C. R. Math. Rep. Acad. Sci. Canada - Vol. II (1980) No. 6

C. R. Math. Rep. Acad. Sci. Canada - Vol. II (1980) No. 6

COMPACTNESS PROPERTIES OF OPERATOR COSINE FUNCTIONS

Dieter Lutz

Presented by J. Aczél, F.R.S.C.

We study properties of operator valued solutions C of d'Alembert's functional equation with compact infinitesimal generator.

In this note an operator cosine function on X is meant to be a strongly continuous function C defined on $\mathbb{R}$ with values in $B(X)$, the algebra of bounded linear operators on a complex Banach space X fulfilling

$$C(t+s) + C(t-s) = 2\,C(t)\,C(s), \quad s,t \in \mathbb{R}, \qquad C(0) = I \quad . \tag{1}$$

The infinitesimal generator A of C is the closed and densely defined operator given by

$$Ax := C''(0)x \quad , \tag{2}$$

whenever the right side makes sense.

If C is an operator cosine function there are constants $M, w \geq 0$ with

$$\|C(t)\| \leq M \cdot e^{w|t|} \quad , \quad t \in \mathbb{R} \quad . \tag{3}$$

Then for $z \in \mathbb{R}$ with $z > w$ we have $z^2 \in \rho(A)$ (= the resolvent set of A, the spectrum of A is denoted by $\sigma(A)$, and the resolvent operator by $R(z,A)$) and

$$z\,R(z^2,A) = \int_0^\infty e^{-zt}\,C(t)dt \quad . \tag{4}$$

It is the aim of the present note to give a proof of the following theorem

Theorem 1: Let A denote the infinitesimal generator of the operator cosine function C on X with

$$\|C(t)\| \leq M \cdot e^{w|t|} , \quad t \in \mathbb{R} .$$

Then

i) A is compact

$\Rightarrow$ ii) $z^2R(z^2,A) - I$ is compact for every $z > w$

$\Rightarrow$ iii) $z^2R(z^2,A) - I$ is compact for some $z > w$

$\Rightarrow$ iv) $C(t) - I$ is compact for every $t > 0$.

Proof:

i) $\Rightarrow$ ii) is valid for every $A \in B(X)$ by [1], Th. 5.7.1.

ii) $\Rightarrow$ iii) is obvious.

iii) $\Rightarrow$ iv): Let $z^2R(z^2,A) - I$ be compact for some $z > w$. Then, by [2], 2.14, for every $x \in X$ we have the identity

$$C(t)x - x = A \int_0^t (t-s)\, C(s)x \, ds \quad . \tag{5}$$

Omitting the argument $x \in X$ and using $R(z^2,A) = z^2R(z^2,A) - I$ we get

$$\begin{aligned} z^2R(z^2,A)(C(t) - I) &= z^2R(z^2,A)\, A \int_0^t (t-s)\, C(s)\, ds \\ &= z^2(z^2R(z^2,A) - I) \int_0^t (t-s)\, C(s)\, ds \quad . \end{aligned}$$

Thus, we have the representation

$$C(t) - I = - (z^2 R(z^2,A) - I)(C(t) - I) + \\ + z^2 (z^2 R(z^2,A) - I) \int_0^t (t-s)\, C(s)\,ds \quad .$$

$S(t) := \int_0^t (t-s)\, C(s)\,ds$ is a bounded linear operator with

$$\| S(t) \| \leq \frac{M t^2}{2} e^{wt} \quad .$$

Thus, $C(t) - I$ is compact.

We strongly guess that iv) implies i) but up to now we have not succeeded in proving this to be true. Obviously iv) implies i) under the additional requirement of C being continuous in the operator norm topology on $B(X)$ since in this case A is bounded and

$$\| A - \frac{2}{t^2} (C(t) - I) \| \to 0$$

for $t \to 0$. In Theorem 2, we obtain a slightly stronger version of this almost trivial converse.

Theorem 2: Let C be continuous in the norm topology on $B(X)$ and let $C(t) - I$ be compact for some $t > 0$ with $\| C(s) - I \| < 1$ for $s \in [0,t]$. Then A is also compact.

Proof: We have

$$\| \frac{2}{t^2} \int_0^t (t-s)\, C(s)\,ds - I \| \\ = \| \frac{2}{t^2} \int_0^t (t-s)(C(s) - I)\,ds \| \\ \leq \frac{2}{t^2} \cdot \sup_{s \in [0,t]} \| C(s) - I \| \cdot \frac{t^2}{2} < 1$$

so $S(t) := \int_0^t (t-s)\, C(s)\,ds$ is continuously invertible and using

(4) we see that

$$A = S(t)^{-1}(C(t) - I)$$

is compact.

[1] Hille,E.; Phillips,R.S: Functional analysis and semi-groups. Providence,R.I.: American Mathematical Society (1957).

[2] Sova,M.: Cosine operator functions. Rozprawy matematyczne 49. Warszawa (1966).

Dieter Lutz
FB 6 - Mathematik -
Universität Essen
P.O.B. 6843
D - 4300 Essen 1
W-Germany

Received September 15, 1980

C. R. Math. Rep. Acad. Sci. Canada - Vol. II (1980) No. 6

INFORMATION FUNCTIONS ON OPEN DOMAIN. III.

J. Aczél F.R.S.C.

Abstract. An (n-place) information function of degree $\alpha = (\alpha_1,\dots,\alpha_n)$ is a real valued solution of the equation

$$f(x) + (1-x)^{\alpha} f\left(\frac{y}{1-x}\right) = f(y) + (1-y)^{\alpha} f\left(\frac{x}{1-y}\right) \quad \text{on } D_o^n \tag{1}$$

(the fundamental equation of information), where

$$D_o^n = \{(x,y) \mid x,y,x+y \in]0,1[^n\}, \tag{2}$$

$1 = (1,1,\dots,1)$, addition (subtraction), multiplication (division) of vectors are done coordinatewise and so are powers

$$z^{\alpha} = (z_1,z_2,\dots,z_n)^{(\alpha_1,\alpha_2,\dots,\alpha_n)} = z_1^{\alpha_1} z_2^{\alpha_2} \dots z_n^{\alpha_n}.$$

Previously [2-7], equation (1) was supposed to hold also at some boundary points of D_o^n which has made the solution much easier (even so the results have been restricted to $n<4$), but has excluded some cases important for application (including those to be determined in this paper) or the domains were complicated. - C.T. Ng [10] has resolved (1) on (2) completely except when $\alpha = (1,0,\dots,0)$ or $(0,1,\dots,0)$ or $\dots(0,\dots,0,1)$. In this paper we settle these exceptional cases, so that (1) is now completely solved on (2).

1. We will write $n = 1+m$, $s = (s,u_1,\dots,u_m) = (s,u)$ etc. and we may confine ourselves to $\alpha = (1,0,\dots,0)$. So (1) goes over into

$$f(s,u)+(1-s)f\left(\frac{t}{1-s},\frac{v}{1-u}\right) = f(t,v)+(1-t)f\left(\frac{s}{1-t},\frac{u}{1-v}\right), \tag{3}$$

$$(s,t) \in D_o, \quad (u,v) \in D_o^m.$$

Keeping $(u,v)\in D_0^m$ fixed for the time being, (3) becomes a special case ($a_1=1$) of the equation

(4) $f_1(s)+(1-s)^{a_1}f_2(\frac{t}{1-s}) = f_3(t)+(1-t)^{a_1}f_4(\frac{s}{1-t})$, $(s,t)\in D_0$

solved recently by Gy. Maksa [9]. He has found, among others, that, for $a_1=1$,

$$f_1(s) = s\ell(s)+(1-s)\ell(1-s)+a_1s+b_1,$$

$$f_3(s) = s\ell(s)+(1-s)\ell(1-s)+a_3s+b_3 .$$

where ℓ is an arbitrary solution of

(5) $\ell(st) = \ell(s)+\ell(t)$ $(s,t\in]0,1[)$.

But $f_1(s) = f(s,u)$, $f_3(s) = f(s,v)$ so that, letting u, v vary again,

(6) $f(s,u) = s\ell(s)+(1-s)\ell(1-s)+a(u)s+b(u)$, $(s\in]0,1[,\ u\in]0,1[^m)$.

We substitute (6) into (3) and get, after cancellations (apply (5)),

$$a(u)s+b(u)+a(\tfrac{v}{1-u})t+b(\tfrac{v}{1-u})(1-s) = a(v)t+b(v)+a(\tfrac{u}{1-v})s+b(\tfrac{u}{1-v})(1-t).$$

Comparison of the coefficients of s and of the terms independent of s and t yields

(7_1) $a(u) = a(\frac{u}{1-v})+b(\frac{v}{1-u})$,

(7_2) $b(u)+b(\frac{v}{1-u}) = b(v)+b(\frac{u}{1-v})$

$[(u,v)\in D_0^m]$ or, with $A(u) := a(u)+b(u)$, $p := u/(1-v)$, $q := 1-v$

$$A(pq) = A(p)+b(1-q) \qquad (p,q\in]0,1[^m).$$

The general solution of this equation (cf. [1]) is given by

$$A(u) = L(u)+c,\ b(1-q) = L(q)$$

with arbitrary constant c and L an arbitrary solution of

$$(8) \qquad L(uv) = L(u)+L(v) \qquad (u,v\in]0,1[^m).$$

In view of the definition of A and of (6) we get

$$(9_1) \qquad b(u) = L(1-u),$$

$$(9_2) \qquad a(u) = L(u)-L(1-u)+c,$$

$$(10) \qquad f(s,u) = s\ell(s)+(1-s)\ell(1-s)+sL(u)+(1-s)L(1-u)+cs$$

$$(s\in]0,1[,\ u\in]0,1]^m)$$

2. All functions of the form (10) with (5) and (8) satisfy (3). So we have proved the following

Theorem. The general solution of (3) [cf. (2)] is given by (10) where c is an arbitrary real constant and ℓ, L are arbitrary real valued solutions of (5) and (8).

Note. The general solution of (8) is given ([8]) by

$$(11) \qquad L(u) = L(u_1,\dots,u_m) = \sum_{j=1}^{m} \ell_j(u_j),$$

where $\ell_1,\dots,\ell_m$ satisfy (5). If f is measurable in s and u, then (cf. [3])

$$(12) \qquad f(s,u_1,\dots,u_m) = as\log s + a(1-s)\log(1-s) + \sum_{j=1}^{m} a_j\,(s\log u_j+(1-s)\log(1-u_j))+cs$$

is the general solution of (3) with arbitrary constant $c,a,a_1,\dots,a_m$.

Equation (3) has originated [with $f(x,u)=I_2(1-x,x;1-u,u)$] from the recursive property of information measures

(13) $I_k(p_1,p_2,p_3,\dots,p_k;q_1,q_2,q_3,\dots,q_k) =$

$$I_{k-1}(p_1+p_2,p_3,\dots,p_k;q_1+q_2,q_3,\dots,q_k) +$$

$$(p_1+p_2)I_2\left(\frac{p_1}{p_1+p_2},\frac{p_2}{p_1+p_2},\frac{q_1}{q_1+q_2},\frac{q_2}{q_1+q_2}\right),$$

$$q_i = (q_{i1},\dots,q_{im}),\ q_{ij}>0,\ p_i>0,\ \sum_{i=1}^{k} p_i = \sum_{i=1}^{k} q_{ij} = 1$$

and from the partial symmetry $I_3(p_1,p_2,p_3;q_1,q_2,q_3) = I_3(p_1,p_3,p_2;q_1,q_3,q_2)$. Equations (13), (10) and (11) lead to

(14) $$I_k(p_1,\dots,p_k;q_1,\dots,q_k) = \sum_{i=1}^{k} p_i\left[\ell(p_i)+\sum_{j=1}^{m}\ell_j(q_{ij})\right]+c(1-p_1)$$

where c is an arbitrary constant and $\ell,\ell_1,\dots,\ell_m$ are arbitrary solutions of (5). If I_2 is measurable then, from (12) and (13),

(15) $$I_k(p_1,\dots,p_k;q_1,\dots,q_k) = \sum_{i=1}^{k} p_i\left(a\log p_i+\sum_{j=1}^{m} a_j\log q_{ij}\right) +$$

$$+ c(1-p_1)$$

with arbitrary constant $a,a_1,\dots,a_m,c$. If I_k is also symmetric, then $c = 0$ in (14) and (15).

Remarks: By using the general solution of (4) given in [9] and methods from [4], we could also obtain in a similar way several results subsumed in [10]. - Since the only nontrivial multiplicative and additive functions from $]0,1[^n$ to R are the projections, the above theorem takes also care of the only case not settled by Theorem G in [10].

On the other hand, we could use the solution (9_1) given in [10], of (7_2), substitute it into (7_1) and obtain (9_2) directly as in [5]. This gives a second proof of the Theorem.

Acknowledgements. The author is grateful to C.T. Ng for helpful remarks, including the observation that the above result and proof can be generalized from n = 2 to arbitrary n. - This research has been supported in part by a Natural Sciences and Engineering Research Council of Canada grant.

REFERENCES

[1] Aczél, J., On a generalization of the functional equation of Pexider. Publ. Inst. Math. (Beograd) 4(18)(1964), 77-80.

[2] Aczél, J., Notes on generalized information functions. Aequationes Math. 22 (1981).

[3] Aczél, J.; Daróczy, Z., On measures of information and their characterizations. Academic Press, New York-San Francisco-London, 1975.

[4] Aczél, J.; Kannappan, Pl., General two-place information functions. Submitted to Proc. Roy. Soc. Edinburgh Sect. A.

[5] Aczél, J.; Ng, C.T., On general information functions. Submitted to Utilitas Math.

[6] Kannappan, Pl., Note on generalized information function. Tôhoku Math. J. 30 (1978), 251-255.

[7] Kannappan, Pl., On two functional equations from information theory. Submitted to J. Indian Math. Soc.

[8] Kuczma, M., Note on additive functions of several variables. Uniw. Śląski w Katowicach Prace Nauk - Prace Mat. 21 (1977), 49-51.

[9] Maksa, Gy., Solution on the open triangle of the generalized fundamental equation of information. Submitted to Utilitas Math.

[10] Ng, C.T., Information functions on open domain. II. C.R. Math. Rep. Acad. Sci. Canada 2 (1980), 155-158.

Faculty of Mathematics,
University of Waterloo,
Waterloo, Ontario N2L 3G1, Canada

Received October 6, 1980

C. R. Math. Rep. Acad. Sci. Canada - Vol. II (1980) No. 6

AN OSCILLATION CRITERION FOR SECOND ORDER SELF-ADJOINT DIFFERENTIAL SYSTEMS

by

Angelo B. Mingarelli

Presented by F.V. Atkinson, F.R.S.C.

The purpose of this note is to provide a partial answer to a conjectured oscillation criterion for the self-adjoint ordinary differential equation

$$y'' + Q(t)y = 0 \qquad t \in [0,\infty) \tag{1}$$

for a vector y where $Q(t) = Q^*(t)$ is a real symmetric $n\times n$ matrix defined and continuous on $[0,\infty)$. This basic assumption on Q will be assumed hereafter. The collection of all $n\times n$ real symmetric matrices will be denoted by S. The distinct points a,b will be said to be (mutually) *conjugate* with respect to (1) if there exists a nontrivial solution y of (1) vanishing at a and b. The equation (1) will be called *disconjugate* on a real interval J if the latter fails to contain two points which are mutually conjugate with respect to (1). Finally equation (1) will be termed *oscillatory* at ∞ if for every $a > 0$ there exists $b > a$ such that (1) is not disconjugate on $[a,b]$. It will be *non-oscillatory* otherwise.

In the following discussion the symbols $\lambda_1(A)$, tr (A) will denote the maximum eigenvalue and the trace of A respectively.

1. It is known (cf., e.g. [3, p. 388 theorem 10.2]) that whenever (1) is disconjugate on $[a,\infty)$ there exists a nontrivial prepared (cf. [1, p 99]) solution of the associated differential matrix system

$$Y'' + Q(t)Y = 0 \tag{2}$$

such that $Y(t)$ is non-singular in (a,∞). In this case

$$V(t) \equiv Y'(t)Y^{-1}(t) \qquad t \in (a,\infty) \tag{3}$$

will be symmetric and $V^2(t) \geq 0$ (ie. $V^2(t)$ is non-negative definite).

Conjecture (cf. [4]). The criterion

$$\lim_{t\to\infty} \lambda_1\{\int_0^t Q(s)ds\} = \infty \tag{4}$$

implies (1) is oscillatory.

It should be mentioned here that the criterion

$$\lim_{t\to\infty} tr\{\int_0^t Q(s)ds\} = \infty \tag{5}$$

does indeed imply that (1) is oscillatory, (cf.[1, p. 101]). However (4) is, in general, weaker than (5). We refer the reader to the papers [4] , [5] , [6] for other discussions and results pertaining to the conjecture. In particular it is known that whenever $Q(t) \geq 0$ the conjecture is verified. On the other hand if $Q(t) \equiv Q$ is a constant matrix then (4) is equivalent to $\lambda_1(A) > 0$ and this, in turn, implies (1) is oscillatory (cf.,[5]).

2. The following result is obtained.

Theorem 1. Let $Q(t)$ satisfy the originally stated hypotheses and assume further that

$$\lim_{t\to\infty} \inf \frac{1}{t} \int_0^t tr\{\int_0^s Q(x)dx\}ds > -\infty \tag{6}$$

Then (4) implies (1) is oscillatory.

It is not known, in general, whether (6) may be waived or not. For example if $Q(t) = Q$ is a constant matrix (6) will be satisfied whenever $tr\, Q \geq 0$. On the other hand

$$\liminf_{t \to \infty} \frac{1}{t} \int_0^t \operatorname{tr} \{ \int_0^s Q(x)dx\}ds = -\infty \qquad (7)$$

will hold whenever $\operatorname{tr} Q < 0$, Q a constant matrix. The conjecture would be completely verified if theorem 1 had a counterpart with (6) replaced by (7).

The proof of theorem 1 depends upon the formulation of matrix analogs of some non-oscillation theorems of Hartman [2] .

Lemma 1. With $Q(t)$ satisfying the usual conditions assume that (1) is non-oscillatory at ∞, [This means that there exists $a > 0$ such that (1) is disconjugate on $[a,\infty)$].

Then a necessary and sufficient condition that

$$\lim_{t\to\infty} \| \int_0^t V^2(s)ds \| < \infty \qquad (8)$$

for every nontrivial prepared solution $Y(t)$ of (2) such that $\det Y(t) \neq 0$, $t \in (a,\infty)$, is that

$$\lim_{t\to\infty} \frac{1}{t} \int_0^t \operatorname{tr} \{ \int_0^s Q(x)dx\} ds = C \qquad (9)$$

exists and is finite.

As in [2] the proof of lemma 1 will show that (9) can be relaxed to (6). We will refer the reader to [2] for details.

The necessity part of lemma 1 can be strengthened as follows.

Corollary 1. A necessary condition that (8) should hold is that

$$\liminf_{t \to \infty} \frac{1}{t} \int_0^t g\{ \int_0^s Q(x)dx\} ds > -\infty \qquad (10)$$

for every positive linear functional $g: S \to \mathbb{R}$.

A linear functional $g: S \to \mathbb{R}$ will be *positive* if $g(A) > 0$ whenever $A > 0$.

Lemma 2. Suppose that (1) is non-oscillatory at ∞, and let $V(t)$ be as in lemma 1. Then (4) will imply that

$$\lim_{t\to\infty} \lambda_1 \{ \int^t V^2(s)ds \} = \infty \tag{11}$$

which is equivalent to the negation of (8).

The proof of theorem 1 can now be reconstructed as it proceeds by assuming the contrary and ending with a contradiction by applying lemma 2 and noting that (6) implies (8) via lemma 1.

References

1. G.J. Etgen and J.F. Pawlowski, Oscillation criteria for second order self-adjoint differential systems, Pacific J. Math. 66 (1976), 99-110.

2. P. Hartman, On nonoscillatory linear differential equations of the second order, Amer. J. Math. 74 (1952), 389-400.

3. _____, Ordinary differential equations, S.M. Hartman, Baltimore 1973.

4. D. Hinton and R.T. Lewis, Oscillation theory for generalized second order differential equations, to appear in Rocky Mtn. J. Math.

5. A.B. Mingarelli, A note on an oscillation criterion for self-adjoint second order differential systems, submitted.

6. _____, On a conjecture for oscillation of second order ordinary differential systems, submitted.

The University of Ottawa, Ottawa, Ontario, K1N 9B4.

Received October 8, 1980

C. R. Math. Rep. Acad. Sci. Canada - Vol. II (1980) No. 6

A NOTE ON FINITELY PRESENTED LATTICES

by

G. Grätzer, F.R.S.C. and A.P. Huhn

Abstract: A new proof is given of a theorem of R. Freese and J. B. Nation, namely, that the group of automorphisms of a finitely presented lattice is finite. The proof is based on the Structure Theorem of Finitely Presented Lattices of G. Grätzer, A. P. Huhn, and E. Lakser.

1. Introduction. Solving Problem 12 of [2] (repeated as Problem 34 of [3]), R. Freese and J. B. Nation in [1] obtained the following result:

Theorem. The automorphism group of a finitely presented lattice is finite.

It should be pointed out that for modular lattices the situation is different, see [5].

[1]The research of both authors was supported by the N.S.E.R.C. of Canada.

The key to this theorem is Lemma 1 of [1], asserting that for any finitely presented lattice L and to any element $d \in L$ there exists a homomorphism f of L onto a finite lattice B such that $f^{-1}(f(d)) = \{d\}$. A homomorphic image with a similar property has been associated with any finitely presented lattice in G. Grätzer, A. P. Huhn, and H. Lakser [4] in a very natural way and this homomorphic image can also be used to prove the Theorem. Our aim is to present this alternative proof.

It is interesting to compare the finite lattices constructed in [1] and in this note. For instance, if L is the free lattice on four generators and d is a free generator, then the finite lattice of [1] is the free distributive lattice on four generators while our construction yields a (four-generated) subdirect product of two copies of 2^4.

2. Proof of the Theorem. We need the following two lemmas about free lattices over partial lattices. Our Lemma 1 takes the place of Lemma 1 of [1]. Observe, that our Lemma 1 is very much easier, in fact, almost a triviality.

Lemma 1. Let P be a finite partial lattice and let $L = F(P)$ be the free lattice generated by P. Then there exists a congruence relation θ of L such that L/θ is finite, and, for all $p \in P$, we have $[p]\theta = \{p\}$.

Proof. For $x \in L$, let $x_P = (x] \cap P$ and $x^P = [x) \cap P$. Then the relation

$$x \equiv y \text{ iff } x_P = y_P \text{ and } x^P = y^P$$

was shown in [4] to be a congruence relation of L. Since there are only finitely many choices for x_P and x^P, the lattice L/θ is finite. $[P]\theta$ consists of all $x \in L$ with $x_P = x^P$, hence $[p]\theta = \{p\}$.

Lemma 2 (see, e.g., [1], [4]). Let $P = \{p_1,\ldots,p_m\}$ and $Q = \{q_1,\ldots,q_n\}$ be partial lattices, and let $F(P)$ and $F(Q)$ be the free lattices generated by P and Q, respectively. Then $F(P)$ and $F(Q)$ are isomorphic if and only if there exist polynomials $u_q(x_1,x_2,\ldots,x_m)$, $q \in Q$, and $v_p(y_1,y_2,\ldots,y_n)$, $p \in P$, satisfying the following conditions:

(1) the mapping $q \to u_q(p_1,p_2,\ldots,p_m)$, $q \in Q$, embeds Q into $F(P)$;

(2) the mapping $p \to v_p(q_1,q_2,\ldots,q_n)$, $p \in P$, embeds P into $F(Q)$;

(3) $v_p(u_{q_1}(p_1,\ldots,p_m),\ldots,u_{q_n}(p_1,\ldots,p_m)) = p$ holds in $F(P)$ for all $p \in P$;

(4) $u_q(v_{p_1}(q_1,\ldots,q_n),\ldots,v_{p_m}(q_1,\ldots,q_n)) = q$ holds in $F(Q)$ for all $q \in Q$.

An isomorphism of $F(P)$ onto $F(Q)$ is the extension of

the mapping of (2) to F(P). (This isomorphism will be denoted by g.) Its inverse is the extension of the mapping of (1) to F(Q).

Now we are ready to prove Theorem 1. We shall work in the lattice $L = F(P)$ of Lemma 1, where $P = \{p_1,\ldots,p_m\}$. By Lemma 2, the automorphisms of F(P), that is, isomorphisms of F(P) onto F(P) are in a one-to-one correspondence with pairs

$$\langle \{u_q \mid q \in P\}, \{v_p \mid p \in P\} \rangle$$

where the u_q and the v_p are polynomials over P satisfying conditions (1) to (4) with $P = Q$. We have to show now that the number of such pairs is finite (where two polynomials are considered equal iff they induce the same function over P). L/θ is finite, therefore, there exists a positive integer k such that, for any $[x]\theta, [y_1]\theta,\ldots,[y_m]\theta \in L/\theta$, if $[x]\theta = w([y_1]\theta,\ldots,[y_m]\theta)$ for some polynomial w, then there is a polynomial w' of rank $\leq k$ such that $[x]\theta = w'([y_1]\theta, [y_2]\theta,\ldots,[y_m]\theta)$. Assume that $\langle \{u_q \mid q \in P\}, \{v_p \mid p \in P\} \rangle$ is as described above. From (4), it follows that

$$u_q(v_{p_1}([q_1]\theta,\ldots,[q_m]\theta),\ldots,v_{p_m}([q_1]\theta,\ldots,[q_m]\theta)) = [q]\theta.$$

Thus one can choose polynomials u_q', $q \in Q$, of rank $\leq k$ with $u_q'(v_{p_1}([q_1]\theta,\ldots,[q_m]\theta),\ldots,v_{p_m}([q_1]\theta,\ldots,[q_m]\theta)) = [q]\theta$. By Lemma 1, $[q_1]\theta$ q consists of q only, thus $u_q'(v_{p_1}(q_1,\ldots,q_m),\ldots,v_{p_m}(q_1,\ldots,q_m)) = q$, that is, (4) holds

with the u_q' in place of the u_q. Now let g be as defined in Lemma 2. Then

$u_q'(p_1,\ldots,p_m) = u_q'(g(v_{p_1}(q_1,\ldots,q_m),\ldots,v_{p_m}(q_1,\ldots,q_m)) =$

$g(u_q'(v_{p_1}(q_1,\ldots,q_m),\ldots,v_{p_m}(q_1,\ldots,q_m))) = g(q)$, which proves (1) for u_q'. (3) can be proved similarly and (2) does not refer to the u_q. Using the same argument once again for the v_p, we conclude that the automorphisms of L are in a one-to-one correspondence with those pairs $\langle\{u_q' \mid q \in P\}, \{u_p' \mid p \in P\}\rangle$ satisfying (1) to (4) where the u_q' and the v_p' are of rank $\leq k$. Obviously, there are only finitely many such pairs, completing the proof of the Theorem.

Finally, we note that there are two more results in [1]: the isomorphism problem for lattices is solvable; the generalized word problem for lattices is solvable. Both these results can be proved using the alternative approach discussed above.

References

[1] R. Freese and J. B. Nation: Finitely presented lattices. Proc. Amer. Math. Soc. 77 (1979), 174-178.

[2] G. Grätzer: Lattice Theory: First Concepts and Distributive Lattices. W. H. Freeman and Co., San Francisco, Calif., 1971.

[3] G. Grätzer: General Lattice Theory. Pure and Applied Mathematics Series, Academic Press, New York, N. Y.; Mathematische Reihe, Band 52, Birkhäuser Verlag, Basel; Akademie Verlag, Berlin, 1978.

[4] G. Grätzer, A. P. Huhn, and H. Lakser: On the structure of finitely presented lattices. (To appear in Canad. J. Math.)

[5] A. P. Huhn: On G. Grätzer's problem concerning automorphisms of a finitely presented lattice. Algebra Universalis 5 (1975), 65-71.

University of Manitoba
Winnipeg, Manitoba
Canada R3T 2N2

and

Bólyai Intézet
6720 Szeged
Hungary

Received October 8, 1980

C. R. Math. Rep. Acad. Sci. Canada - Vol. II (1980) No. 6

POLYNOMIALS WITH D_5 (RESP. A_5) AS GALOIS GROUP

C.U. Jensen and N. Yui

Presented by P. Ribenboim, F.R.S.C.

1. Shafarevich [4] has shown that any finite solvable group G can be realized as a Galois group over the rational number field $\mathbb{Q}$. The actual realization, however, is a non-trivial problem, even for groups of small order. In this paper we consider the case $G = D_5$ (the dihedral group of order 10). In [2] it is shown by class field theory that any imaginary quadratic field admits an infinite number of distinct embeddings in normal fields having D_5 as their Galois group. The (class field theoretic) proof is not useful to derive explicit numerical examples. It is therefore of interest to establish necessary and sufficient conditions for a monic quintic polynomial over $\mathbb{Q}$ to have D_5 as Galois group over $\mathbb{Q}$. As a byproduct of the theory developed for D_5, A_5 (the alternating group of order 60) can also be realized. We obtain a parametric family of quintic polynomials with dihedral Galois group. The detailed and generalized version of this work will appear in [2].

2. Let $f(x)$ be a monic polynomial of degree $n > 1$ over $\mathbb{Q}$ with integral coefficients. We denote by D_f the discriminant of $f(x)$ and by $\mathrm{Gal}(f)$ the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$. Assume that $f(x)$ is irreducible over $\mathbb{Q}$. Then $\mathrm{Gal}(f)$ is isomorphic to a transitive subgroup of S_n (the symmetric group of degree n). In fact, we have

THEOREM A. Let p be a prime not dividing D_f. Then the degrees of the irreducible factors of $f(x)$ mod p form a partition of n which is the cycle type of a permutation in $\mathrm{Gal}(f)$. Conversely, if an element of $\mathrm{Gal}(f)$ is expressed as the product of r cycles of length $\ell_1, \ell_2, \ldots, \ell_r$ with $\sum_{i=1}^{r} \ell_i = n$, then the set

$$M(\ell_1,\ell_2,\ldots,\ell_r) = \left\{ p:\text{prime} \;\middle|\; \begin{array}{l} p \nmid D_f,\ f(x) \bmod p = \prod_{i=1}^{r} f_i(x) \\ \text{where } f_i(x) \in \mathbb{F}_p[x] \text{ with} \\ \deg f_i = \ell_i \end{array} \right\}$$

has positive density.

3. Let $f(x)$ be a monic quintic polynomial over $\mathbb{Q}$ with integral coefficients. We assume that $f(x)$ is irreducible over $\mathbb{Q}$ and that D_f is a perfect square. Then there are three possibilities for $\mathrm{Gal}(f)$, namely, $\mathrm{Gal}(f) \cong A_5$, D_5 or Z_5 (the cyclic group of order 5). Then we have as special cases of THEOREM A the following

PROPOSITION B.

$$\mathrm{Gal}(f) \cong Z_5 \iff \left[\begin{array}{l} M(1,1,1,1,1) \neq \emptyset\ (\tfrac{1}{5}),\ M(5) \neq \emptyset\ (\tfrac{4}{5}) \text{ and} \\ M(\ell_1,\ell_2,\ldots,\ell_r) = \emptyset \text{ for any other} \\ \text{partition } (\ell_1,\ell_2,\ldots,\ell_r) \text{ of } n \end{array} \right].$$

$$\mathrm{Gal}(f) \cong D_5 \iff \left[\begin{array}{l} M(1,1,1,1,1,) \neq \emptyset\ (\tfrac{1}{10}),\ M(1,2,2) \neq \emptyset\ (\tfrac{1}{2}) \\ M(5) \neq \emptyset\ (\tfrac{2}{5}) \text{ and } M(\ell_1,\ell_2,\ldots,\ell_r) = \emptyset \\ \text{for any other partition } (\ell_1,\ell_2,\ldots,\ell_r) \\ \text{of } n \end{array} \right].$$

$$\mathrm{Gal}(f) \cong A_5 \iff \left[\begin{array}{l} M(1,1,1,1,1) \neq \emptyset \ (\tfrac{1}{60}),\quad M(1,2,2) \neq \emptyset \ (\tfrac{1}{4}), \\ M(1,1,3) = \emptyset \ (\tfrac{1}{3}),\quad M(5) \neq \emptyset \ (\tfrac{2}{5}) \ \text{and} \\ M(\ell_1,\ell_2,\ldots,\ell_r) = \emptyset \ \text{for any other} \\ \text{partition} \ (\ell_1,\ell_2,\ldots,\ell_r) \ \text{of} \ n \end{array}\right].$$

(The numbers in the brackets indicate the corresponding densities.)

4. Here we give a practical method of realizing D_5 (resp. A_5) as a Galois group over $\mathbb{Q}$.

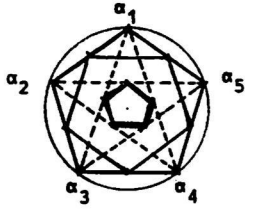
THEOREM C. Let $f(x)$ be a monic quintic polynomial over $\mathbb{Q}$. Assume that $\mathrm{Gal}(f) \not\cong Z_5$. Then necessary and sufficient conditions for $\mathrm{Gal}(f) \cong D_5$ (resp. A_5) are the following:

(1) $f(x)$ is irreducible over $\mathbb{Q}$.

(2) The discriminant D_f is a perfect square.

(3) The polynomial $P_{10}(x) = \prod_{1\le i<j\le 5} \{x-(\alpha_i+\alpha_j)\} \in \mathbb{Q}[x]$ has distinct zeros and decomposes into the product of two irredicible quintic polynomials over $\mathbb{Q}$ (resp. $P_{10}(x)$ is irreducible over $\mathbb{Q}$). Here $\{\alpha_i\}$ is the set of zeros of $f(x)$ (in $\mathbb{C}$).

REMARKS. (a) A geometric interpretation of the condition (3) is given as follows. We make use of the fact that D_5 is the symmetry group of the regular pentagon. We identify the points on the plane with the zeros $\{\alpha_i\}$ of $f(x)$ and the sums $\{\alpha_i+\alpha_j,\ 1\le i<j\le 5\}$ with the lines $\overline{\alpha_i\alpha_j}$. Now D_5 acts intransitively on the set of $\binom{5}{2}=10$ lines with 2 orbits, both of length 5, with multiplicity 2.



While A_5 acts transitively on this set of 10 lines.

(b) If $f(x) = x^5 + ax + b \in \mathbb{Q}[x]$, then $f(x)$ has at most three real zeros and only one if $a > 0$. Consequently, $\mathrm{Gal}(f)$ cannot be isomorphic to $\mathbb{Z}_5$. The condition (2) implies that $\mathrm{Gal}(f) \subseteq A_5$, and hence $f(x)$ can have only one real zero. In this case, the polynomial $P_{10}(x)$ can be expressed as

$$P_{10}(x) = x^{10} - 3ax^6 - 11bx^5 - 4a^2x^2 + 4abx - b^2 \in \mathbb{Z}[a,b][x] .$$

5. Now we confine ourselves to the trinomials of the Bring-Jerrard form : $f(x) = x^5 + ax + b \in \mathbb{Q}[x]$. Using the criterion for solvability by radicals given by Weber [5] p.676, we have

THEOREM D. Let $f(x) = x^5 + ax + b \in \mathbb{Q}[x]$. Then necessary and sufficient conditions for $\mathrm{Gal}(f) \cong D_5$ (resp. A_5) are given as follows:

(1) $f(x)$ is irreducible over $\mathbb{Q}$.

(2) The discriminant $D_f = 4^4a^5 + 5^5b^4$ is a perfect square.

(3) The coefficients a and b are of the form (resp. are not of the form):

$$a = \frac{3125\,\lambda\mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)} \quad ; \quad b = \frac{3125\,\lambda\mu^5}{(\lambda-1)^4(\lambda^2-6\lambda+25)}$$

with $\lambda, \mu \in \mathbb{Q}$, $\lambda \neq 1$; $\mu \neq 0$.

The polynomial $f(x)$ in THEOREM D with dihedral Galois group can be considered as a generic polynomial over $\mathbb{Q}(\lambda)$ with a parameter λ. Hence we have obtained

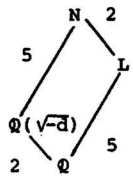
THEOREM E. There exists a parametric family of quintic polynomials of the Bring-Jerrard form with Galois group D_5.

(The detailed study of this parametric family has been carried out in Roland, Yui and Zagier [3].)

6. Here we give some examples of polynomials with Galois group D_5 (resp. A_5)

$f(x)$	D_f	λ	μ	$P_{10}(x)$	Gal(f)
$x^5-5x+12$	$(2^6 5^3)^2$	-5	$-\frac{12}{5}$	$(x^5-5x^3-10x^2+30x-36)$ $\cdot(x^5+5x^3+10x^2+10x+4)$	D_5
$x^5+11x+44$	$(2^7 11^2 7)^2$	11	4	$(x^5-11x^3-22x^2+66x-44)$ $\cdot(x^5+11x^3+22x^2+22x+44)$	D_5
$x^5+20x+32$	$(2^9 5^3)^2$	5	$\frac{8}{5}$	$(x^5+10x^3+20x^2+64)$ $\cdot(x^5-10x^3-20x^2+40x-16)$	D_5
$x^5+20x+16$	$(2^8 5^3)^2$			$x^{10}-60x^6-176x^5-1600x^2$ $+1280x-256$	A_5
$x^5+95x+76$	$(2^5 5^3 19^2)^2$			$x^{10}-285x^6-836x^5-36100x^2$ $+28880x-5776$	A_5

7. Let $f(x) = x^5 + ax + b \in \mathbb{Q}[x]$. Assume that $f(x)$ is irreducible over $\mathbb{Q}$. Let $L = \mathbb{Q}[\alpha]/(f(\alpha))$ be the field defined by $f(x)$ and let N be its normal closure (the splitting field of $f(x)$ over $\mathbb{Q}$). If $Gal(f) \cong D_5$, then N contains a uniquely determined imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. In fact, we have



THEOREM F. The quadratic fields contained in the splitting fields of the first three polynomials listed in 6 are $\mathbb{Q}(\sqrt{-10})$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-5})$. In these cases the above splitting fields are ring class fields, but not Hilbert (absolute) class fields over the corresponding imaginary quadratic fields. (For the last assertion, cf. [1].)

8. We give a necessary condition for a normal extension over $\mathbb{Q}$ to have dihedral Galois group.

THEOREM G. Let $p \equiv 1 \pmod 4$ be a prime and assume that p is regular (i.e, p does not divide the class number of the pth cyclotomic field). If N is a normal extension of $\mathbb{Q}$ with Galois group $\cong D_{pn}$, $n \in \mathbb{N}$, then the discriminant of N over $\mathbb{Q}$ is not a power of p.

REFERENCES

[1] C.U. Jensen, Remark on a characterization of certain ring class fields by their absolute Galois group, Proc. Amer. Math. Soc. Vol. 14, No.5 (1963) 738-741.

[2] C.U. Jensen and N. Yui, Polynomials with D_p as Galois group, Preprint (1980).

[3] G. Roland, N. Yui and D. Zagier, A parametric family of quintic polynomials with Galois group D_5, Preprint (1980).

[4] I. Shafarevich, Constructions of fields of algebraic numbers with given solvable Galois group, Izv. Akad. Nauk. SSSR, Ser. Mat. 18 (1954) 525-578.

[5] H. Weber, Lehrbuch der Algebra, Chelsea, New York.

C.U. Jensen : Matematisk Institut, Københavns Universitet
Universitetsparken 5, 2100, København Ø, Denmark

N. Yui : Fachbereich Mathematik, Universität des Saarlandes
D-6600, saarbrücken, West Germany

Received October 17, 1980

C. R. Math. Rep. Acad. Sci. Canada - Vol. II (1980) No. 6

ON THE SECOND COMMUTATOR SUBGROUP OF $PGL_2(\mathbb{Z})$

Wan Zhe-xian and Wu Xiao-lung

Presented by H.S.M. Coxeter, F.R.S.C.

Let $GL_2(\mathbb{Z})$ denote the group formed by all 2×2 invertible matrices over the ring $\mathbb{Z}$ of rational integers. Clearly the center of $GL_2(\mathbb{Z})$ is $\{\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\}$. Denote the factor group of $GL_2(\mathbb{Z})$ modulo its center by $PGL_2(\mathbb{Z})$ and denote the commutator subgroup of $PGL_2(\mathbb{Z})$ by $PGL_2(\mathbb{Z})'$. It is known (cf. [1], §7.2, pp. 85-86) that (1) $PGL_2(\mathbb{Z})$ is generated by the following three elements

$$S = \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \quad T = \pm\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad \text{and} \quad J = \pm\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},$$

with defining relations

$$S^2 = J^2 = (JS)^2 = (JT)^2 = (ST)^3 = I,$$

where I denotes the identity element of $PGL_2(\mathbb{Z})$, and (2) $PGL_2(\mathbb{Z})'$ is generated by the following two elements

$$U = \pm\begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix} \quad \text{and} \quad V = \pm\begin{pmatrix}1 & 1\\ -1 & 0\end{pmatrix}$$

with defining relations

$$U^3 = V^3 = I.$$

Denote the commutator subgroup of $PGL_2(\mathbb{Z})'$ by $PGL_2(\mathbb{Z})''$. The purpose of the present note is to prove that $PGL_2(\mathbb{Z})''$ is a free group generated by four elements and the factor group

$PGL_2(\mathbb{Z})'/PGL_2(\mathbb{Z})''$ is an abelian group of order 9 and type (3, 3).

Theorem 1. $PGL_2(\mathbb{Z})'/PGL_2(\mathbb{Z})''$ is an abelian group of order 9 and of type (3, 3).

Proof. Let

$$H = \{X \in PGL_2(\mathbb{Z})' \mid \text{the sum of exponents of } U \text{ in the product expression of } X \text{ in } U \text{ and } V \equiv \text{the sum of exponents of } V \text{ in the product expression of } X \equiv 0 \pmod 3\}.$$

Since all relations in U and V are consequences of $U^3 = V^3 = I$, H is well-defined. Since conjugation does not alter both the sum of exponents of U and the sum of exponents of V in the product expression of an element of $PGL_2(\mathbb{Z})'$, H is a normal subgroup of $PGL_2(\mathbb{Z})'$. There are exactly 9 cosets of H in $PGL_2(\mathbb{Z})'$, namely

$$U^2V^2H,\ U^2VH,\ U^2H,\ UV^2H,\ UVH,\ UH,\ V^2H,\ VH,\ H\ ,$$

thus $PGL_2(\mathbb{Z})' : H = 9$ and $PGL_2(\mathbb{Z})'/H$ is an abelian group of order 9 and type (3, 3).

Obviously $PGL_2(\mathbb{Z})'' \subseteq H$. We are going to prove that $H \subseteq PGL_2(\mathbb{Z})''$. Let X be an arbitrary element of H. Since $U^3 = V^3 = I$, we can assume that every exponent of U and V in the product expression of X in U and V is 1 or 2. Clearly, such an expression of X is necessarily unique. We may denote the sum of its exponents by $n(X)$. Let

$$H_m = \{X \in H | n(X) = m\} \quad .$$

It is obvious that $m \equiv 0 (\mathrm{mod}\ 3)$. Thus we may write $m = 3k$. We have $H = \bigcup_{k=0}^{\infty} H_{3k}$. We use induction on k to prove that $H_{3k} \subset PGL_2(\mathbb{Z})''$ for $k = 0, 1, 2, \ldots$.

For $k = 0$, $H_0 = \{I\} \subset PGL_2(\mathbb{Z})''$.

For $k = 1$, H_3 is an empty set.

Consider the case $k = 2$. Without loss of generality, we can assume that the first factor occurring in $X \in H_6$ is U (the case that the first factor is V can be treated similarly). Thus X has the following seven possibilities:

$$X_1 = U^2V^2UV \qquad X_2 = U^2VUV^2$$
$$X_3 = UV^2U^2V \qquad X_4 = UVU^2V^2$$
$$X_5 = UVUVUV = X_4X_2^{-1}X_1$$
$$X_6 = UV^2UVU = X_3X_1^{-1}$$
$$X_7 = UVUV^2U = X_4X_2^{-1}.$$

X_1, X_2, X_3, X_4 are commutators, thus they belong to $PGL_2(\mathbb{Z})''$. Consequently, X_5, X_6 and X_7 also belong to $PGL_2(\mathbb{Z})''$. Thus $H_6 \subset PGL_2(\mathbb{Z})''$.

Now we assume $k \geq 3$ and $H_{3k'} \subset PGL_2(\mathbb{Z})''$ for every $k' < k$. Let X be any element of H_{3k}. If we can prove that there exist Y and $Z \in H$ with the properties $n(Y) < n(X)$, $n(Z) < n(X)$ such that $X = YZ$, then by induction hypothesis we have $Y, Z \in PGL_2(\mathbb{Z})''$, and consequently $X \in PGL_2(\mathbb{Z})''$. We assume the first factor occurring in X is U (the case that the first factor is V can be treated similarly). Define $\ell(X)$ and $m(X)$ to be the sum of exponents of U and the sum of exponents

of V in the product expression of X in U, V respectively (of course, we assume the exponents of U and V are either 1 or 2). Obviously, we have $\ell(X) + m(X) = n(X) = 3k$. Write $X = X_1X_2$, where $n(X_1) = 6$, $n(X_2) = 3k-6$, then $(\ell(X_1), m(X_1)) = (3, 3), (4, 2)$ or $(2, 4)$. We distinguish these three cases.

i) $\ell(X_1) = m(X_1) = 3$. We may take $Y = X_1$, $Z = X_2$.

ii) $\ell(X_1) = 4$, $m(X_1) = 2$. Then we have necessarily $X_1 = Y_1U$ or $X_1 = Y_1UV$. If $X_1 = Y_1U$, then $X = Y_1UX_2 = (Y_1V)(V^2UX_2)$, and we may take $Y = Y_1V$, $Z = V^2UX_2$. If $X_1 = Y_1UV$, then $X = (Y_1V^2)(VUVX_2)$, and we may take $Y = Y_1V^2$, $Z = VUVX_2$.

iii) $\ell(X_1) = 2$, $m(X_2) = 4$. Then we have necessarily $X_1 = Y_1V$, thus $X = (Y_1U)(U^2VX_2)$, and we may take $Y = Y_1U$, $Z = U^2VX_2$. Therefore we have proved $H_{3k} \subset PGL_2(\mathbb{Z})''$.

Consequently, $H = \bigcup_{k=0}^{\infty} H_{3k} \subseteq PGL_2(\mathbb{Z})''$, thus $H = PGL_2(\mathbb{Z})''$ and $PGL_2(\mathbb{Z})'/PGL_2(\mathbb{Z})''$ is an abelian group of order 9 and type (3, 3).

Corollary. $PGL_2(\mathbb{Z})''$ consists of those elements of $PGL_2(\mathbb{Z})'$ such that the sums of exponents of both U and V in their product expressions are both $\equiv 0 \pmod 3$.

Theorem 2. $PGL_2(\mathbb{Z})''$ is a free non-abelian group generated by four independent elements.

Proof. By the proof of the above theorem, we know that $PGL_2(\mathbb{Z})''$ is generated by the following eight elements

$$X_1 = U^2V^2UV \qquad Y_1 = V^2U^2VU$$
$$X_2 = U^2VUV^2 \qquad Y_2 = V^2UVU^2$$
$$X_3 = UV^2U^2V \qquad Y_3 = VU^2V^2U$$
$$X_4 = UVU^2V^2 \qquad Y_4 = VUV^2U^2.$$

Since $Y_1 = X_1^{-1}$, $Y_2 = X_3^{-1}$, $Y_3 = X_2^{-1}$, $Y_4 = X_4^{-1}$, we know that $PGL_2(\mathbb{Z})^n$ is generated by X_1, X_2, X_3 and X_4. We want to prove that any relation of X_1, X_2, X_3 and X_4 is trivial, i.e., is a consequence of relations of the form

$$X_i X_i^{-1} = I \quad \text{or} \quad X_i^{-1} X_i = I \qquad (i = 1, 2, 3, 4) \ .$$

Suppose there is a relation

$$X_{i_1}^{e_1} X_{i_2}^{e_2} \cdots X_{i_n}^{e_n} = I, \ i_r \in \{1, 2, 3, 4\}, \ e_r \in \{\pm 1\}, \ r = 1, 2, 3, \ldots, n \qquad (R)$$

We call n the length of (R). We use induction on n to prove that (R) is trivial.

Since $X_i^{\pm 1} \neq I$ $(i = 1, 2, 3, 4)$, there is no relation of length 1.

Assume the length of (R) is 2. Then we have $X_{i_2}^{e_2} = (X_{i_1}^{e_1})^{-1}$. We necessarily have $i_2 = i_1$, $e_2 = -e_1$. Thus (R) is trivial.

Now assume $n > 2$ and every relation in X_1, X_2, X_3 and X_4 of length $< n$ is trivial. If there is an s $(1 \leq s < n)$ such that $X_{i_s}^{e_s} = X_{i_{s+1}}^{-e_{s+1}}$, then $X_{i_s}^{e_s} X_{i_{s+1}}^{e_{s+1}} = I$ and (R) becomes

$$X_{i_1}^{e_1} \cdots X_{i_{s-1}}^{e_{s-1}} X_{i_{s+2}}^{e_{s+2}} \cdots X_{i_n}^{e_n} = I \ ,$$

which is a relation of length $n-2$ and thus is trivial by induction hypothesis. Hence (R) is trivial, too. Thus without loss of generality we can assume that $X_{i_r}^{e_r} \neq X_{i_{r+1}}^{-e_{r+1}}$, $i = 1, 2, \ldots, n-1$. But for any $i, j, k \in \{1, 2, 3, 4\}$ with $i \neq k$, in the simplest product expression of $X_i X_j$ or $X_i X_k^{-1}$, the first two factors coincide with the first two factors of X_i, the last two factors coincide with the last two factors of X_j or

X_k^{-1}, and the middle four factors cannot be wholly cancelled out. Thus, if we substitute the product expression of every X_{i_r} in U, V into (R), then (R) becomes

$$U^{s_1}V^{t_1} \ldots = I \qquad (R')$$

or

$$V^{s_1}U^{t_1} \ldots = I \ .$$

We consider the first case only, since the second case can be treated similarly. Since every relation in U, V is a consequence of $U^3 = V^3 = I$, in the left-hand of (R'), the first two factors must be the inverses of the last two factors correspondingly, i.e., (R') is of the form

$$U^{s_1}V^{t_1} \ldots V^{3-t_1}U^{3-s_1} = I \ .$$

If (R) starts with $X_{i_1}^{e_1} = U^{s_1}V^{t_1}U_r^{3-s_1}V^{3-t_1}$, then $X_{i_n}^{e_n}$ ending with $V^{3-t_1}U^{3-s_1}$ is necessarily $X_{i_1}^{-e_1}$, i.e., $X_{i_n}^{e_n} = X_{i_1}^{-e_1}$. Thus cancelling out $X_{i_1}^{e_1}$ and $X_{i_n}^{e_n}$, we obtain

$$X_{i_2}^{e_2} \ldots X_{i_{n-1}}^{e_{n-1}} = I \ ,$$

which is trivial by induction hypothesis. Hence (R) is also trivial.

Reference

[1] H. S. M. Coxeter and W. O. J. Moser, Generators and Relations for Discrete Groups, 3rd, ed., Springer, 1972.

Institute for Advanced Study,
Princeton, New Jersey,
U.S.A.

Institute of Mathematics,
Academia Sinica,
Beijing, China.

Received October 23, 1980.

C. R. Math. Rep. Acad. Sci. Canada - Vol. II (1980) No. 6

A REMARK ON STRIPS, I

Peter Scherk, F.R.S.C.

Introduction. In a recent paper, Nomizu [3] studied two m-dimensional manifolds μ and ν in euclidean n-space E^n. He proved that μ can be rolled onto ν along a given curve X on μ. For this rolling, only ν and the m-strip on μ along X seem to be relevant, i.e. the pair consisting of X and the family of the tangent spaces of μ along X. This leads to the question of the rollability of one m-strip onto another. This turns out to be possible if and only if their two curves have the same tangential curvature tensors in corresponding points. Nomizu's theorem is – at least locally – a corollary of this result. – The case $n = 3$, $m = 2$ ought to be well known; cf. [1, 78f] and [2, 78].

In this context it is convenient not to use the language of covariant differentiation and tangential curvature tensors but to speak of tangential and normal derivatives and the Frenet matrices of moving frames.

In this note we develop the necessary apparatus on strips.

1. Strips

1.1 Let V^n denote the n-dimensional euclidean vector space. Let $1 \leq m < n$. An m-strip or strip in E^n is a family

$$\sigma = \{X(s), T(s)\}, \qquad s \in J,$$

of pairs. Here s ranges through an interval J. The curve $\underset{\sim}{X}(s)$ in E^n is continuously differentiable with respect to its arc length s. $T = T(s)$ is an m-space in V^n depending continuously on s such that $\underset{\sim}{X}'(s) \in T(s)$ for all $s \in J$. We call $T(s)$ the tangent vector space of σ at s. The normal vector space $N = N(s) = \{\underset{\sim}{x} \in V^n \mid \underset{\sim}{x} \perp T(s)\}$ will also depend continuously on s.

1.2 The decomposition $V^m = T \oplus N$ determines for each s two orthogonal projections $\pi_T = \pi_{T(s)} : V^n \to T(s)$ and $\pi_N = \pi_{N(s)} : V^n \to N(s)$; thus $\underset{\sim}{x} = \pi_T \underset{\sim}{x} + \pi_N \underset{\sim}{x}$ for every $s \in J$ and every $x \in V^n$.

Suppose the function $\underset{\sim}{x}(s)$ from J into V^n is differentiable in J. Then

$$D_T \underset{\sim}{x}(s) = \pi_T \underset{\sim}{x}'(s) = \lim_{t \to s} \pi_{T(s)} \frac{\underset{\sim}{x}(t) - \underset{\sim}{x}(s)}{t - s}$$

is the tangential derivative of our function at s. Similarly define $D_N \underset{\sim}{x}(s) = \pi_N \underset{\sim}{x}'(s)$. Thus $D_T \underset{\sim}{x}(s) + D_N \underset{\sim}{x}(s) = \underset{\sim}{x}'(s)$.

1.3 Suppose the vector function

$$\underset{\sim}{x}_1(s) = \underset{\sim}{X}'(s) \in V^n, \qquad s \in J,$$

is n-times continuously differentiable and the vectors

$$\underset{\sim}{x}_1 , D_T \underset{\sim}{x}_1 , \ldots , D_T^{m-1} \underset{\sim}{x}_1 \tag{1.2}$$

are linearly independent for every $s \in J$. Then σ has a moving tangential frame, i.e. there is for each $s \in J$ an

orthonormal base

$$\underset{\sim}{x}_1(s) = \underset{\sim}{X}'(s),\ \underset{\sim}{x}_2(s),\ldots,\ \underset{\sim}{x}_m(s) \tag{1.3}$$

of $T(s)$ satisfying the tangential Frenet formulas

$$\begin{aligned}
D_T\underset{\sim}{x}_1 &= \kappa_1\underset{\sim}{x}_2 \\
D_T\underset{\sim}{x}_2 &= -\kappa_1\underset{\sim}{x}_1 + \kappa_2\underset{\sim}{x}_3 \\
D_T\underset{\sim}{x}_3 &= -\kappa_2\underset{\sim}{x}_2 + \kappa_3\underset{\sim}{x}_4 \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
D_T\underset{\sim}{x}_{m-1} &= -\kappa_{m-2}\underset{\sim}{x}_{m-2} + \kappa_{m-1}\underset{\sim}{x}_m \\
D_T\underset{\sim}{x}_m &= -\kappa_{m-1}\underset{\sim}{x}_{m-1}\ .
\end{aligned}$$

The vectors (1.3) and the scalar functions $\kappa_j = \kappa_j(s)$ are uniquely determined up to their signs. We call the matrix of the above set of differential equations the tangential Frenet matrix of σ.

Remarks. (i) The tangent spaces $X(s) + T(s) \subset E^n$ generate for $m \leq \frac{n}{2}$ and envelop for $m > \frac{n}{2}$ a ruled manifold. Its intrinsic geometry is determined by the tangential Frenet matrices of σ.

(ii) For every $s \in J$, the tangential Frenet matrix describes a linear transformation $D_T : T(s) \to T(s)$. Let $\langle\ ,\ \rangle$ denote in these notes the scalar product in V^n. Then D_T determines the bilinear form

$$\begin{cases} T \times T \longrightarrow \mathbb{R} \\ (\underset{\sim}{x}, \underset{\sim}{y}) \longmapsto \langle D_T\underset{\sim}{x}, y\rangle, \end{cases}$$

the tangential curvature tensor of σ at s.

2. Normal Frenet Matrices

2.1 Suppose there is an $(n-m)$-times continuously differentiable vector function $\underset{\sim}{x}_{m+1}$ such that $\underset{\sim}{x}_{m+1}(s) \in N(s)$ and $|\underset{\sim}{x}_{m+1}(s)| = 1$ for all $s \in J$ and that the vectors

(2.1) $$\underset{\sim}{x}_{m+1}, D_N\underset{\sim}{x}_{m+1}, \ldots, D_N^{n-m-1}\underset{\sim}{x}_{m+1}$$

are always linearly independent. Then $\underset{\sim}{x}_{m+1}$ determines an – orthonormal – moving normal frame

(2.2) $$\underset{\sim}{x}_{m+1}(s), \ldots, \underset{\sim}{x}_{m}(s)$$

of σ satisfying the normal Frenet formulas

$$\begin{aligned}
D_N\underset{\sim}{x}_{m+1} &= \kappa_{m+1}\underset{\sim}{x}_{m+2}\\
D_N\underset{\sim}{x}_{m+2} &= -\kappa_{m+1}\underset{\sim}{x}_{m+1} \quad \kappa_{m+2}\underset{\sim}{x}_{m+3}\\
&\cdots\cdots\cdots\cdots\\
D_N\underset{\sim}{x}_{n-1} &= -\kappa_{n-2}\underset{\sim}{x}_{n-2} + \kappa_{n-1}\underset{\sim}{x}_{n}\\
D_N\underset{\sim}{x}_{n} &= -\kappa_{n-1}\underset{\sim}{x}_{n-1}.
\end{aligned}$$

The vectors (2.2) form a base of $N(s)$. The matrix of these equations is a normal Frenet matrix of σ.

2.2 For $m = n-1$, the vector $\underset{\sim}{x}_n$ is uniquely determined up to its sign. Let $m < n-1$.

While the maps $D_{N(s)} : N(s) \to N(s)$ are independent of the choice of $\underset{\sim}{x}_{m+1}$, this is not true of the normal Frenet

matrices. Suppose both $\underset{\sim}{x}_{m+1}(s)$ and $\underset{\sim}{y}_{m+1}(s)$ satisfy the assumptions of 2.1. Let $\kappa_{m+1}, \ldots, \kappa_n$ and $\lambda_{m+1}, \ldots, \lambda_n$ denote the coefficients of the normal Frenet matrices K and λ belonging to $\underset{\sim}{x}_{m+1}$ and $\underset{\sim}{y}_{m+1}$, respectively. Thus

$$\kappa_i = \langle D_N \underset{\sim}{x}_i , \underset{\sim}{x}_{i+1} \rangle \quad , \quad \lambda_i = \langle D_N \underset{\sim}{y}_i , \underset{\sim}{y}_{i+1} \rangle$$

$$K = K(s) = -K^{tr} = (\langle D_N \underset{\sim}{x}_i , \underset{\sim}{x}_j \rangle)_{i,j=m+1,\ldots,n}$$

and $\Lambda = (\langle D_N \underset{\sim}{y}_i , \underset{\sim}{y}_j \rangle)_{i,j=m+1,\ldots,n}$.

To every $s \in J$ there is an orthogonal matrix

$$\Gamma = \Gamma(s) = (\gamma_{ij})_{i,j=m+1,\ldots,n} \tag{2.3}$$

such that $\underset{\sim}{x}_i = \sum_{m+1}^{n} \gamma_{ij} \underset{\sim}{y}_j$, hence $\underset{\sim}{y}_i = \sum_{m+1}^{n} \gamma_{ji} \underset{\sim}{x}_j$ $(i = m+1, \ldots, n)$. Each $\gamma_{ij} = \langle \underset{\sim}{x}_i , \underset{\sim}{y}_j \rangle$ is continuously differentiable. As

$$\gamma_{ij} = \langle D_N \underset{\sim}{x}_i , \underset{\sim}{y}_j \rangle + \langle \underset{\sim}{x}_i , D_N \underset{\sim}{y}_j \rangle ,$$

we obtain

$$\Gamma' = K\Gamma - \Gamma\Lambda . \tag{2.4}$$

2.3 We next verify that every continuous skew-symmetric matrix function

$$\Lambda = \Lambda(s) = \begin{pmatrix} 0 & \lambda_{m+1} & & & \\ -\lambda_{m+1} & 0 & \ddots & & \\ & \ddots & \ddots & \ddots & \\ & & \ddots & 0 & \lambda_{n-1} \\ & & & -\lambda_{n-1} & 0 \end{pmatrix}$$

is the normal Frenet matrix of σ with respect to some suitable y_{m+1}.

It is sufficient to prove: Given the skew-symmetric continuous $(n-m) \times (n-m)$ matrix functions K and Λ, (2.4) has an orthogonal solution Γ.

Let $s_0 \in J$ and let A_0 be a constant orthogonal matrix. Then there exists a unique matrix function $A = A(s)$ defined in J and satisfying $A' = KA$, $A(s_0) = A_0$. Then $A(s)$ is orthogonal for all s. Similarly, the differential equation $B' = -B\Lambda$ or $(B^{tr})' = \Lambda B^{tr}$ has an orthogonal solution $B(s)$ in J. The matrix function $\Gamma = AB$ is orthogonal and satisfies (2.4).

REFERENCES

[1] Appell, P. Traité de mécanique rationelle, vol. 1 (1919).

[2] Blaschke, W. Vorlesungen über Differentialgeometrie. 3rd ed. Springer, Berlin, 1930.

[3] Nomizu, K. Kinematics and differential geometry of submanifolds, Tôhoku Math. J. 30 (1978), 623-637.

Department of Mathematics,
University of Toronto,
Toronto, Canada, M5S 1A1.

Received October 30, 1980

C. R. Math. Rep. Acad. Sci. Canada - Vol. II (1980) No. 6

A GENERALIZATION OF KUZNIETSOV'S IDENTITY FOR KLOOSTERMAN SUMS

Robert A. Smith

Presented by J.H.H. Chalk, F.R.S.C.

If a, b and q are integers with $q \geq 1$, the associated Kloosterman sum is defined by

$$K(a,b;q) = \sum_{x \bmod q}^{*} e_q(ax + b\bar{x}),$$

where the sum is taken over a reduced set of residues mod q, $\bar{x}$ denotes the multiplicative inverse of $x \bmod q$ and $e_q(t) = \exp(2\pi it/q)$ for all $t \in \mathbb{Z}$. Recently, Kuznietsov [3] deduced from the action of the Hecke operators on the L^2-space of non-holomorphic cusp forms of weight zero for $SL(2,\mathbb{Z})$ the following identity for Kloosterman sums

$$K(a,b;q) = \sum_{d \mid (a,b,q)} d\, K\left(1, \frac{ab}{d^2}; \frac{q}{d}\right), \tag{1}$$

where (a,b,q) denotes the greatest common divisor of a, b and q. In searching through the literature, I have been unable to find an earlier reference to this identity, although special cases are certainly well-known (e.g., cf. Salié [4]), and moreover, this identity is implicit in Estermann's 1930 paper [1] in view of my own recent work [6]. An interesting application of (1) appears in the recent work of Iwaniec [2] in connection with the Riemann zeta function. In this note, I will give an elementary

proof of this identity as well as a generalization of it to Mordell's n-dimensional Kloosterman sums; an application of this generalization will appear in my forthcoming paper [6].

Before stating the main result, we recall the definition of the n-dimensional Kloosterman sum (cf. [5]), where n is an arbitrary positive integer. For any $\underline{a} = (a_1, \ldots, a_{n+1}) \in \mathbb{Z}^{n+1}$ and $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$, let $\underline{a} \cdot \underline{x} = a_1x_1 + \cdots + a_nx_n$ and $N\underline{x} = x_1 \cdots x_n$; the associated n-dimensional Kloosterman sum is given by

$$K_n(\underline{a};q) = \sum_{\underline{x} \bmod q}^{*} e_q(\underline{a} \cdot \underline{x} + a_{n+1}\overline{N\underline{x}}),$$

where the summation condition means that each component of $\underline{x}$ runs over a reduced set of residues mod q. For each $a \in \mathbb{Z}$ and $\underline{b} \in \mathbb{Z}^{n+1}$, let

$$\underline{e}(a) = (1, \ldots, 1, a) \in \mathbb{Z}^{n+1} \quad \text{and} \quad \underline{e}(\underline{b}) = \underline{e}(N\underline{b}).$$

THEOREM. For any positive integers n and q, and any $\underline{a} \in \mathbb{Z}^{n+1}$, then

$$K_n(\underline{a};q) = \sum_{\substack{d \mid q \\ d \mid \underline{a}}} d^n K_n\left(\underline{e}\left(\frac{1}{d}\underline{a}\right); \frac{q}{d}\right), \tag{2}$$

where $d \mid \underline{a}$ means that d divides each component of $\underline{a}$.

Proof: First, we will prove Kuznietsov's original identity. Since $K(1,ab;q)$ is real, we have

$$qK(1,ab;q) = \sum_{z \bmod q}^{*} e_q(-z) \sum_{x,y \bmod q} e_q(xyz + ax + by). \tag{3}$$

If we change the order of summation in (3) and observe that the

resulting inner sum is a Ramanujan sum, we can rewrite (3) as

$$qK(1,ab;q) = \sum_{d|q} d\mu\left(\frac{q}{d}\right) \sum_{\substack{\underline{x} \bmod q \\ N\underline{x} \equiv 1 \bmod d}} e_q(\underline{a} \cdot \underline{x}),$$

where we have written $\underline{x} = (x,y)$, $\underline{a} = (a,b)$ and $\underline{a} \cdot \underline{x} = ax + by$. If we write $\underline{x} = d\underline{u} + \underline{v}$, where $\underline{u}$ runs over a complete set of residues mod $\frac{q}{d}$ and $\underline{v}$ runs over a complete set of residues mod d, the inner sum in the last expression becomes $(q/d)^2 E_{q/d}(\underline{a}) K\left(\frac{a}{q/d}, \frac{b}{q/d}; d\right)$, where $E_d(\underline{a}) = 1$ if $d \mid \underline{a}$ and $= 0$ otherwise. Consequently, we obtain

$$K(1,ab;q) = \sum_{d|(a,b,q)} d\mu(d) K\left(\frac{a}{d}, \frac{b}{d}; \frac{q}{d}\right). \tag{4}$$

Kuznietsov's identity now follows from (4) by the Möbius Inversion Formula.

Next, we will prove by induction on n that (2) holds for $q = p^\alpha$ where p is a prime and $\alpha \geq 1$. In view of (1), we may assume that (2) holds for n-1 for $n \geq 2$. If we put $\underline{a} = (\underline{b}, a_n, a_{n+1})$ for fixed $\underline{a} \in \mathbb{Z}^{n+1}$, $K_n(\underline{a};q)$ can be rewritten as

$$K_n(\underline{a};q) = \sum_{y \bmod q}^{*} e_q(a_n y) K_{n-1}(\underline{b}, a_{n+1}\bar{y}; q).$$

If we set $K_n(a;q) = K_n(\underline{e}(a);q)$ for any $a \in \mathbb{Z}$, the induction hypothesis implies that

$$K_n(\underline{a};q) = \sum_{\substack{d|q \\ d|a_{n+1} \\ d|\underline{b}}} d^{n-1} \sum_{y \bmod q}^{*} e_q(a_n y) K_{n-1}\left(\frac{a_{n+1}N\underline{b}}{d^n}\bar{y}; \frac{q}{d}\right). \tag{5}$$

At this point, it will be convenient to have the following

LEMMA. Let q be a prime power. If $d \mid q$ and $a, A \in \mathbb{Z}$, then

$$\sum_{y \bmod q}^{*} e_q(ay) K_{n-1}(A\bar{y}; q/d) = dE_d(a) \sum_{v \bmod q/d}^{*} e_{q/d}\left(\frac{a}{d} v\right) K_{n-1}\left(A\bar{v}; \frac{q}{d}\right).$$

(This result follows immediately by making the substitution $y = (q/d)u + v$, where u runs through a complete set of residues mod d and v runs through a reduced set of residues mod q/d.) If we now apply this lemma, together with (1), to the identity in (5), we obtain

$$(6) \quad K_n(\underline{a}; q) = \sum_{\substack{d \mid q \\ d \mid \underline{a}}} d^n \sum_{r} r \sum_{\underline{x} \bmod q/d}^{*} e_{q/d}(t(\underline{x})) K\left(1, \frac{N\underline{a}\overline{N\underline{x}}}{r^2 d^{n+1}}; \frac{q/d}{r}\right),$$

where the middle sum over r is taken over all common divisors r of q/d, a_n/d and $a_{n+1}N\underline{b}/d^n$, and $t(\underline{x}) = x_1 + \cdots + x_{n-1}$. By an argument similar to the proof of the lemma, the inner sum in (6) is zero unless $r = 1$. Therefore, (6) can be rewritten as

$$K_n(\underline{a}; q) = \sum_{\substack{d \mid q \\ d \mid \underline{a}}} d^n \sum_{\underline{x} \bmod q/d}^{*} e_{q/d}(t(\underline{x})) K\left(1, N\left(\frac{1}{d}\underline{a}\right)\overline{N\underline{x}}; q/d\right),$$

from which (2) immediately follows for $q = p^{\alpha}$.

To complete the proof of the theorem, we may now assume that (2) holds for all $q \geq 1$ containing less than r distinct primes with $r > 1$. Consequently, if q contains exactly r distinct primes, we may write $q = q_1 q_2$ where q_1 and q_2 each contain less than r distinct primes and $(q_1, q_2) = 1$. If m_1 and m_2 are integers satisfying $m_1 q_1 + m_2 q_2 = 1$, Theorem 1

of [5] implies that $K_n(\underline{a};q) = K_n(m_2\underline{a}\,;q_1)K_n(m_1\underline{a};\,q_2)$,

which, by our induction hypothesis, yields

$$K_n(\underline{a};q) = \sum_{\substack{d_i \mid q_i \\ d_i \mid \underline{a}}} (d_1 d_2)^n K_n\left(m_2\underline{e}\left(\frac{1}{d_1}\,\underline{a}\right);\, q_1/d_1\right) K_n\left(m_1\underline{e}\left(\frac{1}{d_2}\,\underline{a}\right);\, q_2/d_2\right)$$

$$= \sum_{\substack{d_i \mid q_i \\ d \mid \underline{a} \\ d = d_1 d_2}} d^n \sum_{\substack{\underline{u}_i \bmod q_i/d_i \\ N(\underline{u}) \equiv 1 \bmod q/d}} e_{q/d}\left(\underline{e}\left(\frac{1}{d}\,\underline{a}\right)\cdot \underline{u}\right)$$

with $\underline{u} = m_2 q_2 \underline{u}_1 + m_1 q_1 \underline{u}_2$. Since $m_2 q_2 \underline{u}_1 + m_1 q_1 \underline{u}_2$ runs through a complete set of residues mod q/d whenever $\underline{u}_i$ runs through a complete set of residues mod q_i/d_i, the proof of the theorem is complete.

REMARK: In [5], an upper bound for the absolute value of $K_n(\underline{a};q)$ is given which, unfortunately, is rather complicated to apply. By means of the Kuznietsov identity for $K_n(\underline{a};q)$, we can now give a much simplier bound. Indeed, by Theorem 6 of [5], we know that if some component of $\underline{b} \in \mathbb{Z}^{n+1}$ is relatively prime to q, then

$$|K_n(\underline{b};q)| \le q^{n/2}\, d_{n+1}(q),$$

where $d_{n+1}(q)$ denotes the number of representations of q as a product of $n+1$ factors. Consequently, (2) implies that

$$|K_n(\underline{a};q)| \le \sum_{\substack{d \mid q \\ d \mid \underline{a}}} d^n \left|K_n\left(\underline{e}\left(\frac{1}{d}\,\underline{a}\right);\, \frac{q}{d}\right)\right|$$

$$\le q^{n/2} \sum_{\substack{d \mid q \\ d \mid \underline{a}}} d^{n/2}\, d_{n+1}(q/d)$$

$$\leq q^{n/2}(\underline{a},q)^{n/2}d_{n+2}(q)$$

where $(\underline{a},q)$ denotes the greatest common divisor of all the components of $\underline{a}$ and q.

REFERENCES

1. T. Estermann, On the representation of a number as the sum of two products, Proc. London Math. Soc. (2) 31 (1930), 123-133.

2. H. Iwaniec, Fourier coefficients of cusp forms and the Riemann zeta function, Séminaire de Théorie des Nombres, Université de Bordeaux (1979/1980), exposé no. 18.

3. N.V. Kuznietsov, The Petersson conjecture for forms of weight zero and the Linnik conjecture (Russian), preprint no. 2, Khab. K.H.I.I., Khabarovsk (1977).

4. H. Salié, Über die Kloostermanschen Summen S(u,v;q), Math. Zeit. 34 (1931), 91-109.

5. R.A. Smith, On n-dimensional Kloosterman sums, Journal of Number Theory 11 (1979), 324-343.

6. R.A. Smith, The generalized divisor problem over arithmetic progressions, (to appear).

Department of Mathematics,
University of Toronto,
Toronto, Canada, M5S 1A1.

Received November 4, 1980

C. R. Math. Rep. Acad. Sci. Canada - Vol. II (1980) No. 6

A REMARK ON STRIPS II

Peter Scherk, F.R.S.C.

In this note we prove the result announced in the preceding paper.

1. Rolling Strips

1.1 Let

$$\tau = \{\underset{\sim}{Y}(s) , U(s) \qquad s \in J$$

denote a second m-strip; thus $\underset{\sim}{Y}'(s) \in U(s)$; cf. I.1.1. Let $M = M(s)$ range through its normal spaces.

Let $C = C(s)$ range through a continuously differentiable family of orthogonal transformations of V^n; $s \in J$. The following definition is suggested by Nomizu's paper [3]: σ *is rolled by means of* C *onto* τ if for all $s \in J$

$$\underset{\sim}{Y}' = C\underset{\sim}{X}' \tag{1.1}$$

$$CT = U, \quad \text{hence} \quad CN = M, \quad \text{and} \tag{1.2}$$

$$C'T \subset M \ , \quad C'N \subset U. \tag{1.3}$$

Remarks. (i) Actually, our rolling is described by the family of euclidean motions

$$\begin{cases} E^n \to E^n \\ \underset{\sim}{X} \mapsto C(s)\underset{\sim}{X} + \underset{\sim}{c}(s). \end{cases}$$

Here $\underset{\sim}{c}(s)$ is defined through

$$\underline{Y}(s) = C(s)\underline{X}(s) + \underline{c}(s) \qquad (s \in J);$$

thus $C'(s)\underline{X}(s) + \underline{c}'(s) = \underline{0}$.

(ii) Our definition is slightly weaker than Nomizu's [3]: he also requires $C'(s) \neq 0$ for every $s \in J$.

1.2 Let $\underline{x}$ and $\underline{y}$ be in V^n. Every $s \in J$ then determines unique decompositions $\underline{x} = \underline{x}_T + \underline{x}_N$ and $\underline{y} = \underline{y}_U + \underline{y}_M$ where $\underline{x}_T \in T$, etc. Obviously, we have e.g. $\underline{x}_T = \pi_T\underline{x}$ and $\underline{x}_N = \pi_N\underline{x}$. By (1.2), $C\underline{x}_T \in U$ and $C\underline{x}_N \in M$. As $Cx = C\underline{x}_T + C\underline{x}_N$, we obtain e.g. $C\pi_T\underline{x} = C\underline{x}_T = (C\underline{x})_U = \pi_U C\underline{x}$. This yields

(1.4) $\qquad C\pi_T = \pi_U C \quad \text{and} \quad C\pi_N = \pi_M C \qquad \text{for every } s \in J.$

1.3 Suppose the function $\underline{x}(s)$ in V^n has a continuous derivative. Then (1.4) yields

(1.5) $$D_U(s)\big(C(s)\underline{x}(s)\big) = C(s)D_{T(s)}\underline{x}(s) + \pi_{U(s)}C'(s)\underline{x}(s).$$

Thus $C(s)\underline{x}(s)$ has a continuous derivative.

We can write (1.5) in the form

$(1.6)_1$ $$D_U C = CD_T + \pi_U C'.$$

Symmetrically,

$(1.6)_2$ $$D_M C = CD_N + \pi_M C'.$$

The formulas (1.3) are equivalent to

$$\pi_U C'T = \pi_M C'N = 0.$$

Thus on account of (1.6), (1.3) is equivalent to

$$(1.3)' \qquad (D_U C - C D_T) T = (D_M C - C D_N) N = 0.$$

1.4 Suppose the strip σ satisfies the assumptions of I.1.3 and I.2.1 and is rolled by means of C onto the strip τ. Let

$$(1.7) \qquad \underset{\sim}{y}_i = C\underset{\sim}{x}_i ; \qquad i = 1, \ldots, n.$$

Then $\underset{\sim}{y}' = \underset{\sim}{y}_1$. The vectors

$$(1.8) \qquad \underset{\sim}{y}_1 , \cdots , \underset{\sim}{y}_m$$

form a continuously differentiable tangential frame of τ and both strips have the same tangential Frenet matrices.

Proof. By (1.2), the vectors (1.8) lie in U. Thus they form an orthonormal base of U for every s. Furthermore, by (1.1), I(1.3) and (1.7), $\underset{\sim}{Y}' = C\underset{\sim}{X}' = C\underset{\sim}{x}_1 = \underset{\sim}{y}_1$.

Let $1 < i < m$. Applying (1.3)' to $\underset{\sim}{x}_i(s)$, we obtain on account of (1.7)

$$D_U \underset{\sim}{y}_i = D_U C \underset{\sim}{x}_i = C D_T \underset{\sim}{x}_i = C(-\kappa_{i-1}\underset{\sim}{x}_{i-1} + \kappa_i \underset{\sim}{x}_{i+1})$$

$$= -\kappa_{i-1}\underset{\sim}{y}_{i-1} + \kappa_i \underset{\sim}{y}_{i+1} ;$$

similarly for $i = 1$ and $i = m$. This proves our statements.

Remark. It can be shown in the same way that $\underset{\sim}{y}_{m+1}, \cdots, \underset{\sim}{y}_n$ form a continuously differentiable normal frame of τ and that σ and τ have the same normal Frenet matrices with respect to

$\underset{\sim}{x}_{m+1}$ and $\underset{\sim}{y}_{m+1}$, respectively.

2. Rollability

2.1 We call the m-strip σ rollable onto the m-strip τ if there is a continuously differentiable family of orthogonal transformations $C = C(s)$ of V^n which satisfy the conditions (1.1) - (1.3). Obviously, rollability is an equivalence relation.

2.2 Theorem. *Suppose the strips σ and τ satisfy the assumptions of I.1.2, I.1.3 and I.2.1. Then σ is rollable onto τ if and only if σ and τ have the same tangential Frenet matrices.*

Proof. By 1.4 this condition is necessary. Suppose conversely that σ and τ have the same tangential Frenet matrices. On account of I.2.3 we may assume that σ and τ also have the same normal Frenet matrices. Define the linear map $C = C(s) : V^n \to V^n$ through

$$C\underset{\sim}{x}_i = \underset{\sim}{y}_i \qquad \text{for } i = 1, \ldots, n.$$

Then C is orthogonal and differentiable and satisfies (1.1) and (1.2).

Suppose e.g. $1 < i < m$. Then both strips having the same tangential Frenet matrices, we have

REFERENCES

[1] Appell, P. Traité de mécanique rationelle, vol. 1 (1919).

[2] Blaschke, W. Vorlesungen über Differentialgeometrie. 3rd ed. Springer, Berlin, 1930.

[3] Nomizu, K. Kinematics and differential geometry of submanifolds, Tôhoku Math. J. 30 (1978), 623-637.

Department of Mathematics,
University of Toronto,
Toronto, Canada, M5S 1A1.

Received November 5, 1980

MAILING ADDRESSES

1.	J. Aczél	Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1.
2.	G. Grätzer	Department of Mathematics, University of Manitoba, Winnipeg, Manitoba, Canada, R3T 2N2.
3.	A.P. Huhn	Bólyai Intézet, 6720 Szeged, Hungary.
4.	C.U. Jensen	Matematisk Institut, Københavns Universitet, Universitetsparken 5, 2100, København Ø, Denmark.
5.	Dieter Lutz	FB6 - Mathematik - Universität Essen, P.O.B. 6843, D-4300 Essen 1, W. Germany.
6.	Angelo B. Mingarelli	Department of Mathematics, University of Ottawa, Ottawa, Ontario, Canada, K1N 9B4.
7.	Peter Scherk	Department of Mathematics, University of Toronto, Toronto, Ontario, Canada, M5S 1A1.
8.	Robert A. Smith	Department of Mathematics, University of Toronto, Toronto, Ontario, Canada, M5S 1A1.
9.	Wu Xiao-lung	Institute of Mathematics, Academia Sinica, Beijing, China.
10.	N. Yui	Fachbereich Mathematik, Universität des Saarlandes, D-6600 Saarbrücken, W. Germany.
11.	Wan Zhe-xian	Institute for Advanced Study, Princeton, Princeton, New Jersey 08540, U.S.A.

INDEX - VOLUME II