms $M_{k[h]}^{(j)}$ with coefficients of $|\ |_j$-modulus

$$\leqq H^{nd(j_{11}+\cdots+j_{mn})} \leqq H^{ndr} \qquad (1 \leqq j \leqq s).$$

Since $\boxed{P^{\mathscr{I}}}_j \leqq 1$ $(1 \leqq j \leqq s)$, we obtain

$$|d_j^{\mathscr{I}}(j_{11}, \ldots, j_{mn})|_j \leqq H^{ndr} \qquad (1 \leqq j \leqq s)$$

and this is the second part of (ii).

10. The index of P with respect to certain rational linear forms

For each j $(j = 0, \ldots, s)$ let $L_i^{(j)}(\mathbf{X}) = \boldsymbol{\alpha}_i^{(j)}\mathbf{X}$ $(i = 1, \ldots, n)$ be linearly independent linear forms with coefficients in $\varphi_j(K) \cap \mathfrak{Q}_j$ and with

$$H(L_i^{(j)}) \leqq H \qquad (i = 1, \ldots, n;\ j = 0, \ldots, s) \tag{10. 1}$$

i.e. with (9. 9). Let

$$M_i^{(j)}(\mathbf{X}) = \boldsymbol{\beta}_i^{(j)}\mathbf{X} \qquad (i = 1, \ldots, n;\ j = 0, \ldots, s)$$

be their respective normalizations with respect to $|\ |_j$. We suppose that $\varepsilon>0$ and that $m>4\varepsilon^{-2}\log(2n(s+1)d)$ i.e. that (9. 10) holds with $w=n(s+1)$. Let P be the polynomial of the Index Theorem 9. 2 and of the Polynomial Theorem 9. 3.

As in section 8, $c_{10},\dots,c_{n0},\dots,c_{1s},\dots,c_{ns}$ will be real numbers of modulus $\leqq 1$ satisfying (8. 1). Given $Q>0$, $\Pi(Q)$ and $\Lambda(Q)$ will be the parallelepiped (8. 2) and the lattice (8. 3) respectively. We have minima $\lambda_1=\lambda_1(Q),\dots,\lambda_n=\lambda_n(Q)$, and we have certain points $\mathbf{g}_1=\mathbf{g}_1(Q),\dots,\mathbf{g}_n=\mathbf{g}_n(Q)$ as in (7. 3). Again, $V=V(Q)$ will be the linear form with coprime integral coefficients vanishing on $\mathbf{g}_1,\dots,\mathbf{g}_q$ where $q=n-1$. If $V=v_1X_1+\cdots+v_nX_n$ write

$$V_{[h]}=v_1X_{h1}+\cdots+v_nX_{hn}\qquad(h=1,\dots,m).$$

Lemma 10. 1. *Suppose that* $0<\delta<1$ *and* $0<\varepsilon\leqq\dfrac{\delta}{15n^2(s+1)}$. *Let* $Q_1,\dots,Q_m$ *satisfy*

$$r_1\log Q_1\leqq r_h\log Q_h\leqq(1+\varepsilon)r_1\log Q_1\qquad(h=1,\dots,m),\tag{10. 2}$$

$$\lambda_q(Q_h)\leqq Q_h^{-\delta}\qquad(h=1,\dots,m),\tag{10. 3}$$

and

$$Q_h^{\delta}>2^{18n}\varepsilon^{-3}H^{5nd(s+1)}\qquad(h=1,\dots,m).\tag{10. 4}$$

Then P *has index* $\geqq m\varepsilon$ *with respect to* $(V_{[1]}(Q_1),\dots,V_{[m]}(Q_m);\mathbf{r})$.

Proof. Let T be the subspace of $\mathbb{Q}^{mn}$ where $V_{[1]}(Q_1),\dots,V_{[m]}(Q_m)$ vanish. It suffices to show that $P^{\mathscr{I}}\equiv 0$ on T whenever $(\mathscr{I}/\mathbf{r})<m\varepsilon$. For $h=1,\dots,m$ let Γ_h be the grid consisting of points

$$\mathbf{u}=u_1\mathbf{g}_1(Q_h)+\cdots+u_q\mathbf{g}_q(Q_q),$$

where $u_1,\dots,u_q$ run through the integers in $1\leqq u_i\leqq[\varepsilon^{-1}]+1$. In view of Lemma 8A of Schmidt [14], it suffices to show that

$$P^{\mathscr{I}}(\mathbf{u}_1,\dots,\mathbf{u}_m)=0\tag{10. 5}$$

whenever $(\mathscr{I}/\mathbf{r})<2\varepsilon m$ and $\mathbf{u}_h\in\Gamma_h$ $(h=1,\dots,m)$. In accordance with (9. 11) we write for $j=0,\dots,s$

$$P^{\mathscr{I}}(\mathbf{u}_1,\dots,\mathbf{u}_m)=\sum_{j_{11},\dots,j_{mn}}d_j^{\mathscr{I}}(j_{11},\dots,j_{mn})M_1^{(j)}(\mathbf{u}_1)^{j_{11}}\cdots M_n^{(j)}(\mathbf{u}_m)^{j_{mn}}.\tag{10. 6}$$

Notice that the points $\mathbf{g}_i(Q_h)$ $(i=1,\dots,q;\ h=1,\dots,m)$ lie in $\mathbb{Z}(p_1,\dots,p_s)^n$. Thus there exists a natural number R which is only divisible by $p_1,\dots,p_s$ such that for i $(1\leqq i\leqq q)$ and for each h $(1\leqq h\leqq m)$ the point $R\mathbf{g}_i(Q_h)$ lies in $\mathbb{Z}^n$. Therefore the points $R\mathbf{u}_h$ with $\mathbf{u}_h\in\Gamma_h$ lie in $\mathbb{Z}^n$ and

$$\prod_{j=0}^{s} |P^{\mathcal{I}}(R\mathbf{u}_1, \ldots, R\mathbf{u}_m)|_j$$

will be an integer. On the other hand $\prod_{j=0}^{s} |R|_j = 1$ and since P as well as $P^{\mathcal{I}}$ are homogeneous we may infer that

$$\prod_{j=0}^{s} |P^{\mathcal{I}}(\mathbf{u}_1, \ldots, \mathbf{u}_m)|_j \in \mathbb{Z}. \tag{10. 7}$$

We first estimate $|P^{\mathcal{I}}(\mathbf{u}_1, \ldots, \mathbf{u}_m)|_0$. Here

$$|M_k^{(0)}(\mathbf{u}_h)|_0 \leqq n(\varepsilon^{-1}+1)\,\lambda_q(Q_h)\,Q_h^{c_{k0}} < \frac{2n}{\varepsilon}\,Q_h^{c_{k0}-\delta} \qquad (1 \leqq k \leqq n;\ 1 \leqq h \leqq m)$$

by (10. 3) and the definition of Γ_h. Therefore

$$|M_k^{(0)}(\mathbf{u}_1)^{j_{1k}} \cdots M_k^{(0)}(\mathbf{u}_m)^{j_{mk}}|_0 < \left(\frac{2n}{\varepsilon}\right)^{j_{1k}+\cdots+j_{mk}} (Q_1^{j_{1k}} \cdots Q_m^{j_{mk}})^{c_{k0}-\delta}. \tag{10. 8}$$

Combining (10. 2) and assertion (i) of Lemma 9. 3 we get for each j

$$d_j^{\mathcal{I}}(j_{11}, \ldots, j_{mn}) = 0 \qquad (0 \leqq j \leqq s)$$

unless

$$\sum_{h=1}^{m} j_{hk} \log Q_h \geqq r_1 \log Q_1 \sum_{h=1}^{m} \frac{j_{hk}}{r_k} \geqq r_1 \log Q_1 \left(\frac{1}{n} - 3n\varepsilon\right) m$$

and

$$\sum_{h=1}^{m} j_{hk} \log Q_h \leqq (1+\varepsilon) r_1 \log Q_1 \sum_{h=1}^{m} \frac{j_{hk}}{r_k} \leqq r_1 \log Q_1 (1+\varepsilon)\left(\frac{1}{n} + 3n\varepsilon\right) m.$$

Since $(1+\varepsilon)\left(\frac{1}{n}+3n\varepsilon\right) < \frac{1}{n} + \frac{7}{2}n\varepsilon$, this implies, that for $k = 1, \ldots, n$ we have only to consider monomials satisfying

$$\left|\left(\sum_{h=1}^{m} j_{hk} \log Q_h\right) - r_1 \log Q_1 \frac{m}{n}\right| < r_1 \log Q_1 \frac{7}{2} nm\varepsilon < r_1 \log Q_1 \frac{m}{n} \frac{\delta}{4(s+1)}. \tag{10. 9}$$

For such monomials we obtain using (10. 8)

$$|M_k^{(0)}(\mathbf{u}_1)^{j_{1k}} \cdots M_k^{(0)}(\mathbf{u}_m)^{j_{mk}}|_0 < \left(\frac{2n}{\varepsilon}\right)^{j_{1k}+\cdots+j_{mk}} Q_1^{r_1 \frac{m}{n}(c_{k0}-\delta) + r_1 \frac{m}{n} \frac{\delta}{4(s+1)} |c_{k0}-\delta|}.$$

In view of assertion (ii) of Lemma 9. 3 and since $|c_{k0}-\delta| \leqq 2$, we see that for $j=0$ every summand in (10. 6) has $|\ |_0$-modulus

$$< 2^{mn}(6n^{3/2}H^{nd+1})^r \left(\frac{2n}{\varepsilon}\right)^r Q_1^{r_1\frac{m}{n}(c_{10}+\cdots+c_{n0}-n\delta)+r_1 m\frac{\delta}{2(s+1)}}.$$

The number of summands in (10. 6) is $\leqq 2^{n(r_1+\cdots+r_m)} = 2^{nr}$, so that

$$|P^{\mathscr{S}}(\mathbf{u}_1,\ldots,\mathbf{u}_m)|_0 < 2^{n(m+r)}(6n^{3/2}H^{nd+1})^r \left(\frac{2n}{\varepsilon}\right)^r Q_1^{r_1\frac{m}{n}(c_{10}+\cdots+c_{n0}-n\delta)} \times Q_1^{r_1 m\frac{\delta}{2(s+1)}}. \tag{10. 10}$$

We now estimate $|P^{\mathscr{S}}(\mathbf{u}_1,\ldots,\mathbf{u}_m)|_j$ for $j \geqq 1$. Here

$$|M_k^{(j)}(\mathbf{u}_h)|_j \leqq Q_h^{c_{kj}} \qquad (1 \leqq k \leqq n;\ 1 \leqq h \leqq m)$$

by the definition of $\mathbf{u}_h$. Again, by assertion (i) of Lemma 9. 3 we have only to consider monomials with (10. 9), and for these we obtain

$$|M_k^{(j)}(\mathbf{u}_1)^{j_{1k}}\cdots M_k^{(j)}(\mathbf{u}_m)^{j_{mk}}|_j \leqq (Q_1^{j_{1k}}\cdots Q_m^{j_{mk}})^{c_{kj}} < Q_1^{r_1\frac{m}{n}c_{kj}+r_1\frac{m}{n}\frac{\delta}{4(s+1)}|c_{kj}|}.$$

Using assertion (ii) of Lemma 9. 3 and the ultrametric triangle inequality and since $|c_{kj}| \leqq 1$ we get

$$|P^{\mathscr{S}}(\mathbf{u}_1,\ldots,\mathbf{u}_m)|_j < H^{ndr}Q_1^{r_1\frac{m}{n}(c_{1j}+\cdots+c_{nj})+r_1 m\frac{\delta}{2(s+1)}} \qquad (j=1,\ldots,s). \tag{10. 11}$$

Combination of (8. 1), (10. 10), (10. 11) yields

$$\begin{aligned}\prod_{j=0}^{s}|P^{\mathscr{S}}(\mathbf{u}_1,\ldots,\mathbf{u}_m)|_j &< 2^{n(m+r)}(6n^{3/2}H^{nd(s+1)+1})^r\left(\frac{2n}{\varepsilon}\right)^r Q_1^{-r_1 m\frac{\delta}{2}} \\ &< (2^{6n}\varepsilon^{-1}H^{nd(s+1)+1})^r (Q_1^{-r_1}\cdots Q_m^{-r_m})^{\frac{\delta}{2(1+\varepsilon)}}\end{aligned}$$

by (10. 2). Now, since $r=r_1+\cdots+r_m$ and by (10. 4) this implies

$$\prod_{j=0}^{s}|P^{\mathscr{S}}(\mathbf{u}_1,\ldots,\mathbf{u}_m)|_j < \sum_{h=1}^{m}(2^{6n}\varepsilon^{-1}H^{nd(s+1)+1}Q_h^{-\delta/3})^{r_h} < 1.$$

The assertion follows from (10. 7).

11. The penultimate minimum

Lemma 11. 1. *Suppose that* $0<\delta<1$ *and*

$$m>900n^4(s+1)^2\delta^{-2}\log(2n(s+1)d). \tag{11. 1}$$

Put

$$E=\frac{1}{12}2^m(180)^{2^{m-1}}. \tag{11. 2}$$

Let $\Pi(Q)$ *and* $\Lambda(Q)$ *be defined by* (8. 2) *and* (8. 3) *respectively, where for each* j $(0\leqq j\leqq s)$ $\boldsymbol{\beta}_1^{(j)},\ldots,\boldsymbol{\beta}_n^{(j)}$ *are independent and normalized vectors in* $\mathcal{Q}_j^n$, *defined over a field of degree* d, *and with heights* $H(\boldsymbol{\beta}_i^{(j)})\leqq H$ $(i=1,\ldots,n;\ j=0,\ldots,s)$. *Suppose that for any integral point* $\mathbf{h}\neq\mathbf{0}$ *there exist* $(i_0,\ldots,i_s)\in\mathfrak{S}$ *for which* (8. 29) *does not hold. Then the numbers* Q *with*

$$\lambda_q(Q)<Q^{-\delta} \tag{11. 3}$$

and with

$$Q^{\delta^2}>(2^{4n}H)^{4d^2(s+1)^3mE} \tag{11. 4}$$

lie in at most $m-1$ *intervals of the type*

$$Q_h<Q\leqq Q_h^E \quad (h=1,\ldots,m-1). \tag{11. 5}$$

Proof. Put

$$\varepsilon=\frac{\delta}{15n^2(s+1)}. \tag{11. 6}$$

This fits well into the hypotheses of Lemma 10. 1. With this value of ε, (11. 1) implies that (9. 10) is satisfied with $w=n(s+1)$, which was required in Lemma 10. 1 as well.

Notice that $m>(\log 2)^{-1}\log(2n(s+1)d)+1$ by (11. 1), so that $2^{m-1}>2n(s+1)d$ and

$$E>2\cdot 2^{m-1}>4n(s+1)d \tag{11. 7}$$

by (11. 2). Combining (11. 1), (11. 4), (11. 7) we get

$$\begin{aligned}Q^{\delta}>Q^{\delta^2}&>(2^{4n}H)^{1000n^4\delta^{-2}(s+1)^2 4d^2 4nd(s+1)}\\&>2^{18n}H^{5nd(s+1)}\left(\frac{15n^2(s+1)}{\delta}\right)^3=2^{18n}\varepsilon^{-3}H^{5nd(s+1)},\end{aligned}$$

thus (10. 4) with ε defined in (11. 6). So apart from (10. 2) all the hypotheses of Lemma 10. 1 are satisfied.

Now suppose the Lemma were false. Let Q_1 be the infimum of the values of Q with (11. 3), (11. 4). Then Q with (11. 3), (11. 4) will have $Q > Q_1$. If all the values of Q with (11. 3), (11. 4) were in the interval $Q_1 < Q \leqq Q_1^E$, the assertion would be correct. Hence there are $Q > Q_1^E$ with (11. 3); let Q_2 be their infimum. Continuing the procedure we find $Q_1, \ldots, Q_m$ with $\lambda_q(Q_h) \leqq Q_h^{-\delta}$ $(h = 1, \ldots, m)$ and

$$Q_{h+1} \geqq Q_h^E \qquad (h = 1, \ldots, m-1). \tag{11. 8}$$

Now let r_1 be so large that

$$r_1 > \varepsilon^{-1} \log Q_m / \log Q_1.$$

For $h = 2, \ldots, m$ put

$$r_h = [r_1 \log Q_1 / \log Q_h] + 1.$$

Then we have for $h = 1, \ldots, m$

$$r_1 \log Q_1 \leqq r_h \log Q_h \leqq r_1 \log Q_1 + \log Q_h < (1+\varepsilon) r_1 \log Q_1, \tag{11. 9}$$

and (10. 2) holds.

Let P be the polynomial of the Index Theorem and of the Polynomial Theorem. Then Lemma 10. 1 says that P has index $\geqq m\varepsilon$ with respect to

$$(V_{[1]}(Q_1), \ldots, V_{[m]}(Q_m); \mathbf{r}).$$

Our next goal is to apply Roth's Lemma. With $\vartheta = \frac{1}{15}$ and with ω given by (9. 4), we have $E = \frac{2}{\omega}$. Hence by (11. 8), (11. 9)

$$\omega r_h \geqq \omega \frac{r_{h+1} \log Q_{h+1}}{(1+\varepsilon) \log Q_h} = \frac{2 r_{h+1}}{(1+\varepsilon) E} \frac{\log Q_{h+1}}{\log Q_h} \geqq r_{h+1}$$

and (9. 5) is satisfied.

Since for any integral point $\mathbf{h} \neq \mathbf{0}$ there exists $(i_0, \ldots, i_s) \in \mathfrak{S}$ with $\prod_{j=0}^{s} |\boldsymbol{\beta}_{i_j}^{(j)*} \mathbf{h}|_j \neq 0$, the same holds true for any rational point $\mathbf{g} \neq \mathbf{0}$. In particular there is for each h an $(i_0, \ldots, i_s) \in \mathfrak{S}$ with $\prod_{j=0}^{s} |\boldsymbol{\beta}_{i_j}^{(j)*} \hat{\mathbf{g}}_n(Q_h)|_j \neq 0$ $(h = 1, \ldots, m)$, so that by Lemma 8. 3 (notice that (11. 4) implies (8. 21)) we have

$$Q_h^{\frac{q\delta}{2d(s+1)}} < \overline{|V_h|} < Q_h^{s+1} \qquad (h = 1, \ldots, m), \tag{11. 10}$$

where $V_h = V(Q_h)$. Put

$$\Gamma = \frac{q\delta}{2d(s+1)^2}. \tag{11. 11}$$

Then (11. 10) in conjunction with (11. 9) yields

$$\boxed{V_h}^{r_h} > Q_h^{r_h(s+1)\Gamma} \geqq Q_1^{r_1(s+1)\Gamma} > \boxed{V_1}^{r_1\Gamma} \qquad (h=2,\ldots,m),$$

which is (9. 6). Moreover by (11. 11), and since $E=\dfrac{2}{\omega}$

$$\boxed{V_h}^{\omega\Gamma} > Q_h^{\omega(s+1)\Gamma^2} = Q_h^{\frac{2\Gamma^2(s+1)}{E}} = Q_h^{\frac{q^2\delta^2}{2d^2(s+1)^3E}} > 2^{3mq^2},$$

where we have used (11. 4). So (9. 7) is satisfied.

We still have to check (9. 8). Now, by the Index Theorem we have

$$\boxed{P}_0 < 2^{mn}(3n^{1/2}H)^r < (2^{4n}H)^{r_1 m},$$

and therefore

$$\begin{aligned}\boxed{P}_0^{q^2} &< (2^{4n}H)^{r_1 mq^2} < (2^{4n}H)^{r_1 mq^2 E\omega} = (2^{4n}H)^{r_1 mE\omega\Gamma^2 4d^2(s+1)^4\delta^{-2}} \\ &< Q_1^{r_1\omega(s+1)\Gamma^2} < \boxed{V_1}_0^{r_1\omega\Gamma}\end{aligned}$$

in view of (11. 4) and (11. 10). Thus (9. 8) is satisfied as well. By Roth's Lemma, the index of P with respect to $(V_{[1]},\ldots,V_{[m]};\mathbf{r})$ is $\leqq \vartheta$. But

$$\vartheta = \frac{1}{15} < m\frac{\delta}{15n^2(s+1)} = m\varepsilon$$

by (11. 1), (11. 6). This contradicts the lower bound given above.

Lemma 11. 2. *Let δ, m, E be as in Lemma* 11. 1. *Let $\Pi(Q)$ and $\Lambda(Q)$ be defined by* (8. 2) *and* (8. 3) *respectively, where for each j $(0\leqq j\leqq s)$ $\boldsymbol{\beta}_1^{(j)},\ldots,\boldsymbol{\beta}_n^{(j)}$ are independent and normalized vectors in $\mathcal{Q}_j^n$, defined over a field of degree d and with heights $\leqq H$. Given Q, let $S=S(Q)$ be the subspace spanned by $\mathbf{g}_1=\mathbf{g}_1(Q),\ldots,\mathbf{g}_q=\mathbf{g}_q(Q)$.*

Then, as Q ranges over values with (11. 3) *and* (11. 4), *$S(Q)$ ranges over less than*

$$m(1+4(s+1)\delta^{-1}\log E)$$

distinct subspaces.

Proof. Suppose at first that there exists an integral point $\mathbf{h}\neq\mathbf{0}$ which satisfies (8. 29) for all $(i_0,\ldots,i_s)\in\mathfrak{S}$. Let $\mathbf{h}$ be a point with this property having smallest possible norm. Notice that in view of (11. 4) condition (8. 30) is satisfied. Thus we may apply Lemma 8. 5 and $S(Q)$ consists of $\mathbf{x}$ with $\mathbf{h}\mathbf{x}=0$.

If there is no such integral point, we may apply Lemma 11. 1. Now (11. 4) implies (8. 32) and Lemma 8. 6 shows that for Q in a particular interval (11. 5), $S(Q)$ will run through not more than $1+4(s+1)\delta^{-1}\log E$ distinct subspaces. Summation over h in $1\leqq h<m$ gives the result.

Let $A_1, \dots, A_n$ be positive real numbers. Suppose that for each j $(1 \leqq j \leqq s)$ $f_{1j}, \dots, f_{nj}$ are nonnegative integers with

$$A_1 \cdots A_n \prod_{j=1}^{s} p_j^{-(f_{1j}+\cdots+f_{nj})} = 1. \tag{11.12}$$

Let $\boldsymbol{\beta}_1^{(0)}, \dots, \boldsymbol{\beta}_n^{(0)}, \dots, \boldsymbol{\beta}_1^{(s)}, \dots, \boldsymbol{\beta}_n^{(s)}$ be as in Lemma 11.2. Define the parallelepiped $\Pi = \Pi(A_1, \dots, A_n) = \Pi(\mathbf{A})$ by

$$|\boldsymbol{\beta}_i^{(0)} \mathbf{x}|_0 \leqq A_i \quad (i = 1, \dots, n), \tag{11.13}$$

and the lattice $\Lambda = \Lambda(f_{11}, \dots, f_{n1}, \dots, f_{1s}, \dots, f_{ns}) = \Lambda(\mathbf{f})$ by

$$|\boldsymbol{\beta}_i^{(j)} \mathbf{x}|_j \leqq p_j^{-f_{ij}} \quad (i = 1, \dots, n;\ j = 1, \dots, s). \tag{11.14}$$

Let $\lambda_i = \lambda_i(A_1, \dots, A_n, f_{11}, \dots, f_{n1}, \dots, f_{1s}, \dots, f_{ns}) = \lambda_i(\mathbf{A}, \mathbf{f})$ be the successive minima of $\Pi(\mathbf{A})$ with respect to $\Lambda(\mathbf{f})$ $(i = 1, \dots, n)$, and let $\mathbf{g}_i = \mathbf{g}_i(\mathbf{A}, \mathbf{f})$ be corresponding points in $\Lambda(\mathbf{f})$. Denote by $S(\mathbf{A}, \mathbf{f})$ the subspace generated by $\mathbf{g}_1(\mathbf{A}, \mathbf{f}), \dots, \mathbf{g}_q(\mathbf{A}, \mathbf{f})$.

Lemma 11.3. *Suppose that* $0 < \delta < 1$,

$$m > 3600 n^4 (s+1)^2 \delta^{-2} \log(2n(s+1)d) \tag{11.15}$$

and that E is given by (11.2).

Then for values of $A_1, \dots, A_n, f_{11}, \dots, f_{n1}, \dots, f_{1s}, \dots, f_{ns}$, Q *with*

$$Q^{\delta^2} > (2^{4n} H)^{16 d^2 (s+1)^3 m E}, \tag{11.16}$$

$$Q^{1/2} \geqq \max\{A_1, \dots, A_n, A_1^{-1}, \dots, A_n^{-1}, p_1^{f_{11}}, \dots, p_1^{f_{n1}}, \dots, p_s^{f_{1s}}, \dots, p_s^{f_{ns}}\} \tag{11.17}$$

and

$$\lambda_q(\mathbf{A}, \mathbf{f}) < Q^{-\delta}, \tag{11.18}$$

$S(\mathbf{A}, \mathbf{f})$ *is among not more than*

$$m\left(\frac{9(s+1)}{\delta}\right)^{n(s+1)} (1 + 8(s+1)\delta^{-1} \log E)$$

fixed subspaces.

Proof. Define real numbers η_{ij} $(i = 1, \dots, n;\ j = 0, \dots, s)$ by $A_i = Q^{\eta_{i0}}$ and $p_j^{-f_{ij}} = Q^{\eta_{ij}}$. Then (11.17) implies $-\frac{1}{2} \leqq \eta_{i0} \leqq \frac{1}{2}$ $(i = 1, \dots, n)$ and $-\frac{1}{2} \leqq \eta_{ij} \leqq 0$ for $j \geqq 1$. Moreover by (11.12) we have

$$\sum_{j=0}^{s} (\eta_{1j} + \cdots + \eta_{nj}) = 0.$$

Let v be the least even integer $\geqq \frac{2(s+1)}{\delta}$. For $1 \leqq i \leqq n$ and $1 \leqq j \leqq s$, define real numbers $\xi_{l_{ij}} = -\frac{1}{2} + l_{ij}\frac{1}{v}$, where l_{ij} is the least integer such that $\eta_{ij} \leqq \xi_{l_{ij}}$. Then

$$0 \leqq l_{ij} \leqq \frac{v}{2} \qquad (i=1, \ldots, n;\ j=1, \ldots, s) \tag{11.19}$$

and

$$\xi_{l_{ij}} - \frac{1}{v} < \eta_{ij} \leqq \xi_{l_{ij}} \qquad (j=1, \ldots, s;\ i=1, \ldots, n). \tag{11.20}$$

Let

$$\xi_{l_{i0}} = -1 + \frac{l_{i0}}{v} \qquad (l_{i0}=0, 1, \ldots, 2v).$$

We claim that it is possible to pick integers $l_{10}, \ldots, l_{n0}$ in $0 \leqq l \leqq 2v$ with

$$|\eta_{i0} - \xi_{l_{i0}}| < \frac{s+1}{v} \qquad (i=1, \ldots, n) \tag{11.21}$$

and

(11.22)

$$|\eta_{10} + \cdots + \eta_{1s} - \xi_{l_{10}} - \cdots - \xi_{l_{1s}}) + \cdots + (\eta_{i0} + \cdots + \eta_{is} - \xi_{l_{i0}} - \cdots - \xi_{l_{is}})| < \frac{1}{v}$$
$$(i=1, \ldots, n).$$

Choose l_{10} with

$$|\eta_{10} + \cdots + \eta_{1s} - \xi_{l_{10}} - \xi_{l_{11}} - \cdots - \xi_{l_{1s}}| \leqq \frac{1}{2v},$$

then

$$|\eta_{10} - \xi_{l_{10}}| \leqq |\eta_{11} - \xi_{l_{11}}| + \cdots + |\eta_{1s} - \xi_{l_{1s}}| + \frac{1}{2v} < \frac{s+1}{v}$$

by (11.20). Thus (11.21), (11.22) are satisfied for $i=1$. If $l_{10}, \ldots, l_{k-1,0}$ have been chosen with (11.21), (11.22) valid for $i=1, \ldots, k-1$, and if

$$(\eta_{10} + \cdots + \eta_{1s} - \xi_{l_{10}} - \cdots - \xi_{l_{1s}}) + \cdots + (\eta_{k-1,0} + \cdots + \eta_{k-1,s} - \xi_{l_{k-1,0}} - \cdots - \xi_{l_{k-1,s}}) > 0$$

(or $\leqq 0$ respectively) pick l_{k0} with

$$|\eta_{k0} + \eta_{k1} + \cdots + \eta_{ks} - \xi_{l_{k0}} - \xi_{l_{k1}} - \cdots - \xi_{l_{ks}}| < \frac{1}{v}$$

and

$$\eta_{k0} + \eta_{k1} + \cdots + \eta_{ks} - \xi_{l_{k0}} - \xi_{l_{k1}} - \cdots - \xi_{l_{ks}} \leqq 0$$

(or $\geqq 0$ respectively).

Then (11. 21), (11. 22) are satisfied for $i=k$ as well. Now, (11. 12) together with (11. 22) for $i=n$ implies

$$\left|\sum_{j=0}^{s}(\xi_{l_{1j}}+\cdots+\xi_{l_{nj}})\right|<\frac{1}{v}, \quad \text{thus} \quad \sum_{j=0}^{s}(\xi_{l_{1j}}+\cdots+\xi_{l_{nj}})=0.$$

Let us first restrict ourselves to values of $A_1, \ldots, A_n, f_{11}, \ldots, f_{ns}$ with fixed

$$l_{10}, \ldots, l_{n0}, l_{11}, \ldots, l_{ns}.$$

Put $c_{ij}=\xi_{l_{ij}}$. Then $|c_{ij}|\leqq 1$ $(j=0, \ldots, s;\ i=1, \ldots, n)$ and (8. 1) holds true. We have

$$\Pi(A_1, \ldots, A_n)=\Pi(Q^{\eta_{10}}, \ldots, Q^{\eta_{n0}})\subseteqq Q^{\frac{s+1}{v}}\Pi(Q^{c_{10}}, \ldots, Q^{c_{n0}})\subseteqq Q^{\frac{\delta}{2}}\Pi(Q),$$

where $\Pi(Q)$ is the parallelepiped defined in (8. 2). Moreover, by (11. 20)

$$\Lambda(f_{11}, \ldots, f_{ns})=\Lambda(Q^{\eta_{11}}, \ldots, Q^{\eta_{ns}})\subseteqq\Lambda(Q^{c_{11}}, \ldots, Q^{c_{ns}})=\Lambda(Q),$$

where $\Lambda(Q)$ is the lattice defined in (8. 3). Therefore (11. 18) implies that the q-th minimum $\lambda_q(Q)$ of $\Pi(Q)$ with respect to $\Lambda(Q)$ satisfies

$$\lambda_q(Q)<Q^{-\delta/2}. \tag{11. 23}$$

Notice that (11. 15), (11. 16), (11. 23) are the same as (11. 1), (11. 4), (11. 3) in Lemma 11. 1 but with $\delta/2$ in place of δ. Thus by Lemma 11. 2 the number of possibilities for $S(Q)$ is

$$\leqq m(1+8(s+1)\delta^{-1}\log E). \tag{11. 24}$$

The vectors $\mathbf{g}_i=\mathbf{g}_i(\mathbf{A}, \mathbf{f})$ $(i=1, \ldots, q)$ lie in $Q^{-\delta/2}\Pi(Q)\cap\Lambda(Q)$. But by (7. 2), (6. 34), (8. 12) and (11. 16) we have

$$\lambda_1(Q)\cdots\lambda_n(Q)\geqq(n!)^{-1}\left(\prod_{j=0}^{s}B_j\right)Q^{-\sum_{j=0}^{s}\sum_{i=1}^{n}c_{ij}}=(n!)^{-1}\left(\prod_{j=0}^{s}B_j\right)$$
$$\geqq(n!)^{-1}H^{-nd(s+1)}>Q^{-\delta}.$$

In view of (11. 23) this implies that $\lambda_n(Q)>Q^{-\delta/2}$. Therefore $S(Q)$ is spanned by $\mathbf{g}_1(\mathbf{A}, \mathbf{f}), \ldots, \mathbf{g}_q(\mathbf{A}, \mathbf{f})$ and we have $S(Q)=S(\mathbf{A}, \mathbf{f})$. So the number of possibilities for $S(\mathbf{A}, \mathbf{f})$ is bounded by (11. 24).

We still have to take into account the number of possible values of $l_{10}, \ldots, l_{n0}, l_{11}, \ldots, l_{ns}$. This introduces a factor

$$(2v+1)^n\left(\frac{v}{2}+1\right)^{ns}\leqq\left(\frac{4(s+1)}{\delta}+5\right)^n\left(\frac{s+1}{\delta}+2\right)^{ns}\leqq\left(\frac{9(s+1)}{\delta}\right)^{n(s+1)}.$$

12. The last two minima

Lemma 12. 1. *Suppose that* $0<\delta<8n(s+1)$ *and that*

$$m>480^2 n^6 (s+1)^4 \delta^{-2} \log(2n(s+1)d). \tag{12. 1}$$

Let E *be given by* (11. 2), *and let* $\mathfrak{y}_1^{(0)}, \dots, \mathfrak{y}_n^{(0)}, \dots, \mathfrak{y}_1^{(s)}, \dots, \mathfrak{y}_n^{(s)}$, H, $A_1, \dots, A_n$, $f_{11}, \dots, f_{ns}$, $\Pi(\mathbf{A})$, $\Lambda(\mathbf{f})$ *be as in the last section. Then for values of* $A_1, \dots, A_n, f_{11}, \dots, f_{ns}, Q$ *with*

$$Q^{\frac{\delta^2}{16n^2(s+1)}} > (2^{4n}H)^{16d^2(s+1)^3 mE}, \tag{12. 2}$$

$$Q \geqq \max\{A_1, \dots, A_n, A_1^{-1}, \dots, A_n^{-1}, p_1^{f_{11}}, \dots, p_s^{f_{ns}}\} \tag{12. 3}$$

and

$$\lambda_q(\mathbf{A}, \mathbf{f}) < Q^{-\delta} \lambda_n(\mathbf{A}, \mathbf{f}), \tag{12. 4}$$

$S(\mathbf{A}, \mathbf{f})$ *is among not more than*

$$m\left(\frac{72n(s+1)^2}{\delta}\right)^{n(s+1)} (1+64n(s+1)^2\delta^{-1}\log E) \tag{12. 5}$$

subspaces.

Proof. Remember that with $B_j = |\det(\mathfrak{y}_1^{(j)}, \dots, \mathfrak{y}_n^{(j)})|_j$ $(j=0, \dots, s)$ we have by (8. 12)

$$1 \geqq B_j \geqq H^{-nd}.$$

By Lemma 6. 7 any point $\mathbf{x} \neq \mathbf{0}$ in $\Lambda(\mathbf{f})$ has $|\mathbf{x}|_0 \geqq \prod_{j=1}^{s} B_j \geqq H^{-nds}$. Writing

$$X_i = \eta_{i1}^{(0)}(\mathfrak{y}_1^{(0)}\mathbf{X}) + \cdots + \eta_{in}^{(0)}(\mathfrak{y}_n^{(0)}\mathbf{X})$$

we infer from Lemma 5. 6 that $|\eta_{ij}^{(0)}|_0 \leqq H^{nd}$ so that

$$|\mathbf{x}|_0 \leqq nH^{nd} \max\{|\mathfrak{y}_1^{(0)}\mathbf{x}|_0, \dots, |\mathfrak{y}_n^{(0)}\mathbf{x}|_0\}.$$

Therefore we have for $\mathbf{x} \neq \mathbf{0}$ in $\Lambda(\mathbf{f})$

$$\begin{aligned}\max\{A_1^{-1}|\mathfrak{y}_1^{(0)}\mathbf{x}|_0, \dots, A_n^{-1}|\mathfrak{y}_n^{(0)}\mathbf{x}|_0\} &\geqq Q^{-1}\max\{|\mathfrak{y}_1^{(0)}\mathbf{x}|_0, \dots, |\mathfrak{y}_n^{(0)}\mathbf{x}|_0\} \\ &\geqq (nH^{nd}Q)^{-1}|\mathbf{x}|_0 \geqq (nH^{nd(s+1)}Q)^{-1}.\end{aligned}$$

Thus

$$\lambda_1 = \lambda_1(\mathbf{A}, \mathbf{f}) \geqq (nH^{nd(s+1)}Q)^{-1}. \tag{12. 6}$$

On the other hand (7. 2) together with Lemma 6. 3 implies in conjunction with (11. 12)

$$(n!)^{-1} \prod_{j=0}^{s} B_j \leqq \lambda_1 \cdots \lambda_n \leqq \prod_{j=0}^{s} B_j,$$

and therefore

$$(n!\, H^{nd(s+1)})^{-1} \leqq \lambda_1 \cdots \lambda_n \leqq 1. \tag{12. 7}$$

Let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be the canonical basis vectors. For $j = 1, \ldots, s$ define $f_j = \max\{f_{1j}, \ldots, f_{nj}\}$. Since $\boldsymbol{\beta}_1^{(j)}, \ldots, \boldsymbol{\beta}_n^{(j)}$ are normalized, (11. 14) shows that the points

$$\left(\prod_{j=1}^{s} p_j^{f_j} \right) \mathbf{e}_i = \mathbf{d}_i$$

say ($i = 1, \ldots, n$) lie in $\Lambda(\mathbf{f})$. Now $|\boldsymbol{\beta}_i^{(0)} \mathbf{d}_k|_0 \leqq Q^s \leqq Q^s A_i Q$, so that

$$\lambda_n = \lambda_n(\mathbf{A}, \mathbf{f}) \leqq Q^{s+1}. \tag{12. 8}$$

Put

$$\varrho_0 = (\lambda_1 \cdots \lambda_{n-2} \lambda_{n-1}^2)^{1/n},$$

$\varrho_1 = \varrho_0/\lambda_1, \ldots, \varrho_{n-1} = \varrho_0/\lambda_{n-1}$ and $\varrho_n = \varrho_{n-1} = \varrho_0/\lambda_{n-1}$. Then the hypotheses of Lemma 7. 1 are satisfied. Hence there is a permutation $v_1, \ldots, v_n$ of $1, \ldots, n$ such that the successive minima $\lambda_1', \ldots, \lambda_n'$ of the parallelepiped Π' defined by

$$|\boldsymbol{\beta}_i^{(0)} \mathbf{x}|_0 \leqq A_i \varrho_{v_i}^{-1} \quad (= A_i' \text{ say}) \qquad (i = 1, \ldots, n) \tag{12. 9}$$

with respect to $\Lambda(\mathbf{f})$ satisfy

$$2^{-n} \varrho_i \lambda_i \leqq \lambda_i' \leqq 4^{n^2} \varrho_i \lambda_i \qquad (i = 1, \ldots, n).$$

In view of (12. 4) and (12. 7) we have

$$\varrho_0 = \left(\lambda_1 \cdots \lambda_n \left(\frac{\lambda_q}{\lambda_n} \right) \right)^{1/n} \leqq \left(\frac{\lambda_q}{\lambda_n} \right)^{1/n} < Q^{-\delta/n}.$$

Thus

$$\lambda_q' \leqq 4^{n^2} \lambda_{n-1} \varrho_{n-1} = 4^{n^2} \varrho_0 < 4^{n^2} Q^{-\delta/n} < Q^{-\delta/2n} \tag{12. 10}$$

by (12. 2) and (11. 7). Again by (12. 2), (11. 7) and by (12. 6)

$$\varrho_1 = \frac{\varrho_0}{\lambda_1} < \lambda_1^{-1} Q^{-\delta/n} \leqq n H^{nd(s+1)} Q Q^{-\delta/n} < Q;$$

moreover by (12. 8), (12. 7) and (12. 4) we get

$$\varrho_n = \varrho_0 \lambda_{n-1}^{-1} = (\lambda_1 \cdots \lambda_n)^{1/n} \lambda_n^{-1} \left(\frac{\lambda_n}{\lambda_{n-1}}\right)^{1-\frac{1}{n}} > (nH^{nd(s+1)})^{-1} Q^{-(s+1)} Q^{\delta(1-\frac{1}{n})}$$

and by (12. 2) this is $> Q^{-(s+1)}$. Therefore

$$Q^{-(s+1)} < \varrho_n \leqq \varrho_{n-1} \leqq \cdots \leqq \varrho_1 < Q$$

and

$$Q^{-2(s+1)} < Q^{-(s+2)} < A_i \varrho_{v_i}^{-1} = A_i' < Q^{s+2} < Q^{2(s+1)}. \tag{12. 11}$$

Now (12. 1), (12. 2), (12. 10) and (12. 11) are the conditions (11. 15), (11. 16), (11. 18) and (11. 17) respectively of Lemma 11. 3, but with $A_1, \ldots, A_n$, Q, δ replaced by

$$A_1', \ldots, A_n', \quad Q^{4(s+1)}, \quad \frac{\delta}{8n(s+1)}.$$

Let $S(A_1', \ldots, A_n', f_{11}, \ldots, f_{ns}) = S(\mathbf{A}', \mathbf{f})$ be the subspace corresponding to the parallelepiped $\Pi' = \Pi'(A_1', \ldots, A_n')$ defined in (12. 9) and to the lattice $\Lambda(\mathbf{f})$. Then Lemma 11. 3 with $\dfrac{\delta}{8n(s+1)}$ in place of δ gives for the number of such subspaces the bound in (12. 5).

To finish the proof of the Lemma we show that $S(\mathbf{A}', \mathbf{f}) = S(\mathbf{A}, \mathbf{f})$. The last assertion of Lemma 7. 1 says that any point $\mathbf{g} \in \Lambda(\mathbf{f})$, $\mathbf{g} \notin S(\mathbf{A}, \mathbf{f})$ has

$$\begin{aligned} \max_i \{|\boldsymbol{\beta}_i^{(0)} \mathbf{g}|_0 \varrho_{v_i} A_i^{-1}\} &= \max_i \{|\boldsymbol{\beta}_i^{(0)} \mathbf{g}|_0 A_i'^{-1}\} \\ &\geqq 2^{-n} \varrho_n \lambda_n > 4^{-2n^2} \lambda_n' \geqq 4^{-2n^2} (\lambda_1' \cdots \lambda_n')^{1/n} \\ &\geqq 4^{-2n^2} (nH^{d(s+1)})^{-1} > Q^{-\delta/2n} \end{aligned}$$

by (7. 8), the analogue of (12. 7) for $\lambda_1', \ldots, \lambda_n'$ and by (12. 2). On the other hand $\lambda_{n-1}' < Q^{-\delta/2n}$ by (12. 10). Therefore such $\mathbf{g}$ cannot lie in $S(\mathbf{A}', \mathbf{f})$. Hence $S(\mathbf{A}', \mathbf{f}) = S(\mathbf{A}, \mathbf{f})$ and the bound (12. 5) holds for the number of possibilities for $S(\mathbf{A}, \mathbf{f})$ as well.

13. Two adjacent minima

Lemma 13. 1. *Let* $\boldsymbol{\beta}_1^{(0)}, \ldots, \boldsymbol{\beta}_n^{(0)}, \ldots, \boldsymbol{\beta}_1^{(s)}, \ldots, \boldsymbol{\beta}_n^{(s)}$, H, $A_1, \ldots, A_n$, $f_{11}, \ldots, f_{ns}$, $\Pi = \Pi(\mathbf{A})$, $\Lambda = \Lambda(\mathbf{f})$, $\lambda_i = \lambda_i(\mathbf{A}, \mathbf{f})$ *and* $\mathbf{g}_i = \mathbf{g}_i(\mathbf{A}, \mathbf{f})$ *be as before. Let* $1 \leqq h < n$ *and* $S_h(\mathbf{A}, \mathbf{f})$ *be the subspace spanned by* $\mathbf{g}_1, \ldots, \mathbf{g}_h$. *Put*

$$l = \binom{n}{h},$$

suppose that $0 < \delta < 8l(s+1)$,

(13. 1) $$m > 960^2 n^2 l^6 (s+1)^4 \delta^{-2} \log(2l(s+1)d)$$

and put

(13. 2) $$E = \frac{1}{12} 2^m (180)^{2^{m-1}}.$$

Then for values $A_1, \ldots, A_n, f_{11}, \ldots, f_{ns}, Q$ *with*

(13. 3) $$Q^{\delta^2} > (2^{4l} H)^{2^{10} d^2 (s+1)^4 m n^2 l^2 E},$$

(13. 4) $$Q \geqq \max\{A_1, \ldots, A_n, A_1^{-1}, \ldots, A_n^{-1}, p_1^{f_{11}}, \ldots, p_s^{f_{ns}}\}$$

and

(13. 5) $$\lambda_h < Q^{-\delta} \lambda_{h+1}$$

$S_h(\mathbf{A}, \mathbf{f})$ *is among not more than*

(13. 6) $$m\left(\frac{144 l n (s+1)^2}{\delta}\right)^{l(s+1)} (1 + 128 l n (s+1)^2 \delta^{-1} \log E)$$

h-dimensional subspaces.

Proof. Put $k = n - h$ and recall from section 7 that $C(n, k)$ is the set of k-tuples $\sigma = \{i_1 < \cdots < i_k\}$ of integers in $1 \leqq i \leqq n$. Define $\boldsymbol{\beta}_\sigma^{(0)}$ by (7. 25) and similarly $\boldsymbol{\beta}_\sigma^{(j)}$ for $j = 1, \ldots, s$. Moreover write

$$A_\sigma = \prod_{i \in \sigma} A_i \quad \text{and} \quad f_{\sigma j} = \prod_{i \in \sigma} f_{ij} \qquad (j = 1, \ldots, s).$$

We apply Lemma 7. 3 with $\boldsymbol{\beta}_i^{(0)} A_i^{-1}$ in place of $\boldsymbol{\beta}_i^{(0)}$. The parallelepiped $\Pi^{(k)}$ given by

$$|\boldsymbol{\beta}_\sigma^{(0)} \mathbf{x}^{(k)}|_0 \leqq A_\sigma \qquad (\sigma \in C(n, k))$$

is the k-th pseudocompound of $\Pi(\mathbf{A})$. The lattice $\Lambda^{(k)}$ defined by

$$|\boldsymbol{\beta}_\sigma^{(j)} \mathbf{x}^{(k)}|_j \leqq p_j^{-f_{\sigma j}} \qquad (\sigma \in C(n, k);\ j = 1, \ldots, s)$$

is the k-th compound of $\Lambda(\mathbf{f})$. Denote the successive minima of $\Pi^{(k)}$ with respect to $\Lambda^{(k)}$ by $v_1, \ldots, v_l$. It is clear that in Lemma 7. 3 we may take

$$\varrho_l = \{n-k+1, n-k+2, \ldots, n\} = \{h+1, h+2, \ldots, n\},$$
$$\varrho_{l-1} = \{n-k, n-k+2, \ldots, n\} = \{h, h+2, \ldots, n\}.$$

Thus Lemma 7. 3 combined with (13. 5) and (13. 3) gives

$$v_{l-1} < (k!)^l l!\, Q^{-\delta} v_l < Q^{-\frac{3}{4}\delta} v_l. \tag{13. 7}$$

By (5. 2) we have

$$H^{-kd} \leqq |\boldsymbol{\beta}_\sigma^{(j)}|_j \leqq 1 \qquad (\sigma \in C(n, k);\ j = 0, \ldots, s). \tag{13. 8}$$

We define the normalized vectors $\boldsymbol{\gamma}_\sigma^{(0)} = |\boldsymbol{\beta}_\sigma^{(0)}|_0^{-1} \boldsymbol{\beta}_\sigma^{(0)}$ and the parallelepiped $N^{(k)}$

$$|\boldsymbol{\gamma}_\sigma^{(0)} \mathbf{x}^{(k)}|_0 \leqq A_\sigma \qquad (\sigma \in C(n, k)).$$

Moreover, for j with $1 \leqq j \leqq s$ we introduce the normalized vectors $\boldsymbol{\gamma}_\sigma^{(j)} = |\boldsymbol{\beta}_\sigma^{(j)}|_j \boldsymbol{\beta}_\sigma^{(j)}$ and the lattice $\Lambda_N^{(k)}$ by

$$|\boldsymbol{\gamma}_\sigma^{(j)} \mathbf{x}^{(k)}|_j \leqq p_j^{-f_{\sigma j}} \qquad (\sigma \in C(n, k);\ j = 1, \ldots, s).$$

Denote the successive minima of $N^{(k)}$ with respect to $\Lambda_N^{(k)}$ by $v_1', \ldots, v_l'$. Now we have

$$\left(\prod_{j=1}^{s} \max_\sigma (|\boldsymbol{\beta}_\sigma^{(j)}|_j^{-1}) \right) \Lambda^{(k)} \subset \Lambda_N^{(k)} \subset \Lambda^{(k)}.$$

Thus by (13. 8) there exists a natural number $b \leqq H^{kds}$ with

$$b\Lambda^{(k)} \subset \Lambda_N^{(k)} \subset \Lambda^{(k)},$$

and also by (13. 8) we get

$$H^{-kd} \Pi^{(k)} \subset N^{(k)} \subset \Pi^{(k)}.$$

Therefore

$$v_i \leqq v_i' \leqq H^{kd(s+1)} v_i \qquad (i = 1, \ldots, l).$$

Together with (13. 7) and (13. 3) this yields

$$v_{l-1}' < H^{kd(s+1)} Q^{-\frac{3}{4}\delta} v_l' < Q^{-\frac{\delta}{2}} v_l'. \tag{13. 9}$$

By Lemma 5. 1, $H(\boldsymbol{\beta}_\sigma^{(j)}) \leqq H^k$ and therefore also $H(\boldsymbol{\gamma}_\sigma^{(j)}) \leqq H^k$ $(\sigma \in C(n, k);\ j = 0, \ldots, s)$. Moreover we have

$$Q^k \geqq \max_\sigma \{A_\sigma, A_\sigma^{-1}, p_1^{f_{\sigma 1}}, \ldots, p_s^{f_{\sigma s}}\}. \tag{13. 10}$$

We may apply Lemma 12. 1 to $N^{(k)}$, $\Lambda_N^{(k)}$ with n, δ, $\boldsymbol{\beta}_i^{(j)}$, H, Q replaced by l, $\delta/2k$, $\boldsymbol{\gamma}_\sigma^{(j)}$, H^k, Q^k respectively. The hypotheses (12. 1), (12. 2), (12. 3), (12. 4) are replaced by (13. 1), (13. 3), (13. 10), (13. 9) respectively. The conclusion is that the subspaces $S^{(k)}$ spanned by the first $l-1$ minimal points of $N^{(k)}$ in $\Lambda_N^{(k)}$ are among a set of not more than (13. 6) subspaces of $\mathbb{R}^l$.

Let again $\mathbf{g}_1, \ldots, \mathbf{g}_n$ be independent points in Λ with $\mathbf{g}_i \in \lambda_i \Pi$ $(i=1, \ldots, n)$. By (7. 29) the points $\mathbf{G}_{\varrho_1}, \ldots, \mathbf{G}_{\varrho_{l-1}}$ lie in

$$k! \lambda_{\varrho_{l-1}} \Pi^{(k)} \subset k! \lambda_{\varrho_{l-1}} H^{kd} N^{(k)}.$$

On the other hand the definition of the compound lattice in section 6 implies that $\mathbf{G}_{\varrho_1}, \ldots, \mathbf{G}_{\varrho_{l-1}}$ lie in $\Lambda^{(k)}$. So $b\mathbf{G}_{\varrho_1}, \ldots, b\mathbf{G}_{\varrho_{l-1}}$ lie in $\Lambda_N^{(k)}$ and in $bk! \lambda_{\varrho_{l-1}} H^{kd} N^{(k)}$, and here $b \leqq H^{kds}$. Now by (13. 5), (7. 28) and (13. 3)

$$k! \lambda_{\varrho_{l-1}} H^{kd(s+1)} < k! H^{kd(s+1)} Q^{-\delta} \lambda_{\varrho_l} \leqq (k!)^l l! H^{kd(s+1)} Q^{-\delta} v_l < v_l \leqq v_l'.$$

Thus $b\mathbf{G}_{\varrho_1}, \ldots, b\mathbf{G}_{\varrho_{l-1}}$ lie in $\Lambda_N^{(k)}$ as well as in the interior of $v_l N^{(k)}$. This implies that $\mathbf{G}_{\varrho_1}, \ldots, \mathbf{G}_{\varrho_{l-1}}$ span $S^{(k)}$ and hence there are not more than (13. 6) possibilities for the span of $\mathbf{G}_{\varrho_1}, \ldots, \mathbf{G}_{\varrho_{l-1}}$ in $\mathbb{R}^l$. By Lemma 7. 4 there are not more than (13. 6) possibilities for the span of $\mathbf{g}_1, \ldots, \mathbf{g}_h$ in $\mathbb{R}^n$, i.e. for S_h.

14. Proof of Proposition B, and hence the Theorem

We introduce a parameter $\mu > 0$. Initially we will study solutions of (4. 6) with

$$|\boldsymbol{\beta}_i^{(0)} \mathbf{x}|_0 > H^{-\mu} |\mathbf{x}|_0^{1-\mu} \qquad (i=1, \ldots, n) \tag{14. 1}$$

and

$$|\boldsymbol{\beta}_i^{(j)} \mathbf{x}|_j > H^{-\mu} |\mathbf{x}|_0^{-\mu} \qquad (i=1, \ldots, n;\ j=1, \ldots, s). \tag{14. 2}$$

Write

$$A_i = A_i(\mathbf{x}) = |\boldsymbol{\beta}_i^{(0)} \mathbf{x}|_0 \Big/ \prod_{j=0}^{s} (|\boldsymbol{\beta}_1^{(j)} \mathbf{x}|_j \cdots |\boldsymbol{\beta}_n^{(j)} \mathbf{x}|_j)^{\frac{1}{n}} \qquad (i=1, \ldots, n),$$

and define nonnegative integers $f_{ij} = f_{ij}(\mathbf{x})$ by

$$|\boldsymbol{\beta}_i^{(j)} \mathbf{x}|_j = p_j^{-f_{ij}} \qquad (i=1, \ldots, n;\ j=1, \ldots, s).$$

Then

$$A_1 \cdots A_n \prod_{j=1}^{s} p_j^{-(f_{1j} + \cdots + f_{nj})} = 1$$

holds true. From $|\boldsymbol{\beta}_i^{(0)} \mathbf{x}|_0 \leqq |\mathbf{x}|_0$ and $|\boldsymbol{\beta}_i^{(j)} \mathbf{x}|_j \leqq 1$ $(j=1, \ldots, s)$ we obtain

$$(H|\mathbf{x}|_0)^{-\mu} \leqq A_i \leqq (H|\mathbf{x}|_0)^{\mu(s+1)} \qquad (i=1, \ldots, n)$$

and

$$1 \leqq p_j^{f_{ij}} \leqq (H|\mathbf{x}|_0)^{\mu} \qquad (i=1, \ldots, n;\ j=1, \ldots, s).$$

Thus with $Q=(H|\mathbf{x}|_0)^{\mu(s+1)}$ we have

$$Q \geqq \max\{A_1, \ldots, A_n, A_1^{-1}, \ldots, A_n^{-1}, p_1^{f_{11}}, \ldots, p_1^{f_{n1}}, \ldots, p_s^{f_{1s}}, \ldots, p_s^{f_{ns}}\}.$$

If we assume moreover that $|\mathbf{x}|_0 > H$, then we get

$$Q=(H|\mathbf{x}|_0)^{\mu(s+1)} < |\mathbf{x}|_0^{2\mu(s+1)}$$

and (4. 6) yields

$$\prod_{j=0}^{s} (|\boldsymbol{\beta}_1^{(j)}\mathbf{x}|_j \cdots |\boldsymbol{\beta}_n^{(j)}\mathbf{x}|_j) < Q^{-\frac{\delta}{2\mu(s+1)}},$$

whence

$$|\boldsymbol{\beta}_i^{(0)}\mathbf{x}|_0 = A_i \prod_{j=0}^{s} (|\boldsymbol{\beta}_1^{(j)}\mathbf{x}|_j \cdots |\boldsymbol{\beta}_n^{(j)}\mathbf{x}|_j)^{\frac{1}{n}} < A_i Q^{-\frac{\delta}{2n\mu(s+1)}}. \tag{14. 3}$$

Thus if $\Pi = \Pi(A_1, \ldots, A_n)$ is the parallelepiped (11. 13) and $\Lambda = \Lambda(f_{11}, \ldots, f_{ns})$ is the lattice (11. 14), then $\mathbf{x}$ lies in $Q^{-\frac{\delta}{2n\mu(s+1)}}\Pi \cap \Lambda$ and the first minimum λ_1 of Π with respect to Λ has $\lambda_1 < Q^{-\delta/(2n\mu(s+1))}$.

On the other hand we have $\lambda_n > (nH^{d(s+1)})^{-1}$ from (7. 2), (6. 22), (8. 12). So if we suppose that

$$|\mathbf{x}|_0^{\delta} > (nH^{d(s+1)})^{6n} \tag{14. 4}$$

then

$$\lambda_n > |\mathbf{x}|_0^{-\delta/6n} \geqq Q^{-\frac{\delta}{6n\mu(s+1)}}. \tag{14. 5}$$

Therefore $\mathbf{x}$ lies in the subspace $S(\mathbf{A}, \mathbf{f})$ spanned by $\mathbf{g}_1, \ldots, \mathbf{g}_q$, where again $\mathbf{g}_i = \mathbf{g}_i(\mathbf{A}, \mathbf{f})$. Let k be minimal such that $\mathbf{x}$ lies in the k-dimensional subspace S_k spanned by $\mathbf{g}_1, \ldots, \mathbf{g}_k$; then $1 \leqq k \leqq q$, and (14. 3) implies $\lambda_k < Q^{-\frac{\delta}{2n\mu(s+1)}}$. By (14. 5) there is an h with $k \leqq h \leqq q$ such that

$$\lambda_h < Q^{-\frac{\delta}{3n^2\mu(s+1)}} \lambda_{h+1}. \tag{14. 6}$$

We want to apply Lemma 13. 1 with $\delta/(3n^2\mu(s+1))$ in place of δ. Since $l = \binom{n}{h} \leqq 2^{n-1}$ and $\log(2l(s+1)d) \leqq \log(2^n(s+1)d) < n\log(2(s+1)d)$, condition (13. 1) will be certainly true if

$$m > 2^{6n+18} n^7 \mu^2 \delta^{-2} (s+1)^6 \log(2(s+1)d). \tag{14. 7}$$

With E given by (13. 2), condition (13. 3) (with δ replaced by $\delta/(3n^2\mu(s+1))$) will hold if

$$Q^{\delta^2} > (2^{4l}H)^{2^{14}d^2(s+1)^6 mn^6 l^2 \mu^2 E}.$$

Since $Q \geqq |\mathbf{x}|_0^{\mu(s+1)}$ this will certainly be true if

$$|\mathbf{x}|_0^{\delta^2} > (2^{2^{n+1}} H)^{2^{12} d^2 (s+1)^5 mn^6 2^{2n} E\mu}. \tag{14. 8}$$

When $0 < \delta < 8l(s+1)^2 3n^2\mu$, so that $\delta/(3n^2\mu(s+1)) < 8l(s+1)$ and $\mu/\delta > (24ln^2(s+1)^2)^{-1}$ we may apply Lemma 13. 1 and conclude that $S_h(\mathbf{A}, \mathbf{f})$ is among not more than

$$m\left(432ln^3(s+1)^3 \frac{\mu}{\delta}\right)^{l(s+1)} \left(1 + 384ln^3(s+1)^3 \frac{\mu}{\delta} \log E\right) \tag{14. 9}$$

subspaces, so that such $\mathbf{x}$ themselves are contained in a collection of not more than this many subspaces. Summing over h in $1 \leqq h < n$, we see that $\mathbf{x}$ with (4. 6), (14. 1), (14. 2), (14. 8) lie in a collection of not more than

$$t_2 = nm\left(216 \cdot 2^{2n}(s+1)^3 \frac{\mu}{\delta}\right)^{2^n(s+1)} \log E \tag{14. 10}$$

subspaces.

Points $\mathbf{x}$ with $\boldsymbol{\beta}_i^{(j)}\mathbf{x} = 0$ for some pair (i, j) $(1 \leqq i \leqq n;\ 0 \leqq j \leqq s)$ lie in a collection of $\leqq n(s+1)$ subspaces. For other integer points $\mathbf{x}$ conditions (14. 1) and (14. 2) are satisfied with $\mu = d$ by Lemma 5. 3. However, if we substitute $\mu = d$ into (14. 10), we obtain a rather bad dependency on d. To improve upon this dependency the following device is useful.

There is a collection of $\leqq n(s+2)$ subspaces containing the integer points lying in a coordinate plane $x_i = 0$ or satisfying $\boldsymbol{\beta}_i^{(j)}\mathbf{x} = 0$ for some pair (i, j). All other points have by Lemma 5. 3

$$|\boldsymbol{\beta}_i^{(0)}\mathbf{x}|_0 \geqq |\mathbf{x}|_0^{1-d} H^{-d} \qquad (i = 1, \ldots, n),$$

and

$$|\boldsymbol{\beta}_i^{(j)}\mathbf{x}|_j \geqq |\mathbf{x}|_0^{-d} H^{-d} \qquad (i = 1, \ldots, n;\ j = 1, \ldots, s).$$

Suppose that

$$10n < \mu < d. \tag{14. 11}$$

First let $\boldsymbol{\beta}^{(0)}$ be one of the vectors $\boldsymbol{\beta}_i^{(0)}$ and assume that we have

$$|\mathbf{x}|_0^{1-\mu} H^{-\mu} \leqq |\boldsymbol{\beta}^{(0)}\mathbf{x}|_0 < |\mathbf{x}|_0^{1-\frac{\mu}{e}} H^{-\frac{\mu}{e}}. \tag{14. 12}$$

Suppose that $\boldsymbol{\beta}^{(0)}$ and $\mathbf{e}_2, \ldots, \mathbf{e}_n$ are linearly independent, where $\mathbf{e}_1, \ldots, \mathbf{e}_n$ are the canonical basis vectors. Then we have

$$|\boldsymbol{\beta}^{(0)}\mathbf{x}|_0 \, |\mathbf{e}_2\mathbf{x}|_0 \cdots |\mathbf{e}_n\mathbf{x}|_0 < |\mathbf{x}|_0^{n-\frac{\mu}{e}} = |\mathbf{x}|_0^{-\delta} \quad \text{with} \quad \delta = \frac{\mu}{e} - n.$$

We want to apply the first part of this section to $\mathbf{\beta}^{(0)}$, $\mathbf{e}_2, \ldots, \mathbf{e}_n$ i.e. for $s=0$. Since $\delta < 8/3n^2\mu$, this is possible. Therefore points $\mathbf{x}$ with (14. 8) (for $s=0$) and (14. 12) lie in a collection of not more than t_2 subspaces. But $\frac{\delta}{\mu} = \frac{1}{e} - \frac{n}{\mu} > \frac{1}{4}$ so that $\frac{\mu}{\delta} < 4$ and we obtain less than

$$t_3 = nm(864 \cdot 2^{2n})^{2^n} \log E$$

subspaces. With our present values of μ, δ, s the relations (14. 7), (14. 8) will hold if

$$m > 2^{6n+22} n^7 \log(2d), \tag{14. 13}$$

$$|\mathbf{x}|_0 > (2^{2^{n+1}} H)^{2^{16} d^2 m n^6 2^{2n} E}. \tag{14. 14}$$

Next let $\mathbf{\beta}^{(j)}$ be one of the vectors $\mathbf{\beta}_i^{(j)}$ $(i=1, \ldots, n;\ j=1, \ldots, s)$. Assume that with μ as in (14. 11) we have

$$|\mathbf{x}|_0^{-\mu} H^{-\mu} \leqq |\mathbf{\beta}^{(j)} \mathbf{x}|_j < |\mathbf{x}|_0^{-\frac{\mu}{e}} H^{-\frac{\mu}{e}}. \tag{14. 15}$$

Suppose again without loss of generality that $\mathbf{\beta}^{(j)}, \mathbf{e}_2, \ldots, \mathbf{e}_n$ are linearly independent. Then we have

$$|\mathbf{e}_1 \mathbf{x}|_0 \cdots |\mathbf{e}_n \mathbf{x}|_0 \, |\mathbf{\beta}^{(j)} \mathbf{x}|_j \, |\mathbf{e}_2 \mathbf{x}|_j \cdots |\mathbf{e}_n \mathbf{x}|_j < |\mathbf{x}|_0^{n - \frac{\mu}{e}} = |\mathbf{x}|_0^{-\delta},$$

where again $\delta = \frac{\mu}{e} - n$ and hence $\frac{\mu}{\delta} < 4$. Again, we apply the first part of this section, this time with $s=1$ and we obtain less than

$$t_4 = nm(6912 \cdot 2^{2n})^{2^{n+1}} \log E$$

subspaces. With our present values of μ, δ, s the relations (14. 7), (14. 8) will hold if

$$m > 2^{6n+28} n^7 \log(4d), \tag{14. 16}$$

$$|\mathbf{x}|_0 > (2^{2^{n+1}} H)^{2^{19} d^2 m n^6 2^{2n} E}. \tag{14. 17}$$

Now if $10n < d$ we carry this out with $\mu = \mu_1, \ldots, \mu_w$ where $\mu_i = de^{1-i}$ and $w = [\log(d/10n)]$. Then we see that points $\mathbf{x}$ with

$$|\mathbf{\beta}^{(0)} \mathbf{x}|_0 < |\mathbf{x}|_0^{1-(\mu_w/e)} H^{-(\mu_w/e)}$$

and with (14. 14) lie in not more than wt_3 subspaces, whereas points $\mathbf{x}$ with

$$|\mathbf{\beta}^{(j)} \mathbf{x}|_j < |\mathbf{x}|_0^{-(\mu_w/e)} H^{-(\mu_w/e)}$$

for some j $(1 \leqq j \leqq s)$ and with (14. 17) lie in not more than wt_4 subspaces.

We now return to (4. 6). For each pair (i, j) $(1 \leqq i \leqq n;\ 0 \leqq j \leqq s)$, we treat $\boldsymbol{\beta}_i^{(j)}$ in the way just described. Thus if we exclude not more than

$$n(s+2)+nwt_3+nwst_4$$

subspaces, then (14. 1), (14. 2) will hold with $\mu = \mu_w/e \leqq 10en$. Hence it holds with $\mu = 10en$. This was when $10n < d$; but when $d \leqq 10n$, then (14. 1), (14. 2) hold with $\mu = 10en$ anyhow.

We may apply the first part of this section with $\mu = 10en$, and we obtain

$$t_2 < nm(6000n2^{2n}(s+1)^3\delta^{-1})^{2n(s+1)}\log E$$

subspaces. With our present value of μ, the conditions (14. 7), (14. 8) will hold if

$$m > 800 \cdot 2^{18}n^9 2^{6n}(s+1)^6\delta^{-2}\log(2(s+1)d), \tag{14. 18}$$

$$|\mathbf{x}|_0 > (2^{2^{n+1}}H)^{2^{17}d^2(s+1)^5mn^7 2^{2n}\delta^{-2}E}. \tag{14. 19}$$

Collecting everything together, we have not more than

$$n(s+2)+nwt_3+nwt_4+t_2$$

subspaces. For $s \geqq 1$ this expression is

$$\begin{aligned} &< n(s+2)+n^2wm(864\cdot 2^{2n})^{2^n}\log E + n^2wms(6912\cdot 2^{2n})^{2^{n+1}}\log E \\ &\quad + nm(6000n2^{2n}(s+1)^3\delta^{-1})^{2n(s+1)}\log E \qquad (14.\ 20) \\ &< n^2m(\log 3d)\,(2^{13}n2^{2n}(s+1)^3\delta^{-1})^{2n(s+1)}\log E. \end{aligned}$$

We now choose m minimal with (14. 18) and get

$$2^m < (2(s+1)d)^{2^{28}n^9 2^{6n}(s+1)^6\delta^{-2}}.$$

In conjunction with (11. 2) this yields

$$\log E < (2(s+1)d)^{2^{28,5}n^9 2^{6n}(s+1)^6\delta^{-2}}.$$

Combining the last relation with (14. 20), we see that the number of subspaces is

$$< (2(s+1)d)^{2^{29}n^9 2^{6n}(s+1)^6\delta^{-2}} \leqq (2(s+1)d)^{2^{25}n(s+1)^6\delta^{-2}} = t_1.$$

As for the norm of $\mathbf{x}$, we observe that

$$2^{18} d^2 (s+1)^5 m n^7 2^{3n} \delta^{-2} E < e^{t_1}.$$

Therefore condition (14. 19) (and a fortiori also the weaker conditions (14. 14), (14. 17)) hold true if

$$|\mathbf{x}|_0 = |\mathbf{x}| > (2H)^{e^{t_1}}.$$

This finishes the proof of Proposition B and therefore also of the Theorem.

References

[1] *E. Bombieri* and *A. J. van der Poorten*, Some quantitative results related to Roth's Theorem, Mac Quarie Math. Reports, Report No. 87-0005, February 1987.
[2] *J. W. S. Cassels*, An introduction to the geometry of numbers, Berlin-Göttingen-Heidelberg, Second Printing 1971.
[3] *H. Davenport* and *K. F. Roth*, Rational approximation to algebraic numbers, Mathematika **2** (1955), 160—167.
[4] *H. Esnault* and *E. Viehweg*, Dyson's Lemma for polynomials in several variables (and the theorem of Roth), Invent. Math. **78** (1984), 445—490.
[5] *W. H. Greub*, Multilinear Algebra, Berlin-Göttingen-Heidelberg 1967.
[6] *H. Luckhardt*, Herbrand-Analysen zweier Beweise des Satzes von Roth; polynomiale Anzahlschranken, Journ. of Symb. Logic **54** (1989), 234—263.
[7] *K. Mahler*, Ein Übertragungsprinzip für konvexe Körper, Casopis Pest. Mat. Fys. **68** (1939), 93—102.
[8] *K. Mahler*, On compound convex bodies I, Proc. London Math. Soc. (3) **5** (1955), 358—379.
[9] *D. Ridout*, The *p*-adic generalization of the Thue-Siegel-Roth theorem, Mathematika **5** (1958), 40—48.
[10] *K. F. Roth*, Rational approximations to algebraic numbers, Mathematika **2** (1955), 1—20.
[11] *H. P. Schlickewei*, Linearformen mit algebraischen Koeffizienten, Manuscripta Math. **18** (1976), 147—185.
[12] *H. P. Schlickewei*, The p-adic Thue-Siegel-Roth-Schmidt theorem, Arch. Math. **29** (1977), 267—270.
[13] *W. M. Schmidt*, Norm form equations, Ann. of Math. **96** (1972), 526—551.
[14] *W. M. Schmidt*, Diophantine approximations, Lect. Notes in Math. **785**, Berlin-Heidelberg-New York 1980.
[15] *W. M. Schmidt*, The subspace theorem in diophantine approximations, Comp. Math. **69** (1989), 121—173.
[16] *E. Weiss*, Algebraic number theory, New York-San Francisco-Toronto-London 1963.

Abteilung Mathematik II der Universität, Oberer Eselsberg, D-7900 Ulm

Eingegangen 23. Mai 1989

J. reine angew. Math. **406** (1990), 109—120

Journal für die reine und angewandte Mathematik

An explicit upper bound for the number of solutions of the S-unit equation

By *Hans Peter Schlickewei* at Ulm

1. Introduction

In 1933 Mahler [5] proved the following result.

Let M_1, M_2, M_3 be disjoint nonempty finite sets of rational primes. Then the equation

$$x_1 + x_2 + x_3 = 0$$

where the x_i are integers only divisible by primes in M_i $(i = 1, 2, 3)$ has only finitely many solutions.

This was extended to equations

$$x_1 + \ldots + x_n + x_{n+1} = 0 \tag{1. 1}$$

independently of each other by Dubois and Rhin [1] and by Schlickewei [7]. They assumed that given a finite set of primes M, the x_i are only divisible by primes in M and that for each pair (i, j) with $i \neq j$, $(x_i, x_j) = 1$, and showed that under these hypotheses (1. 1) has only finitely many solutions.

It turned out that asking for pairwise coprimality of the components of the solutions was too severe. In fact independently of each other van der Poorten and Schlickewei [6] and Evertse [2] proved that (1. 1) has only finitely many integral solutions $\mathbf{x} = (x_1, \ldots, x_n, x_{n+1})$ where each x_i is only composed by primes in M, where g.c.d. $(x_1, \ldots, x_{n+1}) = 1$ and where no proper subsum $x_{i_1} + \ldots + x_{i_m}$ vanishes. It is well known that these conditions are necessary and sufficient. Let us mention that under similar assumptions also the number field case and the case where the x_i lie in a finitely generated multiplicative subgroup contained in $\mathbb{C}$ have been settled. All these results depend essentially upon the p-adic generalization of W. Schmidt's Subspace Theorem proved by Schlickewei [8].

Recently W. Schmidt in his pioneering paper [10] gave a quantitative version of his Subspace Theorem. This in turn was generalized by Schlickewei [9] to include p-adic valuations. In this paper we will apply the main result of [9] to derive an explicit upper bound for the number of solutions of the equation

$$a_1 x_1 + a_2 x_2 + \ldots + a_{n+1} x_{n+1} = 0. \tag{1.2}$$

Here the a_i are supposed to be fixed rational integers and the x_i are integers which are only composed by primes lying in a fixed finite set.

Let $S = \{0, p_1, \ldots, p_s\}$, where $p_1, \ldots, p_s$ are s rational primes. For $v \in S$ we denote by $|\ |_v$ the v-adic absolute value on $\mathbb{Q}$, where $v = 0$ stands for the standard absolute value. An element $x \in \mathbb{Q}$ is called an S-unit if $\prod_{v \in S} |x|_v = 1$.

Theorem. *Let S be as above. Then for $n \geqq 1$ the number of integral solutions $\mathbf{x} = (x_1, \ldots, x_{n+1})$ of (1.2) where the x_i are S-units $(i = 1, \ldots, n+1)$ with*

$$\text{g.c.d.}\ (x_1, \ldots, x_{n+1}) = 1$$

such that no proper subsum $a_{i_1} x_{i_1} + \ldots + a_{i_m} x_{i_m}$ vanishes is bounded by

$$(8(s+1))^{2^{26n+4}(s+1)^6}.$$

Notice that our bound does not depend upon the coefficients $a_1, \ldots, a_{n+1}$ in (1.2) and that the dependence upon the set S is only via the parameter s, but not via the particular primes $p_1, \ldots, p_s$ involved.

The special case $n = 2$ of the Theorem has been proved by Evertse [3]. He gets a better bound than we do. In fact he shows that for $n = 2$ (1.2) has not more than $3 \cdot 7^{2s+1}$ primitive solutions. Silverman [11] showed that for $n = 2$ and $a_1 = a_2 = a_3 = 1$ the number of solutions is bounded by $C \cdot 2^{20s}$, where C is an absolute constant. For $n \geqq 2$, Evertse and Győry [4] showed, that the number of solutions of (1.2) is below some constant which does not depend upon the coefficients a_i. But their method of proof does not allow one to determine how this constant depends upon S and n.

In forthcoming work we will extend the Theorem to include the number field case and even more general situations.

2. A gap principle

Lemma 2.1. *Let $q = (n-1)(s+1)$. Define the set M by*

$$M = \left\{(c_1, \ldots, c_q) \mid c_1 + \ldots + c_q = \frac{2n+1}{2n+2},\ c_i \geqq 0\ (i = 1, \ldots, q)\right\}.$$

There exists a subset M' of M with the following properties.

(i) *M' has cardinality at most $(2e(n+1))^{q-1}$.*

(ii) *For any set of real tuples* $(A_1, B_1), \ldots, (A_q, B_q)$ *with* $0 < A_i \leqq B_i$ $(1 \leqq i \leqq q)$ *and any real number* E *such that* $\prod_{i=1}^{q} A_i \leqq E \prod_{i=1}^{q} B_i$ *there exists a tuple* $(c_1, \ldots, c_q) \in M'$ *satisfying*

$$A_i \leqq E^{c_i} B_i \quad (i = 1, \ldots, q). \tag{2. 1}$$

This is a special case of Lemma 4 of [3]. With the notation of [3] we have to take $B = \frac{2n+1}{2n+2}$, $F_i = A_i/B_i$ $(i = 1, \ldots, q)$.

When we study equation (1. 2) we may suppose without loss of generality that the coefficient vector $\mathbf{a} = (a_1, \ldots, a_{n+1})$ has

$$\text{g.c.d.}\,(a_1, \ldots, a_{n+1}) = 1. \tag{2. 2}$$

In fact as for the primes $p_1, \ldots, p_s$ we may even suppose that for each i $(1 \leqq i \leqq n+1)$ and each $v \in S$, $v \neq 0$ we have

$$|a_i|_v = 1. \tag{2. 3}$$

After renumbering the variables if necessary we may assume moreover that

$$|a_1|_0 \geqq |a_2|_0 \geqq \ldots \geqq |a_{n+1}|_0 > 0 \tag{2. 4}$$

holds true.

Let $M(\mathbb{Q})$ be the set of prime divisors of $\mathbb{Q}$. For a vector $\mathbf{y} = (y_1, \ldots, y_{n+1}) \in \mathbb{Q}^{n+1}$ and for $v \in M(\mathbb{Q})$ put

$$|\mathbf{y}|_v = \begin{cases} (y_1^2 + \ldots + y_{n+1}^2)^{1/2} & \text{if } v \text{ is archimedean,} \\ \max\{|y_1|_v, \ldots, |y_{n+1}|_v\} & \text{if } v \text{ is nonarchimedean} \end{cases}$$

and

$$h(\mathbf{y}) = \prod_{v \in M(\mathbb{Q})} |\mathbf{y}|_v.$$

Then for $\mathbf{a}$ with (2. 2), (2. 4) we get

$$|a_1|_0 \leqq h(\mathbf{a}) = (a_1^2 + \ldots + a_{n+1}^2)^{1/2} \leqq (n+1)\,|a_1|_0. \tag{2. 5}$$

Lemma 2. 2. *Suppose* $\mathbf{a}$ *satisfies* (2. 2), (2. 3), (2. 4). *Put* $H = |a_1 \cdots a_{n+1}|_0$. *Let* C *be a quantity with*

$$C \geqq n^{2(n+3)}. \tag{2. 6}$$

Then the solutions $\mathbf{x}=(x_1, \ldots, x_n, x_{n+1})$ *of* (1. 2), *where for each* i $(1 \leqq i \leqq n+1)$ x_i *is an S-unit and which satisfy*

$$C \leqq h((a_1 x_1, \ldots, a_{n+1} x_{n+1})) \leqq C H^{(1/2n^2)} \tag{2. 7}$$

are contained in the union of not more than

$$(2e(n+1))^{(n+1)(s+1)-1} \tag{2. 8}$$

subspaces each of which is defined by an equation of the type

$$b_1 x_1 + \ldots + b_n x_n = 0.$$

Proof. Let $\mathbf{x}$ be a solution of (1. 2). Given $v \in S$ let $k(v)$ be a subscript with

$$|a_{k(v)} x_{k(v)}|_v \geqq |a_i x_i|_v \quad \text{for each } i \ (1 \leqq i \leqq n+1).$$

Moreover let $l(v)$ be a subscript with

$$|a_{l(v)} x_{l(v)}|_v \geqq |a_i x_i|_v \quad \text{for each } i \text{ with } i \neq k(v).$$

Define $J_v = \{1, \ldots, n+1\} \setminus \{l(v), k(v)\}$. Divide the set of solutions of (1. 2) into classes $K = K(J_0, \ldots, J_s)$, where $\mathbf{x}$ belongs to $K(J_0, \ldots, J_s)$ if it gives rise to $J_0, \ldots, J_s$ in the way described above. Notice that there are

$$\left(\frac{n(n+1)}{2}\right)^{s+1} \tag{2. 9}$$

classes K. In view of (1. 2) we obtain

$$|a_{k(v)} x_{k(v)}|_v = \left| \sum_{\substack{i=1 \\ i \neq k(v)}}^{n+1} a_i x_i \right|_v.$$

Thus we get

$$|a_{k(v)} x_{k(v)}|_v \leqq \begin{cases} n |a_{l(v)} x_{l(v)}|_v & \text{if } v = 0, \\ |a_{l(v)} x_{l(v)}|_v & \text{if } v \in S, \ v \neq 0. \end{cases} \tag{2. 10}$$

Write $A\mathbf{x} = (a_1 x_1, \ldots, a_{n+1} x_{n+1})$. Then clearly we have

$$0 < |a_i x_i|_v \leqq |A\mathbf{x}|_v \quad \text{for each } v \in S \text{ and for each } i. \tag{2. 11}$$

Moreover for $n \geqq 2$ (which we may assume throughout) we get

$$n |a_{k(0)} x_{k(0)}|_0 \geqq |A\mathbf{x}|_0 \tag{2. 12}$$

and

$$|a_{k(v)} x_{k(v)}|_v = |A\mathbf{x}|_v \quad \text{for each } v \in S, \ v \neq 0. \tag{2. 13}$$

Notice that in view of (2. 2) and since the x_i are S-units we have

$$\prod_{v \in S} |A\mathbf{x}|_v = h(A\mathbf{x}).$$

Combining this with (2. 3) we obtain

$$\text{(2. 14)} \qquad \prod_{v \in S} (|a_1 x_1|_v \cdots |a_{n+1} x_{n+1}|_v) = H = H h(A\mathbf{x})^{-n-1} \prod_{v \in S} |A\mathbf{x}|_v^{n+1}.$$

Cancelling on both sides of (2. 14)

$$\prod_{v \in S} (|a_{k(v)} x_{k(v)}|_v \, |a_{l(v)} x_{l(v)}|_v)$$

and using (2. 10), (2. 12), (2. 13) we get

$$\text{(2. 15)} \qquad \prod_{v \in S} \Big(\prod_{i \in J_v} |a_i x_i|_v \Big) \leqq n^3 H h(A\mathbf{x})^{-n-1} \prod_{v \in S} |A\mathbf{x}|_v^{n-1}.$$

We now apply Lemma 2. 1. The quantities $|a_i x_i|_v$ with $v \in S$, $i \in J_v$ play the rôle of the A_i, the quantities $|A\mathbf{x}|_v$ with $v \in S$ play the rôle of the B_i and we put $E = n^3 H h(A\mathbf{x})^{-n-1}$. Relabelling the numbers $c_1, \ldots, c_q$ as c_{iv} $(v \in S,\ i \in J_v)$ we may infer that there exists a tuple $(c_{iv})_{v \in S,\, i \in J_v}$ in M' such that

$$\text{(2. 16)} \qquad |a_i x_i|_v \leqq E^{c_{iv}} |A\mathbf{x}|_v$$

holds true for each $v \in S$ and each $i \in J_v$. We subdivide each class $K = K(J_0, \ldots, J_s)$ of solutions into subclasses $K(J_0, \ldots, J_s, (c_{iv}))$ where (c_{iv}) runs through M'. Two solutions $\mathbf{x}$ and $\mathbf{x}'$ belong to the same subclass if they satisfy (2. 16) with the same tuple (c_{iv}). In view of (2. 9) and of Lemma 2. 1 the total number of subclasses is

$$< \left(\frac{n(n+1)}{2} \right)^{s+1} (2e(n+1))^{(n-1)(s+1)-1} < (2e(n+1))^{(n+1)(s+1)-1}.$$

We will show that each subclass of solutions is contained in an $(n-1)$-dimensional subspace of $\mathbb{Q}^{n+1}$, and naturally this implies the assertion of the Lemma. In fact let $\mathbf{x}_1, \ldots, \mathbf{x}_n$ be n solutions in the same subclass. Assume without loss of generality that $h(A\mathbf{x}_1) = \min\{h(A\mathbf{x}_1), \ldots, h(A\mathbf{x}_n)\}$. Write $\mathbf{x}_k = (x_{k1}, \ldots, x_{k,n+1})$ $(k = 1, \ldots, n)$. Then by (2. 16) we get

$$|a_i x_{ki}|_v \leqq (n^3 H h(A\mathbf{x}_k)^{-n-1})^{c_{iv}} |A\mathbf{x}_k|_v \qquad (v \in S,\ i \in J_v)$$

and thus putting $E_1 = n^3 H h(A\mathbf{x}_1)^{-n-1}$

$$\text{(2. 17)} \qquad |a_i x_{ki}|_v \leqq E_1^{c_{iv}} |A\mathbf{x}_k|_v \qquad (v \in S,\ i \in J_v).$$

Consider the matrix

$$\begin{pmatrix} a_1 x_{11} & \cdots & a_1 x_{n1} \\ \vdots & & \vdots \\ a_{n+1} x_{1,n+1} & \cdots & a_{n+1} x_{n,n+1} \end{pmatrix}.$$

Let $i_1 < i_2 < \ldots < i_n$ be elements of $\{1, \ldots, n+1\}$ and denote by $D(i_1, \ldots, i_n)$ the $(n \times n)$-subdeterminant corresponding to the rows with subscripts $i_1, \ldots, i_n$. Since the $\mathbf{x}_k$ satisfy (1. 2) we see that for any choice of $i_1, \ldots, i_n$ and for each $v \in M(\mathbb{Q})$ we have

$$|D(i_1, \ldots, i_n)|_v = |D(1, \ldots, n)|_v. \tag{2. 18}$$

Given $v \in S$ choose $i_1, \ldots, i_n$ in such a way that $J_v \subset \{i_1, \ldots, i_n\}$. Now for $v = 0$ (2. 17) in conjunction with (2. 11) yields

$$|D(i_1, \ldots, i_n)|_0 \leqq n! E_1^{\sum_{i \in J_0} c_{i0}} \prod_{j=1}^{n} |A\mathbf{x}_j|_0. \tag{2. 19}$$

On the other hand for $v \in S$ with $v \neq 0$ we get again by (2. 17)

$$|D(i_1, \ldots, i_n)|_v \leqq E_1^{\sum_{i \in J_v} c_{iv}} \prod_{j=1}^{n} |A\mathbf{x}_j|_v. \tag{2. 20}$$

Remember that in Lemma 2. 1 we required that

$$\sum_{v \in S} \sum_{i \in J_v} c_{iv} = \frac{2n+1}{2n+2}.$$

Therefore (2. 18), (2. 19), (2. 20) imply

$$\prod_{v \in S} |D(1, 2, \ldots, n)|_v \leqq n! E_1^{(2n+1)/(2n+2)} \prod_{j=1}^{n} \prod_{v \in S} |A\mathbf{x}_j|_v. \tag{2. 21}$$

Next we treat $v \notin S$. From (2. 2) we infer that there exists an $i(v)$ with $1 \leqq i(v) \leqq n+1$ and $|a_{i(v)}|_v = 1$. Choose $\{i_1, \ldots, i_n\} = \{1, \ldots, n+1\} \setminus \{i(v)\}$. Moreover since we are asking for solutions in S-units for such v we have $|x_{ki}|_v = 1$ for each i $(1 \leqq i \leqq n+1)$ and for each k $(1 \leqq k \leqq n)$. So we obtain

$$|D(i_1, \ldots, i_n)|_v \leqq |a_{i_1} \cdots a_{i_n}|_v = |a_1 \cdots a_{n+1}|_v$$

and finally using (2. 3), (2. 18)

$$\prod_{v \notin S} |D(1, \ldots, n)|_v \leqq \prod_{v \notin S} |a_1 \cdots a_{n+1}|_v = H^{-1}. \tag{2. 22}$$

Combination of (2. 21) and (2. 22) yields

$$\begin{aligned} \prod_{v \in M(Q)} |D(1, \ldots, n)|_v &\leqq n!\, E_1^{(2n+1)/(2n+2)} H^{-1} \prod_{j=1}^{n} h(A\mathbf{x}_j) \\ &= n!\, n^{\frac{3(2n+1)}{2(n+1)}} H^{\frac{2n+1}{2n+2}-1} h(A\mathbf{x}_1)^{-\frac{2n+1}{2}} \prod_{j=1}^{n} h(A\mathbf{x}_j). \end{aligned}$$

But (2. 7) implies that

$$h(A\mathbf{x}_j) \leqq H^{(1/2n^2)} h(A\mathbf{x}_1)$$

and we obtain using (2. 6), (2. 7)

$$\prod_{v \in M(Q)} |D(1, \ldots, n)|_v < n^{n+3} H^{-\frac{1}{2n+2}+\frac{n-1}{2n^2}} h(A\mathbf{x}_1)^{-n-\frac{1}{2}+n} < 1.$$

We may conclude that $D(1, \ldots, n) = 0$. Therefore $\mathbf{x}_1, \ldots, \mathbf{x}_n$ are linearly dependent and Lemma 2. 2 follows.

3. The Subspace Theorem

We shall quote here a special version of the quantitative p-adic Subspace Theorem of Schlickewei [9]. Let $\mathbf{x}' = (x_1, \ldots, x_n)$ and $|\mathbf{x}'| = (x_1^2 + \ldots + x_n^2)^{1/2}$. Given a linear form $L(\mathbf{x}') = \lambda_1 x_1 + \ldots + \lambda_n x_n$ put $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_n)$ and $H(L) = h(\boldsymbol{\lambda})$.

Lemma 3. 1. *Let $S = \{0, p_1, \ldots, p_s\}$ be as above. Suppose that for each $v \in S$ we are given linearly independent linear forms $L_1^{(v)}, \ldots, L_n^{(v)}$ in n variables with rational coefficients. Let $0 < \delta < 1$. Consider the inequality*

$$\prod_{v \in S} |L_1^{(v)}(\mathbf{x}') \cdots L_n^{(v)}(\mathbf{x}')|_v < \prod_{v \in S} |\det(L_1^{(v)}, \ldots, L_n^{(v)})|_v \, |\mathbf{x}'|^{-\delta} \tag{3. 1}$$

where $\det(L_1^{(v)}, \ldots, L_n^{(v)})$ denotes the determinant of the coefficient matrix of $L_1^{(v)}, \ldots, L_n^{(v)}$. Then there are proper subspaces $T_1, \ldots, T_t$ of $\mathbb{Q}^n$ with

$$t \leqq (8(s+1))^{2^{26n(s+1)^6\delta^{-2}}} \tag{3. 2}$$

such that every rational integral solution $\mathbf{x}'$ of (3. 1) either lies in one of these subspaces, or has norm

$$|\mathbf{x}'| < \max\{n!^{8/\delta}, H(L_1^{(v)}), \ldots, H(L_n^{(v)}) \ (v \in S)\}. \tag{3. 3}$$

This is a rather special instance of the main result of [9] which is suitable in our context. As an application of Lemma 3. 1 we derive

Lemma 3. 2. *There are*

$$t_1 = (8(s+1))^{2^{26n}\cdot(s+1)^6\cdot 4} n^{s+1} \tag{3. 4}$$

subspaces $T_1, \ldots, T_{t_1}$ *of* $\mathbb{Q}^n$ *each of the type*

$$b_1 x_1 + \ldots + b_n x_n = 0$$

such that for every solution $\mathbf{x} = (x_1, \ldots, x_n, x_{n+1}) = (\mathbf{x}', x_{n+1})$ *of* (1. 2) *either* $\mathbf{x}'$ *lies in one of these subspaces or satisfies*

$$|\mathbf{x}'| < \max\{n!^{16}, n|a_1|_0\}. \tag{3. 5}$$

Proof. Consider the linear forms

$$\begin{cases} L_1(\mathbf{x}') &= a_1 x_1, \\ &\vdots \\ L_n(\mathbf{x}') &= a_n x_n, \\ L_{n+1}(\mathbf{x}') &= a_1 x_1 + \ldots + a_n x_n. \end{cases} \tag{3. 6}$$

Notice that here for any choice of $i_1 < i_2 < \ldots < i_n$ in $\{1, \ldots, n+1\}$ the forms $L_{i_1}, \ldots, L_{i_n}$ are linearly independent and have determinant $\pm a_1 \cdots a_n$. Notice moreover that in view of (1. 2) we have for any solution $\mathbf{x} = (\mathbf{x}', x_{n+1})$

$$L_{n+1}(\mathbf{x}') = -a_{n+1} x_{n+1}. \tag{3. 7}$$

Since we are only interested in solutions $\mathbf{x}$ with g.c.d. $(x_1, \ldots, x_n, x_{n+1}) = 1$ and since the x_i are supposed to be S-units, we infer from (2. 3) that

$$\text{g.c.d.}\,(x_1, \ldots, x_n) = 1. \tag{3. 8}$$

We now divide the solutions $\mathbf{x}$ into classes as follows. Given a solution $\mathbf{x}$ and $v \in S$ define $i(v)$ with $1 \leqq i(v) \leqq n$ by

$$|x_{i(v)}|_v = \max\{|x_1|_v, \ldots, |x_n|_v\}. \tag{3. 9}$$

Put $J(i(v)) = \{1, \ldots, n+1\} \setminus \{i(v)\}$. For $v = p_j \in S$ it will be convenient to use sometimes instead of v simply the subscript j. Now given a tuple $(i(0), \ldots, i(s))$ let

$$K(J(i(0)), \ldots, J(i(s)))$$

be the class of solutions $\mathbf{x}$ satisfying (3. 9) for this tuple. There are

$$n^{s+1} \tag{3. 10}$$

such classes.

Fix one such class and denote it for simplicity by $K(J(0), \ldots, J(s))$. We shall now study the solutions $\mathbf{x}$ in this class. (3. 8) and (3. 9) imply that for j with $1 \leqq j \leqq s$ we have

$$|x_{i(j)}|_j = 1. \tag{3. 11}$$

By our assumptions about $a_1, \ldots, a_{n+1}$ and $\mathbf{x}$ we get with (3. 4)

$$\prod_{j=0}^{s} (|a_1 x_1|_j \cdots |a_{n+1} x_{n+1}|_j) = \prod_{j=0}^{s} |L_1(\mathbf{x}') \cdots L_{n+1}(\mathbf{x}')|_j = |a_1 \cdots a_{n+1}|_0.$$

Cancelling on both sides $|a_{i(j)} x_{i(j)}|_j$ $(j = 0, \ldots, s)$ and using (2. 3), (3. 11) we obtain

$$\prod_{j=0}^{s} \left(\prod_{i \in J(j)} |L_i(\mathbf{x}')|_j \right) = \frac{|a_1 \cdots a_{n+1}|_0}{|a_{i(0)}|_0} |x_{i(0)}|_0^{-1}. \tag{3. 12}$$

But $|\mathbf{x}'| = (x_1^2 + \ldots + x_n^2)^{1/2} < n |x_{i(0)}|_0$, moreover by (2. 4)

$$|a_1 \cdots a_{n+1}|_0 \, |a_{i(0)}|_0^{-1} \leqq |a_1 \cdots a_n|_0.$$

On the other hand we have for $1 \leqq j \leqq s$ $|a_1 \cdots a_n|_j = 1$. Thus we infer from (3. 12) that

$$\prod_{j=0}^{s} \left(\prod_{i \in J(j)} |L_i(\mathbf{x}')|_j \right) \leqq \left(\prod_{j=0}^{s} |a_1 \cdots a_n|_j \right) n |\mathbf{x}'|^{-1}.$$

In view of (3. 5) we may suppose that $|\mathbf{x}'| > n^2$, and finally we get

$$\prod_{j=0}^{s} \left(\prod_{i \in J(j)} |L_i(\mathbf{x}')|_j \right) < \left(\prod_{j=0}^{s} |a_1 \cdots a_n|_j \right) |\mathbf{x}'|^{-(1/2)}. \tag{3. 13}$$

The expression in (3. 13) is of the same shape as (3. 1) in the Subspace Theorem. Here we have $\delta = 1/2$. As for the heights of the forms L_i in (3. 6) we see that

$$H(L_1) = \ldots = H(L_n) = 1,$$

whereas $H(L_{n+1}) = (a_1^2 + \ldots + a_n^2)^{1/2} \leqq n |a_1|_0$ by (2. 2). Therefore the Subspace Theorem says that for our solutions $\mathbf{x} = (\mathbf{x}', x_{n+1})$ the points $\mathbf{x}'$ are contained in the union of not more than

$$(8(s+1))^{2^{26n} \cdot (s+1)^6 \cdot 4}$$

subspaces or satisfy

$$|\mathbf{x}'| < \max \{n!^{16}, n |a_1|_0\}.$$

We still have to sum up over the different classes. This introduces the extra factor n^{s+1} from (3. 10).

Lemma 3. 3. *There are*

$$t_2 \leqq 4n^2(2e(n+1))^{(n+1)(s+1)-1} + (2n)^{16n^2} \tag{3. 14}$$

subspaces $U_1, \ldots, U_{t_2}$ *of* $\mathbb{Q}^n$ *each of the type*

$$b_1 x_1 + \ldots + b_n x_n = 0$$

such that for every solution $\mathbf{x} = (\mathbf{x}', x_{n+1})$ *of* (1. 2) *with*

$$|\mathbf{x}'| < \max\{n!^{16}, n|a_1|_0\} \tag{3. 15}$$

$\mathbf{x}'$ *lies in one of these subspaces.*

Proof. If $n|a_1|_0 \leqq n!^{16}$, then clearly $(2n)^{16n^2}$ subspaces will suffice. Thus we may suppose that

$$n|a_1|_0 > n!^{16}. \tag{3. 16}$$

From (2. 2), (2. 3), (2. 4) we infer that

$$\begin{aligned} h((a_1 x_1, \ldots, a_{n+1} x_{n+1})) &= (a_1^2 x_1^2 + \ldots + a_n^2 x_n^2 + a_{n+1}^2 x_{n+1}^2)^{1/2} \\ &= (a_1^2 x_1^2 + \ldots + a_n^2 x_n^2 + (a_1^2 x_1^2 + \ldots + a_n^2 x_n^2))^{1/2} \\ &\leqq (n+1)\,|a_1|_0\,(x_1^2 + \ldots + x_n^2)^{1/2} = (n+1)\,|a_1|_0\,|\mathbf{x}'|. \end{aligned} \tag{3. 17}$$

Moreover we have by (3. 16)

$$h((a_1 x_1, \ldots, a_{n+1} x_{n+1})) \geqq |a_1|_0 > n!^{15}. \tag{3. 18}$$

Combination of (3. 16), (3. 17), (3. 18), (3. 15) yields

$$|a_1|_0 < h((a_1 x_1, \ldots, a_{n+1} x_{n+1})) < |a_1|_0^3. \tag{3. 19}$$

We apply Lemma 2. 2. It is clear that Lemma 2. 2 remains true if we replace H by a quantity B with $1 \leqq B \leqq H$. Take $B = |a_1|_0$. Then for any $C \geqq n^{2(n+3)}$ solutions $\mathbf{x}$ with

$$C \leqq h((a_1 x_1, \ldots, a_{n+1} x_{n+1})) \leqq C\,|a_1|_0^{(1/2n^2)} \tag{3. 20}$$

are contained in the union of not more than

$$(2e(n+1))^{(n+1)(s+1)-1} \tag{3. 21}$$

subspaces of the type $b_1 x_1 + \ldots + b_n x_n = 0$.

Now by (3. 16) $|a_1|_0 > n^{2(n+3)}$. Thus $4n^2$ intervals of the type (3. 20) suffice to cover the interval (3. 19), and in view of (3. 21) we get no more than

$$4n^2(2e(n+1))^{(n+1)(s+1)-1}$$

subspaces.

Lemma 3. 4. *There are*

$$t_0 \leqq (8(s+1))^{2^{26n+3}(s+1)^6} \tag{3. 22}$$

subspaces of $\mathbb{Q}^n$ *of the type* $b_1 x_1 + \ldots + b_n x_n = 0$, *such that every solution*

$$\mathbf{x} = (x_1, \ldots, x_n, x_{n+1})$$

of (1. 2) *lies in one of these subspaces.*

Proof. By Lemmata 3. 2 and 3. 3 $t_1 + t_2$ subspaces will suffice. Now

$$\begin{aligned} t_1 + t_2 &\leqq (8(s+1))^{2^{26n}\cdot(s+1)^6\cdot 4} n^{s+1} + 4n^2(2e(n+1))^{(n+1)(s+1)-1} + (2n)^{16n^2} \\ &< (8(s+1))^{2^{26n+3}(s+1)^6}. \end{aligned}$$

4. Proof of the Theorem

We shall proceed by induction on n. Denote by $Z(n, s+1)$ the supremum over $a_1, \ldots, a_{n+1}$ of the number of solutions of (1. 2). For $n=1$ it is clear that $Z(1, s+1) = 1$. Now let $n > 1$ and assume the assertion of the Theorem to be true for all $n' < n$.

Let T be one of the subspaces of Lemma 3. 4. Suppose T is given by

$$b_1 x_1 + \ldots + b_n x_n = 0. \tag{4. 1}$$

We first consider only solutions $\mathbf{x} = (x_1, \ldots, x_n, x_{n+1})$ of (1. 2) satisfying (4. 1). We fix a nonempty subset J of $\{1, \ldots, n\}$ and we restrict ourselves moreover to solutions $\mathbf{x}$ with

$$\sum_{i \in J} b_i x_i = 0 \tag{4. 2}$$

but such that no proper subsum of (4. 2) vanishes. By the induction hypothesis (4. 2) has not more than $Z(|J|-1, s+1)$ primitive solutions.

Now the components x_i with $i \in J$ satisfy $(x_i)_{i\in J} = (xc_i)_{i\in J}$, where $(c_i)_{i\in J}$ is one of the primitive solutions of (4. 2) and where x is an S-unit. With this expression for $(x_i)_{i\in J}$ we get in (1. 2)

$$\left(\sum_{i\in J} a_i c_i\right) x + \sum_{\substack{i=1 \\ i\notin J}}^{n+1} a_i x_i = 0. \tag{4. 3}$$

Again by the induction hypothesis, (4. 3) has not more than $Z(n+1-|J|, s+1)$ primitive solutions with components say d, d_i $(i \notin J)$. Therefore the primitive solutions

$$\mathbf{x} = (x_1, \ldots, x_n, x_{n+1})$$

arising from the subset J are of the shape $x_i = dc_i$ for $i \in J$, $x_i = d_i$ for $i \in J$ $(1 \leqq i \leqq n+1)$. And here we have $2 \leqq |J| \leqq n$. Summing up we see that J gives rise to not more than

$$Z(|J|-1, s+1)\, Z(n+1-|J|, s+1) \leqq (Z(n-1, s+1))^2$$

primitive solutions. As there are less than 2^n possibilities for J our subspace T contains

$$< 2^n (Z(n-1, s+1))^2$$

primitive solutions. Using the bound (3. 22) for the number of subspaces we finally get

$$\begin{aligned} Z(n, s+1) &\leqq (Z(n-1, s+1))^2 \cdot 2^n \cdot (8(s+1))^{2^{26n+3}(s+1)^6} \\ &< (8(s+1))^{2^{26(n-1)+5}(s+1)^6} \cdot (8(s+1))^{2^{26n+3}(s+1)^6+n} \\ &< (8(s+1))^{2^{26n+4}(s+1)^6}. \end{aligned}$$

References

[1] *E. Dubois* and *G. Rhin*, Sur la majoration de formes linéaires à coefficients algébriques réels et p-adiques, Démonstration d'une conjecture de K. Mahler, C. R. Acad. Sc. Paris, série A, **282** (1976), 1211.

[2] *J.-H. Evertse*, On sums of S-units and linear recurrences, Comp. Math. **53** (1984), 225—244.

[3] *J.-H. Evertse*, On equations in S-units and the Thue-Mahler equation, Invent. Math. **75** (1984), 561—584.

[4] *J.-H. Evertse* and *K. Győry*, On the numbers of solutions of weighted unit equations, Comp. Math. **66** (1988), 329—354.

[5] *K. Mahler*, Zur Approximation algebraischer Zahlen I, Über den größten Primteiler binärer Formen, Math. Ann. **107** (1933), 691—730.

[6] *A. J. van der Poorten* and *H. P. Schlickewei*, The growth condition for recurrence sequences, Macquarie Univ. Math. Rep. 82-0041, North Ryde, Australia 1982.

[7] *H. P. Schlickewei*, Über die diophantische Gleichung $x_1 + x_2 + \ldots + x_n = 0$, Acta. Arith. **33** (1977), 183—185.

[8] *H. P. Schlickewei*, The p-adic Thue-Siegel-Roth-Schmidt Theorem, Arch. d. Math. **29** (1977), 267—270.

[9] *H. P. Schlickewei*, An upper bound for the number of subspaces occurring in the p-adic subspace theorem in diophantine approximation, J. reine angew. Math. **406** (1990), 44—108.

[10] *W. M. Schmidt*, The subspace theorem in diophantine approximations, Comp. Math. **69** (1989), 121—173.

[11] *J. H. Silverman*, Quantitative results in diophantine geometry, Preprint, M.I.T., Cambridge Mass. (1983).

Abteilung Mathematik II, Universität Ulm, Oberer Eselsberg, D-7900 Ulm

Eingegangen 4. Juli 1988

J. reine angew. Math. **406** (1990), 121—166

Journal für die reine und angewandte Mathematik

The L-Theory of Laurent extensions and genus 0 function fields

By *R. J. Milgram**) at Stanford and *A. A. Ranicki***) at Edinburgh

Introduction

The stable classification of quadratic forms over a field is given by the Witt group. Topology, via surgery theory, has embedded the Witt groups in a general theory of forms over any ring with involution. In this paper we use geometrically inspired methods to make computations. General results on the L-theory of a Laurent polynomial extension are used to study the Witt groups of genus 0 function fields.

Given a ring A with involution $\tau: a \longrightarrow \bar{a}$ and a central unit $u \in A$ such that $\bar{u} = u$ let $A[t, t^{-1}]_u$ denote the Laurent extension ring $A[t, t^{-1}]$ with the involution $\bar{t} = ut^{-1}$, abbreviated to $A[t, t^{-1}]$ for $u = 1$. In Theorem 4. 1 we establish the exact sequence

$$\cdots \longrightarrow L_p^n(A) \xrightarrow{1-u} L_h^n(A) \xrightarrow{i_!} L_h^n(A[t, t^{-1}]_u)$$

$$\xrightarrow{B} L_p^{n-1}(A) \xrightarrow{1-u} L_h^{n-1}(A) \longrightarrow \cdots$$

expressing the free symmetric L-groups of $A[t, t^{-1}]_u$ in terms of the free and projective symmetric L-groups of A. For $u = 1$ the exact sequence of 4. 1 becomes a splitting

$$L_h^n(A[t, t^{-1}]) = L_h^n(A) \oplus L_p^{n-1}(A).$$

Although the exact sequence is stated and proved only for the symmetric L-groups L^* there is an entirely analogous treatment for the quadratic L-groups L_*.

In the case where $\frac{1}{2} \in A$ the symmetric and quadratic L-groups are equal, $L_* = L^*$. If A is a field $\mathbb{F}$ of characteristic different from 2 then $L_0(A) = L^0(A) = W(\mathbb{F})$, the Witt group of non-singular quadratic forms over $\mathbb{F}$ modulo hyperbolics. $W(\mathbb{F})$ is a Hermitian Witt group if the involution on $\mathbb{F}$ is non-trivial.

*) Partially supported by the National Science Foundation and S.F.B. 170, Göttingen.
**) Partially supported by S.F.B. 170, Göttingen.

In § 5—§ 7 we apply the exact sequence of 4. 1 to determine the Witt groups of genus 0 function fields. These are the fields of the form

$$\mathbb{F}\langle\lambda, \mu\rangle = \mathbb{F}(x)[y]/(y^2 - \mu x^2 + 4\lambda\mu)$$

for non-zero λ, μ in the ground field $\mathbb{F}$. Perhaps the most interesting of these fields is $\mathscr{F} = \mathbb{R}(x)[y]/(x^2 + y^2 + 1)$. Here, our methods recover the following result of Knebusch [9] as a special case:

Theorem 5. 3. (i) *There is an exact sequence*

$$0 \longrightarrow \mathbb{Z}/2 \longrightarrow L_0(\mathscr{F}) \longrightarrow \mathbb{Z}/2 \oplus \bigoplus_{\mathscr{I}} \mathbb{Z}/2 \longrightarrow 0$$

where the index set $\mathscr{I}$ is the points $p \in \mathscr{M}_1$, and $\mathscr{M}_1$ is the open Möbius band

$$\{\mathbb{C} - \{0\}/(z \sim -1/\bar{z})\}.$$

The first $\mathbb{Z}/2$ in the right hand sum carries the element $\langle 1\rangle$.

(ii) *The sequence above does not split. In particular the Stufe of $\mathscr{F}$ is 2.*

The Stufe of a field $\mathscr{F}$ is the least integer n (necessarily a power of 2) such that -1 is a sum of n squares in $\mathscr{F}$. As a consequence the exponent of $W(\mathscr{F})$ is $2n$.

In § 6 and § 7 we give a more detailed analysis of these Witt groups, using a commutative square of injections of rings

$$\begin{array}{ccc} \mathbb{F}[x](y) & \longrightarrow & \mathbb{F}\langle\lambda, \mu\rangle \\ \downarrow & & \downarrow \\ \mathbb{K}[t, t^{-1}] & \longrightarrow & \mathbb{K}(t) \end{array}$$

for any elements λ, μ in $\mathbb{F}$ with λ non-zero and μ non-square, $\mathbb{K} = \mathbb{F}(\sqrt{\mu})$ a degree two Galois extension of $\mathbb{F}$, $\mathbb{F}[x](y) = \mathbb{F}[x, y]/(y^2 - \mu x^2 + 4\lambda\mu)$, and

$$x = t + \lambda t^{-1}, \quad y = \sqrt{\mu}(t - \lambda t^{-1}), \quad t = (x + y/\sqrt{\mu})/2.$$

The genus 0 function field $\mathbb{F}\langle\lambda, \mu\rangle$ is the fixed field of the involution on the rational function field $\mathbb{K}(t)$ defined by the extension of the Galois automorphism on $\mathbb{K}$ with

$$\bar{t} = (x - y/\sqrt{\mu})/2 = \lambda t^{-1}.$$

The basic result 7. 14 defines a group V and proves the existence of an exact sequence

$$0 \longrightarrow L_0(\mathbb{K}[t, t^{-1}]_\lambda) \longrightarrow L_0(\mathbb{F}[x](y)) \longrightarrow V \longrightarrow L_3(\mathbb{K}[t, t^{-1}]_\lambda) \longrightarrow L_3(\mathbb{F}[x](y)) \longrightarrow 0.$$

The Witt group $L_0(\mathbb{F}[x](y))$ is the kernel of the "second boundary map" from $L_0(\mathbb{F}\langle\lambda,\mu\rangle)$ to the Witt groups of its various completions, while the group $L_3(\mathbb{F}[x](y))$ is the cokernel. Hence this latter group serves as an explicit reciprocity law for these fields.

The exact sequence above is a special case of one of the sequences in the "Twisting Diagram (0. 1)" appearing in Hambleton, Taylor and Williams [6]. The key new observation here is that $\mathbb{K}[t, t^{-1}]$ is an integral quadratic extension of $\mathbb{F}[x](y)$ (Lemma 6. 4).

The reciprocity law arises as follows. There is the well known exact sequence of Jacobson

$$0 \longrightarrow L_0(\mathbb{K}(t)_\lambda) \longrightarrow L_0(\mathbb{F}\langle\lambda,\mu\rangle) \longrightarrow L_0(\mathbb{K}(t)).$$

(The referee points out that D. W. Lewis [11] has generalized this sequence.) Localization gives an exact sequence

$$0 \longrightarrow L_0(\mathbb{K}[t, t^{-1}]_\lambda) \longrightarrow L_0(\mathbb{K}(t)_\lambda) \longrightarrow \bigoplus_{\mathscr{P}} L_0(\mathbb{K}[t, t^{-1}]_\lambda/\mathscr{P}) \xrightarrow{j} L_3(\mathbb{K}[t, t^{-1}]_\lambda) \longrightarrow 0.$$

Thus the Hermitian Witt group $L_0(\mathbb{K}(t)_\lambda)$ is determined by the L-groups of the quotient fields $\mathbb{K}[t, t^{-1}]_\lambda/\mathscr{P}$ and the groups $L_*(\mathbb{K}[t, t^{-1}]_\lambda)$. Moreover, j above can be regarded as a reciprocity law for $L_0(\mathbb{K}(t)_\lambda)$.

It should be noted that our main exact sequence for a Laurent extension completely determines the groups $L_*(\mathbb{K}[t, t^{-1}]_\lambda)$ in terms of the Witt group of $\mathbb{K}$. The possibility of applying the techniques of L-theory to the study of the Witt groups of genus 0 function fields first came up in conversations with W. Jacob and A. Wadsworth. T. Y. Lam asked us about the special case $\mathscr{F}$ above. We thank the referee for drawing our attention to the recent work of Parimala [14], which contains (§§ 4—6) a thorough study of the Witt rings of conics by methods very different from ours. It seems to require some work to exhibit the precise relationship between her main results, in particular Theorem 6. 2 of [14] and our Theorem 7. 14.

In § 8 we briefly consider the situation where the involution acts trivially on the field $\mathbb{F}$. Here, we obtain explicit reciprocity laws and by way of an example show:

Corollary 8. 6. *If $\mathbb{R}[t, t^{-1}]$ is given the involution which is the identity on $\mathbb{R}$ and $\bar{t} = t^{-1}$ then the associated Hermitian Witt group is (naturally) isomorphic to the uncountable direct sum*

$$L_0(\mathbb{R}(t)) \cong \bigoplus_{S^1} \mathbb{Z}$$

where S^1 denotes the points of the unit circle.

We do not entirely understand the interplay between the L-groups and the real algebraic varieties in the statements of 5. 3 and 8. 6.

The quadratic L-groups $L_*(A)$ are the Wall [25] surgery obstruction groups. Shaneson [22] obtained a geometric splitting of the simple quadratic L-groups

$$L^s_n(A[t, t^{-1}]) = L^s_n(A) \oplus L^h_{n-1}(A)$$

for $A = \mathbb{Z}[\pi]$, $\bar{t} = t^{-1}$ using the realization theorem of [25] to express elements of $L^s_*(\mathbb{Z}[\pi][t, t^{-1}]) = L^s_*(\mathbb{Z}[\pi \times \mathbb{Z}])$ as the surgery obstructions of normal maps with fundamental group $\pi \times \mathbb{Z}$ which are simple homotopy equivalences on the boundary, and applying the codimension 1 splitting theorem of Farrell and Hsiang [4]. The algebraic splitting theorem of Novikov [13] and Ranicki [15] for the quadratic L-groups $L^q_*(A[t, t^{-1}])$ ($\bar{t} = t^{-1}$, $q = s, h$) was proved by an analysis of quadratic forms and formations over $A[t, t^{-1}]$, working by analogy with the analysis of invertible matrices over $A[t, t^{-1}]$ used by Bass, Heller and Swan [2] and Bass [1] to prove the algebraic splitting theorem for $K_1(A[t, t^{-1}])$. Certain discrepancies between the algebraic and geometric methods of proof were clarified in Ranicki [19]. The L-theory splitting theorem is proved here by algebra, using the expression in Ranicki [16], [17] of the L-groups as the cobordism groups of chain complexes with Poincaré duality. The codimension 1 transversality of the geometric proof is replaced by an L-theoretic version of the method of Mayer-Vietoris presentations used by Waldhausen [23], [24] in algebraic K-theory, which is an extension of the linearization trick of Higman [8]. The geometric approach of Wall [25], Thm. 12. 6, applies to the quadratic L-groups of the Laurent polynomial extension $A[t, t^{-1}] = \mathbb{Z}[\pi \times \mathbb{Z}]$ of $A = \mathbb{Z}[\pi]$, with $\bar{t} = ut^{-1}$ both for $u = +1$ and $u = -1$. See Ranicki [17], § 7. 6, for an account of the geometric background to quadratic L-theory splitting theorems for $A[t, t^{-1}]$ with $\bar{t} = \pm t^{-1}$, and also of the case $\bar{t} = t$. The splitting theorem proved here for the symmetric L-groups $L^*(A[t, t^{-1}])$ ($\bar{t} = t^{-1}$) was conjectured in Ranicki [16], § 10. The symmetric L-groups $L^*(\mathbb{Z}[\pi])$ are not geometrically realizable, so that the geometric methods of proof do not apply. See Ranicki [21] for a further development of the L-theory of Laurent extensions.

We thank M. Knebusch for some very helpful comments. In particular he pointed out that the genus 0 function fields were first studied in depth by E. Witt [26].

§ 1. The *K*-theory of Laurent extensions

Let A be an associative ring with 1. We shall be working with left A-modules and positive A-module chain complexes C.

An A-module chain complex C is *finite* if it is a finite-dimensional complex of based f.g. (finitely generated) free A-modules. We assume that the reader is already familiar with the *torsion* $\tau(E) \in K_1(A)$ of a contractible finite complex E. The (*reduced*) *torsion* of a chain equivalence $f : C \to D$ of finite complexes is defined as usual by

$$\tau(f) = \tau(C(f)) \in \tilde{K}_1(A) = \operatorname{coker}(K_1(\mathbb{Z}) \longrightarrow K_1(A))$$

with $C(f)$ the algebraic mapping cone.

An A-module chain complex C is *finitely dominated* if there exists a domination $(D, f: C \to D, g: D \to C, h: gf \simeq 1: C \to C)$ by a finite complex D, or equivalently if it is chain equivalent to a finite-dimensional complex P of f.g. projective A-modules. The *projective class* of C is defined by

$$[C] = [P] = \sum_{r=0}^{\infty} (-)^r [P_r] \in K_0(A)$$

for any such P. An A-module chain complex C is *homotopy finite* if it is chain equivalent to a finite complex. The reduced projective class of a finitely dominated chain complex C is the *finiteness obstruction*

$$[C] = [P] \in \tilde{K}_0(A) = \operatorname{coker}(K_0(\mathbb{Z}) \longrightarrow K_0(A)),$$

with $[C] = 0$ if and only if C is homotopy finite. See Ranicki [18] for the algebraic theory of finiteness obstruction of finitely dominated chain complexes.

Let $A[t, t^{-1}]$ be the Laurent polynomial extension ring, consisting of the polynomials $\sum_{j=-\infty}^{\infty} a_j t^j$ in a central invertible indeterminate t over A with the coefficients $a_j \in A$ such that $\{j \in \mathbb{Z} \mid a_j \neq 0\}$ is finite. The inclusion of rings

$$i: A \longrightarrow A[t, t^{-1}]$$

determines functors

$$\begin{aligned} i_!: (A\text{-modules}) &\longrightarrow (A[t, t^{-1}]\text{-modules}); \\ F &\longrightarrow i_! F = A[t, t^{-1}] \otimes_A F = F[t, t^{-1}], \\ i^!: (A[t, t^{-1}]\text{-modules}) &\longrightarrow (A\text{-modules}); \; E \longrightarrow i^! E = E, \end{aligned}$$

with A acting on $i^! E$ by the restriction of the $A[t, t^{-1}]$-action to $A \subset A[t, t^{-1}]$.

Given an A-module F let F^+, F^- denote the A-modules

$$F^+ = \sum_{j=0}^{\infty} t^j F, \quad F^- = \sum_{j=-\infty}^{-1} t^j F,$$

so that

$$i^! i_! F = F^+ \oplus F^-.$$

If F is a f.g. A-module and G is any A-module it is possible to express every $A[t, t^{-1}]$-module morphism $\alpha: F[t, t^{-1}] \to G[t, t^{-1}]$ as a polynomial

$$\alpha = \sum_{j=-\infty}^{\infty} t^j \alpha_j: F[t, t^{-1}] \longrightarrow G[t, t^{-1}]$$

with the coefficient A-module morphisms $\alpha_j \in \operatorname{Hom}_A(F, G)$ such that $\{j \in \mathbb{Z} \mid \alpha_j \neq 0\}$ is finite.

Given an isomorphism of based f.g. free $A[t, t^{-1}]$-modules

$$\alpha = \sum_{j=-N}^{M} t^j \alpha_j : F[t, t^{-1}] \longrightarrow G[t, t^{-1}]$$
$$(\alpha_j \in \mathrm{Hom}_A(F, G), \quad M, N \geqq 0)$$

there are defined f.g. projective A-modules

$$B_N^+(F, G) = G^+/\alpha(t^N F^+), \quad B_M^-(F, G) = G^-/\alpha(t^{-M} F^-)$$

such that up to isomorphism

$$B_N^+(F, G) = \alpha(t^N F^-) \cap G^+, \quad B_M^-(F, G) = \alpha(t^{-M} F^+) \cap G^-,$$
$$B_N^+(F, G) \oplus B_M^-(F, G) = \sum_{j=-M}^{N-1} t^j F,$$

and such that there are defined nilpotent endomorphisms

$$t : B_N^+(F, G) \longrightarrow B_N^+(F, G), \quad t^{-1} : B_M^-(F, G) \longrightarrow B_M^-(F, G).$$

Bass, Heller and Swan [2] and Bass [1] showed that the torsion group $K_1(A[t, t^{-1}])$ of the Laurent polynomial extension $A[t, t^{-1}]$ fits into a split exact sequence

$$0 \longrightarrow K_1(A) \xrightarrow{i_!} K_1(A[t, t^{-1}])$$
$$\xrightarrow{(BB^+B^-)} K_0(A) \oplus \overline{\mathrm{Nil}}_0(A) \oplus \overline{\mathrm{Nil}}_0(A) \longrightarrow 0,$$

with $\overline{\mathrm{Nil}}_0(A)$ the reduced nilpotent class group. The injection $i_!$ is induced by the inclusion of rings $i : A \longrightarrow A[t, t^{-1}]$. The projections B, B^+, B^- are defined by

$$B : K_1(A[t, t^{-1}]) \longrightarrow K_0(A);$$
$$\tau(\alpha) \longrightarrow [B_N^+(F, G)] - \left[\sum_{j=0}^{N-1} t^j F\right] = \left[\sum_{j=-M}^{-1} t^j F\right] - [B_M^-(F, G)],$$
$$B^+ : K_1(A[t, t^{-1}]) \longrightarrow \overline{\mathrm{Nil}}_0(A); \ \tau(\alpha) \longrightarrow [B_N^+(F, G), t],$$
$$B^- : K_1(A[t, t^{-1}]) \longrightarrow \overline{\mathrm{Nil}}_0(A); \ \tau(\alpha) \longrightarrow [B_M^-(F, G), t^{-1}].$$

Define the *doubly reduced* torsion group

$$\tilde{\tilde{K}}_1(A[t, t^{-1}]) = \mathrm{coker}(K_1(\mathbb{Z}[t, t^{-1}]) \longrightarrow K_1(A[t, t^{-1}])).$$

Proposition 1. 1. *The doubly reduced torsion group fits into a split exact sequence*

$$0 \longrightarrow \tilde{K}_1(A) \xrightarrow{i_!} \tilde{\tilde{K}}_1(A[t, t^{-1}])$$

$$\xrightarrow{(BB^+B^-)} \tilde{K}_0(A) \oplus \overline{\mathrm{Nil}}_0(A) \oplus \overline{\mathrm{Nil}}_0(A) \longrightarrow 0.$$

Proof. This is just the quotient of the split exact sequence for $K_1(A[t, t^{-1}])$ by the split exact sequence for $K_1(\mathbb{Z}[t, t^{-1}])$, using $\overline{\mathrm{Nil}}_0(\mathbb{Z}) = 0$. □

A *Mayer-Vietoris presentation* of an $A[t, t^{-1}]$-module chain complex E is a short exact sequence

$$\mathscr{E}: 0 \longrightarrow i_! C \xrightarrow{f - gt} i_! D \xrightarrow{h} E \longrightarrow 0,$$

with C, D A-module chain complexes and $f, g: C \to D$ A-module chain maps. $\mathscr{E}$ is *finite* if E is a finite $A[t, t^{-1}]$-module chain complex and C, D are finite A-module chain complexes.

Let E be a finite n-dimensional $A[t, t^{-1}]$-module chain complex, and let F_r be the based f.g. free A-module generated by the $A[t, t^{-1}]$-module base of E_r $(0 \leqq r \leqq n)$, so that

$$E_r = i_! F_r = F_r[t, t^{-1}].$$

The *fundamental lattice of* E $\mathbb{N}(E)$ is the lattice of ordered $(2n+2)$-tuples

$$N = (N_0^+, N_1^+, \ldots, N_n^+; N_0^-, N_1^-, \ldots, N_n^-)$$

of elements $N_r^+, N_r^- \in \{0, 1, 2, \ldots, \infty\}$ such that

$$d_E\left(\sum_{j=-N_r^+}^{N_r^-} t^j F_r\right) \subseteqq \sum_{j=-N_{r-1}^+}^{N_{r-1}^-} t^j F_{r-1} \qquad (1 \leqq r \leqq n),$$

with

$$N \leqq N' \quad \text{if} \quad N_r^+ \leqq N_r'^+, \; N_r^- \leqq N_r'^- \qquad (0 \leqq r \leqq n),$$

$$(N \cap N')_r^+ = \min(N_r^+, N_r'^+), \; (N \cap N')_r^- = \min(N_r^-, N_r'^-),$$

$$(N \cup N')_r^+ = \max(N_r^+, N_r'^+), \; (N \cup N')_r^- = \max(N_r^-, N_r'^-).$$

The lattice $\mathbb{N}(E)$ is non-empty, with maximal element

$$\infty = (\infty, \ldots, \infty; \infty, \ldots, \infty) \in \mathbb{N}(E).$$

Every element $N \in \mathbb{N}(E)$ determines a Mayer-Vietoris presentation of E

$$\mathscr{E}(N): 0 \longrightarrow i_! C(N) \xrightarrow{f(N) - g(N)t} i_! D(N) \xrightarrow{h(N)} E \longrightarrow 0,$$

with $C(N)$, $D(N) \subseteq i^! E$ the A-module subcomplexes defined by

$$D(N)_r = \sum_{j=-N_r^+}^{N_r^-} t^j F_r \subseteq i^! E_r = \sum_{j=-\infty}^{\infty} t^j F_r,$$

$$C(N)_r = D(N)_r \cap tD(N)_r = \sum_{j=-N_r^+ +1}^{N_r^-} t^j F_r,$$

and $f(N)$, $g(N)$, $h(N)$ the chain maps defined by

$$f(N): C(N) \longrightarrow D(N); \quad x \longrightarrow x,$$
$$g(N): C(N) \longrightarrow D(N); \quad x \longrightarrow t^{-1}x,$$
$$h(N): i_! D(N) \longrightarrow E; \quad a \otimes x \longrightarrow ax.$$

An element $N \in \mathbb{N}(E)$ is *finite* if all of the N_r^+, N_r^- are finite, in which case $\mathscr{E}(N)$ is a finite Mayer-Vietoris presentation of E. Let $\mathbb{N}^f(E) \subset \mathbb{N}(E)$ be the sublattice of the finite elements. $\mathbb{N}^f(E)$ is non-empty, since the unique minimal element $N \in \mathbb{N}(E)$ is finite, with $N_n^+ = 0$, $N_n^- = 0$. Thus:

Proposition 1. 2 (Waldhausen [23]). *Every finite $A[t, t^{-1}]$-module chain complex E admits a finite Mayer-Vietoris presentation.* □

Let $\mathbb{N}^+(E) \subset \mathbb{N}(E)$ be the sublattice of the elements

$$N^+ = (N_0^+, N_1^+, \ldots, N_n^+; \infty, \infty, \ldots, \infty) \in \mathbb{N}(E)$$

with N_r^+ $(0 \leqq r \leqq n)$ finite. Similarly, let $\mathbb{N}^-(E) \subset \mathbb{N}(E)$ be the subset of the elements

$$N^- = (\infty, \infty, \ldots, \infty; N_0^-, N_1^-, \ldots, N_n^-) \in \mathbb{N}(E)$$

with N_r^- $(0 \leqq r \leqq n)$ finite. There are evident forgetful maps

$$\mathbb{N}^f(E) \longrightarrow \mathbb{N}^+(E);$$
$$N = (N_0^+, N_1^+, \ldots, N_n^+; N_0^-, N_1^-, \ldots, N_n^-) \longrightarrow N^+ = (N_0^+, N_1^+, \ldots, N_n^+; \infty, \infty, \ldots, \infty),$$

$$\mathbb{N}^f(E) \longrightarrow \mathbb{N}^-(E);$$
$$N = (N_0^+, N_1^+, \ldots, N_n^+; N_0^-, N_1^-, \ldots, N_n^-) \longrightarrow N^- = (\infty, \infty, \ldots; N_0^-, N_1^-, \ldots, N_n^-).$$

Given $N^+ \in \mathbb{N}^+(E)$ and $N^- \in \mathbb{N}^-(E)$ there is defined a short exact sequence of A-module chain complexes

$$0 \longrightarrow t^{-N^+}F^+ \cap t^{N^-}F^- \longrightarrow t^{-N^+}F^+ \oplus t^{N^-}F^- \longrightarrow i^! E \longrightarrow 0.$$

If E is a contractible $A[t, t^{-1}]$-module chain complex then $i^! E$ is a contractible A-module chain complex, and the A-module chain complexes $t^{-N^+}F^+$, $t^{N^-}F^-$ are finitely dominated, with $t^{-N^+}F^+ \oplus t^{N^-}F^-$ chain equivalent to the finite chain complex $t^{-N^+}F^+ \cap t^{N^-}F^-$.

Proposition 1.3 (Ranicki [21]). *The projection* $B: \tilde{\tilde{K}}_1(A[t, t^{-1}]) \to \tilde{K}_0(A)$ *is such that*

$$B(\tau(E)) = [t^{-N^+} F^+] = -[t^{N^-} F^-] \in \tilde{K}_0(A)$$

for any contractible finite $A[t, t^{-1}]$*-module chain complex* E *and any*

$$N^+ \in \mathbb{N}^+(E), \quad N^- \in \mathbb{N}^-(E). \quad \square$$

§ 2. The L-theory of finite complexes

We recall the L-theory of f.g. projective chain complexes with Poincaré duality. Readers familiar with Ranicki [16] may skip this section. In § 3 we develop L-theory using chain complexes of infinitely generated based free A-modules.

Let A be an associative ring with 1, together with an involution

$$\tau: A \longrightarrow A; \ a \longrightarrow \bar{a}.$$

Given A-modules M, N define the $\mathbb{Z}$-module

$$M \otimes_A N = M \otimes_{\mathbb{Z}} N / \{ax \otimes y - x \otimes \bar{a}y \mid a \in A, x \in M, y \in N\}.$$

Given an A-module chain complex C let the generator $T \in \mathbb{Z}_2$ act on $C \otimes_A C$ by the transposition involution

$$T: C \otimes_A C \longrightarrow C \otimes_A C; \ x \otimes y \longrightarrow (-)^{pq} y \otimes x \quad (x \in C_p, \ y \in C_q),$$

and define the $\mathbb{Z}$-module chain complex

$$W^{\%} C = \mathrm{Hom}_{\mathbb{Z}[\mathbb{Z}_2]}(W, C \otimes_A C)$$

with W the free $\mathbb{Z}[\mathbb{Z}_2]$-module resolution of $\mathbb{Z}$

$$W: \ldots \longrightarrow \mathbb{Z}[\mathbb{Z}_2] \xrightarrow{1+T} \mathbb{Z}[\mathbb{Z}_2] \xrightarrow{1-T} \mathbb{Z}[\mathbb{Z}_2] \longrightarrow 0.$$

An *n-dimensional symmetric complex over* A (C, ϕ) is an n-dimensional A-module chain complex C together with a cycle $\phi \in (W^{\%} C)_n$. A *morphism* of n-dimensional symmetric complexes over A

$$(f, \chi): (C, \phi) \longrightarrow (C', \phi')$$

is a chain map $f: C \to C'$ together with a chain $\chi \in (W^{\%} C')_{n+1}$ such that

$$\phi' - f^{\%}(\phi) = d\chi \in (W^{\%} C')_n.$$

The morphism is a *homotopy equivalence* if $f: C \to D$ is a chain equivalence.

Given a f.g. projective A-module M let M^* denote the dual A-module of A-module morphisms $f: M \longrightarrow A$, with A acting by

$$A \times M^* \longrightarrow M^*; \quad (a, f) \longrightarrow (x \longrightarrow f(x)\bar{a}).$$

The natural A-module isomorphism

$$M \longrightarrow M^{**}; \quad x \longrightarrow (f \longrightarrow \overline{f(x)})$$

is used to identify

$$M^{**} = M.$$

For any f.g. projective A-modules M, N use the natural isomorphism

$$M \otimes_A N \longrightarrow \mathrm{Hom}_A(M^*, N); \quad x \otimes y \longrightarrow (f \longrightarrow \overline{f(x)} \cdot y)$$

to identify

$$M \otimes_A N = \mathrm{Hom}_A(M^*, N).$$

Thus for a f.g. projective A-module chain complex C a cycle $\phi \in W^{\%}C_n$ is defined by a collection of chains

$$\{\phi_s \in (C \otimes_A C)_{n+s} = \sum_r \mathrm{Hom}_A(C^{n-r+s}, C_r) \mid s \geqq 0\}$$

such that

$$d_C\phi_s + (-)^r \phi_s d_C^* + (-)^{n+s-1}(\phi_{s-1} + (-)^s T\phi_{s-1}) = 0 : C^{n-r+s-1} \longrightarrow C_r$$
$$(r, s \geqq 0, \ \phi_{-1} = 0).$$

A f.g. projective n-dimensional symmetric complex over A (C, ϕ) is *Poincaré* if the A-module chain map $\phi_0 : C^{n-*} \longrightarrow C$ is a chain equivalence, with C^{n-*} the n-dual f.g. projective A-module chain complex defined by

$$d_{C^{n-*}} = (-)^r (d_C)^* : (C^{n-*})_r = C^{n-r} \longrightarrow (C^{n-*})_{r-1} = C^{n-r+1}$$
$$(C^r = (C_r)^*).$$

A f.g. projective *n-dimensional symmetric pair over* A $(f: C \longrightarrow D, (\delta\phi, \phi))$ is defined by a chain map $f: C \longrightarrow D$ from a f.g. projective $(n-1)$-dimensional A-module chain complex C to a f.g. projective n-dimensional A-module chain complex D, together with a cycle $(\delta\phi, \phi) \in C(f^{\%} : W^{\%}C \longrightarrow W^{\%}D)_n$. The symmetric pair is *Poincaré* if a certain A-module chain map $(\delta\phi, \phi)_0 : C(f)^{n-*} \longrightarrow D$ is a chain equivalence, in which case the *boundary*

(C, ϕ) is an $(n-1)$-dimensional symmetric Poincaré complex over A. A *cobordism* of n-dimensional symmetric (Poincaré) complexes (C, ϕ), (C', ϕ') is an $(n+1)$-dimensional symmetric (Poincaré) pair

$$((f\ f'): C \oplus C' \longrightarrow D, (\delta\phi, \phi \oplus -\phi'))$$

with boundary $(C, \phi) \oplus (C', -\phi')$. Homotopy equivalent complexes are cobordant.

The projective (resp. free) symmetric L-group $L^n_p(A)$ (resp. $L^n_h(A)$) was defined in Ranicki [16] for $n \geqq 0$ to be the cobordism group of f.g. projective (resp. finite) n-dimensional symmetric Poincaré complexes over A. See [16], § 6, for the extension of the definition to the range $n<0$.

The *union* of adjoining cobordisms of n-dimensional symmetric complexes

$$\mathscr{C} = ((f_C f_{C'}): C \oplus C' \longrightarrow D, (\delta\phi, \phi \oplus -\phi')),$$
$$\mathscr{C}' = ((f'_{C'} f'_{C''}): C' \oplus C'' \longrightarrow D', (\delta\phi', \phi' \oplus -\phi''))$$

is the cobordism

$$\mathscr{C}'' = \mathscr{C} \cup_{(C', \phi')} \mathscr{C}' = ((f''_C f''_{C''}): C \oplus C'' \longrightarrow D'', (\delta\phi'', \phi \oplus -\phi''))$$

defined by

$$d_{D''} = \begin{pmatrix} d_D & (-)^{r-1} f_{C'} & 0 \\ 0 & d_{C'} & 0 \\ 0 & (-)^{r-1} f'_{C'} & d_{D'} \end{pmatrix} : D''_r = D_r \oplus C'_{r-1} \oplus D'_r \longrightarrow D''_{r-1}$$

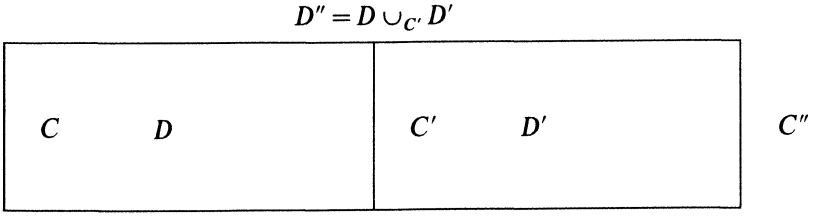
$$= D_{r-1} \oplus C'_{r-2} \oplus D'_{r-1},$$

$$f''_C = f_C \oplus 0 \oplus 0 : C_r \longrightarrow D''_r = D_r \oplus C'_{r-1} \oplus D'_r,$$

$$f''_{C''} = 0 \oplus 0 \oplus f'_{C''} : C''_r \longrightarrow D''_r = D_r \oplus C'_{r-1} \oplus D'_r,$$

$$\delta\phi''_s = \begin{pmatrix} \delta\phi_s & 0 & 0 \\ (-)^{n-r} \phi'_s f^*_{C'} & (-)^{n-r+s+1} T\phi'_{s-1} & 0 \\ 0 & (-)^s f'_{C'} \phi'_s & \delta\phi'_s \end{pmatrix} : D''^{n-r+s+1}$$

$$= D^{n-r+s+1} \oplus C'^{n-r+s} \oplus D'^{n-r+s+1} \longrightarrow D''_r = D_r \oplus C'_{r-1} \oplus D'_r.$$



An n-dimensional symmetric (Poincaré) triad over A

$$X = \left(\begin{array}{ccc} \partial C & \longrightarrow & \partial_+ D \\ \downarrow & \Gamma & \downarrow \\ C & \longrightarrow & D \end{array} , \begin{array}{ccc} \partial\phi & \longrightarrow & \partial_+ \delta\phi \\ \downarrow & \Phi & \downarrow \\ \phi & \longrightarrow & \delta\phi \end{array} \right)$$

is a relative (Poincaré) cobordism to 0 of the $(n-1)$-dimensional symmetric (Poincaré) pair over A

$$\partial X = (\partial C \longrightarrow \partial_+ D, (\partial_+ \delta\phi, \partial\phi)),$$

as defined by a commutative square Γ of chain complexes and cycle $\Phi \in W^{\%}\Gamma_n$. See Ranicki [17], § 1. 3, for further details.

§ 3. The L-theory of locally finite complexes

The algebraic K- and L-theory of a ring A are defined using f.g. projective and f.g. free A-modules. The Laurent polynomial extension ring $A[t, t^{-1}]$ of a ring A is a countably infinitely generated free A-module. The splitting theorem of § 4 expresses the L-groups for $A[t, t^{-1}]$ in terms of the L-groups of A by passing from chain complexes of f.g. free $A[t, t^{-1}]$-modules to locally finite chain complexes of countably infinitely generated free A-modules, and hence to chain complexes of f.g. projective A-modules. In each case only finite-dimensional chain complexes are considered. In § 3 we develop the L-theory of the locally finite chain complexes of countably infinitely generated free A-modules.

A *morphism matrix* is a collection of A-module morphisms

$$\{f_{ij} \in \mathrm{Hom}_A(M(j), N(i)) \mid i \in I, j \in J\}$$

which we also write as

$$f = (f_{ij}) : M = \{M(j) \mid j \in J\} \longrightarrow N = \{N(i) \mid i \in I\}.$$

Morphism matrices

$$f : M = \{M(j)\} \longrightarrow N = \{N(i)\},\ g : N = \{N(i)\} \longrightarrow P = \{P(k)\}$$

can be composed if and only if for each $x(j) \in M(j)$ and k the set

$$\{i \in I \mid g_{ki} f_{ij}(x(j)) \neq 0 \in P(k)\}$$

is finite, in which case the composite morphism matrix $gf : M \longrightarrow N$ is defined by

$$(gf)_{kj} = \sum_{i \in I} g_{ki} f_{ij} : M(j) \longrightarrow N(k).$$

The morphisms of direct sums of A-modules

$$M=\sum_{j\in J} M(j) \longrightarrow N=\sum_{i\in I} N(i)$$

are in one-one correspondence with the morphism matrices $f=\{f_{ij}\}$ such that for each $x(j)\in M(j)$ the set $\{i\in I \mid f_{ij}(x(j))\neq 0\in N(i)\}$ is finite, with the morphism corresponding to f given by

$$f=(f_{ij}): M=\sum_{j\in J} M(j) \longrightarrow N=\sum_{i\in I} N(i);$$

$$x=\sum_{j\in J} x(j) \longrightarrow f(x)=\sum_{i\in I}\sum_{j\in J} f_{ij}(x(j)).$$

If each $M(j)$ is a f.g. projective A-module this condition is equivalent to f being column finite, i.e. the set $\{i\in I \mid f_{ij}\neq 0\}$ being finite for each $j\in J$.

An A-module M is *countably free* (resp. *projective*) if it is expressed as a direct sum

$$M=\sum_{j\in J} M(j)$$

of f.g. free (resp. projective) A-modules $M(j)$, with J countable. An A-module morphism $f: M\longrightarrow N$ between countably free (resp. projective) A-modules is a column finite morphism matrix (f_{ij}). The morphism is *locally finite* if the morphism matrix is also row finite, i.e. the set $\{j\in J \mid f_{ij}\neq 0\}$ is finite for each $i\in I$.

Given countably projective A-modules M, N let $\mathrm{Hom}_A^{lf}(M, N)$ be the subgroup of $\mathrm{Hom}_A(M, N)$ consisting of the locally finite morphisms. If N is f.g. projective then

$$\mathrm{Hom}_A^{lf}(M, N)=\mathrm{Hom}_A(M, N).$$

Remark 3. 1. A locally finite A-module morphism $f: M\longrightarrow N$ of countably projective A-modules can be an isomorphism without being a locally finite isomorphism, i.e. the inverse $f^{-1}: N\longrightarrow M$ need not be locally finite. For example, let $A=\mathbb{Z}$, $M=N=\sum_{i=0}^{\infty}\mathbb{Z}$ and consider the automorphism

$$f=\begin{pmatrix} 1 & -1 & 0 & \cdots \\ 0 & 1 & -1 & \cdots \\ 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix}: \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\oplus\cdots \longrightarrow \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\oplus\cdots,$$

such that the inverse

$$f^{-1}=\begin{pmatrix} 1 & 1 & 1 & \cdots \\ 0 & 1 & 1 & \cdots \\ 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix}: \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\oplus\cdots \longrightarrow \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\oplus\cdots,$$

is not locally finite. □

An A-module chain complex C is *locally finite* if it is a finite-dimensional complex of countably projective A-modules with the differentials $d_C : C_r \to C_{r-1}$ $(r \geqq 1)$ locally finite. A chain map $f : C \to D$ of locally finite complexes is *locally finite* if each $f : C_r \to D_r$ $(r \geqq 0)$ is locally finite. A *locally finite* equivalence is a chain equivalence in the locally finite category. A locally finite chain complex C is *locally finitely dominated* if there exists a finite domination (D, f, g, h) with f, g, h locally finite. A locally finite chain complex C is *locally homotopy finite* if it is locally finite equivalent to a finite complex D.

Locally finite duality is defined with respect to an involution $A \to A$; $a \to \bar{a}$ on the ground ring A, as in the f.g. projective case.

The *locally finite dual* of a countably free (resp. projective) A-module M is the countably free (resp. projective) A-module defined by

$$M^* = \mathrm{Hom}_A^{lf}(M, A)$$

with A acting on M^* as in the f.g. projective case and $M^*(j) = M(j)^*$ $(j \in J)$. (If M is f.g. then M^* is the dual defined above.) If M is countably free then choosing a base $(b_{j1}, b_{j2}, \ldots, b_{jk_j})$ for each $M(j)$ determines a locally finite isomorphism

$$M \longrightarrow M^*;\ b_{jk} \longrightarrow \left(b_{j'k'} \longrightarrow \begin{cases} 1 & \text{if } (j,k) = (j',k'), \\ 0 & \text{otherwise} \end{cases} \right).$$

For any countably projective M there is defined a natural locally finite isomorphism $M \to M^{**}$ as in the f.g. projective case, which is used to identify $M^{**} = M$.

The *dual* of a morphism matrix $f : M \to N$ is the morphism matrix $f^* : N^* \to M^*$ with

$$(f^*)_{ji} = (f_{ij})^* : N^*(i) = N(i)^* \longrightarrow M^*(j) = M(j)^*.$$

The *locally finite dual* of a locally finite morphism $f : M \to N$ is the locally finite morphism $f^* : N^* \to M^*$ defined by

$$f^* : N^* \longrightarrow M^*;\ g \longrightarrow (x \longrightarrow g(f(x))),$$

which has the dual morphism matrix. Locally finite duality defines an isomorphism

$$T : \mathrm{Hom}_A^{lf}(M, N) \longrightarrow \mathrm{Hom}_A^{lf}(N^*, M^*);\ f \longrightarrow f^*,$$

with inverse

$$T : \mathrm{Hom}_A^{lf}(N^*, M^*) \longrightarrow \mathrm{Hom}_A^{lf}(M^{**}, N^{**}) = \mathrm{Hom}_A^{lf}(M, N);\ f \longrightarrow f^*.$$

The dual $f^* : N^* \to M^*$ of an isomorphism of f.g. projective A-modules $f : M \to N$ is also an isomorphism, with inverse

$$(f^*)^{-1} = (f^{-1})^* : M^* \longrightarrow N^*$$

the dual of the inverse $f^{-1} : N \to M$.

Remark 3. 2. Let $f: M \to N$ be a locally finite morphism which is an A-module isomorphism. By 3. 3 (below) the inverse $f^{-1}: N \to M$ is locally finite if and only if the locally finite dual $f^*: N^* \to M^*$ is an A-module isomorphism. In particular, if f^{-1} is not locally finite then f^* is not an isomorphism. For example, let $A = \mathbb{Z}$, $M = N = \sum_{i=0}^{\infty} \mathbb{Z}$ as in 3. 1 and consider the $\mathbb{Z}$-module automorphism

$$f = \begin{pmatrix} 1 & -1 & 0 & \cdots \\ 0 & 1 & -1 & \cdots \\ 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$$

with locally finite dual

$$f^* = \begin{pmatrix} 1 & 0 & 0 & \cdots \\ -1 & 1 & 0 & \cdots \\ 0 & -1 & 1 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots .$$

In this case f^* is not an isomorphism, and the inverse of f

$$f^{-1} = \begin{pmatrix} 1 & 1 & 1 & \cdots \\ 0 & 1 & 1 & \cdots \\ 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$$

is not locally finite. In fact, f^* is a split monomorphism with cokernel $\mathbb{Z}$ which fits into a non locally finite direct sum system of $\mathbb{Z}$-modules

$$\sum_0^\infty \mathbb{Z} \underset{g}{\overset{f^*}{\rightleftarrows}} \sum_0^\infty \mathbb{Z} \underset{\begin{pmatrix} 1 \\ 0 \\ \vdots \end{pmatrix}}{\overset{(1 \quad 1 \ldots)}{\rightleftarrows}} \mathbb{Z}$$

with

$$g = \begin{pmatrix} 0 & -1 & -1 & \cdots \\ 0 & 0 & -1 & \cdots \\ 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \end{pmatrix} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots .$$

This is the canonical example of the Eilenburg swindle in algebraic K-theory. □

The following result is a special case of the proper Whitehead theorem of Farrell, Taylor and Wagoner [5], 4. 2, proved here in a more chain homotopy theoretic way.

Proposition 3. 3. *A locally finite A-module chain map $f: C \to D$ of n-dimensional locally finite A-module chain complexes is a locally finite equivalence if and only if both f and the locally finite n-dual $f^{n-*}: D^{n-*} \to C^{n-*}$ are chain equivalences.*

Proof. The algebraic mapping cone of f is a locally finite chain complex $E = C(f: C \to D)$ with locally finite n-dual

$$E^{n-*} = S^{-1}C(f^{n-*}: D^{n-*} \longrightarrow C^{n-*})$$

with S^{-1} the desuspension by a dimension shift of 1, so that $(E^{n-*})_r = C(f^{n-*})_{r+1}$. (The *suspension* of an A-module chain complex C is the A-module chain complex SC with

$$d_{SC} = d_C: SC_r = C_{r-1} \longrightarrow SC_{r-1} = C_{r-2}.)$$

We have to prove that E is locally finite chain contractible if and only if both E and E^{n-*} are chain contractible. One way is easy: the locally finite n-dual of a locally finite chain contraction $\Gamma: 0 \cong 1: E \to E$ is a (locally finite) chain contraction

$$\Gamma^{n-*}: 0 \cong 1: E^{n-*} \longrightarrow E^{n-*}.$$

Conversely, assume that there exist A-module chain contractions

$$\Gamma_1: 0 \cong 1: E \longrightarrow E, \quad \Gamma_2: 0 \cong 1: E^{n-*} \longrightarrow E^{n-*},$$

so that

$$d\Gamma_1 + \Gamma_1 d = 1: E_r \longrightarrow E_r, \quad d^*\Gamma_2 + \Gamma_2 d^* = 1: E^{n-r} \longrightarrow E^{n-r}.$$

The morphism matrices of Γ_1 and Γ_2 are column finite. The dual morphism matrices Γ_2^* are row finite, satisfying

$$d\Gamma_2^* + \Gamma_2^* d = 1: E_r \longrightarrow E_r.$$

The morphism matrices defined by

$$\Delta = (\Gamma_1 - \Gamma_2^*)\Gamma_1: E_r \longrightarrow E_{r+2}$$

are such that

$$\Gamma_2^* - \Gamma_1 = d\Delta - \Delta d: E_r \longrightarrow E_{r+1}.$$

Every morphism matrix Φ can be expressed as a sum $\Phi_1 + \Phi_2$ with Φ_1 column finite and Φ_2 row finite (e.g. by writing it as a sum of an upper triangular and a lower triangular morphism matrix). Express Δ in this way as $\Delta_1 + \Delta_2$. Since the differentials $d: E_r \to E_{r-1}$ are locally finite the morphism matrices defined by

$$\Gamma = \Gamma_1 + d\Delta_1 - \Delta_1 d = \Gamma_2^* - d\Delta_2 + \Delta_2 d: E_r \longrightarrow E_{r+1}$$

are both row finite and column finite, and so define locally finite A-module morphisms. Thus Γ is a locally finite chain contraction of E. □

Example 3.4. Let $f: C \to D$, $f': C \to D'$ be the locally finite A-module chain maps defined by

$$f = f': C_0 = A \longrightarrow D_0 = D'_0 = \sum_0^\infty A;\ x \longrightarrow (x, 0, 0, \ldots),$$

$$d: D_1 = \sum_0^\infty A \longrightarrow D_0 = \sum_0^\infty A;\ (x_0, x_1, x_2, \ldots) \longrightarrow (x_1, x_2, x_3, \ldots),$$

$$d': D'_1 = \sum_0^\infty A \longrightarrow D'_0 = \sum_0^\infty A;\ (x_0, x_1, x_2, \ldots) \longrightarrow (x_0, x_1 - x_0, x_2 - x_1, \ldots),$$

$$C_r = 0 \text{ for } r \neq 0,\ D_r = D'_r = 0 \text{ for } r \neq 0, 1.$$

Both f and f' are chain equivalences, inducing isomorphisms

$$f_*: H_*(C) = A \longrightarrow H_*(D), \quad f'_*: H_*(C) = A \longrightarrow H_*(D')$$

in homology. Also, f is a locally finite equivalence, with locally finite homotopy inverse $f^{-1}: D \to C$ defined by

$$f^{-1}: D_0 = \sum_0^\infty A \longrightarrow C_0 = A;\ (x_0, x_1, x_2, \ldots) \longrightarrow x_0,$$

and D is locally homotopy finite. However, 3.3 shows that f' is not a locally finite equivalence, since the locally finite 1-dual $f'^{1-*}: D'^{1-*} \to C^{1-*}$ induces A-module morphisms in homology

$$f^* = 0: H_0(D'^{1-*}) = A \longrightarrow H_0(C^{1-*}) = 0,$$
$$f^* = 0: H_1(D'^{1-*}) = 0 \longrightarrow H_1(C^{1-*}) = A$$

which are not isomorphisms, and D' is not locally finitely dominated. D' is essentially the example of 3.1, 3.2 all over again. For $A = \mathbb{Z}$ it shows that the real line $\mathbb{R}$ is not proper homotopy equivalent to a point. □

Remark 3.5. For any f.g. projective A-module $P = \mathrm{im}(p = p^2: A^m \to A^m)$ there is defined a locally finite resolution

$$0 \longrightarrow C_1 \xrightarrow{d} C_0 \xrightarrow{e} P \longrightarrow 0$$

with

$$d: C_1 = \sum_0^\infty A^m \longrightarrow C_0 = \sum_0^\infty A^m;$$
$$(x_0, x_1, x_2, \ldots) \longrightarrow (x_0, -p(x_0) + x_1, -p(x_1) + x_2, \ldots),$$

$$e: C_0 = \sum_0^\infty A^m \longrightarrow P;$$
$$(x_0, x_1, x_2, \ldots) \longrightarrow p(x_0 + x_1 + x_2 + \cdots).$$

C is not locally finitely dominated, by the argument of 3.4 (the special case $P=A$, $m=1$, $p=1$.) Every finitely dominated A-module chain complex is chain equivalent to a finite f.g. projective A-module chain complex, and hence to a locally finite n-dimensional complex (for some $n \geqq 0$), although not necessarily to one which is locally finitely dominated. □

For any countably projective A-modules M, N define the abelian group

$$M \otimes_A^{lf} N = \mathrm{Hom}_A^{lf}(M^*, N).$$

There is defined a natural inclusion

$$M \otimes_A N \longrightarrow M \otimes_A^{lf} N; \quad x \otimes y \longrightarrow (f \longrightarrow \overline{f(x)} \cdot y),$$

and every element of $M \otimes_A^{lf} N$ can be expressed as a locally finite infinite sum of elements $x \otimes y \in M \otimes_A N$. The duality isomorphism

$$T: \mathrm{Hom}_A^{lf}(M^*, N) \longrightarrow \mathrm{Hom}_A^{lf}(N^*, M)$$

can be identified with the transposition isomorphism

$$T: M \otimes_A^{lf} N \longrightarrow N \otimes_A^{lf} M; \quad x \otimes y \longrightarrow y \otimes x.$$

For any locally finite A-module chain complex C define the $\mathbb{Z}[\mathbb{Z}_2]$-module chain complex

$$C \otimes_A^{lf} C = \mathrm{Hom}_A^{lf}(C^*, C),$$

with $T \in \mathbb{Z}_2$ acting by the involution

$$T: C \otimes_A^{lf} C \longrightarrow C \otimes_A^{lf} C; \quad x \otimes y \longrightarrow (-)^{pq} y \otimes x \qquad (x \in C_p,\ y \in C_q),$$

which can also be written as

$$T: \mathrm{Hom}_A^{lf}(C^*, C) \longrightarrow \mathrm{Hom}_A^{lf}(C^*, C); \quad f \longrightarrow (-)^{pq} f^*$$
$$(f \in \mathrm{Hom}_A^{lf}(C^p, C_q)).$$

Let $W_{lf}^{\%} C$ denote the $\mathbb{Z}$-module chain complex

$$W_{lf}^{\%} C = \mathrm{Hom}_{\mathbb{Z}[\mathbb{Z}_2]}(W, C \otimes_A^{lf} C).$$

A *locally finite n-dimensional symmetric complex over A* (C, ϕ) is a locally finite A-module chain complex C together with a cycle $\phi \in (W_{lf}^{\%} C)_n$, as defined by a collection of locally finite A-module isomorphisms

$$\{\phi_s \in (C \otimes_A^{lf} C)_{n+s} = \sum_r \mathrm{Hom}_A^{lf}(C^{n-r+s}, C_r) \mid s \geqq 0\}$$

such that

$$d_C \phi_s + (-)^r \phi_s d_C^* + (-)^{n+s-1}(\phi_{s-1} + (-)^s T \phi_{s-1})$$
$$= 0 : C^{n-r+s-1} \longrightarrow C_r \qquad (r, s \geqq 0,\ \phi_{-1} = 0).$$

A locally finite n-dimensional symmetric complex (C, ϕ) is *Poincaré* if the locally finite chain map $\phi_0 : C^{n-*} \to C$ is a locally finite equivalence. Locally finite symmetric Poincaré pairs, cobordisms and triads are defined by analogy with the f.g. projective cases.

Proposition 3. 6. *The cobordism group of locally finitely dominated (resp. locally homotopy finite) n-dimensional symmetric Poincaré complexes over A is the projective (resp. free) symmetric L-group $L^n_p(A)$ (resp. $L^n_h(A)$).*

Proof. An n-dimensional locally finitely dominated A-module chain complex C is locally finite equivalent to an n-dimensional f.g. projective A-module chain complex D, by the algebraic theory of finiteness obstruction of Ranicki [18]. The n-dual of a locally finite equivalence $f : C \to D$ is a locally finite equivalence $f^{n-*} : D^{n-*} \to C^{n-*}$, and there is induced a $\mathbb{Z}[\mathbb{Z}_2]$-module chain equivalence

$$f \otimes_A f : C \otimes_A^{lf} C \longrightarrow D \otimes_A^{lf} D = D \otimes_A D.$$

Thus there is a natural one-one correspondence between the locally finite equivalence classes of locally finitely dominated n-dimensional symmetric (Poincaré) complexes over A and finitely dominated n-dimensional symmetric (Poincaré) complexes over A. Similarly for pairs. □

Proposition 3. 7. *There is a natural one-one correspondence between the locally finite equivalence classes of locally finite n-dimensional symmetric complexes over A and locally finite n-dimensional symmetric Poincaré pairs over A.*

Proof. This is just the locally finite version of the one-one correspondence of Ranicki [16], 3. 4, for the f.g. projective case, and proceeds as follows.

The *boundary* of a locally finite n-dimensional symmetric complex (C, ϕ) is the locally finite $(n-1)$-dimensional symmetric Poincaré complex

$$\partial(C, \phi) = (\partial C, \partial \phi)$$

with

$$d_{\partial C} = \begin{pmatrix} d_C & (-)^r \phi_0 \\ 0 & (-)^r d_C^* \end{pmatrix} :$$

$$\partial C_r = C_{r+1} \oplus C^{n-r} \longrightarrow \partial C_{r-1} = C_r \oplus C^{n-r+1},$$

$$\partial \phi_0 = \begin{pmatrix} (-)^{n-r-1} T\phi_1 & (-)^{r(n-r-1)} \\ 1 & 0 \end{pmatrix} :$$

$$\partial C^{n-r-1} = C^{n-r} \oplus C_{r+1} \longrightarrow \partial C_r = C_{r+1} \oplus C^{n-r},$$

$$\partial \phi_s = \begin{pmatrix} (-)^{n-r+s-1} T\phi_{s+1} & 0 \\ 0 & 0 \end{pmatrix} :$$

$$\partial C^{n-r+s-1} = C^{n-r+s} \oplus C_{r-s+1} \longrightarrow \partial C_r = C_{r+1} \oplus C^{n-r} \quad (s \geqq 1).$$

(We are assuming here that $d_{\partial C} : \partial C_0 \to \partial C_{-1}$ is a locally finite split surjection.)

The locally finite n-dimensional symmetric Poincaré pair

$$\delta\partial(C,\phi)=(p_C=\text{projection}:\partial C\longrightarrow C^{n-*},(0,\partial\phi))$$

is a null-cobordism of $\partial(C,\phi)$. The locally finite symmetric complex (C,ϕ) is Poincaré if and only if the boundary $\partial(C,\phi)$ is locally finite contractible.

Conversely, a locally finite n-dimensional symmetric Poincaré pair

$$X=(f:C\longrightarrow D,(\delta\phi,\phi))$$

determines the locally finite n-dimensional symmetric complex

$$X/\partial X=(D,\delta\phi)/C=(C(f),\delta\phi/\phi)$$

with

$$(\delta\phi/\phi)_s=\begin{pmatrix}\delta\phi_s & 0\\ (-)^{n-r}\phi_s f^* & (-)^{n-r+s+1}T\phi_{s-1}\end{pmatrix}:$$

$$C(f)^{n-r+s+1}=D^{n-r+s+1}\oplus C^{n-r+s}\longrightarrow C(f)_r=D_r\oplus C_{r-1}$$

which is locally finite equivalent to $\delta\partial(X/\partial X)$. □

We shall also need the relative version of Proposition 3.7:

Proposition 3.8. *There is a natural one-one correspondence between the locally finite equivalence classes of locally finite n-dimensional symmetric pairs over A and locally finite n-dimensional symmetric Poincaré triads over A.*

Proof. Define the *boundary* of a locally finite n-dimensional symmetric pair $(f:C\to D,(\delta\phi,\phi))$ to be the locally finite $(n-1)$-dimensional symmetric Poincaré pair

$$\partial(f,(\delta\phi,\phi))=(\partial f:\partial C\longrightarrow\partial_+ D,(\partial_+\delta\phi,\partial\phi))$$

with

$$d_{\partial_+ D}=\begin{pmatrix}d_D & (-)^r\delta\phi_0 & (-)^r f\phi_0\\ 0 & (-)^r d_D^* & 0\\ 0 & f^* & (-)^r d_C^*\end{pmatrix}:$$

$$\partial_+ D_r=D_{r+1}\oplus D^{n-r}\oplus C^{n-r-1}\longrightarrow\partial_+ D_{r-1}=D_r\oplus D^{n-r+1}\oplus C^{n-r},$$

$$\partial f=\begin{pmatrix}f & 0\\ 0 & 0\\ 0 & 1\end{pmatrix}:$$

$$\partial C_r=C_{r+1}\oplus C^{n-r-1}\longrightarrow\partial_+ D_r=D_{r+1}\oplus D^{n-r}\oplus C^{n-r-1}.$$

The locally finite n-dimensional symmetric Poincaré triad

$$\delta\partial(f,(\phi,\partial\phi))=\left(\begin{array}{ccc} \partial C & \xrightarrow{\partial f} & \partial_+ D \\ \downarrow{\scriptstyle p_C} & & \downarrow{\scriptstyle p_D} \\ C^{n-1-*} & \longrightarrow & C(f)^{n-*} \end{array}\;,\;\begin{array}{ccc} \partial\phi & \longrightarrow & \partial_+\delta\phi \\ \downarrow & & \downarrow \\ 0 & \longrightarrow & 0 \end{array}\right)$$

is a null-cobordism of $\partial(f,(\delta\phi,\phi))$, with p_C, p_D the projections. As in the absolute case $(f,(\delta\phi,\phi))$ is a Poincaré pair if and only if the boundary $\partial(f,(\delta\phi,\phi))$ is a contractible pair.

Conversely, a locally finite n-dimensional symmetric Poincaré triad

$$X=\left(\begin{array}{ccc} \partial C & \longrightarrow & \partial_+ D \\ \downarrow & \Gamma & \downarrow \\ C & \longrightarrow & D \end{array}\;,\;\begin{array}{ccc} \partial\phi & \longrightarrow & \partial_+\delta\phi \\ \downarrow & \Phi & \downarrow \\ \phi & \longrightarrow & \delta\phi \end{array}\right)$$

determines an n-dimensional symmetric pair

$$X/\partial X=(C/\partial C\longrightarrow D/\partial_+ D,(\delta\phi/\partial_+\delta\phi,\phi/\partial\phi))$$

such that X is locally finite equivalent to the triad $\delta\partial_+(X/\partial X)$. □

Remark 3. 9. It follows from the theory developed in § 4 below that every n-dimensional f.g. projective symmetric Poincaré complex (C,ϕ) over A is locally finite equivalent to the boundary (C',ϕ') of a locally finite countably free $(n+1)$-dimensional symmetric Poincaré pair $(f':C'\longrightarrow D',(\delta\phi',\phi'))$ over A, with f' a chain equivalence. This does not contradict 3. 6 since in general f' is not a locally finite equivalence and D' is not locally finite dominated, so that it is not implied that (C,ϕ) is null-cobordant in the f.g. projective category. In particular, consider the 0-dimensional case and suppose given a nonsingular symmetric form $(P,\phi=\phi^*:P\longrightarrow P^*)$ over A with P f.g. projective (e.g. $P=A$, $\phi=1$). Let $P=\mathrm{im}(p=p^2:A^m\longrightarrow A^m)$ and let (A^m,θ) be the (singular) symmetric form defined by

$$\theta:A^m\longrightarrow(A^m)^*;\quad x\longrightarrow(y\longrightarrow\phi(px)(py)).$$

Identifying $(A^m)^*=A^m$ by means of the A-module isomorphism

$$A^m\longrightarrow(A^m)^*;\ (a_1,a_2,\dots,a_m)\longrightarrow((b_1,b_2,\dots,b_m)\longrightarrow\sum_{k=1}^{m}b_k\bar{a}_k)$$

regard θ as an endomorphism of A^m. Use the dual of the locally finite resolution of 3. 5

$$0\longrightarrow\sum_0^\infty A^m\xrightarrow{d}\sum_0^\infty A^m\xrightarrow{e}P\longrightarrow 0$$

to define a locally finite countably free 1-dimensional symmetric complex (B, λ) over A by

$$d_B = d^* : B_1 = \sum_0^\infty A^m \longrightarrow B_0 = \sum_0^\infty A^m;$$

$$(x_0, x_1, x_2, \ldots) \longrightarrow (x_0 - p^*(x_1), x_1 - p^*(x_2), x_2 - p^*(x_3), \ldots),$$

$$\lambda_0 : B^0 = \sum_0^\infty A^m \longrightarrow B_1 = \sum_0^\infty A^m;$$

$$(x_0, x_1, x_2, \ldots) \longrightarrow (\theta(x_0), \theta(x_1), \theta(x_2), \ldots),$$

$$\lambda_0 : B^1 = \sum_0^\infty A^m \longrightarrow B_0 = \sum_0^\infty A^m;$$

$$(x_0, x_1, x_2, \ldots) \longrightarrow (\theta(x_1), \theta(x_2), \theta(x_3), \ldots),$$

$$\lambda_1 : B^1 = \sum_0^\infty A^m \longrightarrow B_1 = \sum_0^\infty A^m;$$

$$(x_0, x_1, x_2, \ldots) \longrightarrow (-\theta(x_0), -\theta(x_1), -\theta(x_2), \ldots).$$

Use the construction of 3.7 to define the locally finite countably free 1-dimensional symmetric Poincaré pair

$$(f' : C' \longrightarrow D', (\delta\phi', \phi')) = \delta\partial(B, \lambda),$$

with

$$f' = \text{projection} : C' = S^{-1}C(\lambda_0) \longrightarrow D' = B^{1-*}.$$

B is contractible but not locally finite so (cf. 3.1), with the locally finite 1-dual B^{1-*} a resolution of P, and C' is a locally finitely dominated countably free complex. f' is a chain equivalence, but not a locally finite equivalence (cf. 3.3). The composite

$$ef' : C' \xrightarrow{f'} B^{1-*} \xrightarrow{e} P$$

is chain homotopic to the locally finite equivalence $e' : C' \to P$ defined by

$$e' : C'_0 = B^1 \oplus B_1 = \sum_0^\infty A^m \oplus \sum_0^\infty A^m \longrightarrow P;$$

$$((x_0, x_1, x_2, \ldots), (y_0, y_1, y_2, \ldots)) \longrightarrow p(x_0 - y_0).$$

The composite $\phi e' : C' \to P^*$ defines a locally finite equivalence of 0-dimensional symmetric Poincaré complexes

$$\phi e' : (C', \phi') = \partial(B, \lambda) \longrightarrow (P^*, \phi).$$

This is an algebraic L-theoretic version of the Eilenberg swindle, corresponding to the expression of any compact closed n-manifold M as the boundary of the non-compact open $(n+1)$-manifold $M \times [0, \infty)$. □

§ 4. The L-theory of Laurent extensions

Given a central unit $u \in A$ such that $\bar{u} = u \in A$ let $A[t, t^{-1}]_u$ denote the Laurent polynomial extension ring $A[t, t^{-1}]$ with the involution $\bar{t} = ut^{-1}$. The inclusion of rings with involution $i: A \to A[t, t^{-1}]_u$ determines a functor preserving duality involutions

$$i_!: (A\text{-modules}) \longrightarrow (A[t, t^{-1}]\text{-modules});$$
$$M \longrightarrow i_! M = A[t, t^{-1}] \otimes_A M = M[t, t^{-1}],$$

both for f.g. projective and countably based free modules. There are induced morphisms in the L-groups

$$i_!: L^n_q(A) \longrightarrow L^n_q(A[t, t^{-1}]_u);$$
$$(C, \phi) \longrightarrow A[t, t^{-1}] \otimes_A (C, \phi) \qquad (q = h, p).$$

Define also morphisms

$$1 - u: L^n_p(A) \longrightarrow L^n_h(A); \quad (C, \phi) \longrightarrow (C, \phi) \oplus (C, -u\phi) \oplus \partial(C, 0).$$

Theorem 4. 1. *The free symmetric L-groups of $A[t, t^{-1}]_u$ fit into a long exact sequence*

$$\ldots \longrightarrow L^n_p(A) \xrightarrow{1-u} L^n_h(A) \xrightarrow{i_!} L^n_h(A[t, t^{-1}]_u)$$
$$\xrightarrow{B} L^{n-1}_p(A) \xrightarrow{1-u} L^{n-1}_h(A) \longrightarrow \ldots . \qquad \square$$

The proof of 4. 1 occupies all of § 4.

The restriction of an $A[t, t^{-1}]$-module M is an A-module $i^! M$, as already defined in § 1. If M is a based f.g. free $A[t, t^{-1}]$-module with base B then $i^! M$ is a countably based free A-module with base $t^j b$ $(j \in \mathbb{Z}, b \in B)$. The restriction of a morphism $f: M \to N$ of based f.g. free $A[t, t^{-1}]$-modules is a locally finite morphism

$$i^! f: i^! M \to i^! N.$$

The morphism of abelian groups defined by restriction

$$i^!: \mathrm{Hom}_{A[t,t^{-1}]}(M, N) \longrightarrow \mathrm{Hom}^{lf}_A(i^! M, i^! N)$$

is an injection. If F, G are the based f.g. free A-modules generated by the $A[t, t^{-1}]$-module bases of M, N and

$$f = \sum_{j=-\infty}^{\infty} f_j t^j : M = \sum_{j=-\infty}^{\infty} t^j F \longrightarrow N = \sum_{j=-\infty}^{\infty} t^j G$$

then

$$i^!f=\begin{pmatrix} \vdots & \vdots & \vdots & \\ \cdots & f_0 & f_{-1} & f_{-2} & \cdots \\ \cdots & f_1 & f_0 & f_{-1} & \cdots \\ \cdots & f_2 & f_1 & f_0 & \cdots \\ & \vdots & \vdots & \vdots & \end{pmatrix}:$$

$$i^!M=\cdots\oplus t^{-1}F\oplus F\oplus tF\oplus\cdots\longrightarrow i^!N=\cdots\oplus t^{-1}G\oplus G\oplus tG\oplus\cdots.$$

We identify

$$(i_!F)^*=i_!(F^*)$$

using the natural $A[t,t^{-1}]$-module isomorphism

$$i_!(F^*)\longrightarrow(i_!F)^*;\quad t^jf\longrightarrow(t^kx\longrightarrow f(x)u^jt^{k-j})$$
$$(j,k\in\mathbb{Z},\ f\in F^*,\ x\in F).$$

We identify

$$i^!(M^*)=(i^!M)^*$$

using the natural A-module isomorphism

$$i^!(M^*)\longrightarrow(i^!M)^*;$$
$$(f:M\longrightarrow A[t,t^{-1}])\longrightarrow([f]_0:i^!M\longrightarrow A;\ x\longrightarrow[f(x)]_0),$$

where $[a]_0=a_0\in A$ for $a=\sum_{j=-\infty}^{\infty}a_jt^j\in A[t,t^{-1}]$. The restriction of an $A[t,t^{-1}]$-module morphism

$$\alpha=\sum_{j=-\infty}^{\infty}\alpha_jt^j:M=\sum_{j=-\infty}^{\infty}t^jF\longrightarrow N^*=\sum_{j=-\infty}^{\infty}t^jG^*;$$
$$x\longrightarrow(y\longrightarrow\sum_{j=-\infty}^{\infty}\alpha_j(x)(y)t^j)\qquad(x\in F,\ y\in G)$$

is the locally finite A-module morphism

$$i^!\alpha:i^!M\longrightarrow(i^!N)^*;$$
$$t^jx\longrightarrow(t^ky\longrightarrow[\alpha(t^jx)(t^ky)]_0=\alpha_{j-k}(x)(y)u^j)$$
$$(x\in F,\ y\in G,\ j,k\in\mathbb{Z}).$$

The dual $A[t, t^{-1}]$-module morphism is given by

$$\alpha^* = \sum_{j=-\infty}^{\infty} \alpha_j^* u^j t^{-j} : N = \sum_{j=-\infty}^{\infty} t^j G \longrightarrow M^* = \sum_{k=-\infty}^{\infty} t^k F^*$$

$$y \longrightarrow (x \longrightarrow \overline{\alpha(x)(y)} = \sum_{j=-\infty}^{\infty} \overline{\alpha_j(x)(y)}\, u^j t^{-j}) \quad (x \in F,\ y \in G).$$

For any finite $A[t, t^{-1}]$-module chain complex E there is defined a restriction map

$$i^! : E \otimes_{A[t,t^{-1}]_u} E = \mathrm{Hom}_{A[t,t^{-1}]}(E^*, E) \longrightarrow i^! E \otimes_A^{lf} i^! E = \mathrm{Hom}_A^{lf}(i^! E^*, i^! E).$$

The *restriction* of a finite n-dimensional symmetric complex (E, Θ) over $A[t, t^{-1}]_u$ is the locally finite n-dimensional symmetric complex over A

$$i^!(E, \Theta) = (i^! E, i^! \Theta).$$

Given a locally finite n-dimensional symmetric complex (C, ϕ) over A and a based free subcomplex $B \subseteqq C$ define the locally finite n-dimensional symmetric complex over A

$$(C, \phi)/B = (C/B, p^{\%}(\phi)),$$

with $p : C \longrightarrow C/B$ the locally finite morphism defined by projection.

The *torsion* of a finite n-dimensional symmetric Poincaré complex (E, Θ) over A is defined by

$$\tau(E, \Theta) = \tau(\Theta_0 : E^{n-*} \longrightarrow E) \in \tilde{K}_1(A).$$

The K-theory map $B : \tilde{\tilde{K}}_1(A[t, t^{-1}]) \longrightarrow \tilde{K}_0(A)$ sends the torsion $\tau(E)$ of a contractible finite $A[t, t^{-1}]$-module chain complex E with $E_r = i_! F_r$ to

$$B(\tau(E)) = [t^{-N^+} F^+] \in \tilde{K}_0(A)$$

for any $N^+ \in \mathbb{N}^+(E)$ (1. 3). The proof of 4. 1 identifies the image under B of the torsion of a finite n-dimensional symmetric Poincaré complex (E, Θ) over $A[t, t^{-1}]_u$ with the finiteness obstruction of an explicitly constructed finitely dominated $(n-1)$-dimensional symmetric Poincaré complex $B(E, \Theta)$ over A,

$$B(\tau(E, \Theta)) = [B(E, \Theta)] \in \tilde{K}_0(A),$$

as follows:

Proposition 4. 2. i) *For any finite n-dimensional symmetric Poincaré complex* (E, Θ) *over* $A[t, t^{-1}]_u$ *with* $E_r = i_! F_r$ *and any* $N^+ \in \mathbb{N}^+(E)$ *there is defined a locally finite n-dimensional symmetric complex* $i^!(E, \Theta)/t^{-N^+} F^+$ *over A, such that the boundary* $\partial(i^!(E, \Theta)/t^{-N^+} F^+)$ *is a locally finitely dominated* $(n-1)$*-dimensional symmetric Poincaré complex over A with*

$$B(\tau(E, \Theta)) = [\partial(i^! E/t^{-N^+} F^+)] \in \tilde{K}_0(A).$$

ii) *The map* $B: L_h^n(A[t, t^{-1}]_u) \to L_p^{n-1}(A)$ *is such that*

$$B(E, \Theta) = \partial(i^!(E, \Theta)/t^{-N^+} F^+) \in L_p^{n-1}(A). \quad \square$$

Remark 4. 3. A finite (resp. finitely dominated) n-dimensional symmetric Poincaré complex (C, ϕ) over A is *highly-connected* if $H_r(C) = 0$ for $2r < n-1$. See Ranicki [16], § 2, for the details of the one-one correspondence between such highly-connected complexes and f.g. free (resp. f.g. projective) nonsingular $(-)^k$-symmetric forms $(n = 2k)$ and formations $(n = 2k+1)$ over A. If (E, Θ) is a highly-connected finite n-dimensional symmetric Poincaré complex over $A[t, t^{-1}]_u$ then the finitely dominated $(n-1)$-dimensional symmetric Poincaré complex $B(E, \Theta)$ constructed in 4. 2 is also highly-connected. The corresponding passage from forms and formations over $A[t, t^{-1}]_u$ to formations and forms over A is the exact analogue for the symmetric case of the formulae of Ranicki [15] in the quadratic case. However, whereas the quadratic L-groups are 4-periodic $L_* = L_{*+4}$ and are represented by highly-connected complexes (corresponding to Witt groups of forms and formations) this is not in general the case for the symmetric L-groups L^* with $* \geqq 2$. $\square$

4. 1 and 4. 2 are proved by first defining the relative L-groups for

$$1-u: L_p^*(A) \to L_h^*(A)$$

as the cobordism groups of "finitely balanced" symmetric Poincaré pairs over A, and then proving that these relative L-groups $L_{h,p}^*(1-u)$ are isomorphic to the absolute L-groups $L_h^*(A[t, t^{-1}]_u)$ of finite symmetric Poincaré complexes over $A[t, t^{-1}]_u$.

An n-dimensional symmetric pair over A

$$X = ((f\,g): C \oplus C' \longrightarrow D, (\delta\phi, \phi \oplus -\phi'))$$

is *u-fundamental* if

$$(C', \phi') = (C, u\phi),$$

in which case it is the (algebraic) fundamental domain of a symmetric complex over $A[t, t^{-1}]_u$, defined as follows.

The *Laurent union* of a (locally finite) u-fundamental n-dimensional symmetric pair $X = ((f\,g): C \oplus C \to D, (\delta\phi, \phi \oplus -\phi))$ over A is the (locally finite) n-dimensional symmetric complex over $A[t, t^{-1}]_u$

$$U(X) = (E, \Theta)$$

with

$$d_E = \begin{pmatrix} d_D & (-)^{r-1}(f - g\,t) \\ 0 & d_C \end{pmatrix}:$$

$$E_r = D_r[t, t^{-1}] \oplus C_{r-1}[t, t^{-1}] \longrightarrow E_{r-1} = D_{r-1}[t, t^{-1}] \oplus C_{r-2}[t, t^{-1}],$$

$$\Theta_s = \begin{pmatrix} \delta\phi_s & (-)^s g\,\phi_s\,t \\ (-)^{n-r-1}\phi_s f^* & (-)^{n-r+s} T\phi_{s-1} \end{pmatrix}:$$

$$E^{n-r+s} = D^{n-r+s}[t, t^{-1}] \oplus C^{n-r+s-1}[t, t^{-1}] \longrightarrow E_r = D_r[t, t^{-1}] \oplus C_{r-1}[t, t^{-1}].$$

The restriction of $U(X)$ is the locally finite n-dimensional symmetric complex over A defined by the countable union

$$i^!U(X) = \bigcup_{j=-\infty}^{\infty} t^j X$$

of the copies of X

$$t^j X = ((f\,g) : t^j C \oplus t^{j+1} C \longrightarrow t^{j+1} D,\ (u^j \delta\phi,\ u^j \phi \oplus -u^{j+1}\phi)) \qquad (j \in \mathbb{Z}).$$

$t^{-1}C$	$D \xleftarrow{f} C$	$\xrightarrow{gt} tD$	$tC \quad t^2D$	t^2C

The boundary $\partial U(X)$ is (locally finite) homotopy equivalent to the Laurent union $U(\partial X)$ of the boundary (locally finite) u-fundamental $(n-1)$-dimensional symmetric Poincaré cobordism $\partial X = ((\partial f\ \partial g) : \partial C \oplus \partial C \longrightarrow \partial_+ D,\ (\partial_+ \delta\phi,\ \partial\phi \oplus -u\partial\phi))$

$$\partial U(X) \cong U(\partial X)$$

(as defined in the proof of 3. 8). Thus if X is a Poincaré pair over A then $U(X)$ is a Poincaré complex over $A[t, t^{-1}]_u$.

The Laurent union $U(X) = (E, \Theta)$ is the L-theory analogue of a Mayer-Vietoris presentation. Indeed, E is the algebraic mapping cone

$$E = C(f - gt : C[t, t^{-1}] \longrightarrow D[t, t^{-1}]).$$

Replacing D by the algebraic mapping cylinder D' of $(f\,g) : C \oplus C \to D$ there is obtained an $A[t, t^{-1}]$-module chain complex E' chain equivalent to E, with a Mayer-Vietoris presentation

$$0 \longrightarrow i_! C \xrightarrow{f'-g't} i_! D' \longrightarrow E' \longrightarrow 0.$$

A u-fundamental n-dimensional (locally finite) symmetric pair over A

$$X = ((f\,g) : C \oplus C \to D,\ (\delta\phi,\ \phi \oplus -u\phi))$$

is *(locally) finitely balanced* if it is (locally) finitely dominated and

$$[C] = [D] \in \tilde{K}_0(A),$$

in which case the Laurent union $U(X)$ is a homotopy (locally) finite symmetric complex over $A[t, t^{-1}]_u$. In particular, this is the case if C, D are finite.

Proposition 4. 4. *The cobordism group of finitely balanced u-fundamental n-dimensional symmetric Poincaré pairs over A is the relative group* $L^n_{h,p}(1-u)$ *in the exact sequence*

$$\dots \longrightarrow L^{n-1}_p(A) \xrightarrow{1-u} L^n_h(A) \xrightarrow{j} L^n_{h,p}(1-u) \xrightarrow{\partial} L^{n-1}_p(A) \longrightarrow \dots,$$

with

$$j : L^n_h(A) \longrightarrow L^n_{h,p}(1-u);\ (D, \delta\phi) \longrightarrow (0 \oplus 0 \longrightarrow D, (\delta\phi, 0 \oplus 0)),$$

$$\partial : L^n_{h,p}(1-u) \longrightarrow L^{n-1}_p(A);$$

$$((f\,g) : C \oplus C \longrightarrow D, (\delta\phi, \phi \oplus -u\phi)) \longrightarrow (C, \phi).$$

$L^n_{h,p}(1-u)$ *is also the cobordism group of locally finitely balanced Poincaré pairs.*

Proof. $L^n_{h,p}(1-u)$ is the cobordism group of homotopy finite n-dimensional symmetric Poincaré cobordisms over A of the type

$$(C \oplus C \oplus \partial C \to D, (\delta\phi, \phi \oplus -u\phi \oplus \partial 0)).$$

Given such a cobordism define a finitely balanced u-fundamental n-dimensional symmetric Poincaré pair

$$(C \oplus C \longrightarrow D', (\delta\phi', \phi \oplus -u\phi))$$
$$= (C \oplus C \oplus \partial C \longrightarrow D, (\delta\phi, \phi \oplus -u\phi \oplus \partial 0)) \cup_{\partial(C,0)} (p_C : \partial C \longrightarrow C^{n+1-*}, (0, \partial 0)),$$

with $p_C : \partial C \to C^{n+1-*}$ the projection. Conversely, given a finitely balanced u-fundamental n-dimensional symmetric Poincaré pair $(C \oplus C \to D, (\delta\phi, \phi \oplus -u\phi))$ define a homotopy finite n-dimensional symmetric Poincaré cobordism

$$(C \oplus C \oplus \partial C \longrightarrow D'', (\delta\phi'', \phi \oplus -u\phi \oplus \partial 0))$$
$$= (C \oplus C \longrightarrow D, (\delta\phi, \phi \oplus -u\phi)) \oplus (p_C : \partial C \to C^{n+1-*}, (0, \partial 0)).$$

Similarly for the locally finite case. □

We show that U defines an isomorphism

$$U : L^n_{h,p}(1-u) \longrightarrow L^n_h(A[t, t^{-1}]_u);\ X \longrightarrow U(X),$$

using the following L-theory analogue of the existence of finite Mayer-Vietoris presentations of finite $A[t, t^{-1}]$-module chain complexes (1. 2):

Proposition 4. 5. *Every finite n-dimensional symmetric Poincaré complex* (E, Θ) *over* $A[t, t^{-1}]_u$ *is homotopy equivalent to the Laurent union* $U(X)$ *of a locally finitely balanced u-fundamental n-dimensional symmetric Poincaré pair over A*

$$X = ((f\,g) : C \oplus C \longrightarrow D, (\delta\phi, \phi \oplus -u\phi))$$

with

$$B(\tau(E, \Theta)) = [C] \in \tilde{K}_0(A). \quad \square$$

The isomorphism inverse to U is then defined by

$$U^{-1}: L^n_h(A[t, t^{-1}]_u) \longrightarrow L^n_{h,p}(1-u);\ (E, \Theta) = U(X) \longrightarrow X,$$

and B is given by

$$B: L^n_h(A[t, t^{-1}]_u) \longrightarrow L^{n-1}_p(A);\ (E, \Theta) \longrightarrow (C, \phi)$$

with $X = ((f\,g): C \oplus C \to D, (\delta\phi, \phi \oplus -u\phi))$ the locally finitely balanced Poincaré pair given by 4. 5. In order to actually verify that U^{-1} and B are well-defined we need the relative version of 4. 5 stated in 4. 6 below.

The *algebraic mapping torus* of a morphism of (locally finite) n-dimensional symmetric complexes over A

$$(f, \chi): (C, u\phi) \longrightarrow (C, \phi)$$

is the (locally finite) $(n+1)$-dimensional symmetric complex over $A[t, t^{-1}]_u$

$$T(f, \chi) = U(Y)$$

defined by the Laurent union of the (locally finite) u-fundamental symmetric cobordism

$$Y = ((1\,f): C \oplus C \longrightarrow C, (\chi, \phi \oplus -u\phi)).$$

The underlying $A[t, t^{-1}]$-module chain complex is the algebraic mapping torus of $f: C \to C$

$$T(f) = C(f - t: i_!C \longrightarrow i_!C).$$

The boundary $\partial T(f, \chi)$ is (locally finite) homotopy equivalent to the Laurent union $U(X)$ of the (locally finite) u-fundamental n-dimensional symmetric pair over A

$$X = \partial Y = ((\partial 1\ \partial f): \partial C \oplus \partial C \longrightarrow \partial_+ C, (\partial_+ \chi, \partial\phi \oplus -u\partial\phi))$$

defined as in the proof of 3. 8.

For any countably based free $A[t, t^{-1}]$-module M define a Mayer-Vietoris presentation

$$0 \longrightarrow i_!i^!M \xrightarrow{\zeta(M)-t} i_!i^!M \xrightarrow{p(M)} M \longrightarrow 0$$

with

$$\zeta(M): i^!M \longrightarrow i^!M;\ x \longrightarrow tx,$$

$$p(M): i_!i^!M \longrightarrow M;\ a \otimes x \longrightarrow ax \qquad (a \in A[t, t^{-1}],\ x \in M).$$

Define also a Mayer-Vietoris presentation of the dual countably based free $A[t, t^{-1}]$-module M^*

$$0 \longrightarrow i_! i^!(M) \xrightarrow{\zeta^*(M) - ut^{-1}} i_! i^!(M) \xrightarrow{p^*(M)} M^* \longrightarrow 0$$

with

$$\zeta^*(M) = \zeta(M)^* : i^!(M^*) = (i^! M)^* \longrightarrow i^!(M^*);$$
$$f \longrightarrow (x \longrightarrow f(tx)),$$
$$p^*(M) = p(M^*) : i_! i^!(M^*) \longrightarrow M^*;$$
$$a \otimes f \longrightarrow af \qquad (a \in A[t, t^{-1}],\ f \in M^*).$$

Proof of 4. 5. Given a finite n-dimensional symmetric complex (E, Θ) over $A[t, t^{-1}]_u$ fix an element

$$N^+ = (N_0^+, N_1^+, \ldots, N_n^+; \infty, \infty, \ldots, \infty) \in \mathbb{N}^+(E).$$

Define a morphism of locally finite n-dimensional symmetric complexes over A

$$(\eta, 0) : (C, u\phi) \longrightarrow (C, \phi)$$

by

$$(C, \phi) = i^!(E, \Theta)/t^{-N^+} F^+,\ \eta : C \longrightarrow C;\ x \longrightarrow tx.$$

The algebraic mapping torus of $(\eta, 0)$ is the locally finite $(n+1)$-dimensional symmetric complex over $A[t, t^{-1}]_u$

$$T(\eta, 0) = U(Y)$$

defined by the Laurent union of the locally finite u-fundamental $(n+1)$-dimensional symmetric pair over A

$$Y = ((1\ \eta) : C \oplus C \longrightarrow C, (0, \phi \oplus -u\phi)).$$

We shall show that (E, Θ) is locally finite homotopy equivalent to the boundary $\partial T(\eta, 0)$, and hence to the Laurent union $U(X)$ of the locally finitely balanced u-fundamental n-dimensional symmetric Poincaré cobordism $X = \partial Y$ over A, with $B(E, \Theta) = \partial(C, \phi)$.

The dual of the locally finite A-module morphism defined by projection

$$i^! E_r = i^! i_! F_r \longrightarrow C_r = t^{-N_r^+} F_r^-$$

is the locally finite A-module morphism defined by injection

$$C^r = t^{-N_r^+} (F^r)^- \longrightarrow i^! E^r = i^! i_! F^r.$$

The $A[t, t^{-1}]$-module morphisms $\eta - t : i_! C_r \to i_! C_r$ are automorphisms (such that the inverses are not locally finite, cf. Remark 3. 1). Also, there are defined Mayer-Vietoris presentations

$$0 \longrightarrow i_! C^r \xrightarrow{\eta^* - ut^{-1}} i_! C^r \xrightarrow{g} E^r \longrightarrow 0$$

with g the (non locally finite) $A[t, t^{-1}]$-module morphisms

$$g : i_! C^r \xrightarrow{\text{inclusion}} i_! i^! E^r \xrightarrow{p^*(E_r)} E^r = i_! F^r.$$

Define a (non locally finite) chain equivalence of locally finite $A[t, t^{-1}]$-module chain complexes

$$e : \partial T(\eta) \longrightarrow E$$

by

$$e = (000\Theta_0 g) : \partial T(\eta)_r = i_! C_{r+1} \oplus i_! C_r \oplus i_! C^{n-r+1} \oplus i_! C^{n-r}$$
$$\longrightarrow E_r = i_! F_r.$$

The (non locally finite) $A[t, t^{-1}]$-module morphisms

$$h : i_! C_r \xrightarrow{\text{inclusion}} i_! i^! E_r \xrightarrow{p(E_r)} E_r = i_! F_r$$

are such that the $A[t, t^{-1}]$-module morphisms

$$e^{lf} = e + d_E(h000) + (h000) d_{\partial T(\eta)} : \partial T(\eta)_r \longrightarrow E_r$$

are locally finite. The locally finite $A[t, t^{-1}]$-module chain map

$$e^{lf} : \partial T(\eta) \longrightarrow E$$

is chain homotopic to e, defining a locally finite equivalence of homotopy finite n-dimensional symmetric Poincaré complexes over $A[t, t^{-1}]_u$

$$(e^{lf}, 0) : \partial T(\eta, 0) \longrightarrow (E, \Theta).$$

Define $\bar{N}^- = (\infty, \infty, \ldots, \infty; \bar{N}_0^-, \bar{N}_1^-, \ldots, \bar{N}_n^-) \in \mathcal{N}^-(E^{n-}*)$ by $\bar{N}_r^- = N_{n-r}^+$ $(0 \leqq r \leqq n)$. Let $N^- = (\infty, \infty, \ldots, \infty; N_0^-, N_1^-, \ldots, N_n^-) \in \mathcal{N}^-(E)$ be so large that

$$\Theta_0(t^{\bar{N}^-}(F^{n-}*)^-) \subseteqq t^{N^-} F^-,$$

so that $i^! \Theta_0 : i^! E^{n-}* \to i^! E$ restricts to a locally finite A-module chain map

$$\lambda = i^! \Theta_0 \,|\, : t^{\bar{N}^-}(F^{n-}*)^- \longrightarrow t^{N^-} F^-$$

and there is defined an exact sequence of locally finite A-module chain complexes

$$0 \longrightarrow t^{N^-} F^- \cap t^{-N^+} F^+ \longrightarrow t^{N^-} F^- \longrightarrow C \longrightarrow 0$$

with $t^{N^-}F^- \cap t^{-N^+}F^+$ finite. By 1.3 and 3.3 the algebraic mapping cone $C(\lambda)$ is locally finitely dominated with finiteness obstruction

$$[C(\lambda)] = -B(\tau(\Theta_0 : E^{n-*} \longrightarrow E)) \in \tilde{K}_0(A).$$

It now follows from the exact sequences

$$0 \longrightarrow t^{N^-}F^- \cap t^{-N^+}F^+ \longrightarrow C(\lambda) \longrightarrow C(\phi_0 : C^{n-*} \longrightarrow C) \longrightarrow 0$$

that

$$[\partial C] = -[C(\phi_0 : C^{n-*} \longrightarrow C)] = B(\tau(E, \Theta)) \in \tilde{K}_0(A). \quad \square$$

An n-dimensional symmetric triad over A

$$X = \left(\begin{array}{ccc} \partial C \oplus \partial C' & \xrightarrow{(\partial f\ \partial g)} & \partial_+ D \\ \downarrow & & \downarrow \\ C \oplus C' & \xrightarrow{(f\ g)} & D \end{array} , \begin{array}{ccc} \partial\phi \oplus -\partial\phi' & \longrightarrow & \partial_+ \delta\phi \\ \downarrow & & \downarrow \\ \phi \oplus -\phi' & \longrightarrow & \delta\phi \end{array} \right)$$

is *u-fundamental* if $\partial C \oplus \partial C' \to C \oplus C'$ is the sum of chain maps $\partial C \to C$, $\partial C' \to C'$ and

$$(\partial C' \longrightarrow C', (\phi', \partial\phi')) = (\partial C \longrightarrow C, u(\phi, \partial\phi)).$$

The *Laurent union* n-dimensional symmetric pair over $A[t, t^{-1}]_u$

$$U(X) = (\partial E \longrightarrow E, (\Theta, \partial\Theta))$$

is defined by analogy with the absolute case $(\partial C \oplus \partial C \to \partial_+ D) = 0$, with

$$\partial E = C(\partial f - \partial g t : \partial C[t, t^{-1}] \longrightarrow \partial_+ D[t, t^{-1}]),$$
$$E = C(f - g t : C[t, t^{-1}] \longrightarrow D[t, t^{-1}]).$$

As in the absolute case X is a fundamental domain of $U(X)$, and the restriction is obtained by glueing together all the copies $t^j X$ $(j \in \mathbb{Z})$ of X

$$i^! U(X) = \bigcup_{j=-\infty}^{\infty} t^j X.$$

	$t^{-1}\partial C$	$\partial_+ D$	∂C	$t\partial_+ D$	$t\partial C$	$t^2\partial_+ D$	$t^2\partial C$
$t^{-1}C$		D	C				
				tD	tC		
						$t^2 D$	$t^2 C$

A u-fundamental (locally finite) symmetric triad over A

$$X = \left(\begin{array}{ccc} \partial C \oplus \partial C & \longrightarrow & \partial_+ D \\ \downarrow & & \downarrow \\ C \oplus C & \longrightarrow & D \end{array} \right), \quad \left(\begin{array}{ccc} \partial\phi \oplus -u\partial\phi & \longrightarrow & \partial_+ \delta\phi \\ \downarrow & & \downarrow \\ \phi \oplus -u\phi & \longrightarrow & \delta\phi \end{array} \right)$$

is (*locally*) *finitely balanced* if it is (locally) finitely dominated and

$$[C] = [D],\ [\partial C] = [\partial_+ D] \in \tilde{K}_0(A),$$

in which case the Laurent union $U(X)$ is a homotopy (locally) finite symmetric pair over $A[t, t^{-1}]_u$.

The *torsion* of a finite n-dimensional symmetric Poincaré pair $(f : \partial E \to E, (\Theta, \partial\Theta))$ over A is defined by

$$\tau(f : \partial E \longrightarrow E, (\Theta, \partial\Theta)) = \tau((\Theta_0, \partial\Theta_0) : C(f)^{n-*} \longrightarrow E) \in \tilde{K}_1(A).$$

4. 5 is the special case $(\partial E, \partial\Theta) = 0,\ \partial X = 0$ of the following relative version:

Proposition 4. 6. *Every finite n-dimensional symmetric Poincaré pair over* $A[t, t^{-1}]_u$ $(f : \partial E \to E, (\Theta, \partial\Theta))$ *is homotopy equivalent to the Laurent union* $U(X)$ *of a locally finitely balanced u-fundamental n-dimensional symmetric Poincaré triad* X *over* A *such that*

$$B(\tau(f : \partial E \longrightarrow E, (\Theta, \partial\Theta))) = [C] \in \tilde{K}_0(A). \quad \square$$

Proof of 4. 1. The Laurent union morphism

$$U : L^n_{h,p}(1-u) \longrightarrow L^n_h(A[t, t^{-1}]_u);\ X \longrightarrow U(X),$$

is onto by 4. 5, and one-one by 4. 6.

§ 5. An example

Let $\mathcal{F} = \mathbb{R}(x)[y]/(x^2 + y^2 + 1)$, the quotient field of $(\mathbb{R}[x, y]/(x^2 + y^2 + 1))$, then we have

Lemma 5. 1. $\mathcal{F}(i) = \mathbb{C}(t)$, *the rational function field, where* i *is, as usual, a primitive* 4^{th}*-root of* 1.

Proof. Define a map $\phi : \mathscr{F}(i) \longrightarrow \mathbb{C}(t)$ by setting

$$\phi(x) = \frac{1}{\sqrt{2}}(t - t^{-1}),$$

$$\phi(y) = \frac{i}{\sqrt{2}}(t + t^{-1}).$$

Now, $\phi\left(\frac{1}{\sqrt{2}}(x - iy)\right) = t$, so ϕ is onto. Since both range and domain are fields ϕ is an isomorphism, and the lemma follows. □

Lemma 5. 2. *Define an involution λ on $\mathbb{C}(t)$ by setting $\lambda(t) = -t^{-1}$, $\lambda(i) = -i$, $\lambda = \mathrm{id}$ on $\mathbb{R} \subset \mathbb{C}$, then the fixed field of λ, $\mathbb{C}(t)^{\lambda}$ is $\mathscr{F}$.*

Proof. Directly we have that $\lambda(\phi(x)) = \phi(x)$, $\lambda(\phi(y)) = \phi(y)$. Hence, $\phi(\mathscr{F}) \subset \mathbb{C}(t)^{\lambda}$, and the result follows by a dimension count. □

The L-groups of a ring A with respect to the trivial involution are denoted simply by $L_*(A)$. When the involution is non-trivial, say τ, we write the corresponding L-groups as $L_*(A, \tau)$.

We now wish to study the Witt group $W(\mathscr{F}) = L_0(\mathscr{F})$ with respect to the trivial (identity) involution on $\mathscr{F}$. From now on we shall only be dealing with the L^h-groups, and so omit h from the terminology.

Theorem 5. 3 (Knebusch [9], § 11). (i) *There is an exact sequence*

$$0 \longrightarrow \mathbb{Z}/2 \longrightarrow L_0(\mathscr{F}) \longrightarrow \mathbb{Z}/2 \oplus \bigoplus_{\mathscr{I}} \mathbb{Z}/2 \longrightarrow 0$$

where the index set $\mathscr{I}$ is the points $p \in \mathscr{M}_1$ and $\mathscr{M}_1$ is the open Möbius band

$$\{\mathbb{C} - \{0\}/(z \sim -1/\bar{z})\}.$$

The first $\mathbb{Z}/2$ carries the element $\langle 1 \rangle$.

(ii) *The sequence above does not split. In particular the Stufe of $\mathscr{F}$ is 2.*

Proof. There is an exact sequence due to N. Jacobson, (see [12], Appendix B)

$$0 \longrightarrow L_0(\mathbb{C}(t), \lambda) \longrightarrow L_0(\mathscr{F}) \longrightarrow L_0(\mathbb{C}(t)). \tag{5. 4}$$

Again, quoting a result of Milnor ([12], Theorem 3. 1, p. 265) for any field $\mathscr{K}$ of characteristic different from 2 there is an exact sequence

$$0 \longrightarrow L_0(\mathscr{K}) \longrightarrow L_0(\mathscr{K}(t)) \longrightarrow \bigoplus_{\mathscr{P}} L_0(\mathscr{K}[t]/\mathscr{P}) \longrightarrow 0 \tag{5. 5}$$

where $\mathscr{P}$ runs over all the primes of $\mathscr{K}[t]$. In our case

$$L_0(\mathbb{C}(t)) = \left(\bigoplus_{z \in \mathbb{C}} L_0(\mathbb{C})\right) \oplus L_0(\mathbb{C}) \quad \text{where} \quad L_0(\mathbb{C}) = \mathbb{Z}/2.$$

Moreover, the involution λ on primes $(t-z)$ becomes $\lambda(t-z)=-\bar{z}t^{-1}(t+1/\bar{z})$, and we see that λ is geometrically the map $z \leftrightarrow -1/\bar{z}$. In particular the extra $\mathbb{Z}/2$ can be identified with the $\mathbb{Z}/2$ over ∞ in S^2 and, clearly, this $\mathbb{Z}/2$ and the $\mathbb{Z}/2$ corresponding to the prime (t) are interchanged by λ as well. (There is room for possible confusion here. The inclusion $L_0(\mathbb{C}) \subset L_0(\mathscr{F})$ includes the $\mathbb{Z}/2$ as the sum of the two terms above.) □

Next, note that

Lemma 5. 6. (i) $\operatorname{im} L_0(\mathscr{F}) \hookrightarrow L_0(\mathbb{C}(t))$ *is contained in* $L_0(\mathbb{C}(t))^{\lambda}$.

(ii) *If* $0 \in L_0(\mathbb{C}(t))$ *has the form* $\mu+\lambda(\mu)$ *then* $0 \in \operatorname{im} L_0(\mathbb{F})$.

Proof. (i) is clear. To see (ii), suppose $\mu=\sum\langle a_i\rangle$, so that

$$\mu+\lambda(\mu)=\sum\langle a_i\rangle \perp \langle\lambda(a_i)\rangle.$$

In our case there are only two invariants determining an element in $L_0(\mathbb{C}(t))$, the rank mod(2) and the discriminant. But $\langle a\lambda(a)\rangle \perp \langle 1\rangle$ and $\langle a\rangle \perp \langle\lambda(a)\rangle$ both have even rank and equal discriminant. Hence they are equivalent in the Witt group, and (ii) follows. □

This identifies the image of $L_0(\mathscr{F})$ in $L_0(\mathbb{C}(t))$. We now must analyze the kernel in the map (5. 4). It is precisely at this point we require our results on Laurent extensions.

Consider first the localization exact sequence

$$L_*(\mathbb{C}[t,t^{-1}],\lambda) \longrightarrow L_*(\mathbb{C}(t),\lambda) \longrightarrow \bigoplus_{\mathscr{P}\,\text{fixed}} L_*(\mathbb{C}[t,t^{-1}]/\mathscr{P},\lambda) \longrightarrow L_{*-1}(\mathbb{C}[t,t^{-1}],\lambda) \longrightarrow \cdots.$$

(See e.g. [17], § 3.) We have already seen that there are no fixed primes. Hence

$$L_*(\mathbb{C}[t,t^{-1}],\lambda) \cong L_*(\mathbb{C}(t),\lambda). \tag{5. 7}$$

Our main result 4. 1 applies to give an exact sequence

$$\cdots \longrightarrow L_*(\mathbb{C},-) \xrightarrow{\langle 1\rangle \perp \langle 1\rangle} L_*(\mathbb{C},-) \longrightarrow L_*(\mathbb{C}[t,t^{-1}],\lambda) \longrightarrow L_{*-1}(\mathbb{C},-) \longrightarrow \cdots$$

where by $L_*(\ ,-)$ we mean the L-group with respect to complex conjugation. It is well known that

$$L_*(\mathbb{C},-)=\begin{cases}\mathbb{Z} & * \text{ even},\\ 0 & * \text{ odd}\end{cases}$$

and the generators are $\langle 1\rangle$ for $*=0$, $\langle i\rangle$ for $*=2$. Then $\circ(\langle 1\rangle \perp \langle 1\rangle)$ is just multiplication by 2 and we have

$$L_*(\mathbb{C}[t,t^{-1}],\lambda)=\begin{cases}\mathbb{Z}/2 & * \text{ even},\\ 0 & * \text{ odd}.\end{cases}$$

The existence of the exact sequence follows.

It remains to show that it does not split. To this end consider the inclusion

$$L_0(\mathbb{C}(t), \lambda) \longrightarrow L_0(\mathscr{F}),$$

which is obtained by taking real forms. A basis for $\mathbb{C}(t)$ over $\mathscr{F}$ is given by 1, i, so that the image of the Hermitian form $\langle 1\rangle$ is $\langle 1\rangle \perp \langle 1\rangle$. The proof is complete. □

Remark 5. 8. We shall see in the next section that $\mathscr{F}$ is an example of a genus 0 function field. Indeed, the original motivation for presenting the exact sequence for Laurent extensions in the generality used here was to apply it to study these Witt groups. T. Y. Lam pointed out to one of us somewhat later that the field $\mathscr{F}$ above was a genus 0 function field, and asked us to determine its Stufe. □

Remark 5. 9. The quotient field

$$\mathscr{F}_{n+1} = \mathbb{R}(x_1, \ldots, x_n)(y)[z]/(y^2 + z^2 + \sum x_j^2 + 1) \tag{5. 10}$$

also satisfies $\mathscr{F}_{n+1}(i) = \mathbb{C}(x_1, \ldots, x_n, t)$ and $\mathscr{F}_{n+1}$ is the fixed field of

$$\lambda : \lambda(i) = -i, \quad \lambda(x_j) = x_j, \quad \lambda(t) = -(1 + \sum x_j^2)t^{-1}.$$

Hence, it appears possible to apply the techniques above to obtain information about $L_*(\mathscr{F}_{n+1})$.

For example, when $n = 1$ it is not hard to show that we have the diagram

(5. 11)

$$\begin{array}{ccccc}
\bigoplus_{r \in \mathbb{R}} (\mathbb{Z}/2) & & & & \\
\downarrow & & & & \\
L_0(\mathbb{C}(t), \lambda) & \longrightarrow & L_0(\mathscr{F}_1) & \longrightarrow & L_0(\mathbb{C}(x)(t)) \\
\downarrow & & \downarrow & & \downarrow \\
\bigoplus_{\mathscr{P} \subset \mathscr{F}_1} L_0(\mathbb{C}(x)[t]/\mathscr{P}, \lambda) & \longrightarrow & \bigoplus_{\mathscr{P} \subset \mathscr{F}_1} L_0(\mathscr{F}/\mathscr{P}) & \longrightarrow & \bigoplus_{\mathscr{Q}} L_0(\mathbb{C}(x)[t]/\mathscr{Q}).
\end{array}$$

Thus the Stufe is $\leqq 4$ in this case. □

§ 6. Genus 0 functions fields

We assume from now on that $\mathbb{F}$ is a field and $\mathrm{char}(\mathbb{F}) \neq 2$. For non-zero $\lambda, \mu \in \mathbb{F}$ let

$$\left\langle \begin{matrix} \lambda, \mu \\ \mathbb{F} \end{matrix} \right\rangle = \mathbb{F}[i, j]/\{i^2 = \lambda,\ j^2 = \mu,\ ij = -ji\}$$

be a quaternion algebra over $\mathbb{F}$, and let

$$\mathbb{F}\langle \lambda, \mu \rangle = \mathbb{F}(x)[y]/(y^2 - \mu(x^2 - 4\lambda)) \tag{6. 1}$$

be the associated transcendence degree 1 extension field of $\mathbb{F}$. $\mathbb{F}\langle\lambda, \mu\rangle$ is a degree 2 extension of the rational function field $\mathbb{F}(x)$. It is a standard result of algebraic number theory (Hasse [7], p. 480) that a genus 0 function field over $\mathbb{F}$ is isomorphic to one of the type $\mathbb{F}\langle\lambda, \mu\rangle$.

Note that y is integral over the polynomial subring $\mathbb{F}[x] \subset \mathbb{F}(x)$ so that $\mathbb{F}[x](y) = \mathbb{F}[x, y]/(y^2 - \mu(x^2 - 4\lambda))$ injects into $\mathbb{F}\langle\lambda, \mu\rangle$.

Lemma 6. 2. *$\mathbb{F}[x](y) \subset \mathbb{F}\langle\lambda, \mu\rangle$ is the integral closure of $\mathbb{F}[x]$ in $\mathbb{F}\langle\lambda, \mu\rangle$. Consequently it is a Dedekind domain.*

(The proof is the usual one: first check traces, and then norms.)

The quotient fields $\mathbb{F}[x](y)/\mathscr{P}$ runs over the prime ideals of $\mathbb{F}[x](y)$ have a special relationship with the quaternion algebra originally used to define $\mathbb{F}\langle\lambda, \mu\rangle$. Specifically, we have

Lemma 6. 3. *Let $\mathscr{P}$ be a prime of $\mathbb{F}[x](y)$, then*

$$(\mathbb{F}[x](y)/\mathscr{P}) \otimes_{\mathbb{F}} \left\langle \begin{matrix} \lambda\, \mu \\ \mathbb{F} \end{matrix} \right\rangle = M_2(\mathbb{F}[x](y)/\mathscr{P}).$$

Proof. $(xj + 2ij)^2 = \mu x^2 - 4\lambda\mu = y^2$ in $\mathbb{F}[x](y)/\mathscr{P}$, so

$$(xj + 2ij - y)(xj + 2ij + y) = 0$$

in $\mathbb{F}[x](y)/\mathscr{P} \otimes_{\mathbb{F}} \left\langle \begin{matrix} \lambda\, \mu \\ \mathbb{F} \end{matrix} \right\rangle$ and the result follows. □

It is not hard to see that the converse is also true, namely, if $\mathbb{K}$ is a finite extension of $\mathbb{F}$ and $\mathbb{K} \otimes_{\mathbb{F}} \left\langle \begin{matrix} \lambda\, \mu \\ \mathbb{F} \end{matrix} \right\rangle = M_2(\mathbb{K})$, then $\mathbb{K}$ is the quotient of $\mathbb{F}[x](y)$ by a prime ideal.

Clearly, every genus 0 function field is a degree two extension of a pure transcendental extension $\mathbb{F}(x)$. But it is also true that either $\mathbb{F}\langle\lambda, \mu\rangle$ is itself pure transcendental, or a degree two extension of it is so. Indeed, if we set $\mathbb{K} = \mathbb{F}(\sqrt{\mu})$, then we have

Lemma 6. 4. *$\mathbb{K}[x](y) = \mathbb{K}[t, t^{-1}]$ where $2\sqrt{\mu}\, t = y + \sqrt{\mu} \cdot x$.*

Proof. Set $2\sqrt{\mu} \cdot z = (y - \sqrt{\mu} \cdot x)$, then

$$4\mu \cdot t \cdot z = y^2 - \mu x^2 = -4\lambda\mu$$

and $t^{-1} \in \mathbb{K}[x](y)$. On the other hand, x and y are obtained in terms of t, z, over $\mathbb{K}$, so the lemma follows. □

From this it follows that the field $\mathbb{K}(t)$ is a degree 2 extension of $\mathbb{F}(x)(y)$ provided that μ is a non-square in $\mathbb{F}$. Indeed, if an automorphism

$$\tau^\lambda : \mathbb{K}(t) \longrightarrow \mathbb{K}(t) \tag{6.5}$$

is defined by the identity on $\mathbb{F}$ and

$$\tau^\lambda(t) = \lambda t^{-1}, \quad \tau^\lambda(\sqrt{\mu}) = -\sqrt{\mu},$$

then the assignations $x \longrightarrow t + \lambda t^{-1}$, $y \longrightarrow \sqrt{\mu}(t - \lambda t^{-1})$ define an isomorphism of $\mathbb{F}\langle\lambda, \mu\rangle$ to the fixed field $\mathbb{K}(t)^{\tau^\lambda}$ of τ^λ. In the terminology of § 4 the ring $\mathbb{K}[t, t^{-1}]$ with the involution τ^λ is denoted by $\mathbb{K}[t, t^{-1}]_\lambda$, and

$$L_*(\mathbb{K}[t, t^{-1}], \tau^\lambda) = L_*(\mathbb{K}[t, t^{-1}]_\lambda).$$

As in § 5 we only consider the L^h-groups, and so omit the superscript h. Since the characteristic of the ground field $\mathbb{F}$ is $\neq 2$ there is no difference between the quadratic L-groups L_* and the symmetric L-groups L^*.

We summarize the discussion so far with the diagram of fields and rings of integers

(6.6)

$$\begin{array}{ccccc}
 & & \mathbb{F}[x] & \longrightarrow & \mathbb{F}(x) \\
 & & \downarrow & & \downarrow \\
\mathbb{F} & \longrightarrow & \mathbb{F}[x](y) & \longrightarrow & \mathbb{F}(x)(y) \\
\downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau^\lambda} & & \downarrow{\scriptstyle \tau^\lambda} \\
\mathbb{K} & \longrightarrow & \mathbb{K}[t, t^{-1}] & \longrightarrow & \mathbb{K}(t)
\end{array}$$

where the labels on the vertical arrows denote the Galois automorphisms.

Finally, we need

Lemma 6.7. *If λ is not a norm from $\mathbb{K}$ the ring $\mathbb{F}[x](y)$ is a principal ideal domain.*

Proof. Let $\mathcal{P}$ be a prime ideal of $\mathbb{F}[x](y)$. Then $\mathbb{K}[t, t^{-1}]\mathcal{P} \subset \mathbb{K}[t, t^{-1}]$ either remains prime or splits as a product $\mathcal{Q}\tau(\mathcal{Q})$ since the extension is unramified. If it splits as a product, since $\mathcal{Q}$ is principal, we can write $\mathcal{Q} = (p(t))$, and thus

$$\mathbb{K}[t, t^{-1}]\mathcal{P} = (p(t)\,\tau(p(t))),$$

so $p(t)\,\tau(p(t)) \in \mathbb{F}[x](y)$ generates $\mathcal{P}$. If it remains prime we have $\mathbb{K}[t, t^{-1}]\mathcal{P} = (h(t))$, and $\tau(h(t)) = uh(t)$ for some unit $u \in \mathbb{K}[t, t^{-1}]$. The units in $\mathbb{K}[t, t^{-1}]$ are all of the form kt^i with $k \neq 0$ in $\mathbb{K}$. Thus, applying τ again we obtain

$$h(t) = k\tau(k)\lambda^i h(t),$$

so $k\tau(k)\lambda^i=1$, and i must be even since λ is not a norm. Let $h_1(t)=t^{i/2}h(t)$, then $\tau(h_1(t))=k\lambda^{i/2}h_1(t)$, and, since the norm of $k\lambda^{i/2}$ is 1, we must have $k\lambda^{i/2}=\frac{\tau(0)}{0}$ for some $\theta\in\mathbb{K}$. If we set $h_2(t)=\tau(\theta)\,h_1(t)$ then $h_2(t)$ is invariant under τ and must generate $\mathscr{P}$. The proof is complete. □

Corollary 6. 8. *If $\lambda\in\mathbb{F}$ is not a norm from $\mathbb{K}$ then the map*

$$L_0(\mathbb{F}[x]\,(y))\longrightarrow L_0(\mathbb{F}\langle\lambda,\mu\rangle)$$

is an injection.

Proof. If $\theta\in L_0(\mathbb{F}[x]\,(y))$ is in the kernel, then θ is represented by a form $(\mathbb{F}[x]\,(y)^r, A)$ which becomes hyperbolic over $\mathbb{F}\langle\lambda,\mu\rangle$. In particular there is a projective kernel in $(\mathbb{F}[x]\,(y)^r, A)$. But since $\frac{1}{2}\in\mathbb{F}$, and projectives are free, it follows that the form is already hyperbolic over $\mathbb{F}[x]\,(y)$. □

Remark. This is a special case of Corollary 3. 3, p. 93 of [12]. □

§ 7. The Witt groups of genus 0 function fields

Our study of the Witt groups $W(\mathbb{F}\langle\lambda,\mu\rangle)=L_0(\mathbb{F}\langle\lambda,\mu\rangle)$ for the fields $\mathbb{F}\langle\lambda,\mu\rangle$ discussed in § 6 is based on the following diagram

(7. 1)

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & L_0(\mathbb{K}[t,t^{-1}],\tau^\lambda) & \longrightarrow & L_0(\mathbb{F}[x]\,(y)) & \longrightarrow & L_0(\mathbb{K}[t,t^{-1}]) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & L_0(\mathbb{K}(t),\tau^\lambda) & \longrightarrow & L_0(\mathbb{F}\langle\lambda,\mu\rangle) & \longrightarrow & L_0(\mathbb{K}(t)) \\
 & & \downarrow & & \downarrow & & \updownarrow \\
0 & \longrightarrow & \bigoplus_{\mathscr{P}\in J} L_0\left(\frac{\mathbb{K}[t,t^{-1}]}{\mathscr{P}},\tau^\lambda\right) & \longrightarrow & \bigoplus_{\mathscr{P}\in V} L_0\left(\frac{\mathbb{F}[x]\,(y)}{\mathscr{P}}\right) & \longrightarrow & \bigoplus_{\mathscr{Q}\in W} L_0\left(\frac{\mathbb{K}[t,t^{-1}]}{\mathscr{Q}}\right) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & L_3(\mathbb{K}[t,t^{-1}],\tau^\lambda) & \longrightarrow & L_3(\mathbb{F}[x]\,(y)) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array}$$

where

1. J is the set of primes $\mathscr{P} \subset \mathbb{F}[x]\,(y)$ which do not split in $\mathbb{K}[t, t^{-1}]$,
2. V is the set of primes $\mathscr{P} \subset \mathbb{F}[x]\,(y)$,
3. W is the set of primes $\mathscr{Q} \subset \mathbb{K}[t, t^{-1}]$,
4. the columns are the localization exact sequences,
5. the two middle rows are exact, since the upper one is just the Jacobson exact sequence, and the lower one is a sum of Jacobson sequences.

Remark 7. 2. The top row in (7. 1) is also exact and $L_0(\mathbb{K}[t, t^{-1}], \tau^\lambda)$ embeds in $L_0(\mathbb{F}[x]\,(y))$ since all the groups include into the corresponding L-groups for the quotient fields.

The fact that the bottom row is exact is more difficult. This was originally shown in Hambleton, Taylor and Williams [6] and Ranicki [20]. The reader familiar with L-theory can skip much of what follows in § 7, but the proof given here is essentially self contained.

From our main results on the L-groups of Laurent polynomial extensions we have, following the notation established in (6. 6),

Lemma 7. 3. $L_1(\mathbb{K}[t, t^{-1}], \tau^\lambda) = L_3(\mathbb{K}[t, t^{-1}], \tau^\lambda)$

$$= \mathrm{Ker}\,((\langle 1\rangle \perp -\langle\lambda\rangle) : L_2(\mathbb{K}, \tau) \longrightarrow L_2(\mathbb{K}, \tau)).$$

Likewise

$$L_0(\mathbb{K}[t, t^{-1}], \tau^\lambda) = L_0(\mathbb{K}, \tau)/\mathrm{im}\,(\langle 1\rangle \perp -\langle\lambda\rangle).$$

Example 7. 4. Suppose $\lambda = -1$, $\mathbb{F} = \mathbb{Q}$, $\mathbb{K} = \mathbb{Q}(i)$, then $L_0(\mathbb{K}, \tau) = \mathbb{Z} \oplus \bigoplus_{p \equiv 3(4)} \mathbb{Z}/2$, and the ring structure gives that the action of $\langle -1\rangle$ is multiplication by -1 on the $\mathbb{Z}$ and the identity on the $\mathbb{Z}/2$'s. Consequently,

$$\mathrm{Ker}\,(\langle 1\rangle \perp -\langle -1\rangle) \text{ is } \bigoplus_{p \equiv 3(4)} \mathbb{Z}/2, \quad \mathrm{coker} = \mathbb{Z}/2 \oplus \Big(\bigoplus_{p \equiv 3(4)} \mathbb{Z}/2\Big).$$

Lemma 7. 5. $L_0(\mathbb{K}[t, t^{-1}]) = L_0(\mathbb{K}) \oplus L_0(\mathbb{K})$ $(\bar{t} = t)$. *Moreover* τ^λ *(thought of now as a Galois automorphism) acts on* $L_0(\mathbb{K}[t, t^{-1}])$ *in terms of this representation by the formula*

$$\tau^\lambda(a, b) = (\tau(a), \langle\lambda\rangle \cdot \tau(b)).$$

Proof. This is direct from Milnor's theorem (5. 5) and the localization exact sequence. (See Ranicki [17], § 5, for another approach). The generators are from $L_0(\mathbb{K}) \hookrightarrow L_0(\mathbb{K}[t, t^{-1}])$ induced by inclusion, for the first summand, and elements of the form $\langle\theta t\rangle$ for the second, where $\theta \in \mathbb{K}$. In particular $\langle\theta\rangle \mapsto \langle\theta t\rangle$ gives the inclusion for the second summand. Finally, the effect of τ^λ on $\langle\theta t\rangle$ is $\langle\tau(\theta)\lambda t^{-1}\rangle \sim \langle\tau(\theta)\lambda t\rangle$ and the lemma follows. □

Corollary 7. 6. $L_0(\mathbb{K}[t, t^{-1}])^{\tau^\lambda} = L_0(\mathbb{K})^\tau \oplus L_0(\mathbb{K})^{\lambda\tau}$.

Lemma 7. 7. *Assume λ is not a norm from $\mathbb{K}$. Let $0 \in L_0(\mathbb{K}[t, t^{-1}]/\mathscr{P})$ be the image of $\mu \in L_0(\mathbb{F}[x](y)/\mathscr{P})$, then there is an element $\alpha \in L_0(\mathbb{F}\langle\lambda, \mu\rangle)$ with*

$$p(\alpha) = \mu + z \quad \textit{where} \quad z \in \operatorname{im}(L_0(\mathbb{K}[t, t^{-1}], \tau^\lambda)).$$

Proof. We have seen that $\mathscr{P} = (p)$ is principal, and suppose that $0 = \langle f\rangle$ with $f \in \mathbb{F}[x](y)/(p)$ is a generator in this image. Then we can represent a lifting of $\langle f\rangle$ as $\langle q(x, y)p\rangle$ (at least up to lower degree) since $q(x, y)$ can always be choosen to represent f with its degree less than that of p. This reduces us to the consideration of the situation at primes of strictly smaller degree than p.

To complete the induction we need to consider also the case where $\mathscr{P}$ splits in $\mathbb{K}[t, t^{-1}]$. For such a prime let $\mathscr{Q}$, $\tau(\mathscr{Q})$ represent the primes over $\mathscr{P}$. Then

$$\mathbb{K}[t, t^{-1}]/\mathscr{Q} \cong \mathbb{K}[t, t^{-1}]/\tau(\mathscr{Q}) \cong \mathbb{F}[x](y)/\mathscr{P},$$

and

$$L_0(\mathbb{F}[x](y)/\mathscr{P}) \longrightarrow L_0(\mathbb{K}[t, t^{-1}]/\mathscr{Q}) \oplus L_0(\mathbb{K}[t, t^{-1}]/\tau(\mathscr{Q}))$$

is the diagonal map. But, if $\langle\theta\rangle \in L_0(\mathbb{K}[t, t^{-1}]/\mathscr{Q})$ is represented by $\sum_i \langle\bar{\theta}_i\rangle \in L_0(\mathbb{K}(t))$, then $\langle\theta\rangle \in L_0(\mathbb{K}[t, t^{-1}]/\tau(\mathscr{Q}))$ is represented by $\sum_i \langle\tau\bar{\theta}_i\rangle$. On the other hand, consider the term $\langle\bar{\theta}\rangle \perp \langle\tau\bar{\theta}\rangle \in L_0(\mathbb{K}(t))$. By an obvious change of variables we have

$$\langle\bar{\theta}\rangle \perp \langle\tau\bar{\theta}\rangle = \langle\bar{\theta}\rangle + \langle\tau\bar{\theta}\rangle \perp \langle\bar{\theta}\tau\bar{\theta}(\bar{\theta} + \tau\bar{\theta})\rangle \tag{7. 8}$$

and hence comes from $L_0(\mathbb{F}\langle\lambda, \mu\rangle)$. The lemma follows. □

Corollary 7. 9. *Let $f \in \mathbb{F}$, then the class $\langle f\rangle \perp \langle\lambda f\rangle \in L_0(\mathbb{K})^{\lambda\tau}$ is in the image from $L_0(\mathbb{F}\langle\lambda, \mu\rangle)$.*

Proof. From 7. 8, we have that

$$\langle ft\rangle \perp \langle\lambda ft\rangle \sim \langle fx\rangle \perp \langle\lambda fx\rangle$$

in $L_0(\mathbb{K}(t))$ and this is in the asserted group. □

More generally we may use the Scharlau transfer to obtain precise information about $L_0(\mathbb{F}[x](y))$. By Theorem 3. 3 of Lam [10], p. 201, there is an exact sequence

$$L_0(\mathbb{F}\langle\lambda, \mu\rangle) \xrightarrow{i_*} L_0(\mathbb{K}(t)) \xrightarrow{\mathrm{tr}_*} L_0(\mathbb{F}\langle\lambda, \mu\rangle) \tag{7. 10}$$

where tr_* is the Scharlau transfer associated with the $\mathbb{F}\langle\lambda, \mu\rangle$-linear homomorphism

$$\phi : \mathbb{K}(t) \longrightarrow \mathbb{F}\langle\lambda, \mu\rangle, \quad \phi(a + b\sqrt{\mu}) = b.$$

Note that ϕ restricts to $\phi| : \mathbb{K} \to \mathbb{F}$, so we have

Lemma 7. 11. tr_* *restricts to give a homomorphism*

$$L_0(\mathbb{K}[t, t^{-1}]) \xrightarrow{\mathrm{tr}_*} L_0(\mathbb{F}[x]\,(y)),$$

the following diagram commutes,

$$\begin{array}{ccc} L_0(\mathbb{K}) & \xrightarrow{\mathrm{tr}_*} & L_0(\mathbb{F}) \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\ L_0(\mathbb{K}[t, t^{-1}]) & \xrightarrow{\mathrm{tr}_*} & L_0(\mathbb{F}[x]\,(y)) \end{array}$$

and $\mathrm{tr}_*(\langle k\rangle) = \mathrm{tr}_*(f + g\sqrt{\mu}) = \langle g\rangle\,(\langle 1\rangle \perp \langle -N(k)\rangle)$, *while*

$$\mathrm{tr}_*(\langle kt\rangle) = \langle xg\sqrt{\mu} + yf\rangle\,(\langle 1\rangle \perp \langle -\lambda N(k)\rangle)$$

after including $L_0(\mathbb{F}[x]\,(y))$ *in* $L_0(\mathbb{F}\langle\lambda, \mu\rangle)$.

Proof. For the form $\langle k\rangle$ we have

$$\phi(A + B\sqrt{\mu})\,(f + g\sqrt{\mu})\,(C + D\sqrt{\mu}) = (AD + BC)f + (AC + BD\mu)g$$

which associates to the matrix

$$\Delta_1 = \begin{pmatrix} g & f \\ f & \mu g \end{pmatrix}.$$

Since $\mathrm{Det}\,\Delta_1 = -N(k)$, the first formula follows. To obtain the second formula, note from 6. 4 that $t = \frac{1}{2}\left(x + \frac{\sqrt{\mu}}{\mu}\,y\right)$, so $\mathrm{tr}_*(\langle kt\rangle)$ is given by the matrix of

$$\frac{1}{2}\left[(AC + \mu BD)\left(\frac{fy}{\mu} + xg\right) + (AD + BC)\,(xf + yg)\right]$$

which is

$$\Delta_2 = \frac{1}{2}\begin{vmatrix} \dfrac{fy}{\mu} + xg & xf + yg \\ xf + yg & fy + \mu xg \end{vmatrix}.$$

Also

$$\mathrm{Det}\,\Delta_2 = \frac{1}{4}\left(\frac{f^2 - g^2\mu}{\mu}\right)(y^2 - \mu x^2) = -\lambda N(k)$$

is a unit in $\mathbb{F}[x]\,(y)$, and 7. 11 follows. □

Remark 7. 12. The image of $L_0(\mathbb{F})$ in $L_0(\mathbb{F}[x](y))$ in 7. 11 is exactly the quotient

$$L_0(\mathbb{F})/\{L_0(\mathbb{F})\cdot(\langle\mu\rangle\perp\langle 1\rangle)(\langle 1\rangle\perp-\langle\lambda\rangle)\}.$$

This is a direct consequence of the commutativity of the diagram obtained by amalgamating the exact sequence for a Laurent extension with the Jacobson sequence

(7. 13)

$$\begin{array}{ccccc}
L_0(\mathbb{K},\tau) & \xrightarrow{\langle 1\rangle\perp\langle\mu\rangle} & L_0(\mathbb{F}) & \longrightarrow & 0 \\
\downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\gamma} & & \downarrow \\
L_0(\mathbb{K},\tau) & \xrightarrow{\langle 1\rangle\perp\langle\mu\rangle} & L_0(\mathbb{F}) & \longrightarrow & L_0(\mathbb{K}) \\
\downarrow & & \downarrow{\scriptstyle\iota} & & \downarrow{\scriptstyle\iota} \\
L_0(\mathbb{K}[t,t^{-1}],\tau^\lambda) & \longrightarrow & L_0(\mathbb{F}[x](y)) & \longrightarrow & L_0(\mathbb{K}[t,t^{-1}])
\end{array}$$

where the map γ is multiplication by $\langle 1\rangle\perp-\langle\lambda\rangle$.

Let $V\subset L_0(\mathbb{K}[t,t^{-1}])$ be the kernel of tr_*. Putting all this together we have

Theorem 7. 14. *There is an exact sequence*

$$0\to L_0(\mathbb{K}[t,t^{-1}],\tau^\lambda)\to L_0(\mathbb{F}[x](y))\to V\to L_3(\mathbb{K}[t,t^{-1}],\tau^\lambda)\to L_3(\mathbb{F}[x](y))\to 0.$$

(This is basically the snake lemma, which is applicable because of 7. 7.) □

7. 14 provides, in general, an effective means of studying the Witt group of a genus 0 function field. The group $L_3(\mathbb{F}[x](y))$ plays the role of a reciprocity law, measuring the extent to which the "second boundary map" is surjective.

§ 8. The case $\mathbb{F}$ acted on trivially by τ

Consider the case of the ring $A=\mathbb{F}[t,t^{-1}]$ where $\mathbb{F}$ is a field of characteristic different from 2, with the involution $\tau: a\to\bar{a}$ given by $\bar{a}=a$ for $a\in\mathbb{F}$, $\bar{t}=t^{-1}$. The L-groups of A are given by

$$L_*(A)=\begin{cases}L_0(\mathbb{F}) & *\equiv 0,\,1\,(4),\\ 0 & *\equiv 2,\,3\,(4)\end{cases}$$

by our main theorem 4. 1 and $L_*(\mathbb{F})=0$ for $*\equiv 1,\,2,\,3(4)$. We wish to use this result to study the (Hermitian) Witt group of the function field $\mathbb{F}(t)$ under the associated involution $\tau:\mathbb{F}(t)\to\mathbb{F}(t)$.

Set $x = t + t^{-1}$ so $\mathbb{F}(t)^r = \mathbb{F}(x)$, and $(t - t^{-1})^2 = x^2 - 4$. It follows that we can write

$$\mathbb{F}(t) = \mathbb{F}(x)\,(\sqrt{x^2-4}) = \mathbb{F}(x)\,(\sqrt{(x-2)\,(x+2)}).$$

$\mathbb{F}[t, t^{-1}]$ is Dedekind, so it is the integral closure of $\mathbb{F}[x]$ in $\mathbb{F}(t)$, and the extension ramifies at exactly the two primes $(x-1)$, $(x+1)$.

We apply the L-theory localization sequences of Carlsson and Milgram [3] and Ranicki [17], § 3, to obtain the two exact sequences

$$(8.1) \qquad 0 \longrightarrow L_0(\mathbb{F}) \longrightarrow L_0(\mathbb{F}(t), \tau) \xrightarrow{\partial_0} \bigoplus_{\mathscr{P} \in \mathscr{I}} L_0^{\mathrm{tor}}(\mathbb{F}[t, t^{-1}]/\mathscr{P}, \tau) \longrightarrow 0,$$

and

$$(8.2) \qquad 0 \longrightarrow L_2(\mathbb{F}(t), \tau) \xrightarrow{\partial_2} \bigoplus_{\mathscr{P} \in \mathscr{I}} L_2^{\mathrm{tor}}(\mathbb{F}[t, t^{-1}]/\mathscr{P}, \tau) \longrightarrow L_0(\mathbb{F}) \longrightarrow 0.$$

Here $\mathscr{I}$ is the set of primes in $\mathbb{F}[x]$ which either ramify or remain prime in $\mathbb{F}[t, t^{-1}]$. Away from the ramified primes we have that $L_0^{\mathrm{tor}}(\mathbb{F}[t, t^{-1}]/\mathscr{P}, \tau) = L_2^{\mathrm{tor}}(\mathbb{F}[t, t^{-1}]/\mathscr{P}, \tau)$ is the ordinary L-theory of the quotient under the induced involution. Here, the isomorphism from L_0^{tor} to L_2^{tor} is given by $\langle\theta\rangle \mapsto \langle\{t - t^{-1}\}\,\theta\rangle$ on generators.

Likewise, for the Hermitian Witt groups of the function fields we have:

Lemma 8.3. *Let $\theta \in \mathbb{F}(x)$ then*

(1) *the forms $\langle\theta\rangle$ generate $L_0(\mathbb{F}(t), \tau)$,*

(2) *$L_0(\mathbb{F}(t), \tau) \cong L_2(\mathbb{F}(t), \tau)$, the isomorphism being given explicitly by*

$$\langle\theta\rangle \mapsto \langle(t - t^{-1})\,\theta\rangle,$$

(3) $$L_*^{\mathrm{tor}}(\mathbb{F}[t, t^{-1}]/(t-1), \tau) = \begin{cases} L_0(\mathbb{F}) & * \equiv 2(4), \\ 0 & * \equiv 0, 1, 3(4), \end{cases}$$ *and similarly for*

$$L_*^{\mathrm{tor}}(\mathbb{F}[t, t^{-1}]/(t+1), \tau),$$

(4) $$\partial_2(\langle(t - t^{-1})\,\theta\rangle) = \langle\{t - t^{-1}\}\rangle\, \partial_0(\langle\theta\rangle) + \langle\theta(1)\rangle_{(t-1)} + \langle\theta(-1)\rangle_{(t+1)}.$$

Proof. 8.3.(1) and 8.3.(2) are well known. 8.3.(3) is true because, while $(t \pm 1)$ are both prime, and both invariant — as ideals — under τ, they do not have invariant generators. In fact $\tau(t \pm 1) = \mp t^{-1}(t \pm 1)$. In tracing the definition of the torsion form, the coefficient $\mp t^{-1}$ evaluated in the quotient determines the type of the corresponding L-group. In these cases $\mp t^{-1} = -1$ at both primes, so parities reverse, and 8.3.(3) follows.

To prove 8.3.(4) it suffices to evaluate $\partial_2(\langle t - t^{-1}\rangle)$. At the prime $t-1$ we write this as $-(t+1)/(t-1)$, after dividing by $(t-1)\,(t^{-1}-1)$. Similarly, at $t+1$ it can be written $(t-1)/(t+1)$, and the result follows directly. □

Corollary 8. 4. *The Hermitian Witt group*

$$W(\mathbb{F}(t), \tau) \cong \bigoplus_{\mathscr{P} \in \mathscr{I}} W(\mathbb{F}[t, t^{-1}]/\mathscr{P}, \tau) \oplus W(F).$$

Here, $\mathscr{I}$ is the set of non-ramified, non-split primes in $\mathbb{F}[x]$. Moreover, the isomorphism above is natural.

(The point is that the map in (8. 1) $L_0(\mathbb{F}) \to L_0(\mathbb{F}(t), \tau)$ is split by the composite

$$\partial_2 \cdot \langle t - t^{-1} \rangle : L_0(\mathbb{F}(t), \tau) \longrightarrow L_0(\mathbb{F})_{(t-1)} \oplus L_0(\mathbb{F})_{(t+1)}$$

using 8. 3.(4). The subscripts are labels, not localizations. Also, $W = L_0$.)

Example 8. 5. Let $\mathbb{F} = \mathbb{R}$, the field of real numbers. The primes of $\mathbb{R}[x]$ are $(x-r)$ or $(x^2 - ax + b)$ with $a^2 - 4b < 0$. All primes of the second type have $\mathbb{R}[x]/\mathscr{P} = \mathbb{C}$, the complex numbers, so they split in $\mathbb{R}[t, t^{-1}]$. But primes of the first type split only if $r^2 < 4$. Hence the non-split primes are the $(x-r)$ with $|r| \leqq 2$, where the two endpoints $(x \pm 2)$ are both ramified. It follows that using the reciprocity law above we have

Corollary 8. 6. *The Hermitian Witt group of $\mathbb{R}[t, t^{-1}]$ is naturally isomorphic to $\bigoplus_{S^1} \mathbb{Z}$.*

Proof. From 8. 3, 8. 4 we obtain $L_0(\mathbb{R}(t), \tau) = \bigoplus_{[-2,2]} \mathbb{Z}$, with an identification of the two $\mathbb{Z}$'s at the endpoints. But that is the result. □

References

[1] *H. Bass*, Algebraic K-Theory, New York 1968.

[2] *H. Bass, A. Heller* and *R. Swan*, The Whitehead group of a polynomial extension, Publ. Math. I.H.E.S. **22** (1964), 61—80.

[3] *G. Carlsson, R. J. Milgram*, Some exact sequences in the theory of hermitian forms, J. Pure and Appl. Alg. **18** (1988), 233—252.

[4] *F. T. Farrell, W. C. Hsiang*, Manifolds with $\pi_1 = G \times_\alpha T$, Amer. J. Math. **95** (1973), 813—845.

[5] *F. T. Farrell, L. R. Taylor* and *J. B. Wagoner*, The Whitehead theorem in the proper category, Compositio Math. **27** (1973), 1—23.

[6] *I. Hambleton, L. R. Taylor* and *B. Williams*, An introduction to maps between surgery obstruction groups, Proc. 1982 Aarhus Conference on Algebraic Topology, Lect. Notes in Math. **1051** (1984), 49—127.

[7] *H. Hasse*, Number Theory, Berlin-Heidelberg-New York 1980.

[8] *G. Higman*, The units of group rings, Proc. London Math. Soc. (2) **46** (1940), 231—248.

[9] *M. Knebusch*, On algebraic curves over real closed fields II, Math. Z. **151** (1976), 189—205.

[10] *T. Y. Lam*, The Algebraic Theory of Quadratic Forms, New York 1973.

[11] *D. W. Lewis*, New improved exact sequences of Witt groups, J. of Algebra **74** (1982), 206—210.

[12] *J. Milnor, D. Husemoller*, Symmetric Bilinear Forms, Berlin-Heidelberg-New York 1973.

[13] *S. P. Novikov*, The algebraic construction and properties of hermitian analogues of K-theory for rings with involution, from the point of view of the hamiltonian formalism. Some applications to differential topology and the theory of characteristic classes, Izv. Akad. Nauk SSSR, ser. mat. **34** (1970), 253—288, 478—500.

[14] *R. Parimala*, Witt groups of conics, elliptic and hyperelliptic curves, J. Number Theory **28** (1988), 69—93.

[15] *A. A. Ranicki*, Algebraic L-theory II, Laurent extensions, Proc. London Math. Soc. (3) **27** (1973), 126—158.

[16] *A. A. Ranicki*, The algebraic theory of surgery I, Foundations, Proc. London Math. Soc. (3) **40** (1980), 87—192.

[17] *A. A. Ranicki*, Exact sequences in the algebraic theory of surgery, Mathematical Notes **26**, Princeton 1981.
[18] *A. A. Ranicki*, The algebraic theory of finiteness obstruction, Math. Scand. **57** (1985), 105—126.
[19] *A. A. Ranicki*, Algebraic and geometric splittings of the K- and L-groups of polynomial extensions, Proc. Symp. Transformation Groups, Poznań 1985, Lect. Notes in Math. **1217** (1986), 321—364.
[20] *A. A. Ranicki*, The L-theory of twisted quadratic extensions, Can. J. Math. **XXXIX** (1987), 345—364.
[21] *A. A. Ranicki*, Lower K- and L-theory, to appear.
[22] *J. Shaneson*, Wall's surgery obstruction groups for $G \times \mathbb{Z}$, Annals of Math. **90** (1969), 296—334.
[23] *F. Waldhausen*, The Whitehead group of a generalized free product, mimeo (1969).
[24] *F. Waldhausen*, Algebraic K-theory of generalized free products, Annals of Math. **108** (1978), 135—256.
[25] *C. T. C. Wall*, Surgery on compact manifolds, London-New York 1970.
[26] *E. Witt*, Zerlegung reeller algebraischer Funktionen in Quadrate, Schiefkörper über reellem Funktionenkörper, J. reine angew. Math. **171** (1934), 4—11.

Department of Mathematics, Stanford University, Stanford, Calif. 94305, U.S.A.

Department of Mathematics, Edinburgh University, Edinburgh EH9 3JZ, Scotland, UK

Eingegangen 22. August 1988, in revidierter Fassung 24. Juni 1989

J. reine angew. Math. **406** (1990), 167—178

Journal für die reine und angewandte Mathematik

Binary forms and unramified A_n-extensions of quadratic fields

By *Jin Nakagawa**) at Joetsu

§ 0. Introduction

Let n be a natural number with $n \geqq 3$ and let V be the vector space of binary forms of degree n with coefficients in $\mathbb{R}$:

$$V = \{f(x, y) = \sum_{j=0}^{n} a_j x^{n-j} y^j;\ (a_j) \in \mathbb{R}^{n+1}\}.$$

We denote by $V_{\mathbb{Z}}$ the set of integral binary forms of degree n. Further, we denote by $V_{\mathbb{Z}}^{\mathrm{irr}}$ the set of integral irreducible binary forms of degree n. If r_1, r_2 are non-negative integers with $r_1 + 2r_2 = n$, we denote by V_{r_1,r_2} the subset of $V - \{0\}$ of all binary forms which are decomposed into r_1 linear forms and r_2 positive definite quadratic forms over $\mathbb{R}$. Let $\Gamma = \mathrm{GL}_2(\mathbb{Z})$. The action of Γ on V is defined by

$$(\gamma \cdot f)(x, y) = f(ax + cy, bx + dy) \quad \left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ f(x, y) \in V\right).$$

We say that $\gamma \cdot f$ is Γ-*equivalent* to f and write $\gamma \cdot f \underset{\Gamma}{\sim} f$. We note that the subset V_{r_1,r_2} of V is stable under the action of Γ. For $f \in V$, we denote by $D(f)$ the *discriminant* of f. We note that $D(\gamma \cdot f) = D(f)$ for any $\gamma \in \Gamma$, $f \in V$. For a given integer D_0, we denote by $h_{r_1,r_2}(D_0)$ the number of Γ-equivalence classes of integral irreducible binary forms $f \in V_{r_1,r_2}$ with $D(f) = D_0$. By the finiteness theorem of Birch and Merriman [1], $h_{r_1,r_2}(D_0)$ is finite. For $X > 0$, put

$$S_{r_1,r_2}(X) = \sum_{|D_0| \leqq X} h_{r_1,r_2}(D_0).$$

*) This research was partially supported by Grant-in-Aid for Scientific Research (No. 01740026), Ministry of Education, Science and Culture of Japan.

In 1951, Davenport obtained asymptotic formulae for $S_{3,0}(X)$ and $S_{1,1}(X)$ (see [2], [3]). In our previous paper [7], we have obtained a lower estimate of $S_{n,0}(X)$ for $n \geqq 4$. There we used a mapping of V to the space of quadratic forms of $n-1$ variables, which is an analogue of "Hessian" of binary cubic forms. In this paper, we shall obtain a lower estimate of $S_{r_1,r_2}(X)$ for $r_2 > 0$. Our method is a weak generalization of the reduction theory of Mathew and Berwick for binary cubic forms with negative discriminants (see [3], [6]).

Applying our estimate of $S_{r_1,r_2}(X)$, we shall study unramified Galois extensions of quadratic fields. Let K be an algebraic number field. For any finite group G, we say that L/K is a *G-extension* if L/K is a Galois extension with Galois group G. We say that an algebraic extension L/K is *strictly (resp. weakly) unramified* if L/K is unramified at any primes (resp. at any finite primes). In 1970, Y. Yamamoto and K. Uchida proved independently that there exist infinitely many real (resp. imaginary) quadratic fields which have weakly unramified A_n-extensions (see [8], [9]). In [10], K. Yamamura proved the corresponding theorem for strictly unramified A_5-extensions. Their arguments were based on the fact that the discriminants of certain special monic polynomials of degree n have an extremely simple form. On the contrary, we shall study the generic binary forms of degree n and we shall prove that there exist infinitely many algebraic number fields of degree n over $\mathbb{Q}$ with r_1 real primes and r_2 imaginary primes whose normal closures over $\mathbb{Q}$ are weakly unramified A_n-extensions over their quadratic subfields.

Finally, we shall study the volume of a "fundamental domain" in the case $r_2 = 1$.

Statement of the results

Theorem 1. *Let n, r_1, r_2 be integers with $n \geqq 4$, $r_1 \geqq 0$, $r_2 \geqq 0$, $r_1 + 2r_2 = n$. Put $\kappa = \dfrac{n+1}{2(n-1)}$. Then there exists a positive constant C_{r_1,r_2} such that*

$$\liminf_{X \to \infty} X^{-\kappa} S_{r_1,r_2}(X) \geqq C_{r_1,r_2}.$$

Theorem 2. *Let n, r_1, r_2 be as in Theorem 1. Then there exist infinitely many algebraic number fields of degree n with r_1 real primes and r_2 imaginary primes whose normal closures over $\mathbb{Q}$ are weakly unramified A_n-extensions over their quadratic subfields.*

Theorem 3. *Let $n \geqq 4$, $r_1 = n-2$, $r_2 = 1$. Then there exists an open cone $\mathfrak{F}$ of $V_{n-2,1}$ with the following properties:*

(i) *If $f \in V_{n-2,1}$ has no linear factors over $\mathbb{Q}$, then there exists an element $\gamma \in \Gamma$ such that $\gamma \cdot f \in \bar{\mathfrak{F}}$. Here $\bar{\mathfrak{F}}$ is the closure of $\mathfrak{F}$ in V;*

(ii) *$\gamma \cdot \mathfrak{F} \cap \mathfrak{F} = \emptyset$ for any $\gamma \in \Gamma - \{\pm 1\}$;*

(iii) *The Euclidean volume of $\mathfrak{F}_1 = \{f \in \mathfrak{F};\ |D(f)| \leqq 1\}$ ($\subset V = \mathbb{R}^{n+1}$) is finite.*

§ 1. Proof of Theorem 1

Let n, r_1, r_2 be integers with $n \geqq 4$, $r_1 \geqq 0$, $r_2 \geqq 0$, $r_1 + 2r_2 = n$. In our previous paper, we have proved Theorem 1 for $r_2 = 0$ (see [7], Theorem 1). So we assume $r_2 > 0$.

Let $H \subset \mathbb{C}$ be the upper half plane and put $\Omega = \{z \in H;\ |z| \geqq 1,\ 0 \leqq \mathrm{Re}\, z \leqq 1/2\}$. We denote by Ω' and Ω° the complex conjugate of Ω and the interior of Ω, respectively. The action of Γ on $\mathbb{C} - \mathbb{R}$ is defined by

$$\gamma \cdot z = (az + b)/(cz + d) \qquad \left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ z \in \mathbb{C} - \mathbb{R}\right).$$

Lemma 1. 1. (i) $\mathbb{C} - \mathbb{R} = \Gamma \cdot \Omega \cup \Gamma \cdot \Omega'$.

(ii) $(\gamma \cdot \Omega \cup \gamma \cdot \Omega') \cap \Omega^\circ = \emptyset$ *for any* $\gamma \in \Gamma - \{\pm 1\}$.

Proof. Put $\gamma_0 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\Gamma^+ = \mathrm{SL}_2(\mathbb{Z})$. Then we have $\Gamma = \Gamma^+ \cup \Gamma^+ \gamma_0$ and $\Omega \cup \gamma_0 \cdot \Omega' = \{z \in H;\ |z| \geqq 1,\ -1/2 \leqq \mathrm{Re}\, z \leqq 1/2\}$. The lemma follows from the fact that $\Omega \cup \gamma_0 \cdot \Omega'$ is a fundamental domain for Γ^+ in H. q.e.d.

Put

$$\mathscr{E}^+ = \{(a_0, \theta_1, \ldots, \theta_{r_1}, \alpha_1, \ldots, \alpha_{r_2}) \in \mathbb{R}^{r_1+1} \times \mathbb{C}^{r_2};$$
$$a_0 > 0,\ \theta_1 < \ldots < \theta_{r_1},\ \alpha_k \in \Omega^\circ\ (1 \leqq k \leqq r_2),\ |\alpha_1| < \ldots < |\alpha_{r_2}|\}.$$

Further, put $\mathscr{E}^- = \{(a_0, \theta_j, \alpha_k) \in \mathbb{R}^{r_1+1} \times \mathbb{C}^{r_2};\ (-a_0, \theta_j, \alpha_k) \in \mathscr{E}^+\}$. Let $\mathscr{E} = \mathscr{E}^+ \cup \mathscr{E}^-$ or $\mathscr{E}^+$ according as n is even or odd. We define a mapping Φ of $\mathscr{E}$ to V_{r_1, r_2} by

$$\Phi(a_0, \theta_1, \ldots, \theta_{r_1}, \alpha_1, \ldots, \alpha_{r_2}) = a_0 \prod_j (x - \theta_j y) \prod_k (x - \alpha_k y)(x - \bar{\alpha}_k y).$$

It is obvious that Φ is a bijective C^∞-mapping of $\mathscr{E}$ to $\Phi(\mathscr{E})$ and $\Phi(\mathscr{E})$ is an open cone in V.

Lemma 1. 2. *If* $f_1, f_2 \in \Phi(\mathscr{E})$ *and* $f_1 \neq f_2$, *then* $f_1 \underset{\Gamma}{\sim} f_2$.

Proof. Let $f_1, f_2 \in \Phi(\mathscr{E})$. Suppose $f_2 = \gamma \cdot f_1$ for some $\gamma \in \Gamma$. Let α be a complex root of $f_1(x, 1)$ with $\mathrm{Im}\, \alpha > 0$. Then $\beta = {}^t\gamma^{-1} \cdot \alpha$ is a complex root of $f_2(x, 1)$. Since $f_1, f_2 \in \Phi(\mathscr{E})$, $\alpha \in \Omega^\circ$ and $\beta \in \Omega \cup \Omega'$. Hence γ must be ± 1 by Lemma 1. 1 (ii). If n is even, then the action of -1 on V is trivial. If n is odd, then γ must be 1, since the coefficients of x^n in f_1 and f_2 are both positive. Hence we have $f_2 = f_1$. q.e.d.

Put $a_0^0 = 1$, $\theta_j^0 = j\ (1 \leqq j \leqq r_1)$, $\alpha_k^0 = (1/4) + k\sqrt{-1}\ (1 \leqq k \leqq r_2)$. Then

$$f_0 = \Phi(a_0^0, \theta_j^0, \alpha_k^0) \in \Phi(\mathscr{E}).$$

Since $\Phi(\mathscr{E})$ is open, we can take a positive number r such that the compact ball $\mathscr{B}_0$ with center at f_0 and radius r is contained in $\Phi(\mathscr{E})$. Put

$$\mathscr{F}_0 = \{tg \in V;\ g \in \mathscr{B}_0,\ t \in \mathbb{R},\ t > 0\}.$$

Then $\mathscr{F}_0$ is a cone and $\mathscr{F}_0 \subset \Phi(\mathscr{E})$. For $X>0$, put

$$\mathscr{F}_{0,X} = \{f \in \mathscr{F}_0;\ |D(f)| \leqq X\}.$$

By Lemma 1. 2, we have

$$S_{r_1,r_2}(X) \geqq \#(\mathscr{F}_{0,X} \cap V_{\mathbb{Z}}^{\mathrm{irr}}).$$

Since $m = \mathrm{Min}\{|D(g)|;\ g \in \mathscr{B}_0\} > 0$, we have

$$t^{2n-2} \leqq m^{-1}|D(g)|\, t^{2n-2} = m^{-1}|D(f)| \leqq m^{-1}X \quad \text{for} \quad f = tg \in \mathscr{F}_{0,X}.$$

Hence $\mathscr{F}_{0,X}$ is bounded. Since $\mathscr{F}_{0,X} = X^{1/2(n-1)}\mathscr{F}_{0,1}$, we have $\mathrm{vol}(\mathscr{F}_{0,X}) = X^{\kappa}\,\mathrm{vol}(\mathscr{F}_{0,1})$, where $\kappa = \dfrac{n+1}{2(n-1)}$. By a well-known fact on lattice points and [7], Proposition 4. 1, we have

$$\lim_{X \to \infty} X^{-\kappa} \#(\mathscr{F}_{0,X} \cap V_{\mathbb{Z}}^{\mathrm{irr}}) = \mathrm{vol}(\mathscr{F}_{0,1}).$$

This completes the proof of Theorem 1.

§ 2. Lattice points with congruence conditions

In this section, we study the number of lattice points with congruence conditions. Our argument is a generalization of that in Davenport and Heilbronn [4], § 5.

Let $\mathscr{D} \subset \mathbb{R}^N$ be a bounded open subset. We denote by $\partial\mathscr{D}$ the boundary of $\mathscr{D}$. Assume that the boundary $\partial\mathscr{D}$ is $(N-1)$-Lipschitz parametrizable, i.e. there are finitely many mappings of $[0,1]^{N-1}$ to $\mathbb{R}^N$ satisfying Lipschitz's condition such that the images cover $\partial\mathscr{D}$. Put $L_0 = \mathbb{Z}^N \subset \mathbb{R}^N$. Let m be a natural number and let $a \in L_0$ be a lattice point. Put $L = \{ml + a \in L_0;\ l \in L_0\}$. For a positive real number t, put

$$t\mathscr{D} = \{tx \in \mathbb{R}^N;\ x \in \mathscr{D}\}.$$

We use the order notation O of Landau. The following lemma is a modified version of Lang [5], Chap. 6, Theorem 2, and is proved by the same argument.

Lemma 2. 1. *$\#(t\mathscr{D} \cap L) = \mathrm{vol}(\mathscr{D})\,(t/m)^N + O((t/m)^{N-1})$ as $t \to \infty$, where the constant in O depends only on N and Lipschitz's constants of the mappings for $\partial\mathscr{D}$.*

Let $\mathscr{D}$, L_0 and N be as above. For a prime number p, we denote by $\mathbb{F}_p$ the finite field of p elements. Suppose that for each prime number p, we are given a subset $W_p \subset \mathbb{F}_p^N$ satisfying the following conditions (L.1) and (L.2):

(L.1) $\quad \#W_p \leqq C p^{N-1-\delta}$,

(L.2) $\quad t\mathscr{D} \cap W_p' = \emptyset$ if $t < p^{\delta'}$,

where $W_p' = \{l \in L_0;\ l \bmod p \in W_p\}$ and C, δ, δ' are positive constants with $\delta + \delta' > 1$. Put $U_p = \mathbb{F}_p^N - W_p$, $U_p' = \{l \in L_0;\ l \bmod p \in U_p\}$. Further we put $U = \bigcap_{p:\text{prime}} U_p'$. Then we have

Lemma 2. 2. $\lim_{t\to\infty} t^{-N} \#(t\mathscr{D} \cap U) = \mathrm{vol}(\mathscr{D}) \prod_{p:\text{prime}} (\# U_p) p^{-N}$.

Proof. First we note that the infinite product converges by (L.1). For a fixed $Y > 0$, we put $m = \prod_{p<Y} p$. By Lemma 2. 1, we have

$$\#\{t\mathscr{D} \cap (\bigcap_{p<Y} U_p')\} = \{\mathrm{vol}(\mathscr{D})\,(t/m)^N + O((t/m)^{N-1})\}\ \{\prod_{p<Y} \# U_p\}.$$

Hence

$$\lim_{t\to\infty} t^{-N} \#\{t\mathscr{D} \cap (\bigcap_{p<Y} U_p')\} = \mathrm{vol}(\mathscr{D}) \prod_{p<Y} (\# U_p) p^{-N}.$$

Since $U \subset \bigcap_{p<Y} U_p'$, we have

$$\limsup_{t\to\infty} t^{-N} \#(t\mathscr{D} \cap U) \leqq \mathrm{vol}(\mathscr{D}) \prod_{p<Y} (\# U_p) p^{-N}.$$

As this is true for all $Y > 0$, we have

$$\limsup_{t\to\infty} t^{-N} \#(t\mathscr{D} \cap U) \leqq \mathrm{vol}(\mathscr{D}) \prod_{p} (\# U_p) p^{-N}.$$

To obtain a lower bound for $t^{-N} \#(t\mathscr{D} \cap U)$, we observe that

$$\bigcap_{p<Y} U_p' \subset U \cup (\bigcup_{p\geqq Y} W_p').$$

Hence

$$\#\{t\mathscr{D} \cap (\bigcap_{p<Y} U_p')\} \leqq \#(t\mathscr{D} \cap U) + \sum_{p\geqq Y} \#(t\mathscr{D} \cap W_p').$$

If $p^{\delta'} > t$, then $t\mathscr{D} \cap W_p' = \emptyset$ by (L.2). By Lemma 2. 1 and (L.1), we have

$$\begin{aligned} t^{-N} \#(t\mathscr{D} \cap W_p') &\leqq \{\mathrm{vol}(\mathscr{D}) p^{-N} + C_1 t^{-1} p^{1-N}\} \# W_p' \\ &\leqq C \cdot \mathrm{vol}(\mathscr{D}) p^{-1-\delta} + C C_1 p^{-\delta-\delta'} \leqq C_2 p^{-\varrho} \quad \text{if} \quad p^{\delta'} \leqq t, \end{aligned}$$

where $\varrho = \mathrm{Min}(1+\delta, \delta+\delta') > 1$ and C_1, C_2 are positive constants which do not depend on p. Hence we have

$$\mathrm{vol}(\mathscr{D}) \prod_{p<Y} (\# U_p) p^{-N} \leqq \liminf_{t\to\infty} t^{-N} \#(t\mathscr{D} \cap U) + C_2 \sum_{p\geqq Y} p^{-\varrho}.$$

Letting $Y \to \infty$, we have

$$\mathrm{vol}(\mathscr{D}) \prod_p (\# U_p) p^{-N} \leqq \liminf_{t \to \infty} t^{-N} \# (t\mathscr{D} \cap U).$$

This completes the proof of the lemma. q.e.d.

§ 3. Proof of Theorem 2

Let n, r_1, r_2 be integers with $n \geqq 4$, $r_1 \geqq 0$, $r_2 \geqq 0$, $r_1 + 2r_2 = n$. In our previous paper, we have proved Theorem 2 for $r_2 = 0$ (see [7], Theorem 4). So we assume $r_2 > 0$. Let

$$f(x, y) = a_0 x^n + a_1 x^{n-1} y + \ldots + a_n y^n \qquad (a_j \in \mathbb{Z})$$

be an integral irreducible binary form of degree n. Let θ be a root of the equation $f(x, 1) = 0$ and put $K_f = \mathbb{Q}(\theta)$. Hence K_f is an algebraic number field of degree n. For each odd prime number p, let V_p denote the set of all binary forms $f(x, y)$ of degree n with coefficients in $\mathbb{F}_p$. We denote by U_p the set of all binary forms $f \in V_p$ satisfying the following condition (U):

(U) $f(x, y)$ has at most one multiple factor, which is of multiplicity two.

Further, for $p = 2$, let U_2 be the set of all binary forms $f(x, y)$ of degree n with coefficients in $\mathbb{F}_2$ such that $D(f) \neq 0$. Put $W_p = V_p - U_p$. By [7], Proposition 2. 3,

$$\# U_p = \begin{cases} p^{n-3}(p^2-1)^2 & \text{if } p \neq 2, \\ 3 \cdot 2^{n-2} & \text{if } p = 2. \end{cases}$$

Let $U_p' = \{f \in V_{\mathbb{Z}};\ f \bmod p \in U_p\}$, $W_p' = V_{\mathbb{Z}} - U_p'$. Further we put $U = \bigcap_{p:\text{prime}} U_p'$. If $f \in W_p'$, then $p | D(f)$, and hence $|D(f)| \geqq p$. By [7], Proposition 2. 2, if $f(x, y) \in \mathbb{Z}[x, y]$ is an integral irreducible binary form and $f(x, y) \in U$, then the normal closure of K_f is a weakly unramified A_n-extension of the quadratic field $\mathbb{Q}(\sqrt{D(f)})$. Let $\mathscr{F}_0$, $\mathscr{F}_{0,X}$ and κ be as in the proof of Theorem 1. Since $\# W_p \leqq 2p^{n-1}$ and $\mathscr{F}_{0,X} \cap W_p' = \emptyset$ if $X < p$, the conditions (L.1) and (L.2) in § 2 are satisfied with $\mathscr{D} = \mathscr{F}_{0,1}$, $\delta = 1$, $\delta' = 1/2(n-1)$. Applying Lemma 2. 2, we have

$$\begin{aligned} \lim_{X \to \infty} X^{-\kappa} \# (\mathscr{F}_{0,X} \cap U \cap V_{\mathbb{Z}}^{\mathrm{irr}}) &= \mathrm{vol}(\mathscr{F}_{0,1}) \prod_{p:\text{prime}} p^{-n-1} \# U_p \\ &= 24\pi^{-4} \mathrm{vol}(\mathscr{F}_{0,1}) > 0. \end{aligned}$$

In particular, there exist infinitely many integral irreducible binary forms $f(x, y)$ such that K_f has just r_2 imaginary primes and the normal closure of K_f is a weakly unramified A_n-extension of the quadratic field $\mathbb{Q}(\sqrt{D(f)})$. Suppose that $K_1, \ldots, K_r$ are algebraic number fields of degree n with just r_2 imaginary primes whose normal closures are unramified A_n-extensions over their quadratic subfields. To prove Theorem 2, it

suffices to show that there exists an algebraic number field K_{r+1} which is different from K_i $(1 \leqq i \leqq r)$ and has the same property. Let D_i be the discriminant of K_i and put

$$\tilde{U} = \{f \in U; (D(f), D_i) = 1 \text{ for } (1 \leqq i \leqq r)\}.$$

Replacing U by $\tilde{U}$, we see that $\mathscr{F}_0 \cap \tilde{U} \cap V_{\mathbb{Z}}^{\mathrm{irr}}$ is an infinite set. Take a binary form $f \in \mathscr{F}_0 \cap \tilde{U} \cap V_{\mathbb{Z}}^{\mathrm{irr}}$ and put $K_{r+1} = K_f$. Then K_{r+1} has the desired property. This completes the proof of Theorem 2.

§ 4. Proof of Theorem 3

Let $n \geqq 4$, $r_1 = n-2$, $r_2 = 1$. We use the same notation as in § 1. Put $\mathscr{F} = \Phi(\mathscr{E})$. In § 1, we have seen that Φ is a bijective C^∞-mapping of $\mathscr{E}$ to $\mathscr{F}$. Take a binary form $f \in V_{n-2,1}$ which has no linear factors over $\mathbb{Q}$. Let α be the unique complex root of $f(x, 1)$ with $\mathrm{Im}\,\alpha > 0$. By Lemma 1.1 (i), there exists an element $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ such that ${}^t\gamma^{-1} \cdot \alpha \in \Omega \cup \Omega'$. Put $g = \gamma \cdot f$ and $\beta = {}^t\gamma^{-1} \cdot \alpha$. Then β, $\bar{\beta}$ are the complex roots of $g(x, 1)$. Let b_0 be the coefficient of x^n in g. Since f has no linear factors over $\mathbb{Q}$, $b_0 = g(1, 0) = f(a, b) \neq 0$. If n is odd and $b_0 < 0$, then we replace γ by $-\gamma$. Then we have $g \in \mathscr{F}$. This proves the assertion (i). The assertion (ii) follows immediately from Lemma 1.1 (ii). We need some lemmas to show the assertion (iii).

Lemma 4.1. *Put* $f = \sum_{j=0}^{n} a_j x^{n-j} y^j = \Phi(a_0, \theta_j, \alpha)$, $\alpha = \xi + \eta\sqrt{-1}$. *Let*

$$J = \frac{\partial(a_0, a_1, \ldots, a_n)}{\partial(a_0, \theta_j, \xi, \eta)}$$

be the Jacobian of the mapping Φ. *Then*

$$|J| = 2|a_0|\,|D(f)|^{1/2}.$$

Proof. We use induction on n. For $n = 2$, the assertion is checked by a direct computation. For $n > 2$, write $f = (x - \theta y)g$, $g = \sum_{j=0}^{n-1} b_j x^{n-1-j} y^j$ $(\theta = \theta_1)$. Then we have

$$a_0 = b_0, \quad a_j = b_j - b_{j-1}\theta \quad (1 \leqq j \leqq n-1), \quad a_n = -b_{n-1}\theta.$$

Hence

$$\frac{\partial(a_i)}{\partial(b_j, \theta)} = \begin{vmatrix} 1 & & & & & 0 \\ -\theta & 1 & & & & -b_0 \\ & -\theta & 1 & & & -b_1 \\ & & & \ddots & & \vdots \\ & & & -\theta & 1 & -b_{n-2} \\ & & & & -\theta & -b_{n-1} \end{vmatrix}$$

$$= -g(\theta, 1).$$

By induction assumption,

$$\frac{\partial(b_0, \dots, b_{n-1})}{\partial(b_0, \theta_2, \dots, \theta_{n-2}, \xi, \eta)} = \pm 2 b_0 |D(g)|^{1/2}.$$

Hence $|J| = |g(0, 1)| \times 2|b_0|\, |D(g)|^{1/2} = 2|a_0|\, |D(f)|^{1/2}$. q.e.d.

Lemma 4. 2. *The following inequalities hold for any real numbers* $y_1, \dots, y_n$ *with* $y_j > 0$ $(2 \leqq j \leqq n)$:

(i) $$\prod_{2 \leqq i \leqq j \leqq n} \sum_{k=i}^{j} y_k \geqq \prod_{i=2}^{n} y_i^{n/2},$$

(ii) $$\prod_{i=1}^{n} \left\{1 + \left(\sum_{k=1}^{i} y_k\right)^2\right\} \geqq 2^{-4} \prod_{i=2}^{n} (1 + y_i^2).$$

Proof. We note that $a + b \geqq i a^{1/i} \{b/(i-1)\}^{(i-1)/i}$ for any $a > 0$, $b > 0$, $i > 1$. For $2 \leqq i < j \leqq n-2$, we have

$$\sum_{k=i}^{j} y_k \geqq i(i-1)^{-(i-1)/i} y_i^{1/i} \left(\sum_{k=i+1}^{j} y_k\right)^{(i-1)/i}$$
$$\geqq y_i^{1/i} \left(\sum_{k=i+1}^{j} y_k\right)^{(i-1)/i}.$$

Hence we have

$$\prod_{j=i}^{n} \sum_{k=i}^{j} y_k \geqq y_i^{n/i} \left\{\prod_{j=i+1}^{n} \sum_{k=i+1}^{j} y_k\right\}^{(i-1)/i}.$$

Using the above estimate, we see that the left hand side of (i) is greater than or equal to

$$\left[y_2^{n/2} \left\{\prod_{j=3}^{n} \sum_{k=3}^{j} y_k\right\}^{1/2}\right] \times \left[\prod_{3 \leqq i \leqq j \leqq n} \sum_{k=i}^{j} y_k\right]$$
$$= \left[y_2^{n/2} \left\{\prod_{j=3}^{n} \sum_{k=3}^{j} y_k\right\}^{3/2}\right] \times \left[\prod_{4 \leqq i \leqq j \leqq n} \sum_{k=i}^{j} y_k\right]$$
$$\geqq \left[(y_2 y_3)^{n/2} \left\{\prod_{j=4}^{n} \sum_{k=4}^{j} y_k\right\}^{2}\right] \times \left[\prod_{5 \leqq i \leqq j \leqq n} \sum_{k=i}^{j} y_k\right]$$
$$\cdots$$
$$\geqq (y_2 y_3 \cdots y_n)^{n/2}.$$

This proves the first inequality. Let i be an integer with $2 \leqq i \leqq n-1$. Assume

$$-y_{i+1}/2 - \sum_{k=2}^{i} y_k \leqq y_1 < -y_i/2 - \sum_{k=2}^{i-1} y_k.$$

If $1 \leqq j \leqq i-2$, then

$$1+(y_1+\ldots+y_j)^2 \geqq 1+(y_i/2+y_{i+1}+\ldots+y_{j+1})^2$$
$$\geqq 1+y_{j+1}^2,$$

since $y_1+\ldots+y_j<-y_{j+1}-\ldots-y_{i-1}-y_i/2<0$. If $j=i-1$, then

$$1+(y_1+\ldots+y_j)^2 \geqq 1+(1/4)\,y_i^2 \geqq (1/4)\,(1+y_i^2).$$

If $j=i$, then $1+(y_1+\ldots+y_j)^2 \geqq 1$. If $j=i+1$, then

$$1+(y_1+\ldots+y_j)^2 \geqq 1+(1/4)\,y_{i+1}^2 \geqq (1/4)\,(1+y_{i+1}^2).$$

If $i+2 \leqq j \leqq n$, then

$$1+(y_1+\ldots+y_j)^2 \geqq 1+(y_{i+1}/2+y_{i+2}+\ldots+y_j)^2$$
$$\geqq 1+y_j^2.$$

Hence the left hand side of (ii) is greater than or equal to $(1/16)\prod_{j=2}^{n}(1+y_j^2)$. By a similar argument, we see that the left hand side of (ii) is greater than or equal to $(1/4)\prod_{j=2}^{n}(1+y_j^2)$ if $y_1 \geqq -y_2/2$ or $y_1<-y_n/2-\sum_{k=2}^{n-1} y_k$. q.e.d.

Let $\mathfrak{F}^+=\Phi(\mathfrak{E}^+)$, $\mathfrak{F}_1=\{f\in\mathfrak{F};\ |D(f)|\leqq 1\}$. Further, put

$$\mathfrak{F}_1^+=\mathfrak{F}^+\cap\mathfrak{F}_1,\quad \mathfrak{E}_1^+=\Phi^{-1}(\mathfrak{F}_1^+).$$

Then $\mathrm{vol}(\mathfrak{F}_1)$ is equal to $2\,\mathrm{vol}(\mathfrak{F}_1^+)$ or $\mathrm{vol}(\mathfrak{F}_1^+)$ according as n is even or odd. Put

$$\Delta=2\eta\prod_{1\leqq i<j\leqq n-2}(\theta_j-\theta_i)\prod_{i=1}^{n-2}\{(\theta_i-\xi)^2+\eta^2\}.$$

By Lemma 4.1, $|D(f)|^{1/2}=a_0^{n-1}\Delta$, $|J|=2a_0^n\Delta$ on $\mathfrak{E}_1^+$, where $f=\Phi(a_0,\theta_j,\xi+\eta\sqrt{-1})$. Hence we have

$$\mathrm{vol}(\mathfrak{F}_1^+)=\int_{\mathfrak{F}_1^+} da_0\cdots da_n$$
$$=\int_{\mathfrak{E}_1^+}|J|\,da_0\,d\theta_1\cdots d\theta_{n-2}\,d\xi\,d\eta$$
$$=\int\left[\int_0^{\Delta^{1/(1-n)}}2a_0^n\,da_0\right]\Delta\,d\theta_1\cdots d\theta_{n-2}\,d\xi\,d\eta$$
$$=\frac{2}{n+1}\int\Delta^{-2/(n-1)}d\theta_1\cdots d\theta_{n-2}\,d\xi\,d\eta.$$

Here the integral in the right hand side is taken over the region

$$\theta_1<\theta_2<\ldots<\theta_{n-2},\quad 0\leqq\xi\leqq 1/2,\quad \eta>0,\quad \xi^2+\eta^2\geqq 1.$$

We make the change of variables $\theta_i = \xi + \eta t_i$ $(1 \leqq i \leqq n-2)$. Then we have

$$d\theta_1 \cdots d\theta_{n-2}\, d\xi\, d\eta = \eta^{n-2}\, dt_1 \cdots dt_{n-2}\, d\xi\, d\eta,$$

$$\Delta = 2\eta^{n(n-1)/2} \prod_{1 \leqq i < j \leqq n-2} (t_j - t_i) \prod_{i=1}^{n-2} (1 + t_i^2).$$

Hence

$$\mathrm{vol}(\mathscr{F}_1^{+}) = \frac{2^{(n-3)/(n-1)}}{n+1} \int \eta^{-2}\, d\xi\, d\eta \times \int L^{-2/(n-1)}\, dt_1 \cdots dt_{n-2},$$

where

$$L = \prod_{1 \leqq i < j \leqq n-2} (t_j - t_i) \prod_{i=1}^{n-2} (1 + t_i^2).$$

The first integral is taken over the region $0 \leqq \xi \leqq 1/2$, $\eta > 0$, $\xi^2 + \eta^2 \geqq 1$ and the second integral is taken over the region $t_1 < t_2 < \ldots < t_{n-2}$.

Let I_1, I_2 be the first and the second integral, respectively. Then we have

$$I_1 = \int_0^{1/2} (1 - \xi^2)^{-1/2}\, d\xi = \pi/6.$$

In the integral I_2, we make the change of variables

$$t_j = \sum_{k=i}^{j} y_k.$$

Put $\lambda = (n-2)/(n-1)$, $\mu = 1/(n-1)$. Then we have

$$I_2 = \int (L_1 L_2)^{-\mu}\, dy_1 \cdots dy_{n-2},$$

where

$$L_1 = \prod_{2 \leqq i \leqq j \leqq n-2} \sum_{k=i}^{j} y_k^2 \times \prod_{i=1}^{n-2} \left\{1 + \left(\sum_{k=1}^{i} y_k\right)^2\right\},$$

$$L_2 = \prod_{i=1}^{n-2} \left\{1 + \left(\sum_{k=1}^{i} y_k\right)^2\right\}.$$

The integral is taken over the region $-\infty < y_1 < \infty$, $y_j > 0$ $(2 \leqq j \leqq n-2)$. By Lemma 4. 2, we have

$$L_1 \geqq 2^{-4} \prod_{k=2}^{n-2} y_k^{(n-2)}(1 + y_k^2).$$

Since the geometric mean is bounded by the arithmetic mean, we have

$$L_2^{-\mu} \leqq (n-2)^{-1} \sum_{i=1}^{n-2} \left\{1+\left(\sum_{k=1}^{i} y_k\right)^2\right\}^{-\lambda}.$$

Hence we have

$$I_2 \leqq 2^{4\mu}(n-2)^{-1} \sum_{i=1}^{n-2} I_{2,i},$$

where

$$I_{2,i} = \int \left[\prod_{k=2}^{n-2} y_k^{-\lambda}(1+y_k^2)^{-\mu}\right]\left[1+\left(\sum_{k=1}^{i} y_k\right)^2\right]^{-\lambda} dy_1 \cdots dy_{n-2}.$$

If we make the change of variables $y_1 = s - \sum_{k=2}^{i} y_k$, then we have

$$I_{2,i} = \int \left[\prod_{i=2}^{n-2} y_i^{-\lambda}(1+y_i^2)^{-\mu}\right][1+s^2]^{-\lambda} ds\, dy_2 \cdots dy_{n-2}$$

$$= \left[\int_0^{\infty} y^{-\lambda}(1+y^2)^{-\mu} dy\right]^{n-3} \times \int_{-\infty}^{\infty} (1+s^2)^{-\lambda} ds.$$

Since $n \geqq 4$, we have $0<\lambda<1$, $\lambda+2\mu>1$ and $2\lambda>1$. Hence the last two integral converge. This completes the proof of the finiteness of $\mathrm{vol}(\mathscr{F}_1)$.

It is an open problem to obtain an asymptotic formula for $S_{r_1,r_2}(X)$. In view of Theorem 3, it is probably true that

$$\lim_{X\to\infty} X^{-\kappa} S_{n-2,1}(X) = \mathrm{vol}(\mathscr{F}_1).$$

The difficulty comes from the fact that the region $\mathscr{F}_1$ is not bounded (see the delicate argument in Davenport [2], [3]).

References

[1] *B. J. Birch, J. R. Merriman*, Finiteness theorems for binary forms with given discriminant, Proc. Lond. Math. Soc. (3) **24** (1972), 385—394.

[2] *H. Davenport*, On the class number of binary cubic forms (I), J. London Math. Soc. **26** (1951), 183—192. Corrigendum, ibid. **27** (1952), 512.

[3] *H. Davenport*, On the class number of binary cubic forms (II), J. London Math. Soc. **26** (1951), 193—198.

[4] *H. Davenport, H. Heilbronn*, On the density of discriminants of cubic fields II, Proc. Roy. Soc. Lond. A **322** (1971), 405—420.

[5] *S. Lang*, Algebraic number Theory, Reading 1970.

[6] *G. B. Mathews, W. E. H. Berwick*, On the reduction of arithmetical binary cubics which have a negative discriminant, Proc. London Math. Soc. (2) **10** (1912), 48—53.
[7] *J. Nakagawa*, Binary forms and orders of algebraic number fields, Invent. math. **97** (1989), 219—235.
[8] *K. Uchida*, Unramified extensions of quadratic number fields II, Tôhoku Math. J. **22** (1970), 220—224.
[9] *Y. Yamamoto*, On unramified Galois extensions of quadratic number fields, Osaka J. Math. **7** (1970), 57—76.
[10] *K. Yamamura*, On unramified Galois extensions of real quadratic fields, Osaka J. Math. **23** (1986), 471—478.

Department of Mathematics, Joetsu University of Education, Joetsu 943, Japan

Eingegangen 7. Juli 1989

J. reine angew. Math. **406** (1990), 179–199

Journal für die reine und angewandte Mathematik

An identity for reproducing kernels in a planar domain and Hilbert-Schmidt Hankel operators

By *Jonathan Arazy* at Haifa, *Stephen D. Fisher* at Evanston, *Svante Janson* at Uppsala and *Jaak Peetre* at Lund and Stockholm

1. Introduction

Let Ω be an open subset of the complex plane and let μ be a positive measure on Ω. We will usually assume that μ is a Radon measure, i.e. that $\mu(K)<\infty$ for every compact subset K of Ω.

We define the (weighted) Bergman space $A(\Omega, \mu)=\{f\in\mathscr{H}(\Omega): \int_\Omega |f|^2\,d\mu<\infty\}$, i.e. the space of all square integrable analytic functions on Ω, and let $\|f\|_A=\|f\|_{L^2(\mu)}$. (We will, whenever convenient, drop Ω and/or μ from $A(\Omega, \mu)$ and similar notations.) We will always assume the following.

(1. 1) For any compact $F\subset\Omega$ there is a constant $C<\infty$ such that,

$$\text{if } f\in A \quad\text{and}\quad z\in F, \quad |f(z)|\leqq C\|f\|_A.$$

This condition says that the point evaluations are continuous on A, and uniformly so on compact subsets, i.e. that the inclusion $A\subset\mathscr{H}(\Omega)$ is continuous. It follows easily that A is a closed subspace of $L^2(\mu)$, and thus a Hilbert space.

The condition (1. 1) is clearly satisfied if μ equals the restriction to Ω of the Lebesgue measure, which we will denote by m. More generally, it holds e.g. if $d\mu/dm$ is a continuous, strictly positive function on Ω. It is also possible to have μ vanishing on a part of Ω, as long as this "hole" does not extend to the boundary.

The Hilbert space A is equipped with a reproducing kernel depending on Ω and μ, which we denote by $K(z, w)$. We collect the definition and basic properties of K in Section 2. Our main result is the following.

Theorem 1. 1. *Suppose that one of the following holds.*

(i) $\int_\Omega |z|^n\,d\mu(z)<\infty$ *for every* n. (Ω *arbitrary.*)

(ii) *The complement of Ω contains a continuum and μ is finite.*

(iii) *The complement of Ω contains a continuum and μ is the Lebesgue measure on Ω.*

Then, for every $f \in \mathscr{H}(\Omega)$,

$$\int_\Omega \int_\Omega |f(z)-f(w)|^2 \, |K(z,w)|^2 \, d\mu(z) \, d\mu(w) = \frac{1}{\pi} \int_\Omega |f'(z)|^2 \, dm(z). \tag{1.2}$$

(*In particular, if one side of* (1.2) *is infinite then so is the other.*)

For convenience, we let in the sequel $I(f, \Omega, \mu)$ and $D(f, \Omega)$ denote the left and right sides of (1.2) respectively, and can thus state the result as

$$I(f, \Omega, \mu) = D(f, \Omega), \quad \text{for any } f \text{ analytic in } \Omega. \tag{1.3}$$

Note that the right side of (1.2) (and (1.3)) is the Dirichlet integral of f, and is independent of μ. Hence a surprising corollary is that the integral $I(f, \Omega, \mu)$, although superficially depending on μ both directly and indirectly through K, in fact does not depend on μ at all (subject to our conditions).

We have tried to give the conditions on Ω and μ is a simple form which includes most cases of interest, but they are not the best possible. They can be somewhat extended using Lemma 2.1 below, and presumably they can be weakened further. On the other hand, some condition is needed as the following example shows.

Example 1.1. Suppose that the complement of Ω is countable (e.g. $\Omega = \mathbb{C}$) and that μ is the Lebesgue measure. If $f \in A(\Omega, \mu)$, then f cannot have any isolated singularities, as is seen by using Plancherel's theorem on the Laurent series expansion. Consequently, f has to be a square integrable entire function, whence $f = 0$. Thus $A = \{0\}$, $K(z, w) = 0$ and $I(f, \Omega, \mu) = 0$ for any f. On the other hand, by the same argument applied to f', $D(f, \Omega) = \infty$ for any non-constant analytic f in Ω.

The motivation for studying $I(f, \Omega, \mu)$ comes from the theory of Hankel operators in general domains, which we now briefly describe. Let Ω, μ and A be as above, and let P denote the orthogonal projection of $L^2(\mu)$ onto A. Given a measurable function f in Ω, which we first, for simplicity, assume is bounded, we define the Hankel operator with symbol f to be

$$H_f(g) = (I - P)(\bar{f} g), \quad g \in A. \tag{1.4}$$

In other words, $H_f = (I - P) M_{\bar{f}}$, where $M_{\bar{f}}$ denotes the multiplication operator $g \to \bar{f} g$. (This is known as the big Hankel operator, as opposed to the small Hankel operator $\bar{P}(\bar{f} g)$ which will not be studied here.) H_f is obviously a bounded operator of A into $A^\perp$. It follows from (2.6) below that it can be expressed as an integral operator

$$H_f(g)(z) = \int \overline{(f(z) - f(w))} \, K(z, w) \, g(w) \, d\mu(w). \tag{1.5}$$

We will here only consider analytic symbols f and it is then easy to show that the right side of (1.5) vanishes when $g \in A^{\perp}$; thus it defines the extension $H_f P$ of H_f to $L^2(\mu)$. Consequently the Hilbert-Schmidt norm of the Hankel operator is given by

$$\|H_f\|_{\mathrm{HS}} = \|H_f P\|_{\mathrm{HS}} = \|(\overline{f(z)} - \overline{f(w)})\, K(z, w)\|_{L^2(\mu \times \mu)} = I(f, \Omega, \mu)^{1/2}. \tag{1.6}$$

We assumed above that the symbol was bounded, but the definition of the Hankel operator may be extended to unbounded symbols by using (1.5) as a definition. We can now reformulate our results as follows.

Theorem 1.2. *Let Ω and μ be as in Theorem* 1.1. *The Hankel operator H_f with analytic symbol f is a Hilbert-Schmidt operator if and only if f belongs to the Dirichlet class; furthermore*

$$\|H_f\|_{\mathrm{HS}} = \left(\frac{1}{\pi} \int_{\Omega} |f'(z)|^2 \, dm(z)\right)^{1/2}. \tag{1.7}$$

There is a third way to describe the results. Let again f be bounded and analytic, and define the Toeplitz operator $T_f g = fg$. (Thus $T_f = M_f$. This holds because we assume f to be analytic; in general $T_f = P M_f$.) T_f is a bounded operator on A, and it is easily seen that $T_f^* T_f - T_f T_f^* = H_f^* H_f$. Hence

$$\mathrm{Tr}\,(T_f^* T_f - T_f T_f^*) = \mathrm{Tr}\,(H_f^* H_f) = \|H_f\|_{\mathrm{HS}}^2 = I(f, \Omega, \mu). \tag{1.8}$$

Thus Theorem 1.2 can be reformulated as a trace formula. For simplicity we consider only bounded f.

Theorem 1.3. *Let Ω and μ be as in Theorem* 1.1. *If f is a bounded analytic function on Ω, then*

$$\mathrm{Tr}\,(T_f^* T_f - T_f T_f^*) = \frac{1}{\pi} \int_{\Omega} |f'(z)|^2 \, dm(z). \tag{1.9}$$

Theorem 1.3 in the case when μ is the Lebesgue measure is due to Berger and Shaw [BS1], Theorem 7, see also [BS2] and [HH, § 1]. They have also some partial results for other measures.

The Hankel operator (1.4) has been studied e.g. by Axler [Ax] (Lebesgue measure in the unit disc) and Arazy, Fisher and Peetre [AFP1] ($d\mu = (1-|z|^2)^{\alpha} dm$ in the unit disc), [AFP2] (Lebesgue measure in finitely connected domains). The latter two papers contain characterizations of the (analytic) symbols that give Hankel operators in the Schatten class S_p, including Theorem 1.2 (for these Ω and μ) as the special case $p = 2$ ($S_2 = \mathrm{HS}$).

Remark 1.1. The Hardy space H^2 in the unit disc or upper half space is not included in our formulation, but it can be regarded as a limiting case with $\Omega =$ unit disc or upper half space and $\mu =$ one-dimensional Lebesgue measure on the boundary (normalized on $\mathbb{T}$). $K(z, w) = (1 - z\bar{w})^{-1}$ and $(2\pi i(\bar{w} - z))^{-1}$, respectively.

Theorem 1.1 holds formally also in these cases, and (1.2) reduces to the well-known formulas

$$\frac{1}{4\pi^2}\int_{\mathbb{T}}\int_{\mathbb{T}}\frac{|f(z)-f(w)|^2}{|1-z\bar{w}|^2}\,|dz|\,|dw| = \frac{1}{\pi}\int_{|z|<1}|f'(z)|^2\,dm(z), \tag{1.10}$$

$$\frac{1}{4\pi^2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{|f(x)-f(y)|^2}{|x-y|^2}\,dx\,dy = \frac{1}{\pi}\int_{\Im z>0}|f'(z)|^2\,dm(z). \tag{1.11}$$

Hankel (and Toeplitz) operators on Hardy spaces (the classical case) are studied in many papers; S_p-results, including Theorem 1.2 for this case, can be found e.g. in [P], [R].

Note that if e.g. Ω is bounded, Theorem 1.2 implies that there are plenty of Hilbert-Schmidt Hankel operators. On the other hand, if $\Omega = \mathbb{C}$, or, more generally, if the complement of Ω is countable, $D(f, \Omega) = \infty$ for any non-constant analytic f (see Example 1.1), and there are no non-trivial Hilbert-Schmidt Hankel operators (provided μ satisfied our conditions).

Unfortunately, the proof of the theorems is much more complicated and less attractive than the statements. It occupies the rest of the paper and is organized as follows.

Section 2 contains a list of properties of the reproducing kernel, together with some elementary invariance properties.

Section 3 exhibits some technical difficulties, and may partly explain why we have not found any simpler proof.

Section 4 contains a formal argument, which may partly explain why the theorems are true. A special case where μ is the Lebesgue measure and Ω and f have some technical restrictions, is rigorously proved by this argument, and is the starting point of the proof. (Another special case, viz. Ω a disc or an annulus and μ a rotation invariant measure, is proved by a completely different method (Taylor expansions and explicit calculations for monomials) in [AFP1]. This could be used as the starting point for the proof when Ω is simply or doubly connected, but we have not been able to derive the result for more complicated domains this way.)

Section 5 contains a proof of the second main step, viz. that the measure μ may be arbitrarily altered on a compact subset of Ω without affecting $I(f, \Omega, \mu)$.

Section 6 contains continuity results which enable us to pass from the Lebesgue measure (treated in Section 4), through measures differing from the Lebesgue measure on larger and larger compact sets, to any measure satisfying (1.1). The details are, however, a little complicated and we will e.g. also vary the domain in the process.

Section 7, finally, contains some open problems.

2. Preliminaries

It is well-known that (1. 1) implies the existence of a reproducing kernel $K(z, w)$, defined on Ω^2, with the following properties,

(2. 1) $K(z, w)$ is continuous, analytic in z and anti-analytic in w,

(2. 2) $K(w, z) = \overline{K(z, w)}$,

(2. 3) $K_w(z) = K(z, w) \in A$ for every $w \in \Omega$, and

(2. 4) $\|K_w\|_A = K(w, w)^{1/2}$,

(2. 5) $f(z) = \langle f, K_z \rangle = \int f(w)\, \overline{K(w, z)}\, d\mu(z) = \int f(w)\, K(z, w)\, d\mu(w)$,
for every $f \in A$ and $z \in \Omega$, and, more generally,

(2. 6) $Pf(z) = \int K(z, w)\, f(w)\, d\mu(w)$, for $f \in L^2(\mu)$ and $z \in \Omega$.

In fact, (2. 3) and (2. 5) serve as a definition of K. For proofs and further properties, see e.g. Aronszajn [A] and Bergman [B].

Before proceeding further, we note that $I(f, \Omega, \mu)$ possesses some simple invariance properties.

If we perform a "change of gauge", i.e. let ϕ be an analytic function different from 0 in Ω and transform $\mu \to |\phi|^{-2}\mu$, then the reproducing kernel transforms as $K \to \phi(z)\, \overline{\phi(w)}\, K(z, w)$, and $I(f, \Omega, \mu)$ is invariant. (The simplest example is multiplication by a constant.)

A "change of variable" by a conformal map $\psi : \Omega_1 \to \Omega$, transforms $\mu \to \mu \circ \psi$ and $K \to K(\psi(z), \psi(w))$. If the symbol f transforms as $f \to f \circ \psi$, it follows that $I(f, \Omega, \mu)$ is invariant. Note that $D(f, \Omega)$ also is invariant, which shows that the relation

$$I(f, \Omega, \mu) = D(f, \Omega)$$

is conformally invariant.

If μ is the Lebesgue measure m in Ω, then the conformal map ψ transforms dm into $d(m \circ \psi) = |\psi'(z)|^2\, dm$. A combination of the two invariances above show that $I(f, \Omega, \mu)$ is conformally invariant.

We summarize these results as a lemma.

Lemma 2. 1. (i) *If* $d\mu_1 = |\phi|^{-2}\, d\mu$, *where* $\phi \in \mathscr{H}(\Omega)$ *with* $\phi(z) \neq 0$, $z \in \Omega$, *then*

$$I(f, \Omega, \mu_1) = I(f, \Omega, \mu).$$

(ii) *If* ψ *is a conformal map of* Ω_1 *onto* Ω, *and* μ *induces the measure* $\mu \circ \psi$ *in* Ω_1, *then*

$$I(f, \Omega_1, \mu \circ \psi) = I(f \circ \psi^{-1}, \Omega, \mu).$$

(iii) *If ψ is a conformal map of Ω_1 onto Ω, then*

$$I(f, \Omega_1, m) = I(f \circ \psi^{-1}, \Omega, m).$$

Remark 2. 1. The invariances discussed here reflect the fact that

$$|K(z, w)|^2 \, d\mu(z) \, d\mu(w)$$

is an invariant measure on Ω^2. Its marginals equal (by (2. 4)) the well-known invariant measure $K(z, z) \, d\mu(z)$ on Ω. (The measure is infinite unless $\dim A < \infty$.)

Remark 2. 2. It is sometimes possible to allow a change of gauge by a function ϕ which has zeroes, e.g. always when $\mu = m$. This will not be further discussed here.

Remark 2. 3. In some highly symmetric cases, the main result follows easily from these invariances. Consider the unit disc with Lebesgue measure. Lemma 2. 1 then shows that $I(f)$ is Möbius invariant. Since the only non-trivial Möbius invariant Hilbert space is the Dirichlet space [AF], it follows that $I(f) = cD(f)$ for some constant $c \leqq \infty$ (independent of f); explicit calculations for e.g. $f = z$ show that $c = 1$.

We also note that we may always treat the components of Ω separately.

Lemma 2. 2. *Suppose that $\Omega = \bigcup \Omega_n$ disjoint, and let μ_n be the restriction of μ to Ω_n. Then,*

$$I(f, \Omega, \mu) = \sum I(f, \Omega_n, \mu_n), \qquad f \in \mathscr{H}(\Omega). \tag{2. 7}$$

Proof. If K_n is the reproducing kernel for μ_n and Ω_n, then

$$K(z, w) = \begin{cases} K_n(z, w) & z, w \in \Omega_n, \\ 0 & z \in \Omega_n, \ w \in \Omega_m, \ m \neq n. \end{cases} \qquad \square$$

3. Two unsuccessful attempts

Let us try to compute $I(f)$ by expanding $|f(z) - f(w)|^2$ in the integral.

$$\begin{aligned} I(f, \Omega, \mu) &= \iint |f(z)|^2 \, |K(z, w)|^2 \, d\mu(z) \, d\mu(w) - \iint f(z) \, \overline{f(w)} \, |K(z, w)|^2 \, d\mu(z) \, d\mu(w) \\ &\quad - \iint f(w) \, \overline{f(z)} \, |K(z, w)|^2 \, d\mu(z) \, d\mu(w) + \iint |f(w)|^2 \, |K(z, w)|^2 \, d\mu(z) \, d\mu(w) \\ &= I_1 - I_2 - I_3 + I_4. \end{aligned} \tag{3. 1}$$

Using (2. 4) we see that

$$I_4 = I_1 = \int |f(z)|^2 \, K(z, z) \, d\mu(z).$$

Further, $I_3 = \overline{I_2}$ and, if we use the reproducing property (2. 5) on the inner integral,

$$I_2 = \iint f(z)\, K(z, w)\, K(w, z)\, d\mu(z)\, \overline{f(w)}\, d\mu(w)$$
$$= \int f(w)\, K(w, w)\, \overline{f(w)}\, d\mu(w) = I_1.$$

Hence $I_1 = I_2 = I_3 = I_4$ and it looks as if we have proved that $I(f) = 0$, which obviously is impossible except in trivial cases. The solution to this paradox is that $I_1 = \infty$ (for any f that does not vanish identically, provided Ω and μ are as in Theorem 1. 1), so the right side of (3. 1) is of the type $\infty - \infty$ (when I_2 and I_3 are well-defined at all).

Let us therefore be more careful, and let us try an expansion of $|f(z) - f(w)|^2$ into two terms.

Suppose that $(f(z) - f(w))\, K(z, w) \in A$ for every w (this holds e.g. if H_f is bounded, see the proof of Lemma 5. 3). Then by the reproducing property (2. 5),

$$\int (f(z) - f(w))\, K(z, w)\, K(w, z)\, d\mu(z) = 0. \tag{3. 2}$$

Thus, performing the z-integral first,

$$\iint \overline{f(w)}\, (f(z) - f(w))\, |K(z, w)|^2\, d\mu(z)\, d\mu(w) = 0. \tag{3. 3}$$

Consequently,

$$I(f) = \iint \overline{f(z)}\, (f(z) - f(w))\, |K(z, w)|^2\, d\mu(z)\, d\mu(w). \tag{3. 4}$$

If we here interchange the order of integration, we obtain, just as in (3. 3), 0! Again, this is not the right answer. We will, however, in Section 5 use this argument to show that $I(f, \mu_1) - I(f, \mu_2) = 0$, for two suitable measures μ_1 and μ_2.

4. A promising attempt

We will present in this section a formal calculation which yields the desired equality $I(f, \mu) = D(f, \Omega)$, for any Ω and μ. There are, however, several technical problems with it. With the lesson of Section 3 in mind, we therefore do not claim that this calculation proves the theorem, although we this time at least get the correct answer. It may, nevertheless, give some intuitive explanation of the result. (The technical proof given in the remaining sections is less intuitive.) Furthermore, the calculation can be made rigorous in some situations, which proves our theorem in a special case which will be needed later.

We begin by introducing a second kernel.

Define for $z \in \Omega$ and $w \in \mathbb{C}$ such that the integral converges,

$$J(z, w) = J_z(w) = \frac{1}{\pi(z - w)} - \int_\Omega \frac{1}{\pi(\zeta - w)}\, K(z, \zeta)\, d\mu(\zeta). \tag{4. 1}$$

Obviously J is a measurable function defined on a measurable subset of $\Omega \times \mathbb{C}$.

We collect the most important properties of this kernel in a lemma. Note in particular that (4. 2) is a natural extension of the reproducing property (2. 5) for analytic functions to arbitrary smooth functions, where the extra term depends only on $\bar{\partial}\phi$ which measures the non-analyticity.

Lemma 4. 1. *Suppose that Ω is bounded and μ finite.*

(i) *For any fixed $z \in \Omega$, the integral in* (4. 1) *converges for a.e. w and defines J_z as a function in $L^1(dm)$.*

(ii) *For a.e. fixed $w \in \Omega$, $J_z(w)$ is defined for all $z \in \Omega \setminus \{w\}$ and is an analytic function of z with a simple pole with residue $1/\pi$ at w.*

(iii) $J_z(w) = 0$ *if* $w \notin \bar{\Omega}$.

(iv) *If $\phi \in C^\infty(\bar{\Omega})$, i.e. ϕ can be extended to a C^∞ function in a neighbourhood of $\bar{\Omega}$, then, for every $z \in \Omega$,*

$$\phi(z) = \int_\Omega K(z, w)\, \phi(w)\, d\mu(w) + \int_{\bar{\Omega}} J(z, w)\, \bar{\partial}\phi(w)\, dm(w). \tag{4. 2}$$

Proof. We begin with (iii). If $w \notin \bar{\Omega}$, then $1/\pi(\zeta - w)$ is a bounded analytic function of ζ on Ω and thus belongs to $A^2(\Omega, \mu)$ (by our assumption on μ). Hence $J_z(w) = 0$ by (2. 5).

In order to prove (i), we rewrite the definition (4. 1) as

$$J_z(w) = \frac{1}{\pi(z - w)} + \frac{1}{\pi w} * K(z, w)\, d\mu(w). \tag{4. 3}$$

Here $1/\pi w \in L^1_{\mathrm{loc}}(dm)$ and, since $K_z \in L^2(\mu) \subset L^1(\mu)$, $K(z, w)\, d\mu(w)$ is a finite measure with compact support. Consequently the convolution is defined a.e. and $J_z \in L^1_{\mathrm{loc}}(dm)$. $J_z \in L^1(dm)$ follows by (iii).

Furthermore, if G is a relatively compact open subset of Ω, let F be a compact subset of Ω such that $\bar{G} \subset F^0$. By the mean value theorem,

$$\sup_{z \in G} |f(z)| \leqq C \int_F |f(z)|\, dm(z)$$

for any $f \in \mathscr{H}(\Omega)$; in particular

$$\sup_{z \in G} |K(z, w)| \leqq C \int_F |K(z, w)|\, dm(z)$$

and

$$\begin{aligned} \int_\Omega \sup_{z \in G} |K(z, \zeta)|\, d\mu(\zeta) &\leqq C \int_F \int_\Omega |K(z, \zeta)\, d\mu(\zeta)\, dm(z) \\ &\leqq C \int_F \|K_z\|_A\, \mu(\Omega)^{1/2}\, dm(z) < \infty. \end{aligned}$$

We obtain as above that, for a.e. w,

$$\int_\Omega \frac{1}{\pi|\zeta-w|} \sup_{z\in G} |K(z,\zeta)|\, d\mu(\zeta) < \infty. \tag{4.4}$$

For every such w, $\int \frac{1}{\pi(\zeta-w)} K(z,\zeta)\, d\mu(\zeta)$ is defined for all $z \in G$; furthermore, it is a continuous function of $z \in G$ by dominated convergence and analytic by Morera's theorem. (ii) follows by exhausting Ω by a sequence $\{G_n\}$ of relatively compact open subsets.

Finally we apply $\bar\partial$ (in distribution sense) to (4.3). Since $\bar\partial \frac{1}{\pi w} = \delta_0$, we obtain

$$\bar\partial J_z = -\delta_z + K(z,w)\, d\mu(w). \tag{4.5}$$

By the definition of distribution derivatives (and (iii)), this is the same as (4.2) for all $\varphi \in C_0^\infty(\mathbb{C})$. Since any function in $C^\infty(\bar\Omega)$ may be extended to a function in $C_0^\infty(\mathbb{C})$, it follows that (4.2) holds for every $\varphi \in C^\infty(\bar\Omega)$. □

Remark 4.1. (4.2) can easily be extended to all Lipschitz functions on $\bar\Omega$ by standard extension and smoothing arguments, but this will not be used here.

Remark 4.2. The proof shows that we could alternatively have defined J_z to be the solution of (4.5) that vanishes on $\bar\Omega^c$.

Remark 4.3. Suppose that Ω is a finitely connected domain with analytic boundary (this can be relaxed) and that μ is the Lebesgue measure. Then, for $z \neq w \in \Omega$,

$$J(z,w) = -\frac{2}{\pi}\frac{\partial}{\partial z} G(z,w), \tag{4.6}$$

$$K(z,w) = -\frac{2}{\pi}\frac{\partial^2}{\partial z\, \partial \bar w} G(z,w), \tag{4.7}$$

where G is the Green's function of Ω. (4.7) is due to Bergman [B], Chapter V, § 4, and (4.6) follows by Remark 4.2. (Bergman proves (in principle) (4.2) directly for this case, by Green's theorem, and then concludes (4.7).)

In particular, for the unit disc $G(z,w) = \log\left|\frac{1-z\bar w}{z-w}\right|$ and we get

$$J(z,w) = \frac{1}{\pi}\frac{1-|w|^2}{(z-w)(1-z\bar w)},$$

$$K(z,w) = \frac{1}{\pi}\frac{1}{(1-z\bar w)^2}. \tag{4.8}$$

Remark 4. 4. It is easily seen that J transforms to $\varphi(z)\,\varphi(w)^{-1}\,J(z, w)$ under the change of gauge $\mu \to |\varphi|^{-2}\mu$ and to $\psi'(w)\,J(\psi(z), \psi(w))$ under the change of variable $\mu \to \mu \circ \psi$.

Our formal argument for (1. 2) now runs as follows. We fix $f \in \mathscr{H}(\Omega)$ and apply Lemma 4. 1 (iv) (pretending that this is allowed) to the function

$$\varphi_z(w) = K(w, z)\,|f(w)-f(z)|^2 \tag{4. 9}$$

for each fixed $z \in \Omega$. Since

$$\bar\partial\varphi_z = K(w, z)\,(f(w)-f(z))\,\bar\partial(\overline{f(w)-f(z)}) = K(w, z)\,(f(w)-f(z))\,\overline{f'(w)},$$

this yields (if $m(\partial\Omega)=0$)

$$\begin{aligned} 0 = \varphi_z(z) = &\int_\Omega |K(z, w)|^2\,|f(w)-f(z)|^2\,d\mu(w) \\ &+\int_\Omega J(z, w)\,K(w, z)\,(f(w)-f(z))\,\overline{f'(w)}\,dm(w). \end{aligned} \tag{4. 10}$$

We integrate (4. 10) over $d\mu(z)$ and obtain, interchanging the order of integration,

$$\begin{aligned} I(f, \mu) &= -\int_\Omega\int_\Omega J(z, w)\,K(w, z)\,(f(w)-f(z))\,\overline{f'(w)}\,dm(w)\,d\mu(z) \\ &= \int_\Omega\int_\Omega J(z, w)\,(f(z)-f(w))K(w, z)\,d\mu(z)\,\overline{f'(w)}\,dm(w). \end{aligned} \tag{4. 11}$$

By Lemma 4. 1 (ii), $J(z, w)\,(f(z)-f(w))$ is for a.e. $w \in \Omega$ an analytic function of z which at w equals $\frac{1}{\pi}f'(w)$. If this function belongs to A (for a.e. w), the reproducing property of K shows that the inner integral on the right side above equals $\frac{1}{\pi}f'(w)$, and thus

$$I(f, \mu) = \int_\Omega f'(w)\,\overline{f'(w)}\,dm(w) = D(f, \Omega) \tag{4. 12}$$

as we wanted to prove.

We will justify this argument only in the simple case when $\partial\Omega$ is smooth and μ is the Lebesgue measure, see also [Ar].

Lemma 4. 2. *If Ω is a finitely connected domain with analytic boundary, μ is the Lebesgue measure and f is analytic in a neighbourhood of $\bar\Omega$, then $I(f, \Omega, \mu) = D(f, \Omega)$.*

Proof. We use the equations in Remark 4. 3. Since $G(z, w)$ may, be the reflection principle, be continued across the boundary of Ω, for every fixed w, we obtain easily (e.g. by comparison with the case of the unit disc, (4. 8)) the estimates

$$|J(z, w)| \leqq C \frac{d(w)}{|z-w|\,(|z-w|+d(z)+d(w))}, \tag{4.13}$$

$$|K(z, w)| \leqq C(|z-w|+d(z)+d(w))^{-2}, \tag{4.14}$$

where $d(\cdot)$ is the distance to the boundary $\partial\Omega$. See [AFP2], Proposition 3.7 and its proof for further details. It is clear that $\varphi_z \in C^\infty(\bar{\Omega})$, whence (4.10) follows, and

$$\iint |J(z, w)|\,|K(w, z)|\,|f(w)-f(z)|\,|f'(w)|\,dm(z)\,dm(w)$$
$$\leqq C \iint d(w)\,(|z-w|+d(w))^{-3}\,dm(z)\,dm(w) < \infty,$$

so the use of Fubini's theorem in (4.11) is justified. Finally, $J(z, w)\,(f(z)-f(w))$ is bounded, and (4.12) follows. □

We will not deal with the problem of extending this result to arbitrary $f \in \mathscr{H}(\Omega)$, since this will be a consequence of our general results in Section 6.

5. Compact perturbations

We will in this section show that we may alter the measure μ on compact subsets of Ω without changing $I(f, \mu)$. We will use the following notation. F is a compact subset of Ω, and μ_1 and μ_2 are two positive measures on Ω which are finite on F and coincide on $\Omega\backslash F$. Hence $\Delta\mu = \mu_2 - \mu_1$ is a finite signed measure with compact support in Ω. We write $A_1 = A(\mu_1)$, $A_2 = A(\mu_2)$ and similarly K_1, K_2, P_1, P_2 etc.

The basic idea in this section is that an argument in Section 3, which seemed to yield $I(f, \mu) = 0$, can be rigorously applied to the difference $I(f, \mu_1) - I(f, \mu_2)$. We begin with some preliminaries.

Lemma 5.1. *Let Ω, μ_1, μ_2 be as above, and suppose that either μ_1 or μ_2 satisfies* (1.1). *Then both measures satisfy* (1.1). *Furthermore, $A_1 = A_2$ as sets and the norms $\| \|_1$ and $\| \|_2$ are equivalent.*

Proof. That $A_1 = A_2$ as sets is immediate. If we knew that both μ_1 and μ_2 satisfied (1.1), then the equivalence of the norms would follow by the closed graph theorem. We will instead prove directly that if μ_1 satisfies (1.1), then $\| \|_1 \leqq C \| \|_2$ for some $C < \infty$. This implies that also μ_2 satisfies (1.1) and, by symmetry, that the norms are equivalent.

Hence, assume that μ_1 satisfies (1.1). It suffices to show that

$$\|f\|_1^2 \leqq C \int_{\Omega\backslash F} |f|^2 d\mu_1, \quad f \in A_1. \tag{5.1}$$

Suppose that this is false. Then there exist functions $f_n \in A_1$ with $\int_\Omega |f_n|^2 d\mu_1 = 1$ and $\int_{\Omega\setminus F} |f_n|^2 d\mu_1 < 1/n$. By (1.1), $\{f_n\}$ is a normal family and we can find a subsequence which converges to some $f \in \mathscr{H}(\Omega)$ with

$$\int_F |f|^2 d\mu_1 = \lim_{n\to\infty} \int_F |f_n|^2 d\mu_1 = 1$$

and, by Fatou's lemma, $\int_{\Omega\setminus F} |f|^2 d\mu_1 = 0$. This, however, is impossible, e.g. by the following argument. Let $R = \sup\{|z| : z \in F \text{ and } f(z) \neq 0\}$. Then $\|z^n f\|_1 \leqq R^n$ and thus, by (1.1), $|z^n f(z)| \leqq C_z R^n$ for every $z \in \Omega$. This implies $f(z) = 0$ when $|z| > R$, which leads to a contradiction. □

Lemma 5.2. *Let Ω, μ_1, μ_2 be as in Lemma 5.1, and let $f \in \mathscr{H}(\Omega)$. If $I(f, \mu_1) < \infty$ then $I(f, \mu_2) < \infty$.*

Proof. The conclusion can be rephrased as: if $H_1 = (I - P_1) M_{\bar{f}}$ is a Hilbert-Schmidt operator from A into $L^2(\mu_1)$, then $H_2 = (I - P_2) M_{\bar{f}}$ is a Hilbert-Schmidt operator from A into $L^2(\mu_2)$. (We here use the definition (1.4) of the Hankel operators; we omit the verification of the fact that the definitions (1.4) and (1.5) agree in this case.) Note that it does not matter which norm we use on A since the two norms are equivalent here, but that the situation is less simple for the ranges.

Define

$$h_w(z) = (f(z) - f(w))\, K_1(z, w). \tag{5.2}$$

Since h_w is analytic, $\|h_w\|_2 \leqq C \|h_w\|_1$ for all w, and thus

$$\begin{aligned} \|H_1\|^2_{\mathrm{HS}(A_1, L^2(\mu_2))} &= \iint |(\overline{f(z)} - \overline{f(w)})\, K_1(z, w)|^2 \, d\mu_2(z)\, d\mu_1(w) \\ &= \int \|h_w\|_2^2 \, d\mu_1(w) \leqq C \int \|h_w\|_1^2 \, d\mu_1(w) = C \|H_1\|^2_{\mathrm{HS}(A_1, L^2(\mu_2))} < \infty. \end{aligned} \tag{5.3}$$

Hence H_1 is a Hilbert-Schmidt operator from A into $L^2(\mu_2)$, and thus so is

$$(I - P_2) H_1 = (I - P_2)(I - P_1) M_{\bar{f}} = (I - P_2) M_{\bar{f}} = H_2$$

(because $P_2 P_1 = P_1$). □

Remark 5.1. It may more generally be shown that $H_1 \in S_p$ iff $H_2 \in S_p$ for any p, $0 < p \leqq \infty$.

Lemma 5.3. *Let Ω, μ_1, μ_2 be as in Lemma 5.1, and let $f \in \mathscr{H}(\Omega)$. Then $I(f, \mu_1) = I(f, \mu_2)$.*

Proof. We may, by Lemma 5.2, assume that $I(f, \mu_1)$ and $I(f, \mu_2)$ both are finite. Let h_w be as in (5.2). It is easily seen that

$$H_1(K_{1w})(z) = (\overline{f(z)} - \overline{f(w)})\, K_1(z, w). \tag{5.4}$$

Hence

$$\|h_w\|_{A_1} = \|H_1(K_{1w})\|_{L^2(\mu_1)} \leqq \|H_1\|\, K_1(w, w)^{1/2} \tag{5.5}$$

and

$$\|f(z)\, K_1(z, w)\|_{A_1} \leqq (\|H_1\| + |f(w)|)\, K_1(w, w)^{1/2}. \tag{5.6}$$

Since $A_1 = A_2$ with equivalent norms, also

$$\|h_w\|_{A_2} \leqq C K_1(w, w)^{1/2}, \tag{5.7}$$

$$\|f(z)\, K_1(z, w)\|_{A_2} \leqq C(1 + |f(w)|)\, K_1(w, w)^{1/2}. \tag{5.8}$$

(C here denotes finite constants depending on f.) Define

$$I^* = \iint |f(z) - f(w)|^2\, K_1(z, w)\, K_2(w, z)\, d\mu_2(z)\, d\mu_1(w). \tag{5.9}$$

(The integral converges absolutely by (5.3), symmetry, and Cauchy-Schwarz's inequality.) Since, by (5.5), $h_w \in A$ for every $w \in \Omega$, we obtain as in (3.3),

$$\overline{f(w)} \int (f(z) - f(w))\, K_1(z, w)\, K_j(w, z)\, d\mu_j(z) = \overline{f(w)}\, h_w(w) = 0, \qquad j = 1, 2$$

and thus, since $\int |f(z)\, h_w(z)\, K_1(w, z)|\, d\mu_2(z) < \infty$ for every w by (5.7) and (5.8),

$$\begin{aligned} I^* - I(\mu_1) &= \int \left(\int \overline{f(z)}\, h_w(z)\, K_2(w, z)\, d\mu_2(z) - \int \bar{f}(z)\, h_w(z)\, K_1(w, z)\, d\mu_1(z)\right) d\mu_1(w) \\ &= \int \left(\int \overline{f(z)}\, h_w(z)\, (K_2(w, z) - K_1(w, z))\, d\mu_2(z)\right. \\ &\quad \left. - \int \overline{f(z)}\, h_w(z)\, K_1(w, z)\, d\Delta\mu(z)\right) d\mu_1(w). \end{aligned} \tag{5.10}$$

We claim that the right side of (5.10) actually is the difference of two absolutely convergent double integrals. In fact, by the reproducing properties of K_1 and K_2,

$$\begin{aligned} K_2(w, z) - K_1(w, z) &= \overline{\int K_2(\zeta, w)\, K_1(z, \zeta)\, d\mu_1(\zeta)} - \int K_1(\zeta, z)\, K_2(w, \zeta)\, d\mu_2(\zeta) \\ &= -\int K_1(\zeta, z)\, K_2(w, \zeta)\, d\Delta\mu(\zeta). \end{aligned} \tag{5.11}$$

Thus, by (5. 3) and (5. 8),

$$\begin{aligned}(5.12)\qquad &\iint |\overline{f(z)}\, h_w(z)\,(K_2(w,z)-K_1(w,z))|\, d\mu_2(z)\, d\mu_1(w)\\ &\leqq \iiint |h_w(z)\, f(z)\, K_1(\zeta,z)\, K_2(w,\zeta)|\, d\mu_2(z)\, d\mu_1(w)\, d|\Delta\mu|(\zeta)\\ &\leqq \int \Big(\iint |h_w(z)|^2\, d\mu_2(z)\, d\mu_1(w)\Big)^{1/2}\\ &\quad\times \Big(\iint |f(z)\, K_1(z,\zeta)\, K_2(w,\zeta)|^2\, d\mu_2(z)\, d\mu_1(w)\Big)^{1/2} d|\Delta\mu|(\zeta)\\ &= \int C\,\|f(z)\, K_1(z,\zeta)\|_{A_2}\, \|K_{2\zeta}\|_{A_1}\, d|\Delta\mu|(\zeta)\\ &\leqq C\int (1+|f(\zeta)|)\, K_1(\zeta,\zeta)^{1/2}\, K_2(\zeta,\zeta)^{1/2}\, d|\Delta\mu|(\zeta)<\infty,\end{aligned}$$

and, using $|h_w(z)| = |h_w(w)|$,

$$(5.13)\qquad \iint |f(z)\, h_w(z)\, K_1(w,z)|\, d|\Delta\mu|(z)\, d\mu_1(w) \leqq \int |f(z)|\, \|h_z\|_{A_1}\, \|K_{1z}\|_{A_1}\, d|\Delta\mu|(z) < \infty.$$

Consequently, by (5. 10) and Fubini's theorem

$$\begin{aligned}(5.14)\qquad I^* - I(\mu_1) &= \iint \overline{f(z)}\, h_w(z)\,(K_2(w,z)-K_1(w,z))\, d\mu_1(w)\, d\mu_2(z)\\ &\quad - \iint \overline{f(z)}\, h_w(z)\, K_1(w,z)\, d\mu_1(w)\, d\Delta\mu(z).\end{aligned}$$

Since $(f(z)-f(w))\,(K_2(w,z)-K_1(w,z))$ as a function of w is analytic, is 0 at $w=z$, and belongs to A by (5. 5) and symmetry,

$$\begin{aligned}&\int h_w(z)\,(K_2(w,z)-K_1(w,z))\, d\mu_1(w)\\ &= \int (f(z)-f(w))\,(K_2(w,z)-K_1(w,z))\, K_1(z,w)\, d\mu_1(w) = 0\end{aligned}$$

by the reproducing property of K_1. Similarly $\int h_w(z)\, K_1(w,z)\, d\mu_1(w) = 0$, and (5. 14) yields $I^* = I(\mu_1)$. By symmetry also $I^* = I(\mu_2)$, which completes the proof. □

6. Passing to the limit

We will in this section complete the proof of the main theorem. The idea is to show that $I(f,\mu_1) = I(f,\mu_2)$ for two different measures by changing μ_1 to μ_2 on a compact subset of Ω, which does not affect $I(f,\mu_1)$ by Lemma 5. 3, and then let the compact subset increase to Ω, so that the measure converges to μ_2 in some (weak) sense. A minor complication is that we do not know any useful result on continuity of $I(f,\mu)$ in μ (until the theorem is proved and we know that $I(f,\mu)$ is constant). We will instead use Fatou's lemma and obtain an inequality, and then interchange the measures to obtain the reverse inequality. The main problem then turns out to be to show that the reproducing kernel $K(z,w)$ converges pointwise as the measure μ converges. We do not know the most general conditions under which this holds, but we are able to give some sufficient conditions. (We will use the equivalent condition (6. 3) below on convergence of norms of point evaluations.)

We begin with a basic lemma which will be used several times. (We assume that (1. 1) holds for all involved measures.)

Lemma 6. 1. *Suppose that* Ω, μ *and* $\{(\Omega_n, \mu_n)\}_1^\infty$ *are such that*

(6. 1) *if* $z \in \Omega$, *then* $z \in \Omega_n$ *for all sufficiently large* n,

(6. 2) $$\varliminf_{n\to\infty} \frac{d\mu_n}{d\mu} \geqq 1.$$

If $z, w \in \Omega$ *and* $t \in \mathbb{C}$, *and* L_{zwt} *is the linear functional* $f \to f(z) + tf(w)$, *then*

(6. 3) $$\|L_{zwt}\|_{A_n^*} \to \|L_{zwt}\|_{A^*}.$$

Then, for every f *analytic in* $\Omega \cup \bigcup_1^\infty \Omega_n$,

(6. 4) $$I(f, \Omega, \mu) \leqq \varliminf_{n\to\infty} I(f, \mu_n, \Omega_n).$$

Proof. $L_{zwt}(f) = \langle f, K_z + tK_w\rangle$. Hence

$$\|L_{zwt}\|_{A^*}^2 = \|K_z + tK_w\|_A^2 = K(z, z) + |t|^2 K(w, w) + 2\Re(tK(z, w)).$$

Taking $t = 0$, we see that (6. 3) implies that $K_n(z, z) \to K(z, z)$ as $n \to \infty$ and then $t = 1$ and $t = i$ yield $K_n(z, w) \to K(z, w)$ as $n \to \infty$, for all $z, w \in \Omega$. Fatou's inequality now yields, since $d\mu_n/d\mu = 0$ outside Ω_n,

$$\begin{aligned}
&\varliminf_{n\to\infty} I(f, \mu_n, \Omega_n) \\
&\geqq \varliminf_{n\to\infty} \int_\Omega \int_\Omega |f(z) - f(w)|^2 |K_n(z, w)|^2 \frac{d\mu_n}{d\mu}(z) \frac{d\mu_n}{d\mu}(w)\, d\mu(z)\, d\mu(w) \\
&\geqq \int_\Omega \int_\Omega \varliminf_{n\to\infty} \left(|f(z) - f(w)|^2 |K_n(z, w)|^2 \frac{d\mu_n}{d\mu}(z) \frac{d\mu_n}{d\mu}(w)\right) d\mu(z)\, d\mu(w) \\
&\geqq I(f, \mu, \Omega). \qquad \square
\end{aligned}$$

Lemma 6. 2. *Suppose that* (Ω, μ) *and* $\{(\Omega_n, \mu_n)\}_1^\infty$ *are such that*

(6. 5) $$\Omega_1 \supset \Omega_2 \supset \ldots \supset \Omega,$$

(6. 6) $$\mu_1 \geqq \mu_2 \geqq \ldots \geqq \mu,$$

(6. 7) $$\frac{d\mu_n}{d\mu_1} \to \frac{d\mu}{d\mu_1} \text{ on } \Omega_1,$$

(6. 8) $\bigcup A_n$ *is dense in* A.

Then, for any $f \in \mathscr{H}(\Omega_1)$,

$$I(f, \mu, \Omega) \leqq \varliminf_{n\to\infty} I(f, \mu_n, \Omega_n). \tag{6.9}$$

Proof. We use Lemma 6.1. Since (6.1) and (6.2) obviously hold, it remains to verify (6.3).

If $L \in A^*$, then $\|L\|_{A_n^*} \leqq \|L\|_{A^*}$ because $\| \ \|_A \leqq \| \ \|_{A_n}$. On the other hand, if $f \in A_m$ for some m and $\|f\|_A \leqq 1$, then $f \in A_n$ for $n \geqq m$ and $\|f\|_{A_n} \to \|f\|_A = 1$ by (6.7) and dominated convergence. Consequently

$$|L(f)| \leqq \varliminf_{n\to\infty} (\|L\|_{A_n^*} \|f\|_{An}) = \varliminf_{n\to\infty} \|L\|_{A_n^*}.$$

By (6.8) this implies that $\|L\|_{A^*} \leqq \varliminf_{n\to\infty} \|L\|_{A_n^*}$. Hence $\|L\|_{A_n^*} \to \|L\|_{A^*}$ for any $L \in A^*$; in particular (6.3) holds. □

We can now prove half of the main result under condition (i) in Theorem 1.1.

Lemma 6.3. *Suppose that every polynomial belongs to* $A(\mu)$. *Then, for any* $f \in \mathscr{H}(\Omega)$,

$$I(f, \mu, \Omega) \geqq D(f, \Omega). \tag{6.10}$$

Proof. Let Ω' be a finite union of open discs with closures that are disjoint and contained in Ω. (Remember that we never have assumed our sets to be connected.) Let $\mu' = m$ on Ω' and define

$$\mu_n = \mu' + \frac{1}{n}\mu \quad \text{on} \quad \Omega_n = \Omega.$$

Lemma 6.2 applies to (Ω', μ') and $\{(\Omega_n, \mu_n)\}$; we verify (6.8) by observing that the polynomials belong to $A(\mu_1)$ and are dense in $A(\mu')$ (as a consequence of Runge's theorem). By Lemma 4.2, $I(f, \mu', \Omega') = D(f, \Omega')$. Furthermore, $n\mu_n - \mu = n\mu'$ has compact support in Ω, whence Lemmas 2.1 (i) and 5.3 yield

$$I(f, \mu_n) = I(f, n\mu_n) = I(f, \mu).$$

Consequently,

$$\frac{1}{\pi}\int_{\Omega'} |f'|^2 \, dm = I(f, \mu', \Omega') \leqq \varliminf_{n\to\infty} I(f, \mu_n, \Omega) = I(f, \mu, \Omega).$$

Finally we take a suitable increasing sequence of such sets Ω', and obtain (6.10) by monotone convergence. □

We next prove the opposite inequality for measures that satisfy a slightly stronger version of (1. 1).

Lemma 6. 4. *Suppose that μ is a Radon measure on Ω and satisfies the following strengthening of* (1. 1): *for every compact $F \subset \Omega$ there is a compact set $F_1 \supset F$ and a constant $C < \infty$ such that*

$$\sup_{z \in F} |f(z)| \leqq C \Big(\int_{F_1} |f|^2 \, d\mu \Big)^{1/2} \tag{6. 11}$$

for every f analytic in a neighbourhood of F_1.

Then, for any $f \in \mathscr{H}(\Omega)$,

$$I(f, \mu, \Omega) \leqq D(f, \Omega). \tag{6. 12}$$

Proof. Define an increasing sequence of open subsets of Ω by

$$\Omega_n = \{z \in \Omega : d(z, \Omega^c) > 1/n \text{ and } |z| < n\}.$$

Note that the complement of Ω_n has a finite number of components and that none of them consists of one point only (there is exactly one unbounded component, and every bounded component is a union of closed discs of radius $1/n$ and has therefore area $\geqq \pi/n^2$).

Hence every component of Ω_n is conformally equivalent to a finitely connected domain with analytic boundary, and Lemmas 4. 2, 2. 1 and 2. 2 yield

$$I(f, \Omega_n, m) = D(f, \Omega_n). \tag{6. 14}$$

By (1. 1), there exists constants C_n such that

$$\sup \{|f(z)| : z \in \overline{\Omega_n}\} \leqq C_n \|f\|_A \quad \text{for all} \quad f \in A. \tag{6. 15}$$

We choose positive numbers ε_n such that

$$\varepsilon_n m(\Omega_n) C_n^2 \leqq \frac{1}{n}, \tag{6. 16}$$

and define

$$\mu_n = \begin{cases} \mu & \text{on} \quad \Omega_{n-1}, \\ \varepsilon_n m & \text{on} \quad \Omega_n / \Omega_{n-1}. \end{cases} \tag{6. 17}$$

By Lemmas 5. 3 and 2. 1, and (6. 14),

$$I(f, \mu_n, \Omega_n) = I(f, \varepsilon_n m, \Omega_n) = I(f, m, \Omega_n) = D(f, \Omega_n). \tag{6. 18}$$

The result thus follows by Lemma 6. 1, provided (6. 3) holds. We verify it as follows. If $f \in A$, then, by (6. 15) and (6. 16),

$$\|f\|_{A_n}^2 \leqq \int_{\Omega_{n-1}} |f|^2 \, d\mu + \varepsilon_n m(\Omega_n/\Omega_{n-1}) \, C_n^2 \|f\|_A^2 \leqq \left(1+\frac{1}{n}\right) \|f\|_A^2. \tag{6. 19}$$

Consequently,

$$\|L_{zwt}\|_{A^*} \leqq (1+1/n) \, \|L_{zwt}\|_{A_n^*}. \tag{6. 20}$$

Conversely, let $f_n \in A_n$ be such that $L_{zwt}(f_n) = \|L_{zwt}\|_{A_n^*}$ and $\|f_n\|_{A_n} = 1$. If F is any compact subset of Ω, then, by assumption, for some C, $N < \infty$ and all $n > N$,

$$\sup_F |f_n(z)| \leqq C \Big(\int_{\Omega_N} |f_n|^2 \, d\mu \Big)^{1/2} \leqq C \, \|f_n\|_{A_n} = C.$$

Thus $\{f_n\}$ is a normal family in a generalized sense (each f_n is defined only on a subset of Ω), and it is easily seen, using the diagonal method, that there exists a subsequence $\{f_{n_k}\}$ of $\{f_n\}$ which converges uniformly on compact subsets of Ω to some $f \in \mathscr{H}(\Omega)$. We may furthermore assume that $\|L_{zwt}\|_{A_{n_k}^*} \to \overline{\lim_{n\to\infty}} \, \|L_{zwt}\|_{A_n^*}$. Since $\int_{\Omega_m} |f_n|^2 \, d\mu \leqq 1$ when $m < n$, $\int_{\Omega_m} |f|^2 \, d\mu \leqq 1$ for all m and thus $f \in A(\Omega)$ with $\|f\|_A \leqq 1$.

It follows that

$$\|L_{zwt}\|_A \geqq |L_{zwt}(f)| = \lim L_{zwt}(f_{n_k}) = \lim \|L_{zwt}\|_{A_{n_k}^*} = \overline{\lim_{n\to\infty}} \, \|L_{zwt}\|_{A_n^*}.$$

Together with (6. 20) this proves (6. 3), and Lemma 6. 1 now yields, for any $f \in \mathscr{H}(\Omega)$,

$$I(f, \mu, \Omega) \leqq \underline{\lim_{n\to\infty}} \, I(f, \mu_n, \Omega_n) = \underline{\lim_{n\to\infty}} \, D(f, \Omega_n) = D(f, \Omega). \qquad \square$$

Remark 6. 1. We do not know whether every measure that satisfies (1. 1) also satisfies (6. 11). We evade this problem by taking an additional limit.

Lemma 6. 5. *If μ is a Radon measure on Ω that satisfies* (1. 1), *then, for any $f \in \mathscr{H}(\Omega)$,*

$$I(f, \mu, \Omega) \leqq D(f, \Omega).$$

Proof. It is easy to construct a strictly positive continuous function φ on Ω such that $\int_\Omega |f|^2 \varphi \, dm \leqq \int_\Omega |f|^2 \, d\mu$ for all $f \in A$ (e.g. let φ be such that $\sup_{\Omega_n/\Omega_{n-1}} |\varphi| \, m(\Omega_n) C_n^2 < 2^{-n}$, with Ω_n and C_n as in the proof of Lemma 6. 4).

Define $\mu_n = \mu + \frac{1}{n}\varphi\, dm$ on Ω. Then Lemma 6.4 applies to (Ω, μ_n), and Lemma 6.2 yields, because $A_n = A$ as sets,

$$I(f, \mu, \Omega) \leqq \varliminf_{n\to\infty} I(f, \mu_n, \Omega) \leqq D(f, \Omega). \qquad \square$$

We are now able to complete the proof of Theorem 1.1, and thus also Theorems 1.2 and 1.3. If condition (i) holds, i.e. $\{z^n\}_0^\infty \subset A(\mu)$, then $I(f, \Omega, \mu) = D(f, \Omega)$ by Lemmas 6.3 and 6.5. In particular, the conclusion holds if Ω is bounded and μ is finite. The cases (ii) and (iii) now follow by Lemma 2.1 (ii) and (iii), since every such Ω is conformally equivalent to a bounded domain.

7. Some open problems

The conditions on Ω and μ in the theorems are not very restrictive but somewhat annoying, and it would be nice to relax them further.

Problem 7.1. *Do Theorems* 1.1—1.3 *hold for every planar domain* Ω *and measure* μ *with* $A(\mu) \neq \{0\}$?

Of greater importance is the possibility to let Ω be a general Riemann surface with a measure μ satisfying (1.1). We may then define A as the space of square integrable analytic functions as before, but it is just as natural to let A consist of analytic functions with values in a given Hermitean line bundle over Ω, e.g. A could be the space of square integrable differential forms. (Of course, we may consider non-trivial line bundles also for planar domains.) We still let f be an analytic function, and observe that the Dirichlet integral $D(f)$ has an invariant meaning.

Problem 7.2. *Prove an extension of Theorems* 1.1—1.3 *for Riemann surfaces*!

Note that there is no obvious generalization of the results to higher dimensions. In fact, even in simple cases such as the unit ball or the polydisc in C^N $(N \geqq 2)$ with Lebesgue measure, there are no non-trivial Hilbert-Schmidt Hankel operators with analytic symbols, and the integral $I(f)$ diverges for every non-constant analytic f, see e.g. [Z].

We have so far assumed that μ is a measure on Ω. What if it is supported on the boundary $\partial\Omega$? (Formally, this case arises as a limit.)

In Remark 1.1 we mentioned the Hardy space $H^2(\mathbb{T})$. The main result then reduces to (1.10), which we rewrite as follows using polarization. Define (for reasonable f and g)

$$I(f, g) = \frac{1}{4\pi^2} \int_{\mathbb{T}} \int_{\mathbb{T}} \frac{(f(z) - f(w))\,\overline{(g(z) - g(w))}}{|z - w|^2} \, |dz|\, |dw| \tag{7.1}$$

and (Δ denotes the unit disc),

$$D(f, g) = \frac{1}{\pi} \int_{\Delta} f'(z)\, \overline{g'(z)}\, dm(z). \tag{7.2}$$

Then $I(f, g) = D(f, g)$.

If f is analytic in a neighbourhood of $\bar{\Delta}$ and g is rational with simple poles outside $\bar{\Delta}$, then, for $z \in \mathbb{T}$, $g(z) = \overline{h(z)}$, where h is rational with simple poles in Δ. Also, it is easy to show, using residue calculus and Green's theorem, that (with the summation extended over all poles of h)

$$I(f, g) = \sum_{\zeta} \operatorname{Res}(h; \zeta)\, f'(\zeta) = D(f, g). \tag{7.3}$$

The argument applies *mutatis mutandis* to the case of a "regular" multiply connected domain Ω with arc-length measure on the boundary (thus K is the Szegő kernel): we have only to invoke the Schottky double R of Ω. (Recall that R is a compact Riemann surface obtained by glueing together two copies of Ω in the obvious way, $R = \Omega \cup \Omega^* \cup \partial\Omega$; for details see e.g. [GP].) In particular, formula (7.3) is valid if we interpret the word "rational" as "rational on R" and the poles of g are imagined as sitting in the mirror image Ω^* of Ω. (If $\Omega = \Delta$ then R can be identified with the Riemann sphere, assigning to a point $a^* \in \Delta^*$ the point $a = 1/\bar{a} \in \mathbb{C} \setminus \Delta$.)

Problem 7.3. *Is there an extension of Theorem* 1.1 *that admits also other measures supported on* $\partial\Omega$*, or measures with mass on both* Ω *and* $\partial\Omega$?

References

[A] *N. Aronszajn*, Theory of reproducing kernels, Trans. Amer. Math. Soc. **68** (1950), 337—404.

[AF] *J. Arazy* and *S. Fisher*, The uniqueness of the Hilbert space among Möbius invariant Hilbert spaces, Ill. J. Math. **29** (1985), 449—462.

[AFP1] *J. Arazy*, *S. Fisher* and *J. Peetre*, Hankel operators on weighted Bergman spaces, Amer. J. Math. **110** (1988), 989—1054.

[AFP2] *J. Arazy*, *S. Fisher* and *J. Peetre*, Hankel operators on planar domains, to appear.

[Ar] *J. Arazy*, Membership of Hankel operators on planar domains in unitary ideals, Analysis in Urbana 1986-7, Proceedings of the special year in modern analysis, Cambridge, to appear.

[Ax] *S. Axler*, The Bergman space, the Bloch space, and commutators of multiplication operators, Duke Math. J. **53** (1986), 315—332.

[B] *S. Bergman*, The kernel function and conformal mapping, Math. Surveys V, Amer. Math. Soc., New York 1950.

[BS1] *C. A. Berger* and *B. I. Shaw*, Selfcommutators of multicyclic hyponormal operators are always trace class, Bull. Amer. Math. Soc. **79** (1973), 1193—1199.

[BS2] *C. A. Berger* and *B. I. Shaw*, Intertwining, analytic structure, and the trace norm estimate, Proceedings of a conference on operator theory (Halifax 1973), pp. 1—6, Lect. Notes in Math. **345**, Berlin-Heidelberg-New York 1973.

[GP] *B. Gustafsson* and *J. Peetre*, Hankel forms on multiply connected plane domains, Part Two, The case of higher connectivity, Complex Variables, to appear.

[HH] *J. W. Helton* and *R. E. Howe*, Integral operators; commutators, traces, index and homology, Proceedings of a conference on operator theory (Halifax 1973), pp. 141—209, Lect. Notes in Math. **345**, Berlin-Heidelberg-New York 1973.

[P] *V. V. Peller*, Hankel operators of the class S_p and their applications (rational approximation, Gaussian processes, the problem of majorizing operators), Mat. Sb. **113** (1980), 538—581, (Russian), English translation: Math. USSR-Sb. **41** (1982), 443—479.

[R] *R. Rochberg*, Trace ideal criteria for Hankel operators and commutators, Indiana U. Math. J. **31** (1982), 913—925.

[Z] *K. Zhu*, Hilbert-Schmidt Hankel operators on the Bergman space, Preprint.

Department of Mathematics, University of Haifa, Haifa 31999, Israel

Department of Mathematics, Northwestern University, Evanston, Illinois 60208, USA

Department of Mathematics, Uppsala University, Thunbergsvägen 3, S-75238 Uppsala, Sweden

Department of Mathematics, University of Lund, Box 118, S-22100 Lund, Sweden

Department of Mathematics, University of Stockholm, Box 6701, S-11385 Stockholm, Sweden

Eingegangen 30. August 1988, in revidierter Fassung 24. August 1989

J. reine angew. Math. **406** (1990), 200—218

Journal für die reine und angewandte Mathematik

On the Galois Theory of function fields of one variable over number fields

By *Florian Pop* at Heidelberg

Introduction and main results

For an arbitrary field K we denote by $\tilde{K}$ the algebraic closure of K and by $G_K = \mathrm{Aut}(\tilde{K}|K)$ the absolute Galois group of K endowed with the Krull topology.

The main result we prove in this paper is:

Theorem. *Let $F|\mathbb{Q}$, $E|\mathbb{Q}$ be two function fields of one variable ($\mathbb{Q}$ not necessarily the exact constant field of F or E). If G_F and G_E are isomorphic, then F and E are isomorphic.*

More precisely, for each group isomorphism $\Phi: G_F \to G_E$ there exists a field isomorphism $\phi: \tilde{E} \to \tilde{F}$ with the property:

$$\Phi(g) = \phi^{-1} g \phi, \quad g \in G_F$$

and ϕ is unique with the property above. As a consequence ϕ maps E isomorphically onto F.

As corollaries one obtains:

Theorem. *Let $F|\mathbb{Q}$ and $E|\mathbb{Q}$ be as above. Denote by* **Homloc**(G_F, G_E) *the space of all group homomorphisms from G_F to G_E which are local homeomorphisms, and by* $\mathrm{Inn}(G_E)$ *the group of all inner automorphisms of G_E. Then* $\mathrm{Inn}(G_E)$ *acts in a canonical way on* **Homloc**(G_F, G_E) *and the canonical mapping*

$$\mathbf{Hom}(E|F) \to \mathbf{Homloc}(G_F, G_E)/\mathrm{Inn}(G_E)$$

is a bijection.

Theorem. *Let Ω_1 be the algebraically closed field of characteristic* 0 *and absolute transcendence degree* 1. *Let* **Aut**(Ω_1) *denote the automorphism group of Ω_1 endowed with the weak topology. Then any continuous automorphism of* **Aut**(Ω_1) *is inner.*

Questions of this kind were first posed by Neukirch (see [25], [26]) who proved the remarkable fact that any (closed) normal subgroup of the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$ is characteristic, i.e., it remains invariant under any continuous group automorphism of $G_{\mathbb{Q}}$. Complete answers were obtained for the global fields by Iwasawa (unpublished) and Uchida, [38], [39]. See also Ikeda [12] and Komatsu [17]. We want to remark that our result here is a step in proving the conjecture that *any finitely generated field is determined by its absolute Galois group*, in this connection see also Grothendieck [9]. Further we remark that as in the case of the global fields one in fact does not need the isomorphism of the absolute Galois groups, but an isomorphism of the Galois groups of solvably closed extensions of the ground function fields. The proofs of these apparently more general assertions are essentially the same as those in the case of the isomorphism of the absolute Galois groups. One should work in this case with *relative henselisations*, as Neukirch proposed in [27].

The main new result we use in the proof is a *Galois characterisation of the constant reductions* of the function fields of one variable over number fields (see § 2).

§ 1. Definitions. Notations. Basic facts

A. Excursion into valuation theory. In this section we recall facts from valuation theory and cohomology theory of profinite groups.

Let $(K, \mathfrak{v})$ be a valued field. We denote the value group of $\mathfrak{v}$ by $\mathfrak{v}K$ and the residue field of $\mathfrak{v}$ by $K\mathfrak{v}$. Let $L|K$ be an algebraic normal extension of K and let $\mathfrak{v}_L$ be a prolongation of $\mathfrak{v}$ to L. We denote the decomposition group, the inertia group and the ramification group of $\mathfrak{v}_L|\mathfrak{v}$ by $Z(\mathfrak{v}_L|\mathfrak{v})$, $T(\mathfrak{v}_L|\mathfrak{v})$ and $V(\mathfrak{v}_L|\mathfrak{v})$ respectively and correspondingly by L^Z, L^T, L^V the decomposition field, the inertia field and the ramification field of $\mathfrak{v}_L|\mathfrak{v}$. It is well known that $T(\mathfrak{v}_L|\mathfrak{v})$ and $V(\mathfrak{v}_L|\mathfrak{v})$ are normal subgroups of $Z(\mathfrak{v}_L|\mathfrak{v})$ and that there exists a canonical exact sequence

$$1 \to T(\mathfrak{v}_L|\mathfrak{v}) \to Z(\mathfrak{v}_L|\mathfrak{v}) \xrightarrow{\pi_{\mathfrak{v}}} \mathrm{Gal}(L\mathfrak{v}_L|K\mathfrak{v}) \to 1. \tag{1. 1}$$

Furthermore one has: $V(\mathfrak{v}_L|\mathfrak{v})$ is a pro-p-group and $T(\mathfrak{v}_L|\mathfrak{v})/V(\mathfrak{v}_L|\mathfrak{v})$ is an abelian (profinite) group of order prime to $p = \mathrm{char}\, K\mathfrak{v}$.

(1. 2) Therefore one has:

1) If $\mathrm{char}\, K\mathfrak{v} = 0$ then $V(\mathfrak{v}_L|\mathfrak{v})$ is trivial and $T(\mathfrak{v}_L|\mathfrak{v})$ is an abelian (profinite) group.

2) If $\mathrm{Gal}(L\mathfrak{v}_L|K\mathfrak{v})$ is solvable then $Z(\mathfrak{v}_L|\mathfrak{v})$ is solvable. In particular: suppose that $\mathfrak{v}$ is a maximal valuation of K, i.e., $K\mathfrak{v}$ has positive characteristic and is algebraic over its prime field. Then $Z(\mathfrak{v}_L|\mathfrak{v})$ is solvable.

Let now L be separably closed, so $\mathrm{Gal}(L|K)$ is isomorphic to the absolute Galois group of K. For this situation we denote $\mathfrak{v}_L$ by $\tilde{\mathfrak{v}}$. Then:

3) The canonical projection $\pi_{\mathfrak{v}}$ has continuous sections, so $Z(\tilde{\mathfrak{v}}|\mathfrak{v})$ is isomorphic to a semi-direct product $T(\tilde{\mathfrak{v}}|\mathfrak{v}) \rtimes G_{K\mathfrak{v}}$ of $T(\tilde{\mathfrak{v}}|\mathfrak{v})$ by $G_{K\mathfrak{v}}$ (see [19]).

4) For $q \neq \operatorname{char} K\mathfrak{v}$ the structure of the q-Sylow groups of $Z(\tilde{\mathfrak{v}}|\mathfrak{v})$ is in some sense well known: they are semi-direct products of a q-Sylow group $T_q(\tilde{\mathfrak{v}}|\mathfrak{v})$ of $T(\tilde{\mathfrak{v}}|\mathfrak{v})$ by a q-Sylow group of $G_{K\mathfrak{v}}$ and can be described as follows. Let $\mathbf{T}_q = \varprojlim \mu_{q^n}$ be the q-Tate module. $G_{K\mathfrak{v}}$ acts in a natural way on each μ_{q^n}, hence on $\mathbf{T}_q$. Let ε_1 denote the dimension of $\mathfrak{v}K/q \cdot \mathfrak{v}K$. Then $T_q(\tilde{\mathfrak{v}}|\mathfrak{v})$ is isomorphic to the direct product of $\mathbf{T}_q$ by itself ε_1 times, on which $G_{K\mathfrak{v}}$ acts coordinatewise.

As a corollary one gets:

5) If $\mathfrak{v}$ is maximal, then the q-Sylow groups ($q \neq \operatorname{char} K\mathfrak{v}$) of $Z(\tilde{\mathfrak{v}}|\mathfrak{v})$ are generated by exactly $\varepsilon_0 + \varepsilon_1$ generators, where $\varepsilon_0 = 0$ if $K\mathfrak{v}$ is q-closed and 1 otherwise, and ε_1 is the dimension of $\mathfrak{v}K/q \cdot \mathfrak{v}K$.

Now we say something about the cohomological dimension of $Z(\tilde{\mathfrak{v}}|\mathfrak{v})$. For a profinite group G denote by $\operatorname{cd}_q G$ the q-cohomological dimension of G. It is well known that $\operatorname{cd}_q G$ equals the q-cohomological dimension of the q-Sylow groups of G.

(1. 3) From 4) above and [35], I, Prop. 22, one now gets for $q \neq \operatorname{char} K\mathfrak{v}$:

1) $\operatorname{cd}_q T(\tilde{\mathfrak{v}}|\mathfrak{v}) = \dim_{\mathbb{F}_q}(\mathfrak{v}K/q \cdot \mathfrak{v}K)$.

2) $\operatorname{cd}_q Z(\tilde{\mathfrak{v}}|\mathfrak{v}) = \operatorname{cd}_q T(\tilde{\mathfrak{v}}|\mathfrak{v}) + \operatorname{cd}_q G_{K\mathfrak{v}}$.

We now briefly recall facts about the so called *core* of a valuation (see [28], § 1). For two valuations $\mathfrak{w}$ and $\mathfrak{w}'$ of a field we say that $\mathfrak{w}' \leqq \mathfrak{w}$ if the valuation ring of $\mathfrak{w}'$ contains the valuation ring of $\mathfrak{w}$. For a Henselian valuation $\mathfrak{v}$ of K set

$$\mathbf{V}(\mathfrak{v}) = \{\mathfrak{v}\} \cup \{\mathfrak{v}' | \mathfrak{v}' \leqq \mathfrak{v},\ K\mathfrak{v}' \text{ separably closed}\}$$

and define the *core* of $\mathfrak{v}$ to be the valuation $\underline{\mathfrak{v}} = \inf \mathbf{V}(\mathfrak{v})$. One has:

(1. 4) Let $\mathfrak{v}$ be a non-trivial Henselian valuation of a non-separably closed field K. If $\mathfrak{v}$ has rank 1 or $K\underline{\mathfrak{v}}$ is not separably closed then $\underline{\mathfrak{v}} = \mathfrak{v}$.

(1. 5) Proposition. *Let $\mathfrak{w}$ and $\mathfrak{w}'$ be Henselian valuations of an arbitrary field. Then $\underline{\mathfrak{w}}$ and $\underline{\mathfrak{w}}'$ are comparable. As consequences one obtains*:

1) *Let $L|K$ be a Galois extension, L not separably closed, and let $\mathfrak{v}$ be a Henselian valuation on L with $\underline{\mathfrak{v}} = \mathfrak{v}$. Then K is Henselian with respect to the restriction of $\mathfrak{v}$ to K.*

2) *Let $L|K$ be a not separably closed algebraic extension of K. Suppose $\mathfrak{v}$ is a Henselian valuation of L with $\underline{\mathfrak{v}} = \mathfrak{v}$. Then L contains a unique henselisation $(K, \mathfrak{v}_K)^h$ of K with respect to the restriction $\mathfrak{v}_K$ of $\mathfrak{v}$ to K. Specially $\mathfrak{v}_K$ has a unique Henselian prolongation to L.*

B. Constant reduction theory. Let $F|K$ be a function field of one variable and denote by L the exact constant field of F. For an arbitrary valuation $\mathfrak{v}$ of F and any subfield R of F we denote by $\mathfrak{v}_R$ the restriction of $\mathfrak{v}$ to R.

We say that a valuation $\mathfrak{v}$ of F is a constant reduction of F if $F\mathfrak{v}|K\mathfrak{v}$ is also a function field of one variable (or equivalently, if $F\mathfrak{v}|L\mathfrak{v}$ is also a function field of one variable). If $f \in F$ is a non-constant function such that $f\mathfrak{v}$ is a non-constant function of $F\mathfrak{v}$, then the restriction of $\mathfrak{v}$ to $K(f)$ is exactly the functional valuation $\mathfrak{v}_{K,f}$ associated

to f, i.e., $\mathfrak{v}(\sum a_k f^k) = \inf \mathfrak{v}(a_k) = \mathfrak{v}_{K,f}(\sum a_k f^k)$ for any element $\sum a_k f^k$ of $K(f)$. Conversely, if $\mathfrak{v}_K$ is a non-trivial valuation of K and f a non-constant function of F then any prolongation of $\mathfrak{v}_{K,f}$ to F is a constant reduction of F.

Let now $\mathfrak{v}$ be a constant reduction of F. We say that a non-constant function f is regular at $\mathfrak{v}$ if $\mathfrak{v}$ prolongs $\mathfrak{v}_{K,f}$ and it holds $[F : L(f)] = [F\mathfrak{v} : L(f)\mathfrak{v}]$. From general valuation theory one gets: if f is a regular function at $\mathfrak{v}$ then $\mathfrak{v}$ is the unique prolongation of $\mathfrak{v}_{L,f}$ to F.

We say that a constant reduction $\mathfrak{v}$ of F is a good reduction of F if the following holds:

i) $L\mathfrak{v}$ is the constant field of $F\mathfrak{v}$.

ii) $\mathfrak{v}$ has a regular function f. Hence $\mathfrak{v}$ is the unique prolongation of $\mathfrak{v}_{L,f}$ to F and it holds $[F : L(f)] = [F\mathfrak{v} : L(f)\mathfrak{v}]$.

iii) The genera $\mathfrak{g}_F$ and $\mathfrak{g}_{F\mathfrak{v}}$ of F and $F\mathfrak{v}$ are the same[1]).

We now recall some fundamental results of constant reduction theory, see for instance [6], [8], [20], [23], [24], [34] and others.

(1. 6) Theorem. *Let $F|K$ be a function field of one variable with the constant field L.*

1) *For any constant reduction $\mathfrak{v}$ of F one has $\mathfrak{g}_F \geqq \mathfrak{g}_{F\mathfrak{v}}$. Suppose $\mathfrak{g}_F \geqq 1$. Then for any valuation $\mathfrak{v}_L$ of L there exists at most one prolongation $\mathfrak{v}$ of $\mathfrak{v}_L$ to F having the property $\mathfrak{g}_F = \mathfrak{g}_{F\mathfrak{v}}$. In particular there exists at most one good reduction $\mathfrak{v}$ of F which prolongs $\mathfrak{v}_L$ to F.*

2) *Suppose $F|L$ is separably generated. Then for any non-constant function f of F there exists a finite set $X_f \subset L$ having the property: if $\mathfrak{v}_L$ is a valuation of L and $\mathfrak{v}_L(X_f) \geqq 0$ then f is regular at $\mathfrak{v}_L$, i.e., $\mathfrak{v}_{L,f}$ has a unique prolongation $\mathfrak{v}$ to F and f is regular at $\mathfrak{v}$.*

Moreover, in this case $L\mathfrak{v}_L$ is the exact constant field of $F\mathfrak{v}$ and it holds $[F : L(f)] = \deg^F f = \deg^{F\mathfrak{v}} f\mathfrak{v} = [F\mathfrak{v} : L(f)\mathfrak{v}]$.

Suppose F is separably generated and conservative (that means its genus does not change by constant extensions). Then for any non-constant function f of F there exists a finite set $X_f \subset L$ having the property: if $\mathfrak{v}_L$ is a valuation of L and $\mathfrak{v}_L(X_f) \geqq 0$ then f is a good function at $\mathfrak{v}_L$, i.e., $\mathfrak{v}_{L,f}$ has a unique prolongation $\mathfrak{v}$ to F, this prolongation is a good reduction of F and f is regular at $\mathfrak{v}$.

C. Some model-theoretical considerations. Let I be an infinite set and $\mathfrak{U}$ a non-principal ultrafilter on I. We say that a family $(c^i)_i$ of real numbers is locally bounded if there exists a real constant $c > 0$ such that the set of all i with $|c^i| \leqq c$ lies in $\mathfrak{U}$. For a family $(A_i)_{i \in I}$ of models of a theory and a non-principal ultrafilter $\mathfrak{U}$ on I we say that an assertion holds locally, if the set of all i for which the assertion holds, lies in $\mathfrak{U}$.

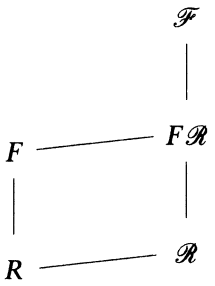
---

[1]) Here and elsewhere in this work the genus of a function field of one variable is the genus as defined in [5], namely that over the exact constant field.

Let $S|R$ be a field extension. We say that R is existentially closed in S if any existential sentence with parameters from R which holds in S does already hold in R (see for instance [3] for definitions and basic facts). One has:

R is existentially closed in S if and only if there exists an ultrapower of R, say $\mathscr{R} = R^I/\mathscr{U}$, and an R-embedding of S in $\mathscr{R}$.

In the above context let $F|R$ be a function field of one variable. Then there exists a canonical commutative diagram:



where $\mathscr{F} = F^I/\mathscr{U}$ and $F\mathscr{R}$ is the compositum of F and $\mathscr{R}$ in $\mathscr{F}$. It is well known that (compare with [28], proof of (3. 5))

$$F\mathscr{R} = \mathscr{F}_{\text{fin}} = \{(x^i)/\mathscr{U} | \deg^F x^i \text{ is locally bounded}\}.$$

Let $E|R$ be another function field of one variable. Let locally $\sigma^i : F \to E$ be R-isomorphisms. Then $\sigma = (\sigma^i)/\mathscr{U}$ defines an $\mathscr{R}$-isomorphism $F\mathscr{R} \to E\mathscr{R}$ by

$$\sigma((x^i)/\mathscr{U}) = (\sigma^i(x^i))/\mathscr{U}.$$

Conversely, if $\sigma : F\mathscr{R} \to E\mathscr{R}$ is an $\mathscr{R}$-isomorphism then locally there exist R-isomorphisms $\sigma^i : F \to E$ such that $\sigma = (\sigma^i)/\mathscr{U}$. Therefore one has

$$\text{Isom}_{\mathscr{R}}(F\mathscr{R}|E\mathscr{R}) = (\text{Isom}_R(F, E))^I/\mathscr{U}.$$

As a corollary one gets: Let $S|R$ be a field extension with R existentially closed in S. Then any R-embedding $S \hookrightarrow \mathscr{R}$ of S in an ultrapower of R defines in a canonical way an embedding

$$\text{Isom}_S(FS|ES) \hookrightarrow (\text{Isom}_R(F, E))^I/\mathscr{U}.$$

Suppose now that $\text{Isom}_R(F, E)$ is finite. Then $(\text{Isom}_R(F, E))^I/\mathscr{U}$ is also finite and has the same cardinality as $\text{Isom}_R(F, E)$, hence the canonical embeddings

$$\text{Isom}_R(F, E) \hookrightarrow \text{Isom}_S(FS|ES) \hookrightarrow (\text{Isom}_R(F, E))^I/\mathscr{U}$$

are all isomorphisms. This applies for instance when the conservative genus $\tilde{\mathfrak{g}}_F$ of F is at least 2, because in this case there exist bounds for the cardinality $|\mathrm{Isom}_R(F, E)|$ which depend only on $\tilde{\mathfrak{g}}_F$ and the degree $[R' : R]$ of the constant field R' of F over R. Actually there exist bounds for the cardinality of $\mathrm{Aut}(F|R')$ depending only on $\tilde{\mathfrak{g}}_F$, see [36], Einleitung. Further, the order of $\mathrm{Aut}(F|R)$ is bounded by $[R' : R] \cdot |\mathrm{Aut}(F|R)|$. One now gets our assertion from the following: If $\mathrm{Isom}_R(F, E)$ is non-empty then $\mathrm{Isom}_R(F, E)$ and $\mathrm{Aut}(F|R)$ have the same cardinality. Thus we have

(1. 7) Corollary. *Let $F|R$ and $E|R$ be function fields of one variable. Suppose that the conservative genus $\tilde{\mathfrak{g}}_F$ of F is at least 2. If $S|R$ is such a field extension that R is existentially closed in S, then the canonical embedding*

$$\mathrm{Isom}_R(F, E) \hookrightarrow \mathrm{Isom}_S(FS|ES)$$

is an isomorphism.

We now give a typical example of field extensions $S|R$ with R existentially closed in S.

Let K be a number field and denote by $\mathbb{P}(K)$ the space of all finite places $\mathfrak{v}_K$ of K. For any non-principal ultrafilter $\mathcal{U}$ on $\mathbb{P}(K)$ let us denote

$$K^* = \left(\prod_{\mathfrak{v}_K} K\mathfrak{v}_K\right)/\mathcal{U}.$$

There exists a canonical embedding

$$K \hookrightarrow K^*, \quad a \mapsto (a_{\mathfrak{v}_K})/\mathcal{U}$$

where $a_{\mathfrak{v}_K} = a\mathfrak{v}_K$ if $\mathfrak{v}_K(a) \geqq 0$ and 0 else.

Ax [2] showed that for any $\sigma \in G_K$ there exist non-principal ultrafilters $\mathcal{U}$ on $\mathbb{P}(K)$ such that $K^{\mathcal{U}} = K^* \cap \tilde{K}$ is the fixed field $\tilde{K}^\sigma$ of σ in $\tilde{K}$.

Further, Jarden [14] showed that "*at random*" the field extension $K^*|K^{\mathcal{U}}$ is elementary.

Combining these two results one has:

(1. 8) Theorem. *Let K be a number field.*

1) *For any $\sigma \in G_K$ there exist non-principal ultrafilters $\mathcal{U}$ on $\mathbb{P}(K)$ such that $K^{\mathcal{U}} = K^* \cap \tilde{K}$ is the fixed field $\tilde{K}^\sigma$ of σ in $\tilde{K}$.*

2) *For almost all $\sigma \in G_K$ (in the sense of Haar measure) and any non-principal ultrafilter $\mathcal{U}$ on $\mathbb{P}(K)$ having $K^{\mathcal{U}} = \tilde{K}^\sigma$ the following holds: $K^*|K^{\mathcal{U}}$ is an elementary extension of fields. Specially, in this context $K^{\mathcal{U}}$ is existentially closed in K^*.*

§ 2. Galois characterisation of the constant p-reduction

Let p be a rational prime number. We say that a constant reduction $\mathbf{v}$ of a function field of one variable $F|K$ is a constant p-reduction if $\operatorname{char} F\mathbf{v} = p$. The main result we prove in this paragraph is the following

(2. 1) Theorem. *Let $F|\mathcal{Q}$, $E|\mathcal{Q}$ be two function fields of one variable ($\mathcal{Q}$ not necessarily the exact constant field of F or E). Let $\mathbf{v}$ be a constant p-reduction of $F|\mathcal{Q}$ and $\tilde{\mathbf{v}}$ an extension of $\mathbf{v}$ to $\tilde{F}$ and let $\iota: Z(\tilde{\mathbf{v}}|\mathbf{v}) \to G_E$ be a monomorphism. Then there exists a unique non-trivial valuation $\mathbf{w}$ of E and a unique prolongation $\tilde{\mathbf{w}}$ of $\mathbf{w}$ to $\tilde{E}$ such that $\iota(Z(\tilde{\mathbf{v}}|\mathbf{v})) \subseteq Z(\tilde{\mathbf{w}}|\mathbf{w})$. Moreover, $\mathbf{w}$ is a constant p-reduction of $E|\mathcal{Q}$ and ι carries $T(\tilde{\mathbf{v}}|\mathbf{v})$ into $T(\tilde{\mathbf{w}}|\mathbf{w})$.*

Proof. The residue field $F\mathbf{v}$ of $\mathbf{v}$ is a function field of one variable over $\mathbb{F}_p$, thus $F\mathbf{v}$ is a global field of characteristic p. Identify the decomposition group $Z(\tilde{\mathbf{v}}|\mathbf{v})$ of $\tilde{\mathbf{v}}|\mathbf{v}$ in G_F with $T(\tilde{\mathbf{v}}|\mathbf{v}) \rtimes G_{F\mathbf{v}}$. Let $\mathbf{v}_0$ be an arbitrary non-trivial valuation of $F\mathbf{v}$ and let $\tilde{\mathbf{v}}_0$ denote an arbitrary prolongation of $\mathbf{v}_0$ to the algebraic closure $\widetilde{F\mathbf{v}}$ of $F\mathbf{v}$. Denote by $\tilde{\mathbf{v}}_1$ the composition of $\tilde{\mathbf{v}}$ by $\tilde{\mathbf{v}}_0$ and by $\mathbf{v}_1$ the composition of $\mathbf{v}$ by $\mathbf{v}_0$. From general valuation theory one gets: $\tilde{\mathbf{v}}_1$ is a prolongation of $\mathbf{v}_1$ to $\tilde{F}$ and the decomposition group $Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1)$ of $\tilde{\mathbf{v}}_1|\mathbf{v}_1$ is exactly $T(\tilde{\mathbf{v}}|\mathbf{v}) \rtimes Z(\tilde{\mathbf{v}}_0|\mathbf{v}_0)$ (which is a closed subgroup of the decomposition group $Z(\tilde{\mathbf{v}}|\mathbf{v})$ of $\tilde{\mathbf{v}}|\mathbf{v}$). One has $\mathbf{v}_1 F = \mathbb{Z} \times \mathbb{Z}$ and $F\mathbf{v}_1$ is a finite field of characteristic p. By (1. 2) and (1. 3) one obtains:

— $Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1)$ is solvable,

— $\operatorname{cd}_q Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1) = 3$ and the q-Sylow groups of $Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1)$ are generated by exactly 3 generators for any rational prime number $q \neq p$.

Let F_1^{abs} be the absolute subfield of the fixed field F_1 of $Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1)$ in $\tilde{F}$ and let $\mathbf{v}_1^{\mathrm{abs}}$ denote the restriction of $\tilde{\mathbf{v}}_1$ to F_1^{abs}. From the above we get:

— $F_1^{\mathrm{abs}}\mathbf{v}_1^{\mathrm{abs}}$ is finite and has characteristic p,

— $\mathbf{v}_1^{\mathrm{abs}}$ is discrete and has rank 1,

— $(F_1^{\mathrm{abs}}, \mathbf{v}_1^{\mathrm{abs}})$ is Henselian.

By [29] it follows that $(F_1^{\mathrm{abs}}, \mathbf{v}_1^{\mathrm{abs}})$ is p-adically closed.

Let E_1 denote the fixed field of $\iota(Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1))$ in $\tilde{E}$. We show that E_1 is Henselian with respect to a maximal valuation $\mathbf{w}_1$. It is clear that $E_1|E_1^{\mathrm{abs}}$ has transcendence degree 1, hence $\operatorname{cd}_q E_1 \leqq 1 + \operatorname{cd}_q E_1^{\mathrm{abs}}$ for any rational prime number q (see for instance [35], II, Prop. 11, combined with I, Prop. 14). On the other hand $\operatorname{cd}_q E_1 = 3$ for any rational prime number $q \neq p$ and so $\operatorname{cd}_q E_1^{\mathrm{abs}} \geqq 2$ for all rational prime numbers $q \neq p$. Applying Satz II from [25] one gets: E_1^{abs} is an algebraic extension of some $\mathcal{Q}_l^{\mathrm{abs}}$ for some rational number l. We remark that $l = p$: for suppose $l \neq p$ and recall that from the above $\operatorname{cd}_l E_1^{\mathrm{abs}} = 2$. Therefore the l-Sylow groups of $G_{E_1^{\mathrm{abs}}}$ are not finitely generated, hence the l-Sylow groups of $G_{E_1} = \iota(Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1))$ are not finitely generated. Hence the l-Sylow groups of $Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1)$ are not finitely generated, and this is a contradiction, because the q-Sylow groups of $Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1)$ are generated by exactly 3 generators for any rational prime number $q \neq p$. So we have the following situation: $E_1|\mathcal{Q}_p^{\mathrm{abs}}$ has transcendence degree 1, $\operatorname{cd}_q E_1 > 1$ for any rational prime number $q \neq p$ and $G_{E_1} \cong Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1)$ is solvable, because $\mathbf{v}_1$ is a maximal valuation. From [28], § 4, (4. 6), it follows that there exists a Henselian valuation $\mathbf{w}_1$ of E_1, which prolongs the p-adic valuation of E_1^{abs}.

We can suppose that w_1 is maximal: if it is not the case, then $E_1\mathbf{w}_1|\mathbb{F}_p$ has transcendence degree 1 and $\mathbf{w}_1 E_1$ has rational rank 1, because the absolute transcendence degree of E_1 is 1. If $T(\mathbf{w}_1)$ is the inertia group of $\mathbf{w}_1$ it follows from (1. 3) 1) that $\mathrm{cd}_q T(\mathbf{w}_1) \leqq 1$ for any rational prime number $q \neq p$. Considering the exact sequence

$$1 \longrightarrow T(\mathbf{w}_1) \longrightarrow G_{E_1} \longrightarrow G_{E_1\mathbf{w}_1} \longrightarrow 1$$

and using $\mathrm{cd}_q E_1 = 3$ it follows (see [35], I, Prop. 15) that $\mathrm{cd}_q E_1\mathbf{w}_1 \geqq 2$ for any $q \neq p$. On the other hand $G_{E_1\mathbf{w}_1}$ is solvable as a quotient of the solvable group G_{E_1}. By [25] one gets: $E_1\mathbf{w}_1$ is Henselian with respect to a non-trivial valuation $\mathbf{w}_0$. Obviously $(E_1\mathbf{w}_1)\mathbf{w}_0$ is algebraic over $\mathbb{F}_p$ and E_1 is Henselian with respect to the composition $\mathbf{w}_1 \circ \mathbf{w}_0$ of $\mathbf{w}_1$ by $\mathbf{w}_0$. Now replace $\mathbf{w}_1$ by $\mathbf{w}_1 \circ \mathbf{w}_0$.

Let us denote by E' the fixed field of $\iota(Z(\tilde{\mathbf{v}}|\mathbf{v}))$ and by E'' the fixed field of $\iota(T(\tilde{\mathbf{v}}|\mathbf{v}))$ in $\tilde{E}$. It is clear that $E''|E'$ is a Galois extension. Denote by $\mathbf{w}''$ the core of the unique extension of $\mathbf{w}_1$ to E'' and let $\mathbf{w}'$ be the restriction of $\mathbf{w}''$ to E'. From (1. 5) one gets: $(E', \mathbf{w}')$ is Henselian.

$$\begin{array}{lcll}
F'' = \tilde{F}^{T(\tilde{\mathbf{v}}|\mathbf{v})} & T(\tilde{\mathbf{v}}|\mathbf{v}) & \xrightarrow{\iota} \iota(T(\tilde{\mathbf{v}}|\mathbf{v})) & \tilde{E}^{\iota(T(\tilde{\mathbf{v}}|\mathbf{v}))} = E''\,\mathbf{w}'' \\
\Big| & \Big| & \Big| & \Big|\;\Big| \\
F_1 = \tilde{F}^{Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1)} & Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1) & \xrightarrow{\iota} \iota(Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1)) & \tilde{E}^{\iota(Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1))} = E_1\cdot \leqq \mathbf{w}_1 \\
\Big| & \Big| & \Big| & \Big|\;\Big| \\
F' = \tilde{F}^{Z(\tilde{\mathbf{v}}|\mathbf{v})} & Z(\tilde{\mathbf{v}}|\mathbf{v}) & \xrightarrow{\iota} \iota(Z(\tilde{\mathbf{v}}|\mathbf{v})) & \tilde{E}^{\iota(Z(\tilde{\mathbf{v}}|\mathbf{v}))} = E'\,\mathbf{w}' \\
\Big| & \Big| & \Big| & \Big|\;\Big| \\
F & G_F & G_E & E\;\mathbf{w}
\end{array}$$

We want now to describe more closely the valuation $\mathbf{w}'$.

1) $\mathbf{w}'$ *is strictly coarser than* $\mathbf{w}_1$, *i.e.*, $\mathbf{w}' < \mathbf{w}_1$.

Suppose that the contrary holds, so $\mathbf{w}' = \mathbf{w}_1$. Then, since $\mathbf{w}_1$ is a maximal valuation, so is $\mathbf{w}'$. Further $(E', \mathbf{w}')$ is Henselian, and $\mathbf{w}'E'$ has rational rank at most 2. So by (1. 2) 5) the q-Sylow groups of $G_{E'}$ are generated by at most 3 generators ($q \neq p$). Now this is a contradiction, because $G_{E'}$ is isomorphic to $Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1) = T(\tilde{\mathbf{v}}_1|\mathbf{v}_1) \rtimes G_{F_\mathbf{v}}$ and the q-Sylow groups of $G_{F_\mathbf{v}}$ are not finitely generated.

2) $\iota(T(\tilde{\mathbf{v}}|\mathbf{v})) \subseteqq T(\tilde{\mathbf{w}}'|\mathbf{w}')$, *where* $\tilde{\mathbf{w}}'$ *is the unique prolongation of* $\mathbf{w}'$ *to* $\tilde{E}$.

We show first that $\iota(T(\tilde{\mathbf{v}}|\mathbf{v}))$ is contained in $T(\tilde{\mathbf{w}}''|\mathbf{w}'')$. Suppose it is not the case. Then $E''\mathbf{w}''$ is not separably closed. By (1. 4) it follows that $\mathbf{w}'' = \mathbf{w}_1$ and now this contradicts 1). Therefore $\iota(T(\tilde{\mathbf{v}}|\mathbf{v})) \subseteqq T(\tilde{\mathbf{w}}''|\mathbf{w}'')$, and now the assertion 2) is clear, since $T(\tilde{\mathbf{w}}''|\mathbf{w}'') \subseteqq T(\tilde{\mathbf{w}}'|\mathbf{w}')$.

3) $\mathrm{char}\, E'\mathbf{w}' = p$.

We first show that $\operatorname{char} E'\mathbf{w}' > 0$. Assume $\operatorname{char} E'\mathbf{w}' = 0$. Then $T(\tilde{\mathbf{w}}'|\mathbf{w}')$ is abelian by (1. 2) 1). By 2) it follows that $T(\tilde{\mathbf{v}}|\mathbf{v})$ is abelian, because $\iota(T(\tilde{\mathbf{v}}|\mathbf{v})) \subseteq T(\tilde{\mathbf{w}}'|\mathbf{w}')$ and ι is an isomorphism. On the other hand $T(\tilde{\mathbf{v}}|\mathbf{v})$ has as quotient the inertia group of the p-adically closed field F_1^{abs} — the absolute subfield of the fixed field of $Z(\tilde{\mathbf{v}}_1|\mathbf{v}_1)$ in $\tilde{F}$ — and this inertia group is not abelian, because it contains the ramification group of $\widetilde{F_1^{\text{abs}}}|F_1^{\text{abs}}$ which is a free not finitely generated pro-p-group. Therefore $\operatorname{char} E'\mathbf{w} > 0$, and to show that $\operatorname{char} E'\mathbf{w}' = p$ it is enough to remark the following: $\mathbf{w}' \leqq \mathbf{w}_1$, so the same holds for their restrictions to $\mathbb{Q}$, $\mathbf{w}'$ is not trivial on $\mathbb{Q}$ and the restriction of $\mathbf{w}_1$ is the p-adic valuation.

4) $E'\mathbf{w}'|\mathbb{F}_p$ *has transcendence degree* 1.

Assuming the contrary, i.e., $E'\mathbf{w}'|\mathbb{F}_p$ is algebraic, it follows that $\mathbf{w}'$ is a maximal valuation. Thus $\mathbf{w}' = \mathbf{w}_1$ and this contradicts 1).

5) $\underline{\mathbf{w}}' = \mathbf{w}'$.

By 4) above $\mathbf{w}'$ has rank 1. Further $(E', \mathbf{w}')$ is Henselian and not separably closed. Now apply (1. 4).

Let now $\mathbf{w}$ be the restriction of $\mathbf{w}'$ to E. It is clear from 4) above that $\mathbf{w}$ is a constant p-reduction of E, so we have also $\mathbf{w} = \underline{\mathbf{w}}$. By (1. 5) 2) it follows that there exists a unique Henselian prolongation of $\mathbf{w}$ to the henselisation $E_{\mathbf{w}}^h$ of $(E, \mathbf{w})$ in E'. Denote also by $\mathbf{w}$ this unique Henselian prolongation of $\mathbf{w}$ to $E_{\mathbf{w}}^h$ and by $\tilde{\mathbf{w}}$ the unique prolongation of the latter $\mathbf{w}$ to $\tilde{E}$. It is clear that the restrictions of $\tilde{\mathbf{w}}$ to E', E'' are respectively $\mathbf{w}'$ and $\mathbf{w}''$. From 1)—4) it follows now that $\tilde{\mathbf{w}}|\mathbf{w}$ has the properties one asks for in (2. 1).

We now show that $\tilde{\mathbf{w}}|\mathbf{w}$ is the only non-trivial valuation of $\tilde{E}|E$ with

$$\iota(Z(\tilde{\mathbf{v}}|\mathbf{v})) \subseteq Z(\tilde{\mathbf{w}}|\mathbf{w}).$$

Let $\tilde{\mathbf{w}}_0|\mathbf{w}_0$ be any valuation of $\tilde{E}|E$ with $\iota(Z(\tilde{\mathbf{v}}|\mathbf{v})) \subseteq Z(\tilde{\mathbf{w}}_0|\mathbf{w}_0)$. Denote by E_0 the fixed field of $Z(\tilde{\mathbf{w}}_0|\mathbf{w}_0)$ in $\tilde{E}$. Then $E_0 \subseteq E'$, so E' is Henselian with respect to the restriction $\mathbf{w}_0'$ of $\tilde{\mathbf{w}}_0$ to E'. From the structure of the Sylow groups of $G_{L'}$ it follows that $\mathbf{w}_0'$ is not maximal (see the proof of 1) above). On the other hand E has absolute transcendence degree 1, so $\mathbf{w}_0'$ has rank 1. By (1. 4) we get now $\mathbf{w}' = \mathbf{w}_0'$, hence $\tilde{\mathbf{w}} = \tilde{\mathbf{w}}' = \tilde{\mathbf{w}}_0'$, and consequently $\mathbf{w} = \mathbf{w}_0$. □

(2. 2) Corollary. *Under the hypothesis of* (2. 1) *suppose that* $\iota(Z(\tilde{\mathbf{v}}|\mathbf{v}))$ *is maximal in the family of all subgroups of* G_E *which are isomorphic to decomposition groups of constant reductions of* E. *Then* $\iota(Z(\tilde{\mathbf{v}}|\mathbf{v}))$ *is the decomposition group of the unique reduction* $\tilde{\mathbf{w}}|\mathbf{w}$ *given by* (2. 1) *and further* $\iota(T(\tilde{\mathbf{v}}|\mathbf{v})) = T(\tilde{\mathbf{w}}|\mathbf{w})$.

Proof. Apply (2. 1) to ι and once again to $\iota^{-1}: Z(\tilde{\mathbf{w}}|\mathbf{w}) \to Z(\tilde{\mathbf{v}}|\mathbf{v})$. □

(2. 3) Corollary. *Under the hypothesis of* (2. 1) *let* $\Phi: G_F \to G_E$ *be an isomorphism. Then* Φ *maps the decomposition group of any constant p-reduction* $\tilde{\mathbf{v}}|\mathbf{v}$ *of* F *onto the decomposition group of a unique constant p-reduction* $\tilde{\mathbf{w}}|\mathbf{w}$ *of* E *for all prime numbers* p. *Further it holds* $\Phi(T(\tilde{\mathbf{v}}|\mathbf{v})) = T(\tilde{\mathbf{w}}|\mathbf{w})$.

Proof. Let $\tilde{\mathbf{v}}|\mathbf{v}$ be a constant p-reduction of F. By (2. 1) there exists a unique constant p-reduction $\tilde{\mathbf{w}}|\mathbf{w}$ of E such that $\Phi(Z(\tilde{\mathbf{v}}|\mathbf{v}))$ is contained in $Z(\tilde{\mathbf{w}}|\mathbf{w})$. Applying now (2. 1) to Φ^{-1} one gets: there exists a unique constant p-reduction $\tilde{\mathbf{v}}'|\mathbf{v}'$ of F such that $\Phi^{-1}(Z(\tilde{\mathbf{w}}|\mathbf{w}))$ is contained in $Z(\tilde{\mathbf{v}}'|\mathbf{v}')$. It follows that $\tilde{\mathbf{v}}|\mathbf{v}$ and $\tilde{\mathbf{v}}'|\mathbf{v}'$ are two constant p-reductions of F with $Z(\tilde{\mathbf{v}}|\mathbf{v}) \subseteqq Z(\tilde{\mathbf{v}}'|\mathbf{v}')$. Therefore $\tilde{\mathbf{v}} = \tilde{\mathbf{v}}'$, so $\Phi(Z(\tilde{\mathbf{v}}|\mathbf{v})) = Z(\tilde{\mathbf{w}}|\mathbf{w})$. Further apply (2. 2). □

§ 3. The proof of the main result

Let $F|\mathcal{Q}$, $E|\mathcal{Q}$ be function fields of one variable ($\mathcal{Q}$ not necessarily the exact constant field of F or E) and let $\Phi: G_F \to G_E$ be an isomorphism. By (2. 3) the isomorphism Φ defines a bijection

$$\tilde{\varphi}: \tilde{\mathbf{v}}|\mathbf{v} \mapsto \tilde{\mathbf{w}}|\mathbf{w}$$

between the family of all constant reductions of F and that of E. Moreover, for any $\tilde{\mathbf{v}}|\mathbf{v}$ it holds $\Phi(Z(\tilde{\mathbf{v}}|\mathbf{v})) = Z(\tilde{\mathbf{w}}|\mathbf{w})$ and $\Phi(T(\tilde{\mathbf{v}}|\mathbf{v})) = T(\tilde{\mathbf{w}}|\mathbf{w})$, hence by (1. 1) it follows that Φ induces an isomorphism

$$\Phi_{\tilde{\mathbf{v}}}: G_{F\mathbf{v}} \longrightarrow G_{E\mathbf{w}}.$$

Hence by Uchida's theorem [38] there exists a (unique) isomorphism

$$\phi_{\tilde{\mathbf{v}}}: \tilde{E}^{T}\tilde{\mathbf{w}} \longrightarrow \tilde{F}^{T}\tilde{\mathbf{v}} \tag{3. 1}$$

such that $\pi_{\tilde{\mathbf{w}}}\Phi(g) = \phi_{\tilde{\mathbf{v}}}^{-1}\pi_{\tilde{\mathbf{v}}}(g)\phi_{\tilde{\mathbf{v}}}$, $g \in Z(\tilde{\mathbf{v}}|\mathbf{v})$. As a consequence, the restriction of $\phi_{\tilde{\mathbf{v}}}$ to $F\mathbf{v}$ defines an isomorphism

$$\phi_{\mathbf{v}}: F\mathbf{v} \longrightarrow E\mathbf{w}. \tag{3. 2}$$

The above isomorphisms $\phi_{\tilde{\mathbf{v}}}$ can be viewed as "*local components*" of the isomorphism ϕ we are looking for. We shall now develop a method of "*interpolating*" these local isomorphisms.

The first step in doing this is to show that our map $\tilde{\varphi}$ has good geometric properties. We begin with some preparations.

Conventions and remarks. I. For any sub-extension $F'|F$ of $\tilde{F}$ denote by $E'|E$ the corresponding subfield of $\tilde{E}$ by Φ. Hence Φ defines an isomorphism

$$G_{F'} \longrightarrow G_{E'}.$$

II. Let $\mathbf{V}$ be a family of constant reductions of F.

1) Let $F'|F$ be a sub-extension of $\tilde{F}$. *The prolongation of* $\mathbf{V}$ *to* F' is by definition the set $\mathbf{V}'$ of all prolongations $\mathbf{v}'$ to F' of the valuations $\mathbf{v} \in \mathbf{V}$. In particular, $\mathbf{V}$ is the restriction of $\mathbf{V}'$ to F.

To emphasize that $\mathbf{v}'$ prolongs $\mathbf{v}$ we shall sometimes write $\mathbf{v}'|\mathbf{v}$.

By general valuation theory one has: Suppose that $F'|F$ is Galois and $\mathbf{V}$ is the restriction to F of a family $\mathbf{V}'$ of constant reductions of F'. Then $\mathbf{V}'$ is the prolongation of $\mathbf{V}$ to F' if and only if $\mathbf{V}'$ is $\mathrm{Gal}(F'|F)$-invariant. Further, two elements of $\mathbf{V}'$ have the same restriction to F if and only if they are conjugated by some $g \in \mathrm{Gal}(F'|F)$.

2) The prolongation of $\mathbf{V}$ to $\tilde{F}$ will be denoted by $\tilde{\mathbf{V}}$.

3) The image of $\tilde{\mathbf{V}}$ by $\tilde{\varphi}$ will be denoted by $\tilde{\mathbf{W}}$ and $\mathbf{W}$ denotes the restriction of $\tilde{\mathbf{W}}$ to E.

It holds: $\tilde{\mathbf{W}}$ is G_E-invariant and its restriction $\mathbf{W}'$ to E' is exactly the prolongation of $\mathbf{W}$ to E'. Furthermore, there exist unique maps

$$\varphi' : \mathbf{V}' \longrightarrow \mathbf{W}', \quad \varphi : \mathbf{V} \longrightarrow \mathbf{W}$$

making the following diagram commutative:

$$\begin{array}{ccc} \tilde{\mathbf{V}} & \xrightarrow{\tilde{\varphi}} & \tilde{\mathbf{W}} \\ \downarrow & & \downarrow \\ \mathbf{V}' & \xrightarrow{\varphi'} & \mathbf{W}' \\ \downarrow & & \downarrow \\ \mathbf{V} & \xrightarrow{\varphi} & \mathbf{W} \end{array}$$

where the vertical arrows are the canonical restriction maps.

We now want to define the so called *geometric families* of constant reductions of a function field of one variable $F|\mathbb{Q}$.

Let t be any non-constant function of F. Denote by $\mathbf{V}_t$ the set of all prolongations of the functional valuations $\mathbf{v}_{K,t}$ to F, where $\mathbf{v}_K \in \mathbb{P}(K)$ runs over the set of all finite places of the constant field K of F. A direct verification involving (1. 6) shows that for any non-constant functions t, u of F the families $\mathbf{V}_t$ and $\mathbf{V}_u$ are almost equal[2]).

Definition. We say that a family $\mathbf{V}$ of constant reductions of F is *geometric* if there exists t such that $\mathbf{V}$ and $\mathbf{V}_t$ are almost equal.

It is obvious that any two geometric families of constant reductions of F are almost equal. Moreover, if $\mathbf{V}$ is a geometric family of constant reductions of F, then it follows by (1. 6) that F has good reduction at almost all $\mathbf{v} \in \mathbf{V}$ and further, any non-constant function t of F is a good function at almost all $\mathbf{v} \in \mathbf{V}$. Therefore, the canonical restriction map

$$\mathrm{pr}_{FK} : \mathbf{V} \longrightarrow \mathbb{P}(K)$$

[2]) We say that two sets are almost equal if their symmetric difference is a finite set.

is almost bijective[3]). From this and applying (1. 6) we get the following local characterisation of the geometric families of constant reductions:

Local Characterisation Lemma. *Let the genus of F satisfy $\mathbf{g}_F \geqq 1$. Then a family $\mathbf{V}$ of constant reductions of F is geometric if and only if $\mathbf{V}$ is almost equal to the family of all good reductions of F.*

Proof. One applies the observations above combined with (1. 6) 1). □

(3. 3) Concerning the behaviour under finite extensions one has the following immediate facts:

1) Let $F'|F$ be a finite extension. Then a family of constant reductions $\mathbf{V}$ of F is geometric if and only if its prolongation $\mathbf{V}'$ to F' is geometric.

2) Suppose that $\mathbf{V}$ is geometric (hence $\mathbf{V}'$ is also geometric) and $F'|F$ is Galois. Then almost all $\mathfrak{v}'|\mathfrak{v}$ are nonramified. Therefore, for almost all $\mathfrak{v}'|\mathfrak{v}$ the canonical projections

$$\pi_{\mathfrak{v}'} : Z(\mathfrak{v}'|\mathfrak{v}) \longrightarrow \mathrm{Gal}(F'\mathfrak{v}'|F\mathfrak{v})$$

are isomorphisms.

What we meant by good geometric properties of φ now reads as follows:

Geometric Continuity Lemma. *φ maps geometric families of constant reductions of F onto geometric families of constant reductions of E.*

Proof. Let $\mathbf{V}$ be a geometric family of constant reductions of F. We show that its image $\mathbf{W}$ by φ is geometric. We begin with:

1) *F and E have the same genus, i.e., $\mathbf{g}_F = \mathbf{g}_E$.*

By (1. 6) it follows that both F and E have good reduction at almost all p-adic valuations. Let $\mathfrak{v}$ be a good reduction of F and $\tilde{\mathfrak{v}}$ a prolongation of $\mathfrak{v}$ to $\tilde{F}$. Let $\tilde{\mathfrak{w}}|\mathfrak{w}$ be the corresponding reduction of E by $\tilde{\varphi}$. Then by (1. 6) the genera of F and E satisfy $\mathbf{g}_{F\mathfrak{v}} = \mathbf{g}_F$, $\mathbf{g}_{E\mathfrak{w}} \leqq \mathbf{g}_E$. On the other hand, $F\mathfrak{v}$ and $E\mathfrak{w}$ are isomorphic by (3. 2). In particular they have the same genus and so one obtains $\mathbf{g}_F \leqq \mathbf{g}_E$. Taking a valuation $\mathfrak{w}$ at which E has good reduction one obtains the opposite inequality, so $\mathbf{g}_F = \mathbf{g}_E$ as contented.

2) *Suppose that $\mathbf{g}_F > 1$. Then φ defines a bijection between the set of all good reductions of F and the set of all good reductions of E.*

It is sufficient to show that the image $\tilde{\mathfrak{w}}|\mathfrak{w}$ of any good reduction $\mathfrak{v} \in \mathbf{V}$ of F is a good reduction of E. Let $\mathfrak{v}$ be a good reduction of F. Then F and $F\mathfrak{v}$ have the same genus by hypothesis. By (3. 2) $F\mathfrak{v}$ and $E\mathfrak{w}$ are isomorphic, so they have the same genus and further F and E have the same genus by 1). Therefore E and $E\mathfrak{w}$ have the same genus. From the reduction theory it follows (see [20], [24], [23]) that $\mathfrak{w}$ is a good reduction of E.

3) *If $\mathbf{g}_F > 1$, then $\mathbf{W}$ is geometric.*

---

[3]) We say that a map $f: A \to B$ is almost bijective if there exist subsets $A' \subseteqq A$ almost equal to A and $B' \subseteqq B$ almost equal to B such that f maps A' bijectively onto B'.

Since $\mathbf{g}_F > 1$ and $\mathbf{V}$ is geometric it follows by the local characterisation Lemma that $\mathbf{V}$ is almost equal to the set of all good reductions of F. Therefore, by 2) it follows that $\mathbf{W} = \varphi(\mathbf{V})$ is almost equal to the set of all good reductions of E. Since $\mathbf{g}_E = \mathbf{g}_F \geqq 1$ it follows by the same lemma that $\mathbf{W}$ is geometric.

We now prove that $\mathbf{W}$ is geometric. Let $F'|F$ be a finite sub-extension of $\tilde{F}$ having genus $\mathbf{g}_{F'}$ at least 2. Adopting the obvious notational conventions it follows by 3) that $\mathbf{W}'$ is geometric. On the other hand, $\mathbf{W}'$ is the prolongation of $\mathbf{W}$ to E'. Hence $\mathbf{W}$ is geometric. □

We now show how one can "interpolate" the family of all reductions $(F\mathfrak{v})_{\mathfrak{v}}$ defined by a geometric family of constant reductions $\mathbf{V}$ of F. Let $\mathcal{U}$ be a non-principal ultrafilter on $\tilde{\mathbf{V}}$ such that its image by the canonical projection

$$\tilde{\mathbf{V}} \longrightarrow \mathbb{P}(\mathbb{Q})$$

is a non-principal ultrafilter on $\mathbb{P}(\mathbb{Q})$. Then the images of $\mathcal{U}$ by $\tilde{\varphi}$ and all canonical projections are non-principal ultrafilters, which we also denote by $\mathcal{U}$. So for instance its images by

$$\tilde{\mathbf{V}} \longrightarrow \mathbf{V}' \longrightarrow \mathbf{V} \longrightarrow \mathbb{P}(K) \longrightarrow \mathbb{P}(\mathbb{Q}).$$

Further denote $F^* = \prod_{\mathfrak{v}} F\mathfrak{v}/\mathcal{U}$ and define correspondingly K^*, $\mathbb{Q}^*$. Taking into account that for any $x \neq 0$ in F one has $\mathfrak{v}x = 0$ for almost all $\mathfrak{v} \in \mathbf{V}$ it follows that there exist canonical embeddings

$$F \hookrightarrow F^*, \quad K \hookrightarrow K^*, \quad \mathbb{Q} \hookrightarrow \mathbb{Q}^*$$

defined by $x \mapsto (x_{\mathfrak{v}})/\mathcal{U}$, where $x_{\mathfrak{v}} = x\mathfrak{v}$ if $\mathfrak{v}x = 0$ and $x_{\mathfrak{v}} = 0$ otherwise. The following diagram is commutative:

$$\begin{array}{ccc} F & \text{——} & F^* \\ | & & | \\ K & \text{——} & K^* = K\mathbb{Q}^*. \\ | & & | \\ \mathbb{Q} & \text{——} & \mathbb{Q}^* \end{array}$$

We now describe the compositum of F and $\mathbb{Q}^*$ in F^*. First we remark that

$$F^*_{\text{fin}} = \{(x_{\mathfrak{v}})/\mathcal{U} \mid \deg^{F\mathfrak{v}} x_{\mathfrak{v}} \text{ is locally bounded}\}$$

is a function field of one variable over K^* with the constant field $K^* = K\mathbb{Q}^*$, and moreover, F^*_{fin} is relatively algebraically closed in F^* (compare with [28], proof of (3. 5)). Furthermore, for $x^* = (x_{\mathfrak{v}})/\mathcal{U}$ in F^*_{fin} locally the degrees $\deg^{F\mathfrak{v}} x_{\mathfrak{v}}$ are equal, and then they locally are equal to the degree of x^* as function in F^*_{fin}.

We now show that the compositum $F\mathcal{Q}^*$ of F and $\mathcal{Q}^*$ of F^* is exactly F^*_{fin}. Indeed, by (1. 6) any non-constant $x \in F$ is a good function at almost all $\mathfrak{v}$, hence it locally holds $\deg^F x = \deg^{F\mathfrak{v}} x\mathfrak{v}$. Therefore, $(x_\mathfrak{v} = x\mathfrak{v})/\mathcal{U}$ locally has bounded degree, thus it lies in F^*_{fin}. Moreover, by what we said above, x has the same degree in F and in F^*_{fin}. We conclude that FK^* and F^*_{fin} are equal. As a consequence, F and $K^* = K\mathcal{Q}^*$ are linearly disjoint over K in F^* and for any non-constant function h of F it locally holds

$$[F\mathcal{Q}^* : \mathcal{Q}^*(h)] = [F\mathfrak{v} : \mathcal{Q}(h)\mathfrak{v}] = [F^* : \mathcal{Q}(h)^*]. \tag{3. 4}$$

Therefore, if we denote by $F^{\mathcal{U}}$ the relative algebraic closure of F in F^* and correspondingly $K^{\mathcal{U}}$, $\mathcal{Q}^{\mathcal{U}}$ we have: $K^{\mathcal{U}} = K\mathcal{Q}^{\mathcal{U}}$, F and $K^{\mathcal{U}}$ are linearly disjoint over K, and finally $F^{\mathcal{U}} = F\mathcal{Q}^{\mathcal{U}}$.

(3. 5) We now describe the behaviour of our interpolation procedure under a finite Galois extension $F'|F$. Let $\mathbf{V}$, $\mathbf{V}'$ and $\mathcal{U}$ be as before. Then $F'^*|F^*$ is a Galois extension, the group $G^* = \prod_{\mathfrak{v}'} \text{Gal}(F'\mathfrak{v}'|F\mathfrak{v})/\mathcal{U}$ acts on F'^* in a canonical way and its fixed field is exactly F^*. Therefore G^* is exactly the Galois group of $F'^*|F^*$. The canonical projection

$$\pi^* : \text{Gal}(F'^*|F^*) \longrightarrow \text{Gal}(F'|F)$$

is injective. We can describe π^* as follows. Since $\text{Gal}(F'|F)$ is finite it has only finitely many subgroups, hence locally $Z(\mathfrak{v}'|\mathfrak{v})$ are equal, say equal to Z. Furthermore, almost all $\mathfrak{v}'|\mathfrak{v}$ are non-ramified and hence almost all canonical projections

$$\pi_{\mathfrak{v}'} : Z \longrightarrow \text{Gal}(F'\mathfrak{v}'|F\mathfrak{v})$$

are isomorphisms. The mapping

$$\iota^* : Z \longrightarrow G^* = \text{Gal}(F'^*|F^*), \quad \iota^*(g) = (\pi_{\mathfrak{v}'}(g))/\mathcal{U}$$

is an isomorphism and it is exactly the inverse of the canonical projection π^*.

Next we remark that $F'\mathcal{Q}^* = F'^*_{\text{fin}}$ is G^*-invariant. Indeed, let $g^* = \iota^*(g)$ $(g \in Z)$ be an arbitrary element of G^*. By what we said above it follows that $g_{\mathfrak{v}'} = \pi_{\mathfrak{v}'}(g)$ locally is a $\mathcal{Q}\mathfrak{v}$-isomorphism of $F'\mathfrak{v}'$. Therefore one locally has $\deg^{F'\mathfrak{v}'} x_{\mathfrak{v}'} = \deg^{F'\mathfrak{v}'}(g_{\mathfrak{v}'}(x_{\mathfrak{v}'}))$ for any $x_{\mathfrak{v}'} \in F'\mathfrak{v}'$. Hence F'^*_{fin} is g^*-invariant. Since $F\mathcal{Q}^*$ is contained in F^*, it is pointwise G^*-invariant and we get: the restriction G' of G^* to $F'\mathcal{Q}^*$ is contained in $\text{Gal}(F'\mathcal{Q}^*|F\mathcal{Q}^*)$. We now show that G' is exactly $\text{Gal}(F'\mathcal{Q}^*|F\mathcal{Q}^*)$. Let f be a non-constant function of $F|K$. Then f is also a non-constant function for $F'|K$. By (3. 4) we have

$$[F'\mathcal{Q}^* : \mathcal{Q}^*(f)] = [F'^* : \mathcal{Q}(f)^*], \quad [F\mathcal{Q}^* : \mathcal{Q}^*(f)] = [F^* : \mathcal{Q}(f)^*],$$

hence $[F'\mathcal{Q}^* : F\mathcal{Q}^*] = [F'^* : F^*]$. Our claim now follows from the injectivity of the restriction map $\text{Gal}(F'^*|F^*) \to \text{Gal}(F'\mathcal{Q}^*|F\mathcal{Q}^*)$. We finally remark, that the canonical projection

$$\pi' : \text{Gal}(F'\mathcal{Q}^*|F\mathcal{Q}^*) \longrightarrow \text{Gal}(F'|F)$$

is injective and has Z as image. The inverse of π' over Z is

$$\iota' : Z \longrightarrow \mathrm{Gal}(F'\mathbb{Q}^*|F\mathbb{Q}^*), \quad \iota'(g)((x_{\mathbf{v}'})/\mathcal{U}) = (\pi_{\mathbf{v}'}(g)(x_{\mathbf{v}'}))/\mathcal{U}.$$

We now show how one gets information on F and E from isomorphic geometric families $\mathbf{V}$ and $\mathbf{W}$. We use the local isomorphisms (3. 1) defined at the beginning of this paragraph.

Preserving the notations of above, the images of $\mathcal{U}$ by $\tilde{\varphi}$ and all canonical projections are again non-principal ultrafilters, which will also be denoted by $\mathcal{U}$. Then the local $\mathbb{Q}\mathbf{v}$-isomorphisms $\phi_{\mathbf{v}} : E\mathbf{w} \to F\mathbf{v}$ define a $\mathbb{Q}^*$-isomorphism

$$\phi^* : E^* \longrightarrow F^*, \quad \phi^*((x_{\mathbf{v}})/\mathcal{U}) = (\phi_{\mathbf{v}}(x_{\mathbf{v}}))/\mathcal{U}.$$

Taking into account that all $\phi_{\mathbf{v}}$ preserve the degree of the functions it follows that ϕ^* defines a $\mathbb{Q}^*$-isomorphism

$$\phi_0 : E^*_{\mathrm{fin}} = E\mathbb{Q}^* \longrightarrow F^*_{\mathrm{fin}} = F\mathbb{Q}^*.$$

Thus, we have obtained the following: enlarging the constants of F and E in a canonical way by $\mathbb{Q}^*$ the two function fields $F\mathbb{Q}^*$ and $E\mathbb{Q}^*$ become $\mathbb{Q}^*$-isomorphic. We do not know yet whether the isomorphism ϕ_0 is defined over $\mathbb{Q}$. Nevertheless, if $\mathbf{g}_F \geqq 2$ and $\mathbb{Q}^*|\mathbb{Q}^{\mathcal{U}}$ is an elementary extension (see (1. 8) for notations), then by (1. 7) ϕ_0 is defined already over $\mathbb{Q}^{\mathcal{U}}$.

Now let $F'|F$ be a finite Galois sub-extension of $\tilde{F}$ and $E'|E$ the corresponding subfield of $\tilde{E}$. Construct the $\mathbb{Q}^*$-isomorphisms

$$\phi'^* : E'^* \longrightarrow F'^*, \quad \phi'_0 : E'\mathbb{Q}^* \longrightarrow F'\mathbb{Q}^*$$

as we did for F and E. We show that ϕ^* is the restriction of ϕ'^* to E^*, hence ϕ_0 is the restriction of ϕ'_0 to $E\mathbb{Q}^*$. Indeed, for any $\tilde{\mathbf{v}} \in \tilde{\mathbf{V}}$ let $\mathbf{v}$, $\mathbf{v}'$ be its restriction to F, F' respectively. Then, by their definition, the local isomorphisms $\phi_{\mathbf{v}}$, $\phi_{\mathbf{v}'}$ are exactly the restrictions of $\phi_{\tilde{\mathbf{v}}}$ to $E\mathbf{w}$, $E'\mathbf{w}'$ respectively. Hence $\phi_{\mathbf{v}}$ is the restriction of $\phi_{\mathbf{v}'}$ to $E\mathbf{w}$ and we are through.

If now additionally, the genus $\mathbf{g}_{F'}$ of F' is at least 2 and $\mathbb{Q}^*|\mathbb{Q}^{\mathcal{U}}$ is elementary, then the isomorphism ϕ'_0 is defined over $\mathbb{Q}^{\mathcal{U}}$ and consequently also ϕ_0 is defined over $\mathbb{Q}^{\mathcal{U}}$. On the other hand we always can choose such an F' and we have obtained:

When for the given non-principal ultrafilter $\mathcal{U}$ the corresponding field extension $\mathbb{Q}^*|\mathbb{Q}^{\mathcal{U}}$ is elementary, then for any finite extension $F'|F$ the isomorphism ϕ'_0 is already defined over $\mathbb{Q}^{\mathcal{U}}$. Hence, its restriction to $E'\mathbb{Q}^{\mathcal{U}}$ is a $\mathbb{Q}^{\mathcal{U}}$-isomorphism

$$\phi^{\mathcal{U}} : E'\mathbb{Q}^{\mathcal{U}} \longrightarrow F'\mathbb{Q}^{\mathcal{U}}.$$

Now let $\Phi' : \mathrm{Gal}(F'|F) \to \mathrm{Gal}(E'|E)$ be the canonical isomorphism induced by the isomorphism Φ. Taking into account that $\Phi(Z(\tilde{\mathbf{v}}|\mathbf{v}))$ is the decomposition group of the corresponding $\tilde{\mathbf{w}}|\mathbf{w}$ and $\mathbf{v}' = \tilde{\mathbf{v}}|_{F'}$, $\mathbf{w}' = \tilde{\mathbf{w}}|_{E'}$ it follows by general valuation theory that $\Phi'(Z(\tilde{\mathbf{v}}|\mathbf{v}))$ is the decomposition group of $\mathbf{w}'|\mathbf{w}$. Therefore, with the notations from (3. 5), $\Phi'(Z)$ locally is the decomposition group of $\mathbf{w}'|\mathbf{w}$. Now construct

$$j^* : \Phi'(Z) \longrightarrow \mathrm{Gal}(E'^*|E^*)$$

as we constructed ι^* in (3. 5).

Directly from the definition of ϕ'^*, ι^* and j^* one gets: $j^*\Phi'(g) = \phi'^{*-1}\iota^*(g)\phi'^*$ for all $g \in Z$, i.e., the following diagram is commutative:

$$\begin{array}{ccc}
\mathrm{Gal}(F'^*|F^*) & \xrightarrow{\phi'^{*-1}()\phi'^*} & \mathrm{Gal}(E'^*|E^*) \\
\downarrow & & \downarrow \\
\mathrm{Gal}(F'\mathbb{Q}^*|F\mathbb{Q}^*) & \xrightarrow{\phi_0'^{-1}()\phi_0'} & \mathrm{Gal}(E'\mathbb{Q}^*|E\mathbb{Q}^*) \\
\downarrow & & \downarrow \\
\mathrm{Gal}(F'|F) & \xrightarrow{\Phi'} & \mathrm{Gal}(E'|E).
\end{array}$$

Finally we remark that our interpolation construction has good functorial properties. Namely, for $F'' \subseteq F'$ finite Galois extensions of F and the corresponding Galois extensions $E'' \subseteq E'$ of E consider the $\mathbb{Q}^*$-isomorphisms ϕ_0' and ϕ_0''. Then it holds:

I. The following diagram is commutative:

$$\begin{array}{ccc}
\mathrm{Gal}(F'\mathbb{Q}^*|F\mathbb{Q}^*) & \longrightarrow & \mathrm{Gal}(F'|F) \\
\downarrow & & \downarrow \\
\mathrm{Gal}(F''\mathbb{Q}^*|F\mathbb{Q}^*) & \longrightarrow & \mathrm{Gal}(F''|F)
\end{array}$$

where the arrows are the canonical restriction maps. Correspondingly, the same holds for E.

II. The restriction of ϕ_0' to $E''\mathbb{Q}^*$ is exactly ϕ_0''.

The proof consists in straightforward verifications which we omit.

Therefore we can take limits over all finite Galois sub-extension $F'|F$ of $\tilde{F}$ and so obtain: For any non-principal ultrafilter $\mathcal{U}$ on $\mathbf{V}$ there exist canonical constant extensions $\tilde{F}\mathbb{Q}^*$, $\tilde{E}\mathbb{Q}^*$ of $\tilde{F}$ and $\tilde{E}$ by $\mathbb{Q}^*$ and a $\mathbb{Q}^*$-isomorphism $\tilde{\phi}$ of $\tilde{E}\mathbb{Q}^*$ onto $\tilde{F}\mathbb{Q}^*$ making the following diagram commutative:

$$\begin{array}{ccc} \mathrm{Gal}(\tilde{F}\mathbb{Q}^*|F\mathbb{Q}^*) & \xrightarrow{\tilde{\phi}^{-1}(\,)\tilde{\phi}} & \mathrm{Gal}(\tilde{E}\mathbb{Q}^*|E\mathbb{Q}^*) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(\tilde{F}|F) & \xrightarrow{\Phi} & \mathrm{Gal}(\tilde{E}|E). \end{array} \tag{3. 6}$$

When $\mathbb{Q}^*|\mathbb{Q}^{\mathcal{U}}$ is an elementary extension, the above isomorphism $\tilde{\phi}$ is defined over $\mathbb{Q}^{\mathcal{U}}$. Hence, in this case, the restriction ϕ of $\tilde{\phi}$ to $\tilde{E}\mathbb{Q}^{\mathcal{U}}$ is an isomorphism

$$\phi : \tilde{E}\mathbb{Q}^{\mathcal{U}} \longrightarrow \tilde{F}\mathbb{Q}^{\mathcal{U}}.$$

Taking into account that $\tilde{F}\mathbb{Q}^{\mathcal{U}} = \tilde{F}$, i.e., $\mathrm{Gal}(\tilde{F}\mathbb{Q}^{\mathcal{U}}|F\mathbb{Q}^{\mathcal{U}}) = G_{F\mathbb{Q}^{\mathcal{U}}}$ (and correspondingly the same for E), we can interpret (3. 6) as follows:

(3. 7) *If $\mathbb{Q}^*|\mathbb{Q}^{\mathcal{U}}$ is an elementary extension then there exists a $\mathbb{Q}^{\mathcal{U}}$-isomorphism $\phi : \tilde{E} \to \tilde{F}$ such that $\Phi(g) = \phi^{-1} g \phi$ for all $g \in G_{F\mathbb{Q}^{\mathcal{U}}}$.*

We now come back to the proof of the main result. Let $\mathbf{V}$ be a fixed geometric family of constant reductions of F. Denote by Σ the set of all elements σ of $G_{\mathbb{Q}}$ which have the property (1. 8) 2). It is clear that Σ is a dense subset of $G_{\mathbb{Q}}$.

Let $\sigma \in \Sigma$ and $\mathcal{U} = \mathcal{U}_\sigma$ a corresponding non-principal ultrafilter. Fix a preimage of $\mathcal{U}$ by the canonical projection $\tilde{\mathbf{V}} \to \mathbb{P}(\mathbb{Q})$ and denote it also by $\mathcal{U}$. Finally, the images of the latter $\mathcal{U}$ by $\tilde{\varphi}$ and all other canonical projections are non-principal ultrafilters, which we also denote by $\mathcal{U}$. One concludes that there exists a $\mathbb{Q}^{\mathcal{U}}$-isomorphism $\phi : \tilde{E} \to \tilde{F}$ with the properties from (3. 7). We show that ϕ does not depend on $\mathcal{U}$: Let ϕ', ϕ'' be isomorphisms corresponding to non-principal ultrafilters $\mathcal{U}'$, $\mathcal{U}''$. For all $g \in G_{F\tilde{\mathbb{Q}}}$ one has:

$$\Phi(g) = \phi'^{-1} g \phi' = \phi''^{-1} g \phi'',$$

so $\phi = \phi \circ \phi''^{-1}$ is a $\mathbb{Q}$-isomorphism of $\tilde{F}$ which commutes with $G_{F\tilde{\mathbb{Q}}}$. On the other hand there exists exactly one such isomorphism, namely the identity (see the lemma below). Hence we have proved:

There exists a field isomorphism $\phi : \tilde{E} \to \tilde{F}$ such that $\Phi(g) = \phi^{-1} g \phi$ for all $g \in \bigcup_{\mathcal{U}} G_{F\mathbb{Q}^{\mathcal{U}}}$, where $\mathcal{U}$ runs over the family of all non-principal ultrafilters which have the property (1. 8) 2).

On the other hand $\bigcup_{\mathcal{U}} G_{F\mathbb{Q}^{\mathcal{U}}}$ is the preimage of Σ by the canonical projection $\pi_{F\mathbb{Q}} : G_F \to G_{\mathbb{Q}}$, so it is a dense subset of G_F. Now continuity reasons imply:

$$\Phi(g) = \phi^{-1} g \phi, \quad g \in G_F.$$

The proof is finished. □

Lemma. *Let $F|K$ be a function field of one variable. Then the only automorphism ϕ of $\tilde{F}$ which commutes with $G_{F\tilde{K}}$ is the identity.*

Proof. For any prime divisor P of $F|\tilde{K}$ denote by $\tilde{\mathfrak{v}}_P|\mathfrak{v}_P$ the valuation defined by $\mathfrak{v}_P$ together with one of its prolongations to $\tilde{F}$. Denote by Z_P the decomposition group of $\tilde{\mathfrak{v}}_P|\mathfrak{v}_P$. Then $\tilde{\mathfrak{v}}_P \circ \phi$ is also a rank 1 valuation of $\tilde{F}$, and its decomposition group in $(G_{F\tilde{K}})^\phi = G_{F\tilde{K}}$ is $(Z_P)^\phi = Z_P$. Applying (1. 4) and (1. 5) we obtain $\tilde{\mathfrak{v}}_P = \tilde{\mathfrak{v}}_P \circ \phi$. Therefore, for any element $f \neq 0$ in $\tilde{F}$ we have $\tilde{\mathfrak{v}}_P(\phi(f)/f) = 0$, i.e. $\phi(f)/f$ is a constant $a \in \tilde{K}$ depending on f. It follows that any non-constant function f of $\tilde{F}$ is invariant by ϕ, hence ϕ is the identity. □

References

[1] *E. Artin, J. Tate*, Class field theory, Harvard 1961.
[2] *J. Ax*, Solving diophantine problems modulo every prime, Ann. of Math. **85** (1967), 161—183.
[3] *J.-L. Bell, A.-B. Slomson*, Models and ultraproducts: an introduction, Amsterdam 1969.
[4] *N. Bourbaki*, Algèbre commutative, Paris 1964.
[5] *C. Chevalley*, Introduction to the theory of algebraic functions of one variable, AMS, New York 1951.
[6] *M. Deuring*, Reduction algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers, Math. Z. **47** (1942), 643—654.
[7] *O. Endler*, Valuation theory, Berlin-Heidelberg-New York 1972.
[8] *B. W. Green, M. Matignon, F. Pop*, On valued function fields I., manuscr. math. **65** (1989), 357—376.
[9] *A. Grothendieck*, Letter to Faltings, June '83.
[10] *H. Hasse*, Zahlentheorie, Berlin 1963.
[11] *K. Hensel*, Neue Grundlagen der Arithmetik, J. reine angew. Math. **127** (1902), 51—84.
[12] *M. Ikeda*, Completeness of the absolute Galois group of the rational number field, J. reine angew. Math. **291** (1977), 1—22.
[13] *U. Jannsen, K. Wingberg*, Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper, Invent. math. **70** (1982), 70—98.
[14] *M. Jarden*, Elementary statements over large algebraic fields, Trans. AMS **164** (1972), 67—91.
[15] *E. Kani*, Nonstandard diophantine geometry, Dissertation, Heidelberg 1978.
[16] *H. Koch*, Die Galoissche Theorie der p-Erweiterungen, Math. Monogr. **10**, Berlin 1970.
[17] *K. Komatsu*, A remark to a Neukirch's conjecture, Proc. Japan Acad. **50** (1974), 253—255.
[18] *W. Krull*, Allgemeine Bewertungstheorie, J. reine angew. Math. **167** (1931), 160—196.
[19] *F.-V. Kuhlmann, M. Pank, P. Roquette*, Immediate and purely wild extensions of valued fields, manuscr. math. **55** (1986), 39—67.
[20] *E. Lamprecht*, Zur Eindeutigkeit von Primdivisoren, Arch. Math. **8** (1957), 30—38.
[21] *E. Lamprecht*, Restabbildungen von Divisoren I, Arch. Math. **8** (1957), 255—264.
[22] *S. Lichtenbaum*, Duality theorems for curves over p-adic fields, Invent. math. **7** (1969), 120—136.
[23] *M. Matignon*, Genre et genre résiduel des corps de fonctions valués, manuscr. math. **58** (1987), 179—214.
[24] *H. Mathieu*, Das Verhalten des Geschlechts bei Konstantenreduktionen algebraischer Funktionskörper, Arch. Math. **20** (1969), 597—611.
[25] *J. Neukirch*, Über eine algebraische Kennzeichnung der Henselkörper, J. reine angew. Math. **231** (1968), 75—81.
[26] *J. Neukirch*, Kennzeichnung der p-adischen und endlichen algebraischen Zahlkörper, Invent. math. **6** (1969), 269—314.
[27] *J. Neukirch*, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, J. für Math. **238** (1969), 135—147.
[28] *F. Pop*, Galoissche Kennzeichnung p-adisch abgeschlossener Körper, J. reine angew. Math. **392** (1988), 145—175.
[29] *A. Prestel, P. Roquette*, Formally p-adic fields, Lect. Notes in Math. **1050**, Berlin 1984.
[30] *P. Ribenboim*, Théorie des valuations, Les Presses de l'Université de Montréal, Montréal 1964.
[31] *L. Ribes*, Introduction to profinite groups and Galois cohomology, Queen's papers in pure and appl. Math. **24**, Queen's Univ. Kingston 1970.

[32] *A. Robinson, P. Roquette*, On the finiteness theorem of Siegel und Mahler concerning diophantine equations, J. Number Th. **7** (1975), 121—176.
[33] *P. Roquette*, Some tendencies in contemporary algebra, in: Perspectives in Mathematics, Anniversary of Oberwolfach 1984, Basel 1984, 393—422.
[34] *P. Roquette*, Zur Theorie der Konstantenreduktion algebraischer Mannigfaltigkeiten, J. reine angew. Math. **200** (1958), 1—44.
[35] *J. P. Serre*, Cohomologie Galoisienne, Lect. Notes in Math. **5**, Berlin 1965.
[36] *H. Stichtenoth*, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, Arch. Math. **24** (1973), 527—544.
[37] *J. Tate*, Cohomology of abelian varieties over p-adic fields, Notes by S. Lang, Priceton Univ., May 1959.
[38] *K. Uchida*, Isomorphisms of Galois groups of algebraic function fields, Ann. of Math. **106** (1977), 589—598.
[39] *K. Uchida*, Isomorphisms of Galois groups of solvably closed Galois extensions, Tôhoku Math. J. **31** (1979), 359—362.

Mathematisches Institut der Universität, Im Neuenheimer Feld 288, D-6900 Heidelberg

Eingegangen 19. Januar 1989, in revidierter Fassung 13. September 1989