IRISH MATHEMATICAL SOCIETY BULLETIN

The aim of the BULLETIN is to inform Society members about the activities of the Society and about items of general mathematical interest. It appears twice each year: in March and December.

The Bulletin seeks articles of mathematical interest written in an expository style. All areas of mathematics are welcome, pure and applied, old and new. The Bulletin is typeset using TEX. Authors are invited to submit their articles in the form of TEX input files. Articles submitted in this form will be given the same consideration as typed articles.

Correspondence concerning the Bulletin should be addressed to:

Irish Mathematical Society Bulletin
Department of Mathematics
University College
Galway
Ireland

Correspondence concerning the Problem Page should be sent directly to the Problem Page Editor at the following address:

Faculty of Mathematics
Open University
Milton Keynes, MK7 6AA
UK

The Irish Mathematical Society acknowledges the assistance of EOLAS, The Irish Science And Technology Agency, in the production of the Bulletin.

CONTENTS

THE IRISH MATHEMATICAL SOCIETY

OFFICERS AND COMMITTEE MEMBERS

President	Prof. Seán Dineen	Department of Mathematics University College Dublin
Vice-President	Dr. Fergus Gaines	Department of Mathematics University College Dublin
Secretary	Prof. A.G. O'Farrell	Department of Mathematics Maynooth College Maynooth
Treasurer	Dr. Gerard M. Enright	Department of Mathematics Mary Immaculate College Limerick

Committee Members: M. Brennan, N. Buttimore, R. Critchley, B. Goldsmith, D. Hurley, T. Hurley, R. Ryan, R. Timoney.

LOCAL REPRESENTATIVES

Cork	RTC	Mr. D. Flannery
	UCC	Dr. M. Stynes
Dublin	Carysfort	Dr. J. Cosgrove
	DIAS	Prof. J. Lewis
	Kevin St.	Dr. B. Goldsmith
	NIHE	Dr. M. Clancy
	TCD	Dr. R. Timoney
	UCD	Dr. F. Gaines
Dundalk	RTC	Dr. E. O'Riordan
Galway	UCG	Dr. R. Ryan
Limerick	MICE	Dr. G. Enright
	NIHE	Dr. R. Critchley
	Thomond	Mr. J. Leahy
Maynooth		Prof. A. O'Farrell
Waterford	RTC	Mr. T. Power

EDITORIAL

The first issue of the Irish Mathematical Society Newsletter (later to become the Bulletin) was published ten years ago, in 1978, two years after the foundation of the Society itself. That first issue, modest though it may have been, contained all the ingredients which have ensured the popularity of it and its successors, and contributed in no small way to the remarkable growth of the Society over the intervening years. While the physical appearance may have changed during this time in which the editorship was based first in Dublin, then in Cork and now in Galway, the basic policy of the Bulletin remains unchanged; it is to publish a broad range of news, letters, reviews and articles which will inform, entertain and challenge our readers.

We hope that the **News** section and the **Book Reviews** will be found to be lively, informative and up to date. We welcome **Articles** which are expository in style. Particularly welcome are surveys of newly developing areas, both in pure and applied mathematics in all its manifestations. The **Notes** section is intended primarily for presentations of mathematics which will be of interest to those teaching the subject at either undergraduate or postgraduate level—an illuminating viewpoint, or a new proof, for example. Under the heading of **Mathematical Education** we seek articles concerned with the teaching of mathematics at all levels. Articles on any aspect of the **History of Mathematics** are also welcome. Finally, we invite readers who would like to express their views on any topic of interest to the mathematical community to contribute to the **Letters** column.

IRISH MATHEMATICAL SOCIETY

ORDINARY MEETING

December 22, 1988

An Ordinary meeting of the Society was held at 12.15pm in the DIAS. The President S. Dineen took the chair. There were 20 members present.

1. The minutes of the Ordinary Meeting of April 16^{th}, 1987 were approved and signed.

2. The Treasurer presented his report, which was approved unanimously (proposed by R. Critchley and seconded by M. Brennan). It was reported that the committee wished to increase the reciprocity subscription for AMS members to $6, and this was agreed. Also, through the efforts of F. Holland, the Society was now recognised by the Revenue as being established for charitable purposes only.

3. The Secretary presented his report.

4. It was agreed to consider holding a meeting of the Society in September. It was also agreed that the President would set up a discussion at the Easter DIAS Symposium on the degree programmes involving Mathematics currently on offer in Ireland and on the carreers followed by graduates of these programmes. Written information which could be available by then would be very welcome.

5. It was announced that the Committee was seeking a member who could represent the Society at the American Mathematical Society Centennial Celebration in Providence, August 8-12, 1988. The Society would be sending greetings to the AMS on the occasion of their centennial year.

   The committee decided to solicit tasteful advertisements for the Bulletin.

   The committee had also decided to support three conferences in 1988, to be held in Dublin (Matrix Theory, March), Galway (Groups, May) and Limerick (Computers in Primary Education, February).

6. A.G. O'Farrell was elected Secretary, G.M. Enright was re-elected Treasurer and the following were elected committee members: R. Critchley, D. Hurley, T. Hurley and R. Timoney. All are elected for two-year terms. (S. Dineen (President), F. Gaines (Vice-president), M. Brennan, N. Buttimore, B. Goldsmith and R. Ryan were elected in December 1986 for two-year terms.)

7. T. Laffey reported that he and F. Holland were progressing with their preparations for sending a team to the Mathematical Olympiad in Australia in 1988. Introductory sessions for secondary school pupils had been successfully held in Dublin and Cork so far.

8. The committee nominated Professor J.L. Synge to honorary membership of the Society. (This nomination is to be voted on at the next Ordinary meeting of the Society.)

Richard M. Timoney,
Secretary

IRISH MATHEMATICAL SOCIETY

SECRETARY'S REPORT

It seems to me appropriate, as I come to the end of my term of office as Secretary, to reflect on my activities during my periods as Secretary. I would like however, first, to thank all those who responded to my various requests for help or information. Specifically I would like to thank the local representatives.

During the past year, the one succesful venture I can point to is the setting up of departmental electronic mailboxes for the Mathematics departments at all the HEANET sites in Ireland. The electronic addresses for these are MATHDEP@VAX1.MAY.IE, MATHDEP@VAX2.NIHED.IE, MATHDEP@VAX1.NIHEL.IE, MATHDEP@DEC20.TCD.IE, MATHDEP@IRUCCVAX.UCC.IE, MATHDEP@IRLEARN.UCD.IE and MATHDEP@VAX1.UCG.IE. (This and other HEANET addresses are now easily accessible to all BITNET users in the USA and elsewhere. The mail is routed to HEANET automatically through a gateway facility at UCD and, conversely, HEANET users can send messages to BITNET users through this same gateway.)[1]

Although this facility has the potential to be very useful as a means of delivering messages to mathematicians at other departments whose electronic addresses are unknown, it has not yet been widely availed of, perhaps because its existence is not sufficiently widely known. Until there is a steady trickle of usage, its reliability may be in question, since the person checking for mail to MATHDEP may not do so regularly if there does not seem to be traffic.

The EUROMATH project is perhaps relevant in this context as it aims to facilitate electronic mail usage between mathematicians, among other objectives. A significant part of this project is being carried out at NIHE Dublin under John Carroll. Some years ago Irish mathematics departments showed their enthusiasm for the basic ideas of EUROMATH by contributing towards the costs of preparing a proposal for EEC funding. Members may recall that A.K. Seda of UCC represented the Society at some of the early meetings on the scheme and was largely responsible for bringing it to our attention.

Other positive notes in the recent past of the Society were the joint meeting with the London Mathematical Society on Operator algebras (which was organised by T.T. West) and the recriprocity agreement with the American

[1]Ed: Addresses amended 3/88

Mathematical Society. In my view the Bulletin has continued to improve steadily under the editorships of D. Hurley, P. Fitzpatrick and R. Ryan and I certainly hope that this trend will be maintained.

There are a few matters on which I feel that the Society needs to exert more effort, through the committee. I think it would help if the committe could arrange to meet more frequently. It is often hard to generate enthusiasm for committee meetings which involve special long journeys for at least some of the members. It might be reasonable to have a policy that committee meetings should be arranged to coincide with conferences which are partly sponsored by the Society (*e.g.* Groups in Galway). September is a time when a committee meeting would often be useful. This year there was a plan to hold a conference (or meeting of the Society) in UCD in September, which fell through. We should perhaps consider having a one-day meeting of the Society annually (say in September) much as the LMS and the AMS do on a more frequent schedule.

I think that it is important that the Society should make it a priority to cater equitably for all strands of mathematical interests in Ireland. A step in this direction would be to find out what the strands currently are. To some extent the Bulletin and the DIAS Symposia may serve this function, but I feel that a report on the needs of or for mathematics in Ireland could be a valuable focus for future planning on many levels.

Richard M. Timoney
December 22, 1987

NEWS

Personal Items

- **Professor J.A. Barroso** (Rio de Janeiro) is presently visiting the Mathematics Department of UCD.

- **Professor Irene Hazou** of Bethlehem University, West Bank, visited the Mathematics Department of UCD recently to discuss curriculum development in mathematics. Her visit was sponsored by HEDCO (the Higher Educational Development Corporation).

- **Professor Wang Ming-Ci**, Vice-Chairman of the Mathematics Department of Chengdu University of Science and Technology, Sichuan, China, and a member of the Guiding Committee of Mathematical Education in China, visited the Mathematics Department of University College Galway recently to investigate the teaching of mathematics to Engineering students in Ireland. She lectured to the department on the present state of mathematical education in China.

- **Professor H.G. Dales** of Leeds University, is presently visiting the Mathematics Department of Maynooth College.

- **Professor J. Verdera** of the University of Barcelona, will be visiting the Mathematics Department of Maynooth College during June and July.

- **John Kinsella** has been appointed Lecturer in Mathematics in NIHE Limerick.

- **Peter Danaher** (Auckland) has taken up a one-year appointment in the Statistics Department at UCD.

- **Siddartha Sen** of the Department of Applied Mathematics at TCD, is presently visiting Fermi Lab and Carnegie-Mellon University in the United States.

- **Paul McGill** has resigned his position in the Mathematics Department of Maynooth College.

- **Eamonn Murphy** has been appointed Assistant Lecturer in Mathematics and Statistics in NIHE Limerick.

- **Joe Buckley** has left the Department of Mathematics in NIHE Limerick to take up a position in Australia.

- **Phil Rippon**, our Problem Page Editor, has been promoted to Senior Lecturer in the Mathematics Department at the Open University.

- **Niall Ó Murchadha** of the Experimental Physics Department of UCC has been promoted to Statutory Lecturer.

- **Pól Mac Aonghusa** has been appointed to a one-year position in the Mathematics Department of Maynooth College.

- **David Walsh** has been promoted to Senior Lecturer in Mathematics in Maynooth College.

Statistics Position in UCD

Professor Phil Boland will welcome applications for a three-year appointment in the Statistics Department of University College Dublin.

New Appointments to LMS Editorial Board

Professor Brian Twomey of the Mathematics Department, UCC and Dr. Phil Rippon of the Open University have been appointed to the Editorial Board of the London Mathematical Society for a 5-year period, beginning on 1st January 1988. Authors wishing to submit a paper for publication in any of the three journals (Bulletin, Journal and Proceedings) of the LMS send papers in the first instance to the appropriate member of the Editorial Board. Professor Twomey will handle papers in Complex Analysis and Fourier Analysis, while Dr. Rippon will deal with Potential Theory and Complex Analysis.

National Committee Newsletter

The National Committee for Mathematics of the Royal Irish Academy hopes to publish a mathematics newsletter between issues of the IMS Bulletin. The editors are T. J. Laffey and M. Hayes. They will welcome any items about conferences and other mathematical events.

Lecturing in Developing Countries

The ICSU and the TWAS (Third World Academy of Sciences) are jointly organizing a Lectureship Programme through which they will finance the travel of scientists from any part of the world to give scientific lectures in developing countries. Further details can be obtained from the National Committee for Mathematics of the Royal Irish Academy.

Charitable Status for IMS

Thanks to the efforts of Finbarr Holland, the Irish Mathematical Society is now regarded by the Revenue Commissioners as established for charitable purposes only.

ICM 90

The next International Congress of Mathematicians will be held in Kyoto in 1990. The National Committee for Mathematics of the Royal Irish Academy has been asked for suggestions for speakers and, in accordance with previous practice, will welcome any assistance that IMS members can provide. Each suggestion should be motivated, and should include a short list of publications. These should be sent to the National Committee for Mathematics, Royal Irish Academy, 19 Dawson Street, Dublin 2, before 31st October 1988.

The outgoing President of the IMU, Jürgen Moser, has appealed for funds to enable young mathematicians from developing countries to attend the Congress. For ICM 86 the IMU provided travel grants for over thirty young mathematicians, but contributions from members did not come up to expectations. He is appealing for a better response this time. Donations to the Special Development Fund can be sent to the Academy up to the end of 1989. Cheques should be made payable to "Royal Irish Academy" with a covering note clearly stating that the contribution is intended for the IMU Special Development Fund.

A Remarkable Coincidence!

We invite readers to compare the following extracts from Mathematical Reviews:

Harte, Robin(IRL–CORK) 85b:47024
Almost open mappings between normed spaces.
*Proc. Amer. Math. Soc.***90**(1984), *no.* 2, 243–249

Harte, Robin(IRL–CORK) 85d:47024
A quantitative Schauder theorem.
*Math. Z.***185**(1984), *no.* 2, 243–245

As Lady Bracknell might have said: "To publish two papers on page 243, Mr. Harte, may be regarded as misfortune; to review both as number 47024 looks like carelessness"!

Would any reader care to estimate the odds?

International Mathematical Olympiad

The Minister for Education has approved the travel grant to send an Irish team, for the first time, to participate in the International Mathematical Olympiad in Australia in July.

Following an analysis of the Intermediate Certificate Examination and the Irish National Mathematics Contest held in the last two years, invitations were issued in December 1987 to about 300 pre-Leaving students to present themselves for preliminary assessment for the six-member team that will represent Ireland. After a series of tests, this number has been reduced and about 50 of them—drawn from about thirty different schools—have been identified as having outstanding mathematical problem-solving ability. These talented students are receiving special training in UCD, UCC, MICE and UCG under the direction of Tom Laffey, Finbarr Holland, Pat O'Sullivan and Ted Hurley, respectively.

These training sessions have generated a lot of interest amongst teachers and students alike and all those who have taken part have found it a rewarding experience. Special topics suggested by previous IMO problems have been covered at the sessions, and so far Modular Arithmetic, Combinatorics and a little Geometry have been discussed at some or all of the centres. Students' understanding of the material is being carefully monitored and we await with interest the results of this year's INMC and IIMC. We should be in a position after these contests to nominate the likely team members. Our intention is then to provide these with an intensive week's training to build up team morale and to fine-tune them in preparation for Australia.

Anyone who would like to assist at the training sessions is invited to contact the centre nearest to him/her. We would especially like to hear from people with expertise in Trigonometry, Solid Geometry, Combinatorics and Graph Theory and people who enjoy solving or creating problems. Especially in the latter case, we invite people to send in their favourite elementary problems.

One beneficial side-effect of this undertaking has been the strengthening of relations with mathematics teachers. It is hoped that the pupils will be encouraged to keep up their interest in mathematics, even if they do not get on the team.

EUROMATH
The Integrated Database And Communications System For European Mathematicians

The objective of EUROMATH is to improve the research environment for European mathematicians with the aid of modern information technology. By establishing an integrated information retrieval and communication system as well as a technical word processing standard, it will strive to stimulate the research potential within mathematics in Europe, increase the availability of mathematical research and create an environment which will encourage mathematicians towards increased collaboration through effective communication.

The first phase of the EUROMATH project will produce guidelines for the provision of the following inter-related facilities:

- Information Retrieval: Access to various directories, to (reviews of) published literature, to other databases as well as drafts and notes of individual mathematicians.
- Inter-personal Communication: Provision of suitable electronic mail and electronic conferencing facilities.
- Document Preparation and Delivery: The establishment of a European standard for mathematical communication embracing the main activities of entering, editing, transmitting, receiving and printing mathematical documents.

Traditionally, mathematicians have relied on computers mainly for such specific tasks as scientific computation and symbolic manipulation. A goal of EUROMATH is to expand computer usage by enabling easy access to modern communication facilities. Its basic concept is however equally applicable to other scientific disciplines. The success of EUROMATH could inspire others to see the benefits of a modern, full-scale solution to the communication needs of a scientific community.

The CEC project EUROMATH (The Integrated Database and Communications System for European Mathematicians), is a collaborative effort link-

ing CWI (Amsterdam), DDC (Copenhagen) and NIHE (Dublin) in a technical partnership under the management team of CRC (Dublin) and EMT (European Mathematical Trust), to which the Irish Mathematical Society is affiliated. The NIHE (Dublin) Manager is:

Dr. John Carroll,
School of Mathematical Sciences,
NIHE,
Dublin 9, Ireland.
EARN/BITNET: CARROLLJ@VAX2.NIHED.IE

IRISH MATHEMATICAL SOCIETY

Ordinary Membership

The subscription for Ordinary Membership for the session 1987/88 is £5. Payment is now overdue and should be forwarded to the Treasurer without further delay.

Institutional Membership

Institutional Membership of the Irish Mathematical Society is available for the session 1987/88 for a subscription of £35. The support of its Institutional Members is of great benefit to the Society. Institutional Members receive two copies of the Bulletin, and may nominate up to five students for free membership.

Reciprocity Membership

Members of the Irish Mathematics Teachers Association and of the American Mathematical Society are entitled to reciprocity membership of the Irish Mathematical Society at special rates. Further details may be obtained from the Treasurer, Dr. G. Enright, at the following address:

Department of Mathematics
Mary Immaculate College of Education
Limerick

LETTERS

Why People Should Be Paid To Do Research In Mathematics

Dear Editor,

Brendan McCann's question: "Should people be Paid to Do Research in Mathematics?" (Issue 19) is fair, and one which a mathematician ought to ponder. I hope you see fit to let me share some of my thoughts about it. In discussing any question beginning with "should", it is sure that varying ethical outlooks will produce different conclusions.

To begin with, I do not accept it as given that "technology has outstripped man's needs." In fact McCann refutes this in the same paragraph when he states that "over half the world's adults are illiterate." Perhaps he does not view this as a problem to which technology can contribute. But I do. In fact, I take it as given that technology has contributed more to the human condition including human rights than any philosophical or political movement. While it is true that Mr. McCann and I are receiving more material comforts than we really need, it does not follow that everyone is. The solution to this maldistribution is (A) more technology and (B) more generosity. And it seems to me that (A) is the best way to (B).

The assertion "There is no reason to suppose that mankind will perish without further mathematical research." is a gem. You can replace "further mathematical research" with so many things: art, journalism, rock and roll, Guinness, medicine even. It seems to me that bare survival is not the issue here. Nor is the potential contributions of mathematics to technology, despite my technophile assertions above. In the sequel I shall argue as follows: (1) all human creativity including mathematical creativity should be supported by society; (2) the scheme by which mathematical creativity is presently rewarded is better than that by which most other creativity is rewarded; (3) there are practical benefits to societies which adequately reward mathematical creativity besides the eventual application of mathematical theory to technology.

There is every reason to suppose that humanity will cease to be humanity without further creativity in literature, art, philosophy, athletics and mathematics. Creativity must be a defining factor of human culture. My definition of creativity is as broad as possible including motion picture actors and directors amateur and professional athletes, billiard and chess players, musicians, circus performers etc. All of these persons do their bit with greater or less proficiency, and seek a reward for it. At times the reward is given in a most indirect way. For example, outstanding college wrestlers, for whom there are few professional athletic opportunities after graduation, sometimes receive high paying jobs in sales and public relations from firms which feel that their customers have heard of these former champions and would like to spend time with them.

We all know the scheme by which creativity in mathematics is rewarded, and I shall not dwell on it. Mathematicians are hired as professors, and their teaching load is reduced to allow time for research. Better research credentials lead to better positions and earlier promotion.

The first justification for this arrangement has nothing to do with research. It is this: teaching college level mathematics requires a tremendous preparation and intellectual effort. I claim that teaching calculus for a year requires the same intellectual effort as trying an involved case at law. A lawyer demands a high fee because of his preparation and effort. A mathematician demands a smaller fee and an environment in which he can do research. The value of the mathematician's teaching justifies his salary and the environment.

The second justification is this: The value of mathematical creativity in the educational process has long been recognized most visibly in the requirement of theses and dissertations. It is obvious that the best person to direct research is someone who does research.

Consider some of the alternatives to the system by which mathematicians are rewarded. Actors and actresses struggle in poverty until they are recognized, and then are overcompensated. This appears to be usual in the performing arts. Most writers are neglected, but the few who appeal to the public become wealthy. The case of the artist is the least happy. How many dealers and collectors became rich because of Van Gogh? And what good did this do Van Gogh? The rewards of a mathematician are most equally distributed even in comparison with practioners of other sciences.

The support of mathematicians by royalty is a historical fact. The monarch had various motivations for doing this besides help wih infrequent technical matters; namely, to ornament his court, to prove his nation was more civilized

or just as civilized as another. The public relations value of mathematics still exists, and it works at many levels. If a state university boasts a productive mathematics department, it helps to attract industry. Does it help very much? Probably not; but how much is one half of one percent of fifty billion dollars? Moreover, the reputation of the mathematics department helps the graduates of the university when they seek employment. The added cost per student of a research oriented department versus a department of exploited teachers probably amounts to half of what the student spends on preparing his resume. And it probably makes twice the impression on the average prospective employer.

The much repeated argument that the most unlikely mathematical theory has resulted in advances in applied science is probably true enough; but I'm not fond of it. In the first place most mathematical contributions to technology have been by mathematicians who have been directly motivated by the technology. In the second place, a lot of mathematical aplications turn out to be of this sort: some economist or physicist comes upon some mathematical theory which appeals to him; he continues to expand the theory and but now calls it mathematical economics or mathematical physics. It seems to me that the other reasons I have cited demonstrate that the answer to McCann's question is "Yes."

William H. Ruckle
106 Whippoorwill Drive
Semeca. SC 29678, USA.

ARTICLES

Minimal Fitting Classes

Brendan McCann

This short survey provides an introduction to a developing area of fini soluble group theory. In it all groups considered will be taken to be finite a soluble, though some of the ideas discussed will have a more general validit Background to the group theory involved can be found in [8]. We begin wi the definition of a Fitting Class:

Definition 1 A *Fitting Class* $\mathcal{F}$ is a set of groups such that

(a) if G belongs to $\mathcal{F}$ then so does every isomorphic copy of G — this is t "class" property of $\mathcal{F}$;

(b) If $N \lhd G \in \mathcal{F}$ then $N \in \mathcal{F}$ i.e., $\mathcal{F}$ is closed with respect to norm subgroups;

(c) If $G = N_1N_2$, where N_1 and N_2 are normal subgroups of G and belong $\mathcal{F}$, then $G \in \mathcal{F}$ i.e., $\mathcal{F}$ is closed with respect to "normal products";

(d) $\mathcal{F}$ is non-empty — so all groups of order one are in $\mathcal{F}$.

Some examples of Fitting Classes are: $\mathcal{S}_p$ the class of all p-groups for t prime p; $\mathcal{S}_\pi$ the class of all (soluble) π-groups, where π is a collection of prim $\mathcal{N}_\pi$, the class of all nilpotent π-groups.

In order to provide a group-theoretic motivation for the study of Fitti Classes we mention briefly a result of Fischer, Gaschütz and Hartley [5]:

Theorem *If G is a finite soluble group and $\mathcal{F}$ is a Fitting Class, then the exists a unique conjugacy class of $\mathcal{F}$-injectors in G.*

An $\mathcal{F}$-injector is a subgroup, I, of G such that if N is subnormal in G (i if there exists a finite chain $N \lhd N_1 \lhd \cdots \lhd N_k = G$) then $I \cap N$ is $\mathcal{F}$-maxim in N, that is $I \cap N \in \mathcal{F}$ and $I \cap N$ is contained in no other subgroup of which is in $\mathcal{F}$.

For example, the $\mathcal{S}_p$-injectors of G are the Sylow p–subgroups of G, and the Hall π-subgroups are the $\mathcal{S}_\pi$-injectors.

Rather than pursue this structure-theoretic aspect of soluble group theory, we turn to the more mundane question of determining the smallest (i.e. minimal) Fitting Class containing some given group G. In most cases this is complicated and requires extensive knowledge about automorphism groups and normal products.

Definition 2 The Fitting class $\mathbf{Fit}(G)$ is defined by

$$\mathbf{Fit}(G) = \bigcap \{\mathcal{F} : \mathcal{F} \text{a Fitting Class containing} G\}$$

$\mathbf{Fit}(G)$ can be considered as the Fitting Class generated by G, since it is a Fitting Class which contains G and is contained in every Fitting Class of which G is an element. If G is non-trivial $\mathbf{Fit}(G)$ will contain all finite direct products of copies of G and its normal subgroups. However, there are also normal products which are not *direct* products - and this fact makes the construction of Fitting Classes in general very difficult: For example the group $S_3 \times C_2$ (S_3 is the symmetric group on three symbols, C_2 a cyclic group of order 2) is the normal (but not direct) product of two subgroups isomorphic to S_3. Thus by 1(c) $S_3 \times C_2 \in \mathbf{Fit}(S_3)$ and then by 1(b) we also have $C_2 \in \mathbf{Fit}(S_3)$. So there are 2-groups in $\mathbf{Fit}(S_3)$, even though S_3 itself has no (sub)normal 2-subgroups.

There is one case where minimal Fitting Classes have been determined, namely: if P is a non-trivial p-group then $\mathbf{Fit}(P) = \mathcal{S}_p$ (see [8] for a sketch of the proof); and, more generally, if H is nilpotent and $|H| = P_1^{\alpha_1} \dots P_k^{\alpha_k}$ where P_i is a prime and $\alpha_i \neq 0, \quad i = 1, \dots, k$, then

$$\mathbf{Fit}(H) = \mathcal{N}_\pi$$

where

$$\pi = \{p_1, \dots, p_k\}\,.$$

By considering non-nilpotent soluble groups, we come to the idea of Fitting length:

Definition 3 The Fitting length (also known as nilpotent length) of the soluble group G is the smallest number k such that there exists a series:

$$1 = N_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_k = G\,,$$

with N_i/N_{i-1} nilpotent (for $i \geq 1$) and $N_i \lhd G$ (for each i).

Thus nilpotent groups are of Fitting length one, – the terms "metanilpotent" and "nilpotent by nilpotent" are used for fitting length two. The task of determining minimal metanilpotent Fitting Classes has turned out to be very complicated indeed. We return to the group S_3, which is the "smallest" metanilpotent group. We already have $C_2 \in \mathbf{Fit}(S_3)$ and so:

$$\mathbf{Fit}(C_2) = S_2 \subseteq \mathbf{Fit}(S_3)$$

Furthermore, from Hawkes [6], we have that if $G = PQ$, $P \lhd G$, P an elementary abelian 3-group, Q a 2-group, then $G \in \mathbf{Fit}(S_4)$.

However $\mathbf{Fit}(S_3)$ is *not* the class of all "3 by 2" groups (that is $\{2,3\}$-groups with normal Sylow 3-groups), since Camina [2] has shown: $D_{18} \notin \mathbf{Fit}(S_3)$ – where D_{18}, the dihedral group of order 18, is "the" non-trivial extension of C_9 by C_2.

In fact we do not know at present what groups $\mathbf{Fit}(S_3)$ consists of, and the same applies to the Fitting classes generated by most other "well-known" small soluble groups, such as e.g. A_4, the alternating group on four symbols, or D_{14}.

Some progress has been made with metanilpotent groups whose structures are more complicated than those of S_3 or A_4. By specifying a suitable group, H, say, of the form $H = AB$, $A \lhd H$, A a p-group of nilpotent class 2 or greater, B a q-group $p \neq q$, and by placing suitable restrictions on the q-automorphisms of H, constructions of Hawkes [6] and Cossey [3] will define a Fitting Class containing H, thus narrowing the range of groups which might possibly be in $\mathbf{Fit}(H)$. Indeed, Brison, using the Hawkes construction, has in [1] been able to give an example of a minimal Fitting class for a metanilpotent group. It must be noted, however, that these are rather isolated examples and that much awaits discovery in the area of minimal metanilpotent Fitting Classes.

Given that Fitting Classes of Fitting length three or more must contain metanilpotent groups, the determination of minimal Fitting classes for groups of Fitting length three or more will have to wait until the metanilpotent question has been resolved. However, some progress has been made on the following less general question:

If G_1 and G_2 are both groups of Fitting length k, do either of the relations:

$$G_1 \in \mathbf{Fit}(G_2) \text{ or } G_2 \in \mathbf{Fit}(G_1)$$

hold?

In the case of Fitting length three, this question can be resolved in certain cases by using constructions due to Dark [4] and McCann [7,8]. These constructions take a single group G, which satisfies suitable restrictions about normal structure and its automorphism group, and derive a Fitting Class from it which is, like those of Hawkes, "near to being" $\mathbf{Fit}(G)$. The fact that G has Fitting length three is exploited in the proof in each case.

In order to state one of the nicer results we recall the definition of the Frattini subgroup:

The Frattini subgroup, $\Phi(G)$, of G is the intersection of all maximal subgroups of G. $\Phi(G)$ can also be characterized in the following way:

$\Phi(G)$ consists of those elements which can be discarded from any set of generators so that the reduced set still generates G. Now let G be a group such that

$$G/\Phi(O_2(G)) \cong S_4$$

where $O_2(G)$ is the product of all normal 2-subgroups of G. Then either $G \cong S_4$ or $G \notin \mathbf{Fit}(S_4)$ and $S_4 \notin \mathbf{Fit}(G)$. (The constructions used are essentially those of [8]).

Apart from direct applications of results about Fitting classes of Fitting length three or less, little is known about minimal Fitting classes of groups of Fitting length four or greater. It is possible that, due to their more complicated nilpotency structure, different problems will arise in the determination of such classes, but at present one can only speculate (no doubt vainly) as to what future research will reveal.

References

[1] O. Brison, *Relevant Groups for Fitting Classes*, J. Algebra 68, 1981, 31-54.

[2] A.R. Camina, *A note on Fitting Classes*, Math. Zeitschrift 136, 1974, 351-352.

[3] J. Cossey, *On metanilpotent Fitting Classes*, Research Report No. 18, 1986, Australian National University, Canberra.

[4] R.S. Dark, *Some examples in the theory of injectors of finite soluble groups*, Math. Zeitschrift 127, 1972, 145-156.

[5] B. Fischer, W. Gaschütz and B. Hartley, *Injektoren endlicher auflösbare Gruppen*, Math. Zeitschrift 102, 1963, 300-305.

[6] T.O. Hawkes, *On metanilpotent Fitting Classes*, J. Algebra 63, 1980, 495-483.

[7] B. McCann, *On Fitting Classes of Groups of Nilpotent Length Three*, Dissertation, Universität Würzburg, 1985.

[8] B.McCann, *Examples of minimal Fitting Classes of Finite Groups*, Archiv der Mathematik,49(3), 1987, 179–186

Department of Mathematics
University College Galway

Asymmetric Cryptography

Patrick Fitzpatrick

1 Introduction

In recent years a great deal of attention has been focussed internationally on the twin problems of *security* and *authentication* in the use of electronic communication systems for a wide variety of transactions including information storage and retrieval, banking and financial transactions and the transfer of legal documents (contracts, invoices etc.). These problems may be summarised as follows:
(a) security – the message must not be capable of interpretation or alteration in any way by an unauthorised person;
(b) authentication — the identities of the parties involved in the communication must be reliably established in such a way that neither can later repudiate any part of the transaction.

The need for cryptographic systems is thus placed firmly in the public domain and is no longer the sole preserve of government, diplomatic and military establishments.

The classical solution to problem (a) is the encryption of messages using a secret key known only to the transmitter and receiver. The key itself must be exchanged by some reliable method — a trusted courier, for instance. However, as the number of participants grows (consider, for example, the national and international branch network of a large banking corporation) the problem of *distribution and secure storage of keys* becomes exceedingly difficult. Moreover, the classical method provides no solution whatever to problem (b).

Since the publication of Diffie and Hellman's fundamental paper [8], it has widely been recognised that *asymmetric* (or *two-key* or *public-key)* cryptosymtems represent *in theory* the best approach towards a solution of these problems. In practice there are few realistic working models — proposed implementatins have either been shown to be insecure or too costly for application in general. As a consequence, a good deal of research has also been devoted to other methods (such as Siegenthaler's work on *stream ciphers* [40, 41]) and, in addition, attempts have been made to apply asymmetric tech-

niques to restricted types of transaction. This latter area is the subject of a major research effort by the EC [31].

The purpose of this article is to review progress in asymmetric cryptography, concentrating on the two principal proposed schemes — *knapsack methods* and *RSA methods*. These topics were the subject of M.Sc. project work carried out at University College, Cork in 1987 and I am grateful to my students Ian Holland, Harry Lande and Michelle Sliney for their endeavours, the results of which can be found in [14], [18] and [44] respectively. This survey owes much to their diligence.

Many readers will also be familiar with the central ideas of asymmetric cryptography. Simmons' Intelligencer article [43] is an excellent introduction (see also Gardner [9]), while Denning [7], DeMillo [6] and Simmons [42] all provide more comprehensive treatments of cryptography and data security. We conclude this introduction with a brief summary of the essence of these ideas.

Both parties to a communication have an *encryption function* E and a *decryption function* D with the following properties:

(i) $D(E(M)) = M$ for every valid message M;

(ii) E and D are easy to compute;

(iii) it is computationally infeasible to determine D from a knowledge of E.

A fourth property which may or may not be present is

(iv) $E(D(M)) = M$ for every valid message M.

The *key distribution problem* is solved when each user places his encryption function in a public file. When user A wishes to communicate "plaintext" M to user B he transmits the "ciphertext" $E_B(M)$ using $B's$ public encryption function E_B. On receipt, B calculates $D_B(E_B(M)) = M$ using his (secret) decryption function D_B. (In practice the actual algorithms used will be known to all parties — including potential intruders. The unknown part is the encryption/decryption key. Here, and throughout the paper we are referring to "algorithm plus key" as the "encryption/decryption function".) The *security problem* is solved provided an intruder can neither interpret $E_B(M)$ — which is the classical requirement — nor tamper with it. Property (iii) is crucial in this regard. Finally, the *authentication problem* is solved in the presence of property (iv), by the following protocol: A sends both $E_B(M)$ and $E_B(S)$

where $S = D_A(M)$; on receipt B computes $D_B(E_B(M)) = M$ and compares it with $E_A(D_B(E_B(S))) = E_A(S) = E_A(D_A(M)) = M$ using A's public encryption function E_A. If these are identical B is assured not only that A is the transmitter (since only A knows D_A) but also that the message sent was in fact M. Thus S is A's (*message dependent*) *signature* appended to the particular plaintext M, so it is ensured that A cannot later deny having sent the message or repudiate any of its content. Acknowledgement by B and message confirmation is required also and it is clear how an independent third party (such as a court of law) can establish the facts of transmission and reception together with the content of the message, in much the same way as is currently the case with paper transactions.

The existence or otherwise of functions satisfying (i) — (iii) or (iv) has not yet been established. Attempts so far have concentrated on the idea of putting some well-known hard problem between knowledge of E and D in such a way that some additional information will allow (computationally) easy access from one to the other. Thus the encryption function is regarded as a *"one-way" function,* that is, a function F for which $f(x)$ is easy to compute for every x, but for which, given y, it is computationally infeasible to determine x such that $f(x) = y$ without some additional *"trapdoor" information*. The two best-known attempts have tried respectively to put the knapsack problem and the integer factorisation problem between E and D. We take these up in turn.

2 Knapsack Methods

The *general knapsack problem* is as follows. Given a set of n postive integer weights $\mathbf{a} = (a_1, \ldots, a_n)$ determine whether a weight N can be obtained by adding together a subset of the given weights, that is, whether there exists a binary vector with n components $\mathbf{m} = (m_1, \ldots, m_n)$ such that $N = \mathbf{m}.\mathbf{a}$. It is well-known (see [10], for example) such that in this generality KNAPSACK is in the *class NP* — a proposed solution $\mathbf{m}$ can be checked in polynomial time, but no polynomial time algorithm is known for determining a solution $\mathbf{m}$ from $\mathbf{a}$ and N. Moreover, KNAPSACK is *NP-complete* so in a sense it is among the most difficult of *NP* problems. However, some instances of KNAPSACK are easy to solve. In particular, if the a_j form a *superincreasing sequence*: $a_{k+1} > \sum_{j=k+1}^{n} a_j$ for $k = 1, \ldots, n-1$ this is clearly the case, since then $m_n = 1$ if and only if $N \geq a_n$ and, for $1 \leq k \leq n-1$, $m_k = 1$ if and only if

$N - \sum_{j=k+1}^{n} m_j a_j \geq a_k$.

The original knapsack cryptosystem proposed by Merkle and Hellman [28] uses the following scheme. Select a superincreasing sequence $\mathbf{a}'$ and two positive integers P, Q such that P is invertible modulo Q and $\sum_{j-1}^{n} a_j' < Q$. Define $a_j \equiv a_j' P \pmod{Q}$ for all j. Now given the (binary encoded) message block $\mathbf{m}$ of length n, transmit $N = \mathbf{m}.\mathbf{a}$. Here $\mathbf{a}$ is the public-key part of the system. Only the receiver, who knows the secret trapdoor information (P, Q), can compute

$$\begin{aligned} N' &\equiv P^{-1}N \equiv P^{-1}(\sum m_j a_j) \\ &\equiv P^{-1}(\sum m_j a'_j)P \equiv \sum m_j a'_j \pmod{Q} \end{aligned}$$

and since $\sum a'_j < Q$, $N' = \sum m_j a'_j$. This is easily solved since $\mathbf{a}'$ is superincreasing. Note that this algorithm can be used for either security or authentication but not both because property (iv) does not hold — many plaintexts M are not valid ciphertexts so $E(M)$ cannot be calculated.

In 1980, Shamir and Zippel [39] showed that the basic Merkle-Hellman scheme — henceforth referred to as MH — could be broken "almost certainly" if the modulus were known to the cryptanalyst. Later Shamir [37] described a method by which MH could be broken "with high probability" in polynomial time. The essential point in his argument is that there are usually many so-called *trapdoor pairs* (P_0, Q_0) any one of which has the property that $\mathbf{a}'P_0 \pmod{Q_0}$ is superincreasing and gives the correct decryption of the ciphertext. He reduces the search for one of these pairs to a system of linear inequalities in several variables — arguing that four suffice in almost all cases — which he then solves using Lenstra's integer programming algorithm [21].

Merkle and Hellman also suggest in [28] that iterating their basic scheme could lead to improved security. However, building on Shamir's work, Adleman [1] (see also [3]) was able to demonstrate how to break the iterated system. He uses the *"lattice reduction"* algorithm of Lenstra, Lenstra and Lovasz [22] to convert a system of nonlinear equations — under some plausible hypotheses — to a system of linear inequalities and then uses Shamir's approach. He does not prove rigorously that his method works and extensive computer calculations were required to verify that it does so "with high probability in almost all cases" (see [3] for references and further details).

Several other variants of MH are known. Merkle and Hellman [28] themselves suggest a multiplicative version as follows:

Choose n relatively prime numbers $b_1, \ldots, b_n$, a prime p such that $p > b_1 b_2 \cdots b_n$ and a primitive root c modulo p. Determine a_j such that $b \equiv c^{a_j} \pmod{p}$ and use $\mathbf{a} = (a_1, \ldots, a_n)$ as the public key, keeping c and p secret. To transmit the (binary encoded) message $\mathbf{m} = (m_1, \ldots, m_n)$ calculate $k = \sum_{j=1}^{n} m_j a_j$ and send k. The receiver, knowing c and p, can find $m \equiv c^k \pmod{p}$ and since $m \equiv c^k \equiv \prod c^{m_j a_j} \equiv \prod b_j^{m_j} \pmod{p}$ and $p > \prod b_j$ then $m = \prod b_j^{m_j}$ so $m_j = 1$ if and only if $b_j \mid m$. The intruder must either find the m_j knowing only k and $\mathbf{a}$ or else find c and p. The latter brings in the well-known hard problem of computing logarithms in a finite field $(\mathbf{Z}_p)$. This scheme was successfully attacked by Odlysko [30] under the assumption that some of the b_j were known (indeed practical constraints would probably require them to be small — the first few primes, for example), and later by Adleman in more generality (see [3]).

It was clear from the start that a possible source of crytographic weakness in MH lay in the fact that the early knapsack weights in the superincreasing sequence would be significantly shorter (in binary length) then the later ones. Graham (see Lempel [20]) and Shamir [39] independently described another variant of MH in which they disguised the superincreasing structure by "padding" the weights before the modular multiplication so that they all had approximately the same length. This Graham-Shamir scheme has been attacked in certain cases — Brickell and Simmons [3] give the details — using methods similar to those of Adleman. incidentally, at the same time Odlysko [30] successfully attacked the method outlined by Shamir [36] for using the knapsack scheme for signatures instead of security.

In more recent developments Shamir [38] (see also Willett [46]) has described an iterated knapsack cryptosystem which starts from an arbitrary initial knapsack and thus avoids introducing the superincreasing structure. Also, Goodman and McAuley [13] have developed a knapsack based method which brings in the integer factorisation problem. To our knowledge neither of these methods has been cryptanalysed.

3 RSA Methods

The original RSA system (Rivest, Shamir and Adleman [34]) is probably the best known feature of the asymmetric cryptography literature. Given $n = pq$ where p and q are prime the Euler phi function of n is $\varphi(n) = (p-1)(q-1)$. If $(e, \varphi(n)) = 1$ and d is chosen so that $ed \equiv 1 \pmod{\varphi(n)}$ then a message

m (an integer between 0 and $n-1$) can be encrypted as $c \equiv m^e \pmod n$ and decryption is described by the congruence $c^d \equiv m^{ed} \equiv m^{1+k\varphi(n)} \equiv m \pmod n$ since $m^{k\varphi(n)} \equiv 1 \pmod n$ for any k. The public key is (e, n) and the private key is d. (It is clear that the selection of e, d works when $(m, n) = 1$ and easy to see that the equations hold also when p or q — but not both, of course — divides m.)

The essential feature of the method is that there is no known way using present day technology of factoring integers with about 200 decimal digits in any reasonable time. Recent work at the Sandia Laboratories [5] using a CRAY I computer is based on the "quadratic sieve" algorithm of Pomerance [32] and focuses on numbers with between 65 and 100 digits. Other fast factoring algorithms are due to Morrison-Brillhart [29] and Schroeppel (see [35]) with running times for factoring a 150-digit number of about 9×10^8 years and 2×10^{13} years respectively. Since no-one has yet been able to find a way of breaking the RSA scheme which does not involve factoring the modulus (or determining $\varphi(n)$ — it is easy to show this amounts to the same thing), the security is, at present therefore, very high and could be increased if necessary simply by increasing the lengths of p and q (but see the conclusion). Also since the RSA is commutative in the sense of property (iv), it can be used for authentication as well as security. On the other hand, the operation of modular exponentiation is very slow and leads to a throughput rate for the data which compares unfavourably with competing methods (such as stream ciphers or conventional ciphers like the Data Encryption Standard [4]).

As a consequence, the greatest efforts — apart from trying to break the RSA without factoring the modulus — have gone into trying to improve the speed of the algorithms used in its initialisation and implemention: random number generation, primality testing, determination of greatest common divisor and modular multiplication and exponentiation. The primality test suggested in [34] is the probabilistic one of Solovay and Strassen [45] although the OSIS report [31] claims that the test given by Knuth [15 p.379] is provably better. Of course the primes used should in some sense be randomly chosen — several good pseudo-random number generators are known (see, for example Golomb [12]), but the latest work [31] suggests using some physical process (such as heat, white noise or radioactive decay) as a source of truly random numbers. Finally, algorithms for calculations like the GCD and modular arithmetic are constantly being refined and improved (Blakley [2], for instance). Recent work by Kung and his associates on *systolic algorithms* and the corresponding computer architecture in providing a new and exciting

stimulus in this field [16, 17].

In a more general context the RSA may be regarded as using the polynomial function $g_e(x) = x^e$ to permute the elements of the ring $\mathbf{Z}_n$ (where $(e, \varphi(n)) = 1$). Lidl [23] and Lidl and Müller [24] consider other possible *"permutation polynomials"* for use in RSA-type cryptosystems. One such class of functions is the set of *Dickson polynomials* (or *Chebyshev polynomials of the first kind)* defined by

$$g_e(a, x) = \sum_{j=0}^{e/2} \frac{e}{e-j} \binom{e-j}{j} (-a)^j x^{e-2j} \quad (\text{for } a = \pm 1)$$

(when $a = 0$ we recover the RSA polynomial). In [24], it is shown that $(g_u \circ g_v)(a, x) = g_{uv}(a, x) = (g_v \circ g_u)(a, x)$ and Lausch et al [19] prove that $g_e(a, x)$ induces permutation of $\mathbf{z}_n$ with $n = pq$ and p, q prime if and only if $(e, (p^2-1)(q^2-1)) = 1$. Also, g_v is the inverse of g_u if and only if $uv \equiv= 1 \pmod{(p^2-1)(q^2-1)}$ which means that in using these polynomials for cryptosystems the inherent difficulty of factoring n is again brought into the calculation of the inverse v.

Further generalisations are possible using (Chebyshev) polynomials in several variables (see [24]) or rational functions (Rédei [33]) to induce permutations on $\mathbf{Z}_n$. To our knowledge none of these polynomial generalisations of the RSA has actually been analysed as part of a practical cryptosystem.

4 Conclusion

It is somewhat surprising that only a few proposals have been made for algorithms to implement asymmetric cryptosystems. In fact, apart from those mentioned above (and various short-lived variations — see, for example [26], [11]) only one other has been given, namely, a suggestion by McEliece [27] (see also [25] p.360) that *error-correcting Goppa codes* be used — the data is transmitted with many errors which only the recipient knows how to correct. In practice the Merke-Hellman scheme has never been used and the Graham-Shamir system has only been used briefly (by Western Electric), while the RSA was adopted by several groups and implemented on LSI chips at MIT (by Rivest et al) and at Sandia National Laboratories. As mentioned in the introduction the RSA is now the cryptosystem of choice by the European working group OSIS in the design of a secure *"token"* based payment and

financial transfer protocol. These implementations represent, however, only a small minority of the current applications of cryptography. Conventional cryptosystems such as the Data Encryption Standard or DES [4] are in use to a much greater extent and this reflects both a lack of confidence in asymmetric techniques together with the relative inefficiency of the RSA method.

Until now the approach to the design of asymmetric cryptosystems has been to take some known hard problem and build it into the derivation — without trapdoor knowledge — of the content of the message and the decryption function from knowledge of the ciphertext and the encryption function. Thus solving the hard problem implies breaking the cryptosystem and *it is hoped* that the converse is also the case, that is, that the cryptosystem cannot be broken *without* solving the hard problem. In no case has this been proved and, of course, as Shamir and others have amply demonstrated, breaking the knapsack cryptosystems so far proposed is *not* equivalent to solving KNAPSACK in polynomial time.

Thus there remains the underlying doubt as to whether any proposed scheme is secure and whether it will continue to be so into the future. But, in addition, there is he even more fundamental question: Do there exist genuine asymmetric cryptographic functions? Simmons [43] calls this "one of the most important questions in contemporary applied mathematics".

References

[1] Leonard M. Adleman, *On breaking the iterated Merkle-Hellman public-key cryptosystem*, Advances in Cryptology (ed. D. Chaum), 303-308 (Plenus 1985).

[2] G.R. Blakley, *A computer algorithm for calculating the product AB modulo M*, IEEE Trans. C-32, 497-500 (1983).

[3] Earnest F. Brickell and Gustavus J. Simmons, *A status report on knapsack based public-key cryptosystems*, Congressus Numerantium, 37, 3-72 (1983).

[4] *Data Encryption Standard (DES)*, National Bureau of Standards Publ. FIPS-PUB-46 (1977).

[5] James A. Davis and Diane B. Holdridge, *Factorization using the quadratic sieve algorithm*, Sandia Report SAND 83-1346 (1983).

[6] R. DeMillo et al, *Applied Cryptography, Cryptographic Protocols and Data Security*, Proc. Symp. in Appl. Math. 29, (AMS short course lecture notes) 1983.

[7] D.E. Denning, *Cryptography and Data Security*, Addison-Wesley 1982.

[8] W. Diffie and M.E. Hellman, *New directions in cryptography, IEEE Trans.* IT-22, 644-654 (1976).

[9] M. Gardner, *Mathematical Games (section)*, Sc. Amer. 237, 120-124 (1977).

[10] M. Garey, and D. Johnson, *Computers and Intractibility*, Freeman 1979.

[11] J-M. Goethals and C. Couvreur, *A cryptanalytic attack on the Lu-Lee public-key cryptosystem*, Philips J. Res. 35, 301-306 (1980).

[12] S.E. Golomb, *Shift Register Sequences*, Holden-Day 1967.

[13] R.M.F. Goodman, and A.J. McAuley, *New trapdoor-knapsack public-key cryptosystem*, IEE Proc. 132, 289-292 (1985).

[14] Ian M. Holland, *The RSA cryptosystem: Implementation considerations*, M.Sc. Project in Inf. Th., University College, Cork (June 1987).

[15] Donald E. Knuth, *The Art of Computer Programming Vol. 2 – Seminumerical Algorithms (2nd ed)* Addison-Wesley 1981.

[16] H.T. Kung, *Why systolic architectures?* Comp. Mag. 15, 37-46 (1982).

[17] H.T. Kung and R.P. Brent *Systolic VLSI arrays for polynomial GCD computation*, Technical Report Carnegie-Mellon University Comp. Sc. Dept. (May 1982).

[18] Henry A. Lande, *A survey of the RSA cryptographic scheme and related subjects*, M.Sc. Project in Inf. Th., University College Cork (June 1987).

[19] H. Lausch, W. Müller, and W. Nöbauer, *Uber die Struktur einer durch Dicksonpolynome dargestellten Permutations gruppe des Restklassenringes modulo n*, J. Reine Angew. Math. 261, 88-99 (1973).

[20] Abraham Lempel, *Cryptology in transition,* ACM Computing Surveys 11, 285-303 (1979).

[21] H.W. Lenstra Jr., *Integer programming with a fixed number of variables*, Math. of Op. Res. 8, 538-548 (1983).

[22] A.K. Lenstra, H.W. Lenstra Jr. and L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. 261, 515-534 (1982).

[23] R. Lidl, *On cryptosystems based on polynomials and finite fields*, Proc. EUROCRYPT 84, Lecture Notes In Comp. Sc. 209,10–15 (1985).

[24] R. Lidl and W. Müller, *Permutation polynomials in RSA cryptosystems*, Advances in Cryptology (ed. D. Chaum), 293-301 (Plenum 1984).

[25] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, C.U.P. 1986.

[26] S.C. Lu and L.N. Lee, *A simple and effective public-key cryptosystem*, Comsat Tech. Rev., 15-24 (1979).

[27] R.J. McEliece, *A public-key cryptosystem based on algebraic coding theory*, DSN Progress Rep. 42-44, Jet Propulsion Lab. (1978).

[28] R. Merkle and M. Hellman, *Hiding information and signatures in trapdoor knapsacks*, IEEE Trans IT-24, 525-530 (1978).

[29] M.A. Morrison and J. Brillhart, *A method for factoring and the factorization of F_7*, Math. of Computation 29, 183-205 (1975).

[30] Andrew M. Odlysko, *Cryptanalytic attacks on the multiplicative knapsack cryptosystems and on Shamir's fast signature scheme*, IEEE Trans. IT-30, 594-601 (1984).

[31] *Open Shops for Information Services*, OSIS European Working Group Final Report 1985-05-21 (1985).

[32] C. Pomerance, *Analysis and comparisn of some integer factoring algorithms*, Number Theory and Computers (ed. H.W. Lenstra Jr. and R. Tijdeman) Math. Centrum Tracts 154 (1978).

[33] L. Rédei, *Uber eindeutig umkehrbare Polynome in endlichen Körpern*, Acta Sci. Math. (Szeged) 11, 85-92 (1946).

[34] R. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM 21, 120-126 (1978).

35] J. Sattler and C.P. Schnorr, *Ein Effizienzvergleich der Faktorisierungsterfahren von Morrison-Brillhart und Schroeppel*, Computing 30, 91-110 (1983).

[36] A. Shamir, *A fast signature scheme*, MIT Lab. for Comp. Sc. Rep. TM-107 (July 1978).

[37] A. Shamir, *A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem*, Proc. IEEE Symp. Found. Comp. Sc. 145-152 (1982).

[38] A. Shamir, *Embedding cryptographic trapdoor in arbitrary knapsack systems*, Inform. Process Lett. 17, 77-79 (1983).

[39] A. Shamir and R.E. Zippel, *On the security of the Merkle-Hellman cryptographic scheme*, IEEE Trans. IT-26, 339-340 (1980).

[40] T. Siegenthaler, *Correlation immunity of nonlinear combining functions for cyptographic applications*, IEEE Trans. IT-30, 776-780 (1984).

[41] T. Siegenthaler, *Decrypting a class of stream ciphers using ciphertext only*, IEEE Trans. C-34, 81-85 (1984).

[42] G.J. Simmons (ed.), *Secure Communications and Asymmetric Cryptosystems*, AAAS Selected Symposia Series, Westview Press (1982).

[43] G.J. Simmons, *Cryptology: The Mathematics of secure communication*, Math. Intelligencer 1, 233-246 (1979).

[44] Michelle Sliney, *Trapdoor knapsack public-key cryptosystems*, M.Sc. Project in Inf. Th., University College Cork (June 1987).

[45] R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comp. 6, 84-85 (1977).

[46] M. Willett, *Trapdoor knapsacks without superincreasing structure*, Inform. Process Lett. 17, 7-11 (1983).

Department of Mathematics
University College Cork

Planks' Constants

S.D. McCartan T.B.M. McMaster

One of the hazards to be faced by the student of general topology is t proof of existence of spaces which are $T_{3\frac{1}{2}}$ (i.e. completely regular, or T chonoff) but not T_4 (i.e. normal). The standard example, the Tychon Plank (see [3]), has perhaps an unnecessarily austere public image since i usual presentation requires familiarity with ordinals which many undergra uates have not acquired. We here call attention to an alternative exampl due essentially to Thomas [4], which has no such prerequisite. Assuming elementary understanding of cardinal numbers we go on to show how to exe the construction to produce a family of non-normal Tychonoff spaces, and discuss some questions which this extension raises.

Example 1 (The Thomas Plank (see [3]).) Let X and Y be infinite di crete spaces, where X is uncountable. Form their Alexandroff ("one-point compactifications $A(X) = X \cup \{\infty\}$ and $A(Y) = \cup\{\infty\}$, their product spa $A(X) \times A(Y)$, and its subspace

$$P = (A(X) \times A(Y)) \setminus \{(\infty, \infty)\}$$

(If desired, $A(X)$ may be defined as carrying the Fort topology $\gamma \cup \epsilon(\infty$ where γ denotes the cofinite topology, and $\epsilon(\infty)$ the excuded point topolog in which the non-universal open sets are those to which ∞ does not belon — see [3].) Since $A(X)$ and $A(Y)$ are compact and T_2, as may be seen eith from the local compactness of X and Y or directly from the definition, so their product which is thus T_4 and $T_{3\frac{1}{2}}$ also. Now the subsets

$$T = X \times \{\infty\}, \quad R = \{\infty\} \times Y$$

are closed in P. If, however, it were possible to find dispoint open subset G,H of P with $T \subseteq G$ and $R \subseteq H$, choose a countably infinite subset Y' of and note that

(i) H would have to contain all but finitely many points on each horizont cross-section $X \times \{y'\}$ of $X \times Y'$, from which it follows that $(X \times Y') \setminus$ is at most countable, whereas

(ii) G must contain at least one point (indeed, infinitely many points) on each vertical cross-section $\{x\} \times Y'$ of $X \times Y'$, and so $(X \times Y') \cap G$ is uncountable.

These observations cannot be reconciled with the disjointness of G and H, and the contradiction establishes that P is not T_4.

Note that this example could be simplified by taking Y to be countable, thus rendering the selection of Y' unnecessary. (Indeed, even further siimplification can be achieved by abstraction. Begin with an uncountably infinite set X, let $z \in X$ and let Y be a countably infinite subset of $S \setminus \{z\}$. Consider X with the Fort topology $\gamma \cup \varepsilon(z)$, the product space $X \times X$, and its subspace $P = (X \times X) \setminus \{(z, z)\}$; then $T = (X \setminus \{z\}) \times \{z\}$, $R = \{z\} \times Y$ are each closed in P, and a routine modification of the previous argument will suffice.)

Remarks The source of the contradiction here is the existence of a cardinal number, in this case $\aleph_0$, which is less than that of X but exceeds that of the complement of a "neighbourhood of infinity". It is easily seen that we can obtain other examples of non-T_4 spaces just by replacing $\aleph_0$ by another infinite cardinal; further, it will be convenient to allow different cardinals to be associated with X and with Y. More thought, however, is needed to ensure that we not not lose the $T_{3\frac{1}{2}}$ property in the process, since the demonstration of this depended on three results which could be described as "cardinality-sensitive", namely

(a) $A(X)$ is compact,

(b) the product of two compact spaces is compact,

(c) compact plus T_2 implies T_4.

This is what will occuply most of our attention for the remainder of the present note.

Definitions Let α denote an infinite cardinal number. A topological space X is called α-compact (see [1] or, for a more recent reference, [2]) if every open cover of X has a subcover consisting of fewer than α sets. Thus, for example, $\aleph_0$-compactness is just (classical) compactness, and $\aleph_1$-compactness is the Lindelöf property. Given any space X, choose an object ∞ which does not belong to X and denote by $A_\alpha(X)$ the topological space defined on $X \cup \{\infty\}$ by declaring open

(i) the open subsets of the space X,

(ii) the complements in $X \cup \{\infty\}$ of the α-compact closed subsets of X, and

(iii) $X \cup \{\infty\}$ itself.

The obvious modifications of the Alexandroff argument will sow that $A_\alpha(X)$ is a α-compact and contains X as a subspace, and that X is dense in $A_\alpha(X)$ precisely when X is not α-compact.

Lemma 1 *Suppose that X is a discrete space. Then $A_\alpha(X)$ is $T_{3\frac{1}{2}}$ for any finite cardinal α.*

Proof It is certainly T_1 since singletons are α-compact. Now if F is a given closed subsety of $A_\alpha(X)$ and $p \notin F$, we consider two cases:

(a) $p = \infty$. Define $f : A_\alpha(X) \to [0,1]$ by $f(y) = 1$ if $y \notin F$, $f(y) = 0$ if $y \in F$.

(b) $p \neq \infty$. Define $f : A_\alpha(X) \to [0,1]$ by $f(p) = 1$, $f(y) = 0$ for all $y \neq p$.

In either case f is constant on a neighbourhood of ∞ and thus continuous there. Every other point of $A_\alpha(X)$ is isolated, so continuity elsewhere is automatic.

Example 2 Choose any two infinite cardinal numbers α and β. Denote by $\bar{\alpha}$ the supremum of all cardinals less than α, so that if α has an immediate predecessor than $\bar{\alpha}$ is the predecessor, while if not we have $\bar{\alpha} = \alpha$. Choose sets X and Y whose cardinalities satisfy

$$\text{card}(X) > \bar{\alpha}\,, \quad \text{card}(X) > \beta\,, \quad \text{card}(Y) \geq \beta\,.$$

Give X and Y their discrete topologies. By the lemma, the subspace

$$P = (A_\alpha(X) \times A_\beta(Y)) \setminus (\infty, \infty)$$

of the product space $A_{alpha}(X) \times A_\beta(Y)$ is $T_{3\frac{1}{2}}$. Now if T,R,G and H are as in Example 1, choose a subset Y' of Y having cardinality β and observe that

(i) the relative complement of H in each horizontal cross-section of $X \times Y'$ has cardinality at most $\bar{\alpha}$, and so the cardinality of $(X \times Y') \setminus H$ cannot exceed $\beta.\bar{\alpha}$ which is less than $\text{card}(X)$, whereas

(ii) G must contain at least one point on each vertical cross-section of $X \times Y'$, so the cardinality of $(X \times Y') \cap G$ is at least $\text{card}(X)$.

Thus the same contradiction as before has arisen, and P cannot be T_4.

Remarks Since $\bar{\aleph}_0 = \aleph_0$, the special case $\alpha = \beta = \aleph_0$ coincides with Example 1. If instead we choose $\alpha = \aleph_1$ (noting that $\bar{\aleph}_1 = \aleph_0$) and $\beta = \aleph_0$, we obtain a construct whose behaviour closely resembles that of the Tychonoff Plank. What we have obtained, then, is a family of "planks", parameterized so to speak by the two cardinals α and β which we regard as the "constants" describing a particular plank. The authors would at this point like to apologise for the excruciating pun in the title of this paper.

It is interesting to note what happens when one attempts to establish the $T_{3\frac{1}{2}}$ property (for Example 2) not directly, as in the lemma but by re-examining the points (a), (b) and (c) in the remarks following Example 1. Now $A_\alpha(X)$ is α-compact, but it is not in general true that a product of α-compact spaces is α-compact (see [3] for a simple example — Sorgenfrey's half-open square topology on a real plane—of a Lindelöf space X such that $X \times X$ is not Lindelöf) nor that an α-compact T_2 space is T_4 (for instance, see [3] again for the relatively prime integer topology on the positive integers). There are, however, special circumstances in which this line of argument recovers its validity, as we shall now see.

Definitions (i) An infinite cardinal number α is called *additively inaccessible* if it cannot be expressed as the sum of a lesser number of smaller cardinals: that is, if it is impossible to obtain a set of cardinality α by forming the union of a family of subsets, where each subset *and* the index set of the family have cardinality less than α. It is easily seen that a cardinal which has an immediate predecessor is additively inaccessible, but the problem of existence of other examples would lead us too deeply into axiomatic set theory to be appropriately discussed in this note.

(ii) A topological space in which each intersection of fewer than α open sets is open is called *α-saturated* (see [1] again). Thus every space is $\aleph_0$-saturated, a discrete space is α-saturated for every cardinal number α, and it is readily checked that, for discrete X, $A_\alpha(X)$ is α-saturated provided that α is additively inaccessible; indeed, we can as readily obtain a more general result:

Proposition 1 *Let α be an additively inaccessible cardinal number; then*

(i) *the union of fewer than α subsets of a space X, each of which is α-compact, is α-compact;*

(ii) *if X is α-saturated then so is $A_\alpha(X)$.*

Proof (i) If $\{C_i : i \in I\}$, where $\text{card}(I) < \alpha$, is a family of α-compact sets whose union is contained in that of a family $\{G_j : j \in J\}$ of open sets, then for each i in I there is a subset $J(i)$ of J such that $C_i \subseteq \bigcup\{G_j : j \in J(i)\}$ and $\text{card}(J(i)) < \alpha$. So $\bigcup\{C_i : i \in I\} \subseteq \bigcup\{G_j : j \in J'\}$ where the set $J' = \bigcup\{J(i) : i \in I\}$ has cardinality less than α.

(ii) Consider $x \in G = \bigcap\{G_i : i \in I\}$ where $\text{card}(I) < \alpha$ and each G_i is open in $A_\alpha(X)$, X being α-saturated. If $x \in X$ then $\bigcap\{G_i \cap X : i \in I\}$ is an open neighbourhood (in X) of x and is contained in G. If $x = \infty$ then $X \setminus G$ is α-compact by (i), and closed in X because X is α-saturated. Thus G is a neighbourhood of each of its elements, and must be open.

Proposition 2 *Let X and Y be α-saturated and α-compact, where α is additively inaccessible. Then $X \times Y$ is α-compact.*

Proof Given an open covering $\{G_\beta : \beta \in B\}$ of $X \times Y$, let y be any element of Y. For each x in X we can choose $\beta(x,y)$ in B, open $H(x,y) \subseteq X$ and open $J(x,y) \subseteq Y$ such that

$$(x,y) \in H(x,y) \times J(x,y) \subseteq G_{\beta(x,y)} .$$

Now fewer than α of the sets $H(x,y)$ will suffice to cover X; and if J_y denotes the (open) intersection of the $J(x,y)$ which correspond to these, we see that $X \times J_y$ is covered by a subfamily $\{G_\beta : \beta \in B_y\}$ of the given cover for which $\text{card}(B_y) < \alpha$.

Now the sets J_y, for y in Y, cover Y; so there is a subset Y' of Y such that $\text{card}(Y') < \alpha$ and $Y \subseteq \bigcup\{J_y : y \in Y'\}$. Then

$$X \times Y = \bigcup\{X \times J_y : y \in Y'\} \subseteq \bigcup\{G_\beta : \beta \in \bigcup\{B_y : y \in Y'\}\}$$

where $\bigcup\{B_y : y \in Y'\}$ has cardinality less than α, as required.

Proposition 3 *If X and Y are α-saturated topological spaces, then so is $X \times Y$.*

The proof is elementary.

Proposition 4 *An α-compact, α-saturated, T_2 topological space is T_4.*

The proof is the obvious modification of that of the classical case $\alpha = \aleph_0$

Remarks These four propositions constitute an alternative proof that the space $A_\alpha(X) \times A_\beta(Y)$ in Example 2 is T_4 (and therefore that P is $T_{3\frac{1}{2}}$), but only in the case where α and β are additively inaccessible and equal. Thus they add nothing to our understanding of Example 2, and are included here partly for their intrinsic interest and partly to point out how a relatively innocuous-looking topological question can quickly lead to areas of set theory in which Zermelo-Fraenkel will not suffice.

References

[1] M. Fitzpatrick and S.D. McCartan, *Homogeneity and Extremely Convergent Spaces*, Proc. Royal Irish Acad., 76A (1976) 111-116.

[2] M. Ó Searcóid, *An Essay on Perfection*, Bull. Irish Math. Soc., 18(1987) 9-17.

[3] L.A. Steen and J.A. Seebach, *Counterexamples in Topology*, Holt, Rinehart and Winston Inc., New York, (1970).

[4] J. Thomas, *A Regular Space, not Completely Regular*, Amer. Math. Monthly, 76(1969), 181.

Department of Pure Mathematics
The Queen's University of Belfast
Belfast BT7 1NN, Northern Ireland.

MATHEMATICAL EDUCATION

The New School Syllabi: How New?

Michael Brennan

When second level schools reopened in September 1987, Mathematics teachers faced the task of interpreting and teaching the three new Junior Cycle Maths Syllabi (hereafter the A–Course, B–Course and C–Course) drawn up by the Dept. of Education's Syllabus Committee over the years 1982-84. To help the teachers along, the publishing houses produced 6 or 7 competing textbooks and the Curriculum and Examinations Board attempted to produce a set of sample papers. These papers have not been published. One feature of them—the exclusion of multiple-choice questions—has probably been lost in the political turmoil of the CEB era.

Background

Pressure for revising the old syllabi (which had stood since 1973) came from three sources external to the Department:
1. from teachers who felt that the old Intermediate Certificate Higher course was too long, that Geometry was offputting, that the Lower course was too hard, the below–40% student success rate too high, and that a substantial percentage of Lower Course pupils were not being catered for by the syallabus;
2. from third level Mathematicians who felt that the Intermediate and Leaving Certificate syllabi were not producing students with a good grasp of the basics, And that the Geometry, in particular, was unsatisfactory;
3. from a certain number of industrial/commercial interests who were calling for "relevance" in the syllabi. Pilot schemes in alternative syllabi had taken place. (In the event, these had no noticeable influence on the revision).

The Revision

At the outset the Department of Education, adopting an earlier proposal from the IMTA, announced that there would be 3 Junior Cycle Syllabi to cater for a wide spread of ability. Until the exams are taken in 1990 nobody can say what percentages of pupils will follow each course to the bitter end but a reasonable estimate would be A: 30%, B: 50%and C: 20% at most. The A– and B–courses are modifications of the Higher and Lower Intermediate Certificate courses respectively, and the C–course is a new course for the very weak student.

Educational cutbacks will, however, limit options, especially in smaller schools. Also, parents and pupils may be unwilling to accept that the C–Course is where their best chances lie. Numbers following the C–Course may be falsely low. That would be a pity. There is enthusiasm in the IMTA for the C–Course which, it is felt, is custom-built, not merely a cut-down model of the older syllabi.

The new A– and B– courses by contrast are in the main exactly that —cut-down versions of previous Higher and Lower syllabi. The revision of the syllabi was carried out by reading through the topics listed in the Rialacha agus Clár and deciding which ones stayed in and which did not! In a small number of places new material was added. Did this result in a shortened A–Course, one of the objectives of the revision? Yes, but it is arguable whether or not it was shortened enough. The main reduction took place in Geometry: the number of proofs was cut from 29 to 19. But Statistics has been substantially lengthened.

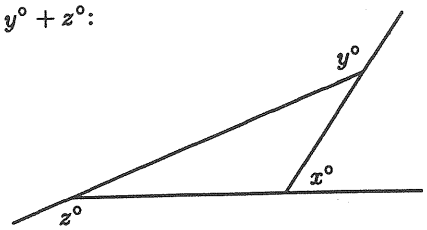
In the B–Course more time will be given to numerical work with financial bills of all kinds, with train timetables and distance charts. Here the number of Theorems has gone from 15 to 11 but the number of proofs (including construction proofs) from 18 to nil!

On the C–Course, Geometry stops at constructing triangles and Algebra at $3x + 4 = 19$ although powers are included. But all the traditional topics are touched on except trigonometry.

Proofproof

Maths has abeen proofproofed for the majority of pupils by these changes—unless one considers the solutions to questions such as the following as proofs:

(1) Evaluate $x^\circ + y^\circ + z^\circ$:



(2) Show that the triangle with vertices $a(1,2)$, $b(5,2)$, $c(3,1)$ is isoscele (Distance Formula supplied).

These appeared on one draft of a B–Course sample paper.

It is right that we should mark the departure of Geometry proofs by recall ing why Geometry has become so unpopular with teachers and pupils alike The non-intuitive nature of the old Geometry lies at the heart of it. Equipol lence, which students meet soon after finding their way along the corridors o their post-Primary school, combined with seemingly irrelevant proofs abou the image of a line under a central symmetry ... , together with the inabilit of teachers to think up unseen problems which were assailable by isometries did to death the cause of Geometry proofs, or indeed of any proofs, for up t 70% of our pupils, between 1973 and 1987.

In the new A–Course the treatment of Geometry reverts to a Hall an Stevens type, with congruence of triangles prominent. Proofs using isometrie will be accepted but equipollence and definitions of isometries as sets of cou ples are gone. Three extra theorems and "Equipollent couples" (undefined! appear in the B–syllabus, not for any good pedagogical reasons, I think. Th overall impression is of a war-torn Geometry course straddling two syllabi the A and B, unsure of who its ancestors are. There must surely be anothe revision in the years ahead to set it on simpler, more clear-cut lines.

As for the B and C courses it's a pity that some formal exercise in provin has not replaced the Geometry — such as proving that Superman is bette than Spiderman. Anything.

Quantity or Quality?

From a third level person's viewpoint, quantity in second level syllabi is spoil ing quality in the student. It will happen again with these syllabi: there ar

still too many topics blurring out the essentials. The trouble is, no syllabus committee is going to reduce the Junior Cycle syllabi to the seminal exercises of manipulating an arithmetic quotient, solving an algebraic equation, converting units, carrying through a 3-line proof (if A then B; but A; hence B) and postpone or forget altogether sets, relations, graphs, timetables, percentages, interest, trigonometry, statistics and geometry. Practicing a minimal set of skills like the first four mentioned would bore a large class and probably a teacher. Yet current syllabi preoccupation with a large number of detailed topics is hindering the teacher's purpose: that of nurturing mathematical skills in every pupil.

In Brief Then ...

Apart from hacking at the Geometry and throwing in an Iarnród Éireann timetable and an ogive there is little that is new in the new A and B syllabi. The emergence of the C–Course is a great achievement—unless that old dog cutback debilitates it at birth. The disappearance of proofs for the majority should be seen as an interesting experiment (to be kept under review?). As for relevance, "Relevance!" is an ephemeral cry made about syllabi. It comes and goes like a sí-ghaoithe and will come in due course to meet the new syllabi. The truth is, what industry needs, as what third level needs, is people with thinking skills. Mathematics classes are good vehicles for producing these skills — if the classes were not so crowded, the teachers not so harried and the syllabi not so full.

And by 1990 ...

By 1990 three new Leaving Certificate Syllabi must be ready to meet the pioneering class of '87.

When a ministerial order suspended the Department of Education Senior Cycle Syllabus Committee in 1986 (to make way for the CEB) the Committee had completed work on new Leaving Cert B and C syllabi. If this Committee's work is not discarded, work only needs to be done on the A syllabus (which leaves very little in the current revisions for third level people to influence [1]). For the record, the Junior Cycle Syllabus Committee consisted of 3 teachers' representatives, 3 school management representatives and 2–3

department inspectors. There was a third level representative on the Senior Cycle Committee.

There are questions still to be answered: What course should those first year pupils follow who started in September 1987 and who would normally have done the Group Certificate in 1990? Will calculators be allowed in time? And will the next Junior Cycle review be even more democratic than the last one? But we can at least raise our hats to the first syllabus in Irish schools which will have a certificate at three levels

References

[1] D.J. Hurley and M. Stynes, *Basic Mathematical Skills of UCC Students*, IMS Bulletin 17 (1986), 68–75.

Department of Physical and Quantitative Sciences
Waterford Regional Technical College.

The Theory of Blunders!

T.C. Hurley

We all come across mathematical blunders of all types and sizes when correcting scripts, answering questions, during discussions or when checking homework. Very often, these blunders can be corrected with no recurrence by convincing the students of the error of their ways e.g. a frequent error which occurs in different guises is $\frac{1}{a}+\frac{1}{b}=\frac{1}{a+b}$, so ask them to work out $\frac{1}{3}+\frac{1}{5}$ and $\frac{1}{3+5}$.

What happens on many occasions is that the student fails to stop and think that perhaps something he or she has been doing all his or her mathematical life, and getting away with it, may be incorrect, and in fact *utterly* false. A student at one time came up to me having failed the exam totally convinced he should have passed. I looked up his script and discovered that everywhere he should have integrated he differentiated and everywhere he should have differentiated he integrated, and nearly all done correctly! He flew through the exam at the next attempt. Why hadn't I spotted this during the year? (I have a reason, closely approaching an excuse!)

We don't expect such blunders from a student in our small honours classes, but they still occur and we can be on the lookout by marking some work before the official examination. We haven't anywhere approaching the resources to sort out these problems in our large pass classes. Unfortunately very often the first time we see some of our students' work is at the end of the year and then it is too late. What we need to do is take in work regularly, go through it ourselves and return the work *individually* pointing out errors and asking that problems, similar to those where the errors occurred, be attempted and handed in again for checking. Of course this is impossible with the very large numbers we have to cater for e.g. this year I have some classes of approximately 180, 130 and 100 students and to give this kind of attention to even one of these would take up all of my time, with no lectures anywhere else.

Is there a solution? One solution, not necessarily unique, would be to double the staff numbers in our Mathematics Departments, but of course this is impractical without even considering our present economic climate. (I have presented a solution so as a Mathematician need I go any further?) From my own experience of teaching small classes here and abroad I am totally

convinced that with the proper tuition most of the glaring blunders can be eliminated.

What I think we need to do as a first step is to convince the students that such blunders occur, in fact they *themselves* do make such errors and, to really get it to sink in, that such blunders will lose lots of marks thereby dramatically increasing the probability of failure. Explain the difference between a blunder and a slip, which all of us make from time to time. This hopefully will produce a type of self-reconsideration and discussion amongst themselves and with us and tutors when available. Whenever I point out a silly error in class there is always a great commotion, thinking perhaps it is a joke on some poor individual, but the class is never convinced when I point out that over 40% of them made that particular error on last year's exam.

I thought I'd try something out on this year's first year pass class. In order to set the background, the first year pass class at U.C.G., excluding Engineers, is broken into two groups, a "fast" stream getting 3 hours of lectures a week and a "slow" stream getting 4 hours of lectures a week, but both leading to the same examination. The streams are divided very roughly by the Leaving Certificate or Matriculation results, those with apparently weaker results going into the "slow" stream. I had the "slow" stream so I tried the true-false test reproduced below on these apparently weaker students but I feel the results would not have deviated very much had all the first year class been included. This true-false test most consisted of blunders I frequently encountered with a few other items thrown in just for discussion or fun. (Note in particular that question 19 is one of the fun ones which certainly produced some reaction and discussion.)

The test was given at the beginning of the lecture and students were informed that they had 40–45 minutes in which to complete it. They were asked to keep a record of their answers on the question sheet for discussion later and answer sheets were to be completed anonymously. All had finished within 35 minutes and answer slips were collected. For the rest of that class and for all of the next, I went through the quiz demonstrating where possible why such a statement was false (by e.g. assuming the statement was true and then proving that $0 = 1$). There were interesting discussions during and especially after each class.

Following the discussions with the students and reading through the questions now, I can see a number of improvements that could be made, but in the interests of accurate statistics, they are reproduced here as given. I am sure others have examples of their favourite and frequently occurring blunders and

I would be most happy to hear about these. I would be interested also to hear of other methods, tried or untried, on how to try to eliminate these glaring errors which occur right up to degree level.

Previous articles [1, 2, 3] report on deficiencies in the mathematical skills of our students but the reader will appreciate the differences between what is discussed in these and what is contained here although of course the two are interconnected in many ways.

The Questions

Which of the following are true(T) and which are false(F)?

1. $\frac{1}{a} + \frac{1}{b} = \frac{1}{c} \Rightarrow a + b = c.$
2. $x > y \Rightarrow \frac{1}{x} > \frac{1}{y}$, for all $x, y, x \neq 0, y \neq 0.$
3. $0^0 = 1.$
4. $x > y \Rightarrow \frac{1}{x} < \frac{1}{y}$ for all $x, y, x \neq 0, y \neq 0.$
5. $(x^2 + y^2)^2 = x^4 + y^4.$
6. $\sin ax = a \sin x.$
7. $\infty + \infty = \infty$ and $\infty - \infty = 0.$
8. $1^0 = 1.$
9. $\frac{1}{2} \div \frac{1}{2} = \frac{1}{4}.$
10. A function always has an inverse.
11. If $9 + h^2 = 64$ then $h = \pm\frac{8}{3}.$
12. $x > 0 \Rightarrow \frac{1}{x} < 0.$
13. $\frac{0}{0} = 1.$

14. $\dfrac{(x-1)(x+1)}{(x-1)(x+2)} = \dfrac{2}{3}$ when $x = 1$.

15. $3.(x+y)^{-1} = 3.x^{-1} + 3.y^{-1}$.

16. $-(x^2+4x+4) = -x^2+4x+4$.

17. $a^{-2} = \dfrac{1}{\sqrt{a}}$.

18. $(a^2)^3 = a^5$.

19. This question is false!

20. $\log x + \log x^2 = 3 \log x$.

21. $+\sqrt{0.04} = .02$.

22. The solution set of the equation $x(x+2) = 0$ is $x = -2$.

23. $(\sqrt{x})^{1/3} = (x^3)^{1/2}$.

24. $\dfrac{3(x-2)}{x^2-4} = \dfrac{3}{4}$ when $x = 2$.

25. $60° = \dfrac{\pi}{3}$ radians.

26. If $x^2 < 4$ then $x < \pm 2$.

Percentage Responses

Question	% answering True	% answering False	% not answering
1:	32%	68%	0%
2:	8%	92%	0%
3:	44%	55%	1%
4:	86%	13%	0%
5:	13%	89%	0%
6:	32%	65%	3%
7:	68%	31%	1%
8:	62%	38%	0%
9:	20%	80%	0%
10:	61%	36%	3%
11:	13%	87%	0%
12:	34%	66%	0%
13:	17%	83%	0%
14:	31%	69%	0%
15:	57%	42%	0%
16:	2%	98%	0%
17:	58%	40%	2%
18:	63%	37%	0%
19:	61%	22%	17%
20:	48%	49%	3%
21:	25%	73%	3%
22:	86%	15%	0%
23:	29%	67%	4%
24:	1%	98%	1%
25:	84%	13%	3%
26:	76%	23%	1%

There is a story (true or false?) that a certain teacher, nameless of course, in a certain school, nameless also, informed the school inspector that he/she advised his/her Intermediate Certificate class to *always* choose B in the multiple choice part of the Mathematics paper as he/she had done a survey of the previous few years and B had come up more often than any other. I believe there will be no multiple choice questions when the new Intermediate Certificate syllabus is examined.

References

[1] N. O'Murchu and C.T. O'Sullivan, *Mathematical Horses for Elementary Physics courses*, I.M.S. Newsletter, 6(1982), 50-54.

[2] *Report on the Basic Mathematical skills test of First Year Students in Cork RTC in 1984*, I.M.S. Newsletter, 14(1985), 33-43.

[3] Donal Hurley and Martin Stynes, *Basic Mathematical skills of U.C.C. students*, Bull. I.M.S. 17(1986), 68-75.

Department of Mathematics
University College
Galway

NOTES

Wedderburn's Theorem Revisited (Again)

Des MacHale

In a previous note in this Bulletin [3] we proved the following theorem which generalises the theorem of Wedderburn that a finite division ring is a field.

Theorem 1 *Let R be a ring with unity. If more than $|R| - \sqrt{|R|}$ elements of R are invertible, then R is a field.*

The bound $|R| - \sqrt{|R|}$ is the best possible because of the existence of $\mathbf{Z}_{p^2}$, which has exactly $p^2 - p$ invertible elements for any prime p, but yet is not a field.

Another formulation of Wedderburn's theorem is the following: If R is a finite ring with unity and every non-zero element of R is invertible, then R is commutative.

This naturally leads to the following question: If R is a finite ring with unity, can we force the conclusion that R is commutative by assuming that a proper subset of the non-zero elements are invertible? The purpose of this note is to prove the following:

Theorem 2 *Let R be a finite ring with unity. If every non-zero ring commutator $[x, y] = xy - yx$ of R is invertible then R is commutative.*

Proof Let $c = [x, y] \neq 0$. Consider the sequence $c, c^2, c^3, \ldots$ Since R is finite, $c^i = c^j$ for some $j > i \geq 1$. By hypothesis, c is invertible, so $c^{j-i} = 1$ and thus $c^{j-i+1} = c$. R now satisfies the hypothesis of a theorem of Herstein [1], $[a, b]^{n(a,b)} = [a, b]$ for $n(a, b) \geq 1$. If we are prepared to invoke the full power of this theorem, it follows at once that R is commutative. Alternatively, we can use the following more elementary result of Herstein [2]: If R is a finite ring in which every nilpotent element is cenmtral, then R is commutative.

We argue as follows. Let x, y, r be elements of R with $xy \neq 0$. Then $(yx-xy)^n = yx-xy$ implies that $(yx)^n = yx = 0$. Similarly, $(x(ry)-(ry)x)^n = x(ry) - (ry)x$ implies that $xry = 0$. A simple induction argument now shows that all nilpotent elements are central. Thus R is commutative.

Of course, R need not be a field, as the example $(\mathbf{Z}_4, \oplus, \otimes)$ shows.

Finally, we are indebted to Professor T.J. Laffey who has supplied the following ingenious alternative proof of Theorem 1.

Let R be a finite ring with unity 1, let $T = T(R)$ be its group of units and suppose that $T \neq R \setminus \{0\}$. Let $0 \neq x \in R \setminus T$ and let $T_0 = \{ t \in T \mid xt = x \}$. We note that T_0 is a subgroup of T and that $V = \{ xv \mid v \in T \}$ is a subset of $R \setminus (T \cup \{0\})$, with $|V| = |T|/|T_0|$. Let $W = \{ t-1 \mid t \in T_0 \}$. We note that $|W| = |T_0|$ and that $W \subset R \setminus T$, since $t - 1 \in T$ and $xt = x$ implies $x = 0$. Hence $|R| \geq |T| + |V| + 1 = |T| + |T|/|T_0| + 1$ and also $|R| \geq |T| + |T_0|$. Hence we deduce that $|R| - |T| \geq \max(|T_0|, |T|/|T_0| + 1$. So $|R| - |T| \geq \sqrt{|R|} + 1$.

References

[1] I.N. Herstein, *Noncommutative Rings*, Carus Mathematical Monographs, No. 15, Mathematical Association of America, Washington DC, 1968.

[2] I.N. Herstein, *A note on rings with central nilpotent elements*, Proc. Amer. Math. Soc. 5(1954), 620.

[3] D. MacHale, *Wedderburn's theorem revisited*, Irish Math. Soc. Bulletin 17(1986), 44–46.

Department of Mathematics
University College Cork.

Periodic Functions

Seán Dineen

This article arose out of correspondence between the author and Mark Heneghan regarding certain inconsistencies in the treatment of periodic functions in our secondary school texts. A complete and rigorous treatment of this topic requires the introduction of such concepts as convergent sequence, continuity, greatest lower bound, induction and linear independence. We have tried to minimize the impact of these concepts and at the same time to clarify the situation regarding the sum of periodic functions.

Definition 1 A function $f : \mathbf{R} \mapsto \mathbf{R}$ is *periodic* if there exists $a \neq 0$ such that

$$f(x + a) = f(x) \qquad \text{for all } x \in \mathbf{R}. \tag{1}$$

Any real number a satisfying (1) is called a *period* of f.

Remarks (1) If a is a period of f then so is $-a$, since $f(x) = f(x - a + a) = f(x - a)$.
(2) If a is a period of f and n is an integer then na is also a period of f. This follows from the identity

$$f(x + na) = f(x + (n-1)a + a) = f(x + (n-1)a) \, ,$$

using induction and our first remark.
(3) If a and b are periods of f then $a+b$ is also a period of f, since $f(x+a+b) = f(x + a) = f(x)$.

Example 1 Let f be given by $f(x) = \sin x$. Then f is periodic since $f(x + 2\pi) = f(x)$ for all $x \in \mathbf{R}$.

Example 2 Let f be given by

$$f(x) = \begin{cases} 0 & \text{if } x \text{ is rational} \\ 1 & \text{if } x \text{ is irrational} \end{cases}$$

If a and x are rational and y irrational then $a + x$ is rational and $a + y$ is irrational, and hence $f(x + a) = 0 = f(x)$ and $f(y + a) = 1 = f(y)$. Thus

every rational number is a period of f. If b is irrational and x is rational the $b+x$ is irrational and $f(x+b)=1\neq f(x)$ and hence b is not a period of f.

Examples 1 and 2 are typical of the only cases that can occur, as th following proposition demonstrates.

Proposition 1 *If f is a periodic function then exactly one of the followin holds:*

(a) there exists a sequence $(a_n)_n$ of positive periods of f which converges t zero;

(b) there exists a positive number a such that na, $n=0,\pm1,\pm2,\ldots$ form a the periods of f.

Proof If (a) does not hold then there exists a positive number δ such tha the interval $[0,\delta)$ does not contain a positive period of f. We claim that n interval of the form $[a,a+\delta)$ contains two distinct periods of f. Suppos otherwise, so that there exist periods b and c with $a\leq b<c\leq a+\delta$ for som a. By Remarks (1) and (3) $c-b$ is also a period of f, but since $0<c-b<$ this is a contradiction. Hence our claim is proven.

Now consider the intervals $I_1=[0,\delta]$, $I_2=[\delta,2\delta],\ldots,I_n=[(n-1)\delta,n\delta],\ldots$ Since f is periodic at least one of these intervals contains a period of f. Le n_1 be the least positive integer such that I_{n_1} contains a period of f. We hav seen that I_{n_1} can contain only one period. This is then the smallest positiv period of f. We denote it by a. By Remark (2), na, $n=0,\pm1,\pm2,\ldots$ ar periods of f. Suppose b is a further period. Then there exists an integer such that $na<b<(n+1)a$. By Remarks (1) and (3) $(n+1)a-b$ is also period of f. Since $0<(n+1)a-b<a$ this is a contradiction, and so no suc b exists. This completes the proof.

Remarks (4) If case (a) of Proposition 1 applies then, using our earlier re marks, it is not difficult to show that the periods of f form a dense subset o R.

(5) If f is continuous and $(a_n)_n$ is a sequence of periods of f which converge to a, it is easy to see that a is also a period of f. Hence, using (4), we ca conclude that if a continuous function f has a sequence of periods which con verges to 0 then f is a constant function.

(6) If one is willing to use the concept of greatest lower bound then the proo of Proposition 1 can be shortened.

Definition 2 If case (b) of Proposition 1 applies to f then the smallest positive period of f is called *the period* of f.

Thus we have singled out a special period of f. The statement "f has period a" should be read as "f is a periodic function and *the period* of f is a".

Combining Proposition 1 and Remark 5 we see that if f is a non-constant, continuous periodic function and a is a period of f then there exists a positive integer n such that the period of f is a/n. To determine n one must investigate further the function f.

Example 3 Let $f(x)=\sin x$. By Example 1, f is periodic and the period of f is $2\pi/n$ for some positive integer n.

Now $f(0)=0=\sin(2\pi/n)$. If $n>2$ then $2\pi/n<\pi$ and $\sin(2\pi/n)>0$. Hence $n\leq 2$. We now check $n=2$. Since $f(\pi/2+2\pi/2)=f(3\pi/2)=-1$ and $f(\pi/2)=1$ it follows that 2 is not the correct value for n. Hence $n=1$ and the period of f is 2π.

This result can, of course be obtained from a graph; while this suffices in practise, it is not a full proof.

We now consider the sum $f+g$ of two periodic functions (the case $f-g$ is handled in the same fashion).

Lemma 1 *If f and g are periodic and k is a common period of f and g then k is also a period of $f+g$.*

The proof is obvious.

Remark (7) If k is the period of both f and g, this does not give us precise information on the period of $f+g$ as the following example shows.

Example 4 Let $f(x)=\sin x+\cos(x/2)$, and let $g(x)=\sin x-\cos(x/2)$. It is easily seen that f and g are periodic and that 4π is the period of both functions (see Example 6). $(f+g)(x)=2\sin x$ and so the period of $f+g$ is 2π.

Example 5 Let $f(x)=\sin ax+\cos bx$ where a and b are non-zero real numbers. We shall now show that f is periodic if and only if a/b is a rational number.

We confine ourselves to the case where a and b are both positive; the other cases are handled similarly.

Suppose first that a/b is rational. Let $a/b = p/q$ where p and q are positive integers. Then $2\pi p/a = 2\pi q/b = k$, say.

Let $g(x) = \sin ax$ and $h(x) = \cos bx$. Since

$$g\left(x + \frac{2\pi}{a}\right) = \sin\left[a\left(x + \frac{2\pi}{a}\right)\right] = \sin(ax + 2\pi) = \sin ax = g(x)$$

and

$$h\left(x + \frac{2\pi}{b}\right) = \cos\left[b\left(x + \frac{2\pi}{b}\right)\right] = \cos(bx + 2\pi) = \cos bx = h(x)$$

we have that $2\pi/a$ is a period of g and $2\pi/b$ is a period of h. By Remark (2) $k = p\frac{2\pi}{a} = q\frac{2\pi}{b}$ is a common period of g and h. Hence by Lemma 1 k is a period of $f = g + h$ and so f is a periodic function

Conversely, suppose that $f = g + h$ is periodic. Let k be a non-zero period of f. Then $f(0) = f(k) = f(-k) = 1$. Hence

$$\begin{aligned} \sin(ak) + \cos(bk) &= 1 \\ \sin(-ak) + \cos(bk) &= 1 \end{aligned}$$

and this implies $\cos bk = 1$ and $\sin ak = 0$. Therefore $bk = 2n\pi$ and $ak = m\pi$ for some integers n,m and so $\frac{a}{b} = \frac{m}{2n}$ is a rational number.

The example above shows how to construct non-periodic functions which are sums of periodic functions; $\sin x + \cos(\sqrt{2}x)$, for instance, is not periodic.

In our next example we show how to find the period of $\sin ax + \cos bx$.

Example 6 Let $a = \frac{p}{q}b$ where p and q are positive integers which have no common factors. By Example 5 $f(x) = \sin(ax) + \cos(bx)$ is periodic, and we wish to find its period.

We introduce an auxiliary function $g(x) = \sin(px) + \cos(qx)$. Then g is also periodic, and f and g are related as follows:

$$\begin{aligned} g\left(\frac{b}{q}x\right) &= \sin\left(p\frac{b}{q}x\right) + \cos\left(q\frac{b}{q}x\right) \\ &= \sin(ax) + \cos(bx) + f(x) \\ \text{and} \quad f\left(\frac{q}{b}x\right) &= g\left(\frac{b}{q}\frac{q}{b}x\right) = g(x)\,. \end{aligned}$$

We now find a relationship between the periods of f and g. If l is a period of f then

$$g\left(x + \frac{b}{q}l\right) = g\left(\frac{b}{q}\left(\frac{q}{b}x + l\right)\right) = f\left(\frac{q}{b}x + l\right) = f\left(\frac{q}{b}x\right) = g(x)$$

Hence $\frac{b}{q}l$ is a period of g. Since the period of a continuous periodic function is the smallest positive period, it follows that

$$(\text{the period of } g) \le \frac{b}{q}\,(\text{the period of } f)$$

Similarly, if k is a period of g then $\frac{q}{b}k$ is a period of f. Hence

$$(\text{the period of } f) \le \frac{q}{b}\,(\text{the period of } g)$$

Therefore, we have

$$(\text{the period of } f) = \frac{q}{b}\,(\text{the period of } g)$$

We now proceed to show that the period of g is 2π. Since $g(x + 2\pi) = \sin p(x+2\pi) + \cos q(x+2\pi) = \sin(px+2\pi) + \cos(qx+2\pi) = \sin px + \cos qx = g(x)$, it follows that the period of g is $2\pi/\alpha$ for some positive integer α. We must show that $\alpha = 1$. Now

$$\sin px + \cos qx = \sin\left[p\left(x + \frac{2\pi}{\alpha}\right)\right] + \cos\left[q\left(x + \frac{2\pi}{\alpha}\right)\right]$$

Hence

$$\sin px - \sin\left[p\left(x + \frac{2\pi}{\alpha}\right)\right] = \cos\left[q\left(x + \frac{2\pi}{\alpha}\right)\right] - \cos qx\,,$$

and

$$2\cos\left(px + \frac{p\pi}{\alpha}\right)\sin\left(-\frac{p\pi}{\alpha}\right) = -2\sin\left(qx + \frac{q\pi}{\alpha}\right)\sin\left(\frac{q\pi}{\alpha}\right)\,,$$

so that

$$\cos\left(px + \frac{p\pi}{\alpha}\right)\sin\left(\frac{p\pi}{\alpha}\right) = \sin\left(qx + \frac{q\pi}{\alpha}\right)\sin\left(\frac{q\pi}{\alpha}\right) \qquad (2)$$

Now suppose $\alpha \neq 1$; we shall show that this leads to a contradiction. Since p and q have no common factor, at least one of p/α and q/α is not an integer. Suppose that p/α is not an integer. Then the left hand side of (2) is not zero, and hence the same is true of the right hand side, which implies that q/α is also not an integer. Similarly, if we assume that q/α is not an integer, then it follows that p/α is not an integer. Therefore we have

$$\sin\frac{p\pi}{\alpha} \neq 0 \qquad \text{and} \qquad \sin\frac{q\pi}{\alpha} \neq 0\,.$$

If we differentiate (2) $4n$ times we get

$$p^{4n}\cos\left(px+\frac{p\pi}{\alpha}\right)\sin\left(\frac{p\pi}{\alpha}\right) = q^{4n}\sin\left(qx+\frac{q\pi}{\alpha}\right)\sin\left(\frac{q\pi}{\alpha}\right)$$

Letting $x = 0$ we get

$$\left(\frac{q}{p}\right)^{4n} = \frac{\cos\left(\frac{q\pi}{\alpha}\right)\sin\left(\frac{p\pi}{\alpha}\right)}{\sin^2\left(\frac{q\pi}{\alpha}\right)} \neq 0 \tag{3}$$

Now if $p \neq q$ then when $n \to \infty$ the left hand side of (3) tends to either 0 or ∞. However, the right hand side of (3) is a non-zero constant. Hence $p = q$. Since p and q have no common factors, this can occur only when $p = q = 1$. In this case, (2) becomes

$$\cos\left(x+\frac{\pi}{\alpha}\right) = \sin\left(x+\frac{\pi}{\alpha}\right)$$

and hence $\tan(x+\pi/\alpha) = 1$ for all x. If we let $x = -\pi/\alpha$ we obtain a contradiction, and hence we must have $\alpha = 1$.

To summarise the above, we have shown the following: the period of $\sin(px)+\cos(qx)$ is 2π, and the period of $\sin((p/q)bx)+\cos(bx)$ is $2\pi q/b$ when p and q are positive integers with no common factor. We can use this to find the period of $\sin nx + \sin nx$, where m and n are arbitrary positive integers, i.e., making no assumption about common factors. Let $d = \gcd(m,n)$. Then there are positive integers m', n' such that $m = m'd$, $n = n'd$ and $\gcd(m',n') = 1$. Letting $a = m$ and $b = n$ we see that the period of $\sin nx + \cos mx$ is

$$2\pi\frac{m'}{m} = \frac{2\pi}{\gcd(m,n)}$$

Similarly, the period of $\sin(x/n) + \cos(x/m)$ is

$$\frac{2\pi nm}{\gcd(m,n)}$$

Periodic functions of the form $\sin ax \pm \sin bx$ and $\cos ax \pm \cos bx$ are treated in the same way, and simple functions such as $\sin ax \cos bx$ can be reduced to the cases discussed above by the use of appropriate trigonometric identities.

At this point, the reader may well ask the following questions:

(a) Is there any criterion for deciding if the sum of periodic functions is periodic?

(b) Are there any general methods of determining the period of a sum from the periods of the component functions?

(c) How does one determine the period of a general trigonometric polynomial i.e., a linear combination of powers of the functions $\sin x$ and $\cos x$?

(d) How large is the class of functions consisting of trigonometric polynomials?

A special case of question (a) is answered in Example 5. The same method can be used to obtain the following general result:

Proposition 2 *Let f and g be continuous periodic functions such that $f+g$ is non-constant. Let a and b be non-zero periods of f and g respectively. Then $f+g$ is periodic if and only if a/b is rational; furthermore, every period of $f+g$ has the form na/m for some integers n and m.*

This result is not true in general without the assumption of continuity.

As regards (d), the Stone-Weierstrass theorem shows that every continuous periodic function can be approximated uniformly by trigonometric polynomials, and the theory of Fourier Series shows that every continuous periodic function is the (pointwise) infinite sum of sines and cosines. Thus, by considering sums of sines and cosines, one is led to a very large class of functions, and there is no general simple method for calculating the period of a trigonometric polynomial.

There are, however, a number of techniques which can be used for arbitrary periodic functions, and which may help to locate the period. We briefly discuss these in our final example.

Example 7 The function $f(x) = 3\sin x - 4\sin^3 x$ has period $2\pi/3$. The easiest way to see this is to note that $f(x) = \sin 3x$. In the general case, however, we may not have such a nice formula for f, or we may be considering something like $\sin 16x$ expanded in sines and cosines and may not recognise the simple form of the function. Hence, we illustrate some techniques for finding the period without using the fact that $f(x) = \sin 3x$.

First, one checks easily that f is not constant. Now, since $\sin x$ has period 2π, we know that the period of f is $2\pi/n$ for some positive integer n. If $2\pi/n$ is the period of f then, since $f(0) = 0$ and $f(x) = \sin x\,(3 - 4\sin^2 x)$, we must have either $\sin(2\pi/n) = 0$ or $3 - 4\sin^2(2\pi/n) = 0$. Now $\sin(2\pi/n) = 0$ implies $n \leq 2$ and $3 - 4\sin^2(2\pi/n) = 0$ implies $\sin(2\pi/n) = \pm\sqrt{3}/2$. Since $f(x) > 0$ for small positive values of x it follows that the first positive zero of f is at least $\pi/3$. Hence $2\pi/n \geq \pi/3$, i.e. $n \leq 6$. It remains therefore to check the cases $n = 1, \ldots, 6$.

Now $f \geq 0$ on $[0, \pi/3]$, and the factorisation $\sin x\,(3 - 4\sin^2 x)$ shows that $f \leq 0$ on $[\pi/3, 2\pi/3]$. Hence $2\pi/n \geq 2\pi/3$, giving $n \leq 3$. Since 2π is a period of f, it suffices to check the cases $n = 2$ and $n = 3$.

$n = 2$: Since $f(\pi/2) \neq f(3\pi/2)$ we cannot have $n = 2$.

$n = 3$: Checking some values of x such as $\pi/6$ and $\pi/2$, one finds that $n = 3$ is not ruled out. Hence we check to see if $2\pi/3$ is a period of f.

Now

$$\sin\left(x + \frac{2\pi}{3}\right) = -\frac{1}{2}\sin x + \frac{\sqrt{3}}{2}\cos x$$

and

$$\sin^2\left(x + \frac{2\pi}{3}\right) = \frac{1}{4}\sin^2 x - \frac{\sqrt{3}}{2}\sin x\cos x + \frac{3}{4}\cos^2 x\,.$$

Hence

$$\begin{aligned} f\left(x + \frac{2\pi}{3}\right) &= \frac{1}{2}\left(-\sin x + \sqrt{3}\cos x\right)\left(3 - \sin^2 x + 2\sqrt{3}\sin x\cos x - 3\cos^2 x\right) \\ &= \sin x\left(-\sin x + \sqrt{3}\cos x\right)\left(\sin x + \sqrt{3}\cos x\right) \\ &= \sin x\left(3\cos^2 x - \sin^2 x\right) = \sin x\left(3 - 4\sin^2 x\right) \\ &= f(x) \end{aligned}$$

Hence $2\pi/3$ is a period of f, and therefore it is *the* period of f.

To summarise the methods used in this example:

(1) By inspection, find one period of the function (the smaller the better).

(2) Locate some zeros of f. The period is at least equal to the maximum distance between *adjacent* zeros. If it is not possible to find any zeros, try to locate points at which f takes the same value and proceed as above.

(3) The first step rules out all but a finite number of possible values. Using (2), check these values at a number of points. This will generally rule out most values.

(4) Finally, check which of the remaining values are periods of f.

At some stage one should also check that the function is non-constant. If one begins to get a constant value for f while carrying out the above steps, one should try to prove that f is constant.

Department of Mathematics
University College Dublin Dublin 4.

Lagrange Multipliers

Tony Christofides

It is not uncommon to hear a person say "I don't really understand Lagrange multipliers". The object of this note is to offer some explanation of what they are.

We recall that a necessary condition for the real-valued function $f(\mathbf{x})$, $(\mathbf{x} = (x_1, \ldots, x_n) \in \mathbf{R}^n)$ to have a stationary point at $\mathbf{a} \in \mathbf{R}^n$, subject to the "side conditions"

$$g_1(\mathbf{x}) = \ldots = g_k(\mathbf{x}) = 0 \tag{1}$$

is the existence of suitable Lagrange Multipliers, i.e. real numbers $\lambda_1, \ldots, \lambda_k$, such that

$$f'(\mathbf{a}) + \lambda_1 g_1'(\mathbf{a}) + \cdots + \lambda_k g_k'(\mathbf{a}) = 0 \tag{2}$$

Here, of course, $f', g_1', \ldots, g_k'$ are the derivatives of the relevant functions, so that f', for instance, is the vector

$$\left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right)$$

We shall assume throughout that we are dealing with functions which possess the required degrees of differentiability. Condition (2), together with the equations

$$g_1(\mathbf{a}) = \ldots = g_k(\mathbf{a}) = 0$$

usually enable one to determine the points $\mathbf{a}$.

Now think of the points satisfying the side conditions (1) as a variety V in $\mathbf{R}^n$. A point $\mathbf{a}$ is a stationary point of f subject to (1) if the directional derivative of f at $\mathbf{a}$ "in any direction contained in V" vanishes. More precisely, $\mathbf{a}$ is such that the directional derivative of f at $\mathbf{a}$ in the direction $\mathbf{u}$ is zero for every unit vector $\mathbf{u}$ tangent to V at $\mathbf{a}$.

This directional derivative is the scalar product $\langle f'(\mathbf{a}), \mathbf{u}\rangle$. Thus $f'(\mathbf{a})$ is in the orthogonal complement of the tangent space to V at $\mathbf{a}$. Let us denote this tangent space by $T_{\mathbf{a}}V$. Assuming that the side conditions (1) are not redundant, $g_1'(\mathbf{a}), \ldots, g_k'(\mathbf{a})$ are linearly independent and span the

normal space to V at $\mathbf{a}$. Thus these vectors form a basis for the orthogonal complement of $T_{\mathbf{a}}V$, and therefore

$$f'(\mathbf{a}) + \lambda_1 g_1'(\mathbf{a}) + \cdots + \lambda_k g_k'(\mathbf{a}) = 0$$

for some $\lambda_1, \ldots, \lambda_k$

More analytically now, let $f : A \to \mathbf{R}$, and $g_i : A \to \mathbf{R}$, for $i = 1, \ldots, k$ be sufficiently smooth functions—say with continuous second order derivatives—on an open subset A of $\mathbf{R}^n$. Suppose we have a "parametrisation" or "local coordinate system" for V at $\mathbf{a}$. Thus, we have an open subset B of $\mathbf{R}^k$ and a homeomorphism $\varphi : B \to \mathbf{R}^n$ which maps B onto an open set in V containing $\mathbf{a}$. We assume that φ is as smooth as the other functions considered. The existence of such a function is guaranteed by the implicit function theorem.

The problem of finding stationary points of f subject to (1) can now be reduced to that of finding ordinary stationary points, with no side conditions, for the function $f \circ \varphi$.

Letting $\varphi^{-1}(\mathbf{a}) = \mathbf{t}_0$, we apply the chain rule to the equation

$$(f \circ \varphi)'(\mathbf{t}_0) = 0\,,$$

which is a necessary condition for $\mathbf{t}_0$ to be a stationary point for $f \circ \varphi$. This gives

$$(f \circ \varphi)'(\mathbf{t}_0) = f'(\mathbf{a})\varphi'(\mathbf{t}_0) = 0$$

Hence $f'(\mathbf{a})$ is orthogonal to each of the columns of the matrix $\varphi'(\mathbf{t}_0)$, and it is well known that these columns span $T_{\mathbf{a}}V$.

In order to determine the nature of the stationary point $\mathbf{a}$, one must look at the quadratic part of $f(\mathbf{a}+\mathbf{h}) - f(\mathbf{a})$ for values of $\mathbf{h}$ for which $\mathbf{a}+\mathbf{h}$ lies on V, i.e. those $\mathbf{h}$ such that $\mathbf{a}+\mathbf{h} = \varphi(\mathbf{t}_0 + \mathbf{s})$, $\mathbf{s} \in \mathbf{R}^k$. Then

$$f(\mathbf{a}+\mathbf{h}) - f(\mathbf{a}) = Q(s) + \eta(\mathbf{s})$$

where

$$Q(\mathbf{s}) = \frac{1}{2}\left(f''(\mathbf{a})\left(\varphi'(\mathbf{t}_0)\mathbf{s}\right)^2 + f'(\mathbf{a})\varphi''(\mathbf{t}_0)(\mathbf{s})^2\right)$$

$|\eta(\mathbf{s})|$ being of the order of $\|\mathbf{s}\|^3$. Bear in mind that $f''(\mathbf{a})$ is a scalar valued bilinear mapping, while $\varphi''(\mathbf{t}_0)$ is a bilinear mapping with values in $\mathbf{R}^n$.

Let M be the matrix associated with the bilinear form Q. If M is non-singular and definite then $\mathbf{a}$ is an extreme point of f subject to (1). If M is non-singular and indefinite then $\mathbf{a}$ will be a conditional saddle point of f.

Finally, if M is singular, no conclusions can be drawn concerning the nature of the stationary point a.

We conclude with some examples.

Example 1 A sufficient condition for $f(x,y)$ to have a minimum at a stationary point (a,b) subject to a side condition parametrised by $x=\varphi_1(t)$, $y=\varphi_2(t)$ is

$$\begin{pmatrix} \varphi_1' & \varphi_2' \end{pmatrix} \begin{pmatrix} f_{xx} & f_{xy} \\ f_{xy} & f_{yy} \end{pmatrix} \begin{pmatrix} \varphi_1' \\ \varphi_2' \end{pmatrix} + \begin{pmatrix} f_x & f_y \end{pmatrix} \begin{pmatrix} \varphi_1'' \\ \varphi_2'' \end{pmatrix} > 0$$

Example 2 Let $f(x,y)=1-2xy$. Then f has a maximum at $(0,0)$ subject to $y-x^3=0$, but has neither a maximun nor a minimum at $(0,0)$ subject to $y-x^2=0$. In both cases we have $M=0$.

Example 3 The function $f(x,y,z)=1-2xy-2xz-2yz$ has a stationary point at $(0,0,0)$. Parametrising the side condition $y=z$ by $\varphi(r,s)=(r,s,s)$, we find that

$$M=\begin{pmatrix} 0 & -2 \\ -2 & -2 \end{pmatrix}$$

which is indefinite. $f(x,y,z)$ has a maximum at $(0,0,0)$ subject to $x=y=z$, but has a minimum at $(0,0,0)$ subject to $-x=y=z$. The point $(0,0,0)$ is a saddle point subject to $y=z$.

Department of Mathematics
University College Galway

A Note on Integrating Composed Functions

Paul Barry

This note groups together several concepts that are met at different places in a first course on real analysis in a way that allows graphical representation. It provides a generalisation of the formula (see [1]):

$$\int_{f(a)}^{f(b)} f^{-1}(y)\,dy+\int_a^b f(x)\,dx=bf(b)-af(a) \tag{1}$$

which has a certain pedigree—see [2], [3] and particularly [4], where a proof is given in the case where f and f^{-1} are assumed only to be integrable.

We shall use the (Riemann-)Stieltjes integral as given, for instance, in [7]. We deal only with definite integrals.

We begin by recalling the formula for integration by parts for the Stieltjes integral. Let $u,v:[c,d]\to\mathbf{R}$, and assume the integral $\int_c^d u\,dv$ exists. Then

$$\int_c^d u\,dv+\int_c^d v\,du=u(d)v(d)-u(c)v(c) \tag{2}$$

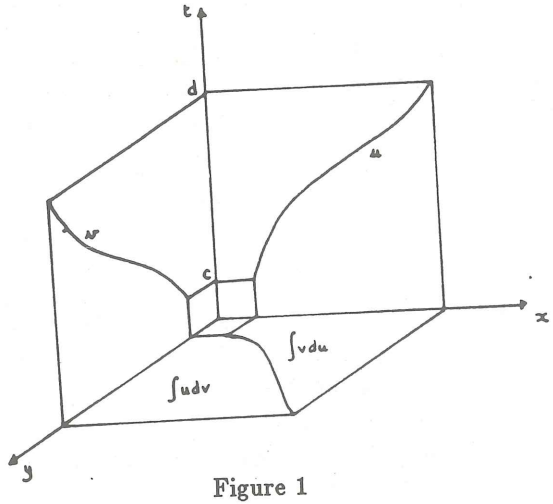


Figure 1

A particular case of this is illustrated in figure 1 where u and v are increasing. In this special case, note that $y = v \circ u^{-1}(x)$ represents the curve in the (x, y)-plane which also has parametric representation $t \mapsto (u(t), v(t))$. If moreover u and v are differentiable, we note that

$$\begin{aligned} \frac{dy}{dx} &= v'\left(u^{-1}(x)\right)\left(u^{-1}\right)'(x) \\ &= v'(t) \cdot \frac{1}{u'\left(u^{-1}(x)\right)} = \frac{v'(t)}{u'(t)} \end{aligned}$$

shows the link between the chain rule and the derivative of a parametrised curve.

We now apply these results to the following situation, where for sinplicity we shall assume that $f : [a, b] \to [c, d]$ is strictly increasing, with $f(a) = c$ and $f(b) = d$. Let $g : [c, d] \to \mathbf{R}$ be integrable with respect to f^{-1}. Then from (2) we obtain

$$\begin{aligned} \int_c^d f^{-1}\, dg + \int_c^d g\, df^{-1} &= f^{-1}(d)g(d) - f^{-1}(c)g(c) \\ &= f^{-1}\left(f(b)\right) g\left(f(b)\right) - f^{-1}\left(f(a)\right) g\left(f(a)\right) \end{aligned}$$

Letting $F = g \circ f$, we get

$$\int_c^d f^{-1}\, dg + \int_c^d g\, df^{-1} = bF(b) - aF(a) \tag{3}$$

By imposing stronger conditions on f and/or on g, we can find more manageable forms of (3). For example, if we assume that f is continuous, then the formula for change of variable in a Stieltjes integral yields the following:

$$\int_c^d f^{-1}(y)\, dg(y) = \int_{f^{-1}(c)}^{f^{-1}(d)} f^{-1}\left(f(x)\right)\, dg\left(f(x)\right) = \int_a^b x\, dF(x)$$

and

$$\int_c^d g(y)\, df^{-1}(y) = \int_{f^{-1}(c)}^{f^{-1}(d)} g\left(f(x)\right)\, df^{-1}\left(f(x)\right) = \int_a^b F(x)\, dx$$

Hence we obtain (not surprisingly!)

$$\int_a^b x\, dF(x) + \int_a^b F(x)\, dx = bF(b) - aF(a) \tag{4}$$

Finally, if we assume that g^{-1} exists and is continuous, then another appeal to the formula for substitution in a Stieltjes integral yields

$$\int_c^d f^{-1}(y)\, dg(y) = \int_{g(c)}^{g(d)} f^{-1}\left(g^{-1}(z)\right)\, dg\left(g^{-1}(z)\right) = \int_{F(a)}^{F(b)} F^{-1}(z)\, dz$$

Hence we get the following formula relating the integral of a composed function and its inverse:

$$\int_{F(a)}^{F(b)} F^{-1}(z)\, dz + \int_a^b F(x)\, dx = bF(b) - aF(a) \tag{5}$$

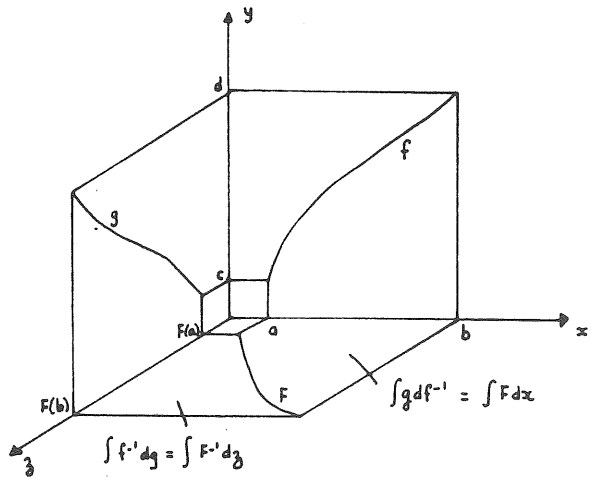


Figure 2

The special case $g(y) = y$ yields (1). Formulas (3)–(5) are illustrated in a special case in figure 2. Notice that in this case the curve $z = F(x)$ has parametrisation $y \mapsto (f^{-1}(y), g(y))$. In the case that f and g are differentiable, the $F'(x) = g'(y)/(f^{-1})'(y) = g'(y)f'(x)$ as we would expect.

As an example in this latter case, we take $f(x) = \tan x$ On $[0, \pi/4]$, and $g(y) = y^2$ on $[0, 1]$. Then (3) and (5) yield

$$\int_0^1 \arctan\sqrt{z}\, dz + \int_0^{\pi/4} \tan^2 x\, dx = 2\int_0^1 y \arctan y\, dy + \int_0^1 \frac{y^2}{1+y^2}\, dy = \frac{\pi}{4}$$

In particular, we find (see figure 3):

$$\int_0^1 \arctan\sqrt{z}\,dz = \frac{\pi}{2} - 1$$

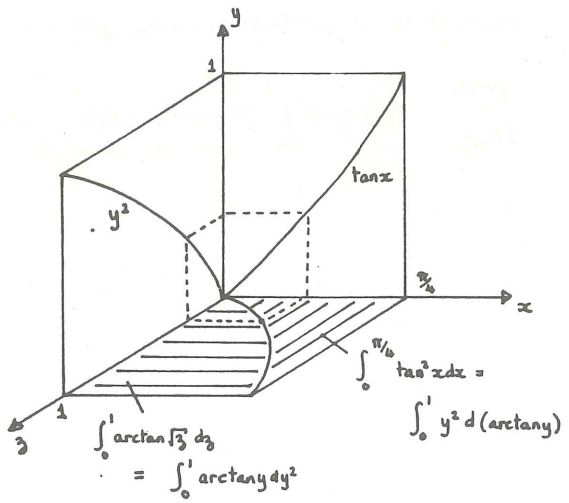


Figure 3

A less elementary but perhaps more instructive example is obtained by taking $f(x) = e^x$ and $g(y) = [y]$. Using (3), we get

$$\int_1^n \ln y\, d[y] + \int_0^{\ln(n)} [e^x]\,dx = n\ln(n) \qquad (6)$$

The first integral here is $\sum_2^n \ln(j) = \ln(n!)$. Hence we obtain

$$\ln(n!) = n\ln(n) - \int_0^{\ln(n)} [e^x]\,dx\,, \quad \text{or}$$

$$n! = \frac{n^n}{e^{\int_0^{\ln(n)} [e^x]\,dx}}$$

By estimating the integral appearing here, we can obtain some simple bounds

on $n!$. For example

$$\int_0^{\ln(n)} [e^x]\,dx < \int_0^{\ln(n)} e^x\,dx = n - 1$$

and hence

$$n! > e\left(\frac{n}{e}\right)^n$$

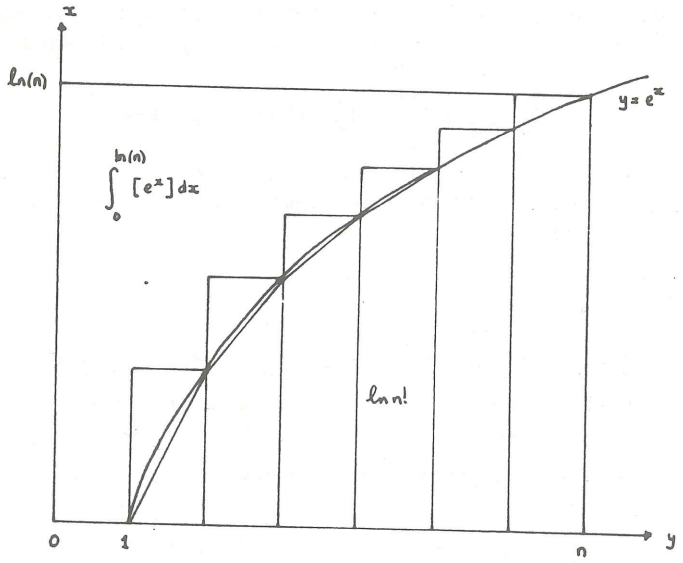


Figure 4

On the other hand, subtracting the areas of the triangles in figure 4,

$$\int_0^{\ln(n)} [e^x]\,dx > \int_0^{\ln(n)} e^x\,dx - \sum_{j=2}^{n} \frac{1}{2}\left(\ln(j) - \ln(j-1)\right)$$

$$= n - 1 - \frac{1}{2}\ln(n)$$

which yields $n! < e\sqrt{n}(n/e)^n$. Hence at very little expense (6) yields the following well known bounds:

$$e\left(\frac{n}{e}\right)^n < n! < e\sqrt{n}\left(\frac{n}{e}\right)^n$$

Reverting to the general case, where f is arbitrary and $g(y) = [y]$, we obtain the formula

$$\sum_{f(a)<n\le f(b)} f^{-1}(n) + \int_a^b [f(x)]\,dx = b\,[f(b)] - a\,[f(a)] \qquad (7)$$

For example, $\sum_1^{N^2} \sqrt{n} = N^3 - \int_0^N [x^2]\,dx$.

So far we have only considered increasing functions. The reader may be interested in deriving and interpreting graphically the following equation:

$$\sum_1^N \frac{1}{n^s} + \int_1^{N^{-s}} \left[x^{-(1/s)}\right] dx = N^{1-s} - 1$$

I would like to record my indebtedness to my colleague Tom Power for references [4] and [8].

References

[1] B.M. Dean, *Integrating inverse functions*, IMS Bull. 19(1987), 82–83.

[2] F.D. Parker, *Integrals of inverse functions*, Amer. Math. Monthly 62(1955), 439–440.

[3] J.H. Staib, *The integration of inverse functions*, Math. Magazine 39(1966), 290–291, reprinted in [8].

[4] J.R. Giles, *Real Analysis*, John Wiley & Sons, 1972; Ex. 4. p. 107, and pp. 162–164.

[5] K. Kreith, *A geometric construction of composite functions*, Amer. Math. Monthly 69(1962), reprinted in [8].

[6] L.M. Graves, *The Theory of Functions of Real Variables*, McGraw-Hill, 1956.

[7] T.M. Apostol, *Mathematical Analysis*, Addison-Wesley, 1969.

[8] T.M. Apostol et al. (ed.), *Selected Papers on Calculus*, MAA, 1969.

Department of Physical and Quantitative Sciences
Regional Technical College, Waterford

CONFERENCES

Operator Theory and Operator Algebras University College Cork

The Third Annual Conference on Operator Theory and Operator Algebras will be held in University College Cork, from Wednesday 29th June to Saturday 2nd July, 1988. The principal speakers will include

I.D. Berg (Illinois)
L. Brown (Purdue)
L. Cuntz (Marseille)
Z. Slodkowski

Further information can be obtained from the organizers:

G.J. Murphy & R.E. Harte
Department of Mathematics
University College
Cork, Ireland.

Conference on Functional Analysis El Escorial, Spain

A Conference on Functional Analysis will be held in El Escorial, Madrid, from June 13 to 18, 1988. The Organising Committee consists of J. Ansemil, F. Bombal and J.G. Llavona.

It is expected that the main speakers will include R. Aron, K.D. Bierstedt, J. Diestel, J.M. Isidro and M. Valdivia.

Further information can be obtained from

Departmento de Análisis Matemático
Facultad de Matemáticas
Universidad Complutense
28040 Madrid, Spain

EARN:W116@EMDUCM11

Groups In Galway 88

It has been decided to celebrate the tenth anniversary of this meeting by adding an extra day to the usual (two-day) format. The 1988 meeting will commence after lunch on Thursday May 26 and conclude after lunch on Saturday May 28.

Among the speakers will be Laci Kovacs and Mike Newman, both from ANU, Canberra. Any enquiries should be addressed to:

Dr. J. McDermott
Groups in Galway 88
Department of Mathematics
University College Galway
Galway, Ireland.

Real Analysis Symposium, Coleraine

A Symposium on Real Analysis will take place in Coleraine From August 9th to 12th, 1988.

The main speakers will include P. Bullen (British Columbia), G. Cross (Waterloo, Ontario), R. Henstock (Ulster), J. Kurzweil (Prague), P.Y. Lee (Singapore), J. Mawhin (Louvain), W. Pfeffer (California Davis) and C.A. Rogers (U.C. London).

Further details can be obtained from:

P. Muldowney
Magee College
Derry, Northern Ireland

BOOK REVIEWS

MATHEMATICS AND OPTIMAL FORM by Stefan Hildebrandt and Anthony Tromba
Scientific American Books, 1985, xvi+215pp. ISBN 0-7167-5009-0

> "Namely, because the shape of the whole universe is most perfect and, in fact, designed by the wisest creator, nothing in all the world will occur in which no maximum or minimum rule is simehow shining forth."
> *Leonhard Euler*

This quotation from Euler illustrates the depth of the current connecting mathematics with the search for an understanding of the origin, purpose and structure of the world. One of the oldest examples of the search for a unifying principle is that of Xenophanes (about 565–470 BC) who established the existence of a unique God, who is necessarily spherical, by an argument from homogeneity. More recently, we have the string theories of particle physics which seek to derive all four fundamental forces of nature by considering Riemann surfaces embedded as minimal surfaces in a ten-dimensional space-time.

The authors of this book are well-known for their work on variational problems in partial differential equations, and particularly on minimal surfaces. Thus they have a professional interest in soap films, where fascinating photographs of complex bubbles go hand in hand with hard analysis, a priori estimates, and novel geometric constructs.

The book appears in the excellent Scientific American Library series, and therefore raises hopes that are not entirely filled in this case. There are lots of entertaining anecdotes and quotations, and many interesting pictures. There is an impressive variety of examples of extreme behaviour and extremal principles. What is missing is the unfolding of a logical argument, or a series of deepenong insights such as is offered by some other books in the collection such as Weinberg: "The Discovery of Subatomic Particles", and Atkins: "The Second Law". Also, there is an inclination to include material which, while of considerable interest, is not closely relevant to the main theme. For example, a

page is given to the story Aeneas and Dido, as an offshoot of the isoperimetric property of the circle.

All in all, this is a fascinating collection, drawn from legends. philosophy, natural science, literature and art, illustrating mankind's search for perfection.

D.J. Simms
School of Mathematics
Trinity College, Dublin.

CALCULUS FOR PHYSICS by Richard Dalven
McGraw-Hill, 1984, x+149pp. St£8.25

Cries of frustration emanating from both teachers and pupils have been heard with increasing frequency in introductory physics courses in recent years - inadequate mastery of elementary mathematics being the source of the anguish on both sides. Indeed, the pages of this Bulletin have not been immune from the consequences of this problem [1,2]. While considerable study of the situation on both sides of the Atlantic has isolated some of the causes of this worldwide problem, finding sensible remedies has proved more difficult.

The widespread nature of this very real problem, however, has spawned a growth industry of books, self-teaching aids, computer-aided-learning packages and similar patent medicines, all designed to help the student to overcome his/her difficulties prior to, or in parallel with, an introductory course in physics. The principal difficulty with these appraoches is that they tend to assume that the student has infinite time at his/her disposl to undertake remedial study of the required mathematical techniques. Some "Mathematics for Introductory Physics" or "Calculus for the Scientist and Engineer" books exceed 1000 pages! Many of the self-pacing aids require long intensive sessions and lack suitable instructional material. The physics teacher who attempts to incorporate some revision of mathematical methods into the course, soon finds

himself teaching a course in mathematics only, and usually an inadequate one at that.

Here at last is a litle book which manages to get the balance right for those students whose problems are principally due to an inadequate background in elementary calculus. The book is designed for students taking their first course in physics and who have already taken, or are taking concurrently, a course in differentiation and integration. In the Irish situation this book would be useful for students taking Leaving Certificate higher level courses in both physics and mathematics or for those taking a first year course in introductory physics at a third-level institution. Richard Dalven is an experienced lecturer in freshman physics at the University of California at Berkeley and he shows a great sympathy for the problems encountered by students at this level. No pretence is made that this book represents a course in mathematics; rather, this is a review of introductory calculus, particularly where it is applied in elementary physics courses. Throughout the book the student is referred to his/her course in calculus in a refreshingly direct and informal tone. ('I would suggest that you work through this material fairly slowly, using your calculus book to refresh your memory on the mathematical points').

In a mere 118 pages of text all the essential topics needed for an introductory physics course are reviewed. No attempt is made to teach physics *per se* and the applications taken from physics are confined to the very simple. An emphasis is placed, however, on the interpretation of the key concepts in differentiation and integration as they arise in physics at this level.

Physics teachers are often amazed at the resistance of some mathematics teachers to invoke examples from everyday experience as an aid to understanding. This waste of good pedagogical opportunity seems extraordinary to this reviewer who had the particular privilege to be introduced to calculus by the late Mr. Fred Holland. Thirty years on, I still vividly recall him racing up and down the classroom with the floor covered with chalk lines as he kept reducing the distance over which he timed himself. His use of his pupils' understanding of the idea of speed to communicate insight of the nature of a derivative was, like all his teaching, masterful.

Dr. Dalven's book comprises two main sections, *viz*, derivatives and differentials (Chapter 2) and sums and integrals (Chapter 3). These are preceded by a short chapter in which the ideas of variables, functions and graphs are reviewed. It seems to be precisely in the area of the essential concepts of variables and functional relationships that the point of view of the mathematician has diverged most strongly from the physicist in recent years. Surely teachers

of mathematics and physics should give some thought to why so many of our students fail to recognize in our respective approaches what must in the last resort be one and the same concepts. Dr. Dalven's viewpoint in these matters is unreservedly that of a physicist, although throughout the book his approach is as mathematically rigorous as is possible keeping his primary objectives in mind.

The presentation of differentiation is standard, workmanlike and full of insight. The usual interpretation in terms of graphs is given in a clear and precise way. Special attention is given to functions of time because of their central importance in physics and applications to the description of motion in one dimension are discussed in some detail.

Two short sections are devoted to differentials and it must be said that this reviewer has some considerable reservations about these. In the first place, one wonders if it is really necessary to introduce the idea of a differential at all at this level. The same material can just as well be presented as relationships between small but finite changes in physical quantities which, in any event, are what are measured in any physical situation. Avoidance of the concept of a differential altogether would also avoid the highly dubious implication that certain 'differentials' (e.g. the change in heat energy giving rise to an infinitesimal increase in the temperature of a thermodynamic system) are perfect differentials in the mathematical sense. A student reader might be best advised to skip over both sections on differentials (about ten pages in all).

It is the final chapter (integration) that should make this book most useful for a student taking a course in introductory physics. The idea of an integral is interpreted in two ways both of which arise naturally in physics. First of all the integral is presented as an 'antiderivative' and later it is introduced as a 'sum of infinitesmal elements'. The 'antiderivative' approach is the easiest and most natural way, at an elementary level, to determine the potential energy function corresponding to a given force field. On the other hand, if one wants to compute the magnetic field strength at a point due to the electric current in a particular circuit, the integral seen as a sum of infinitesmal elements is a more obvious approach to take.

The general presentation of the book is pleasant and easy to read in keeping with the low-key of unhysterical approach of the author in the text. The chapters are broken up into sections at the end of each of which there is a short set of exercises. Worked solutions to all these exercises are given in an appendix. Any student embarking on a third-level programme that includes a

course in physics could do a lot worse than to buy this book and work through it carefully.

Unfortunately, many students entering Irish third-level institutions to take courses including physics have deficiencies in their mathematical foundation of a more fundamental nature than those which Dr. Dalven sets out to remedy. There is not much point in worrying about calculus when the basic manipulative skills of elementary algebra, geometry and trigonometry are missing. All these topics are meant to be covered at a perfectly adequate level in the Intermediate Certificate programme. Why is it that such a large fraction of students who go on to take mathematics courses at Leaving Certificate and third level turn out to be totally lacking in such skills?

References

[1] O Murchu, N. and O'Sullivan, C., *Mathematical Horses for Elementary Physics Courses*, Irish Mathematical Society Newsletter, 6, Dec. 1982, 50-54.

[2] *Report on the Basic Mathematical Skills Test of First Year Students at Cork R.T.C. in 1984*, Irish Mathematical Society Newsletter, 14, Sept. 1985, 33-43.

Colm T. O'Sullivan
Department of Physics
University College, Cork.

PROBLEM PAGE

Editor: Phil Rippon

Ray Ryan has had the excellent idea of numbering the problems according to the issue in which they appear. This should make it much easier to keep track of earlier problems. For example, the problems in the previous Bulletin will be referred to from now on as Problems 19.1, 19.2 and 19.3.

This relabelling exercise reminds me of the story about the Real Analysis textbook which contained an apology by the author for numbering the sections before he had defined the positive integers!

I came across the first problem this time at an Open University Summer School. A student there was tormenting the Maths tutors with it (and also with Problem 18.1, whose solution appears below).

20.1 *Find a formula, whose value is 64, which uses the integer 4 twice and no operations other than:*

$$+, -, \times, /, \uparrow, \sqrt{\ } \text{ and } !$$

I gather that Mícheál Ó Searcóid has devised a formula for 64 which uses only one 4, but this requires the functions [ ] and ln as well. Also, it is possible to display 64 on a calculator (more precisely, on some calculators) using a single 4 followed by the four key strokes: $\times\times ==$. This was pointed out by the daughter (aged 14) of one of my colleagues here at the OU.

Next, here is another problem from my colleague John Mason.

20.2 *Given n positive integers $a_k, k = 1, 2, \ldots, n$ (not necessarily distinct), prove that some sum of the form*

$$a_{k_1} + a_{k_2} + \ldots + a_{k_m}, \qquad 1 \le k_1 < k_2 < \ldots < k_m \le n,$$

is equal to 0 mod n.

Finally, a pretty geometric problem which I heard from Harold Shapiro some years ago.

20.3 *Show that if a square lies within a triangle, then its area is at most half the area of the triangle.*

Now for solutions to the problems in Issue 18.

18.1 *Find the next entry in the following sequence:*

$$1, 11, 21, 1211, 111221, 312211, \ldots.$$

This problem has circulated widely in recent years and provoked much interest and anguish! To understand the pattern, think of any given term, such as 1211, as a string of positive integers and then describe this string in the form:

one one, one two, two ones.

This description yields the next string: 111221. The string following 312211 is, therefore, 13112221.

As mentioned in Issue 18, this problem is associated with John Conway who has made a remarkable investigation of the behaviour of sequences determined by this process (which he calls "Audioactive Decay"). This is written up in Eureka, vol 46, 1986, the journal of the Archimedeans, which is the Cambridge students mathematical society.

A string of digits is said to *split* if it can be written as a product LR of strings L and R, such that

$$(LR)_n = L_n R_n, \qquad \text{for } n = 1, 2, \ldots.$$

Here L_n denotes the nth descendant of L under this process. A string with no non-trivial splitting is called an *element*. Conway lists a sequence of 92 *common elements* (each with an appropriate name) all of which are involved in the descendants of every string, except 22 (hydrogen) and the empty string. Furthermore, eventually only the common elements (and possibly a few 'isotopes') are involved.

For example, the 7th descendant of the string 1 is

11132.13211,

which is written here as the product of the two common elements Hafnium and Stannium. All descendants of this compound involve only the 92 common elements.

Finally, apart from the two exceptions above, the lengths of strings involving common elements increase exponentially at a universal rate $\lambda = 1.3035\ldots$ and the relative abundances of the common elements in such strings tend to fixed positive values.

18.2 *Find an infinite family of pairs of distinct integers m, n such that m,n have the same prime factors, and $m-1$,$n-1$ have the same prime factors.*

This problem came from the book 'It seems I'm a Jew' by Freiman and Nathanson, which chronicles the methods which have apparently been used to discriminate against Jewish students in the Soviet Union. By setting high school students fiendishly difficult problems in oral exams, it seems that even the most able can be excluded for the prestigious Faculty of Mechanics and Mathematics at Moscow State University. In an appendix to the book, Andrei Sakharov discusses such problems, including the one above, which he describes as 'incredibly difficult' at this level. The solution

$$m = 2^k - 1, \quad n = \left(2^k - 1\right)^2, \qquad k = 1, 2, \ldots,$$

is easy to verify, once you've seen it.

Phil Rippon
Faculty of Mathematics
Open University
Milton Keynes, MK7 6AA, UK

INSTRUCTIONS TO AUTHORS

Authors may submit articles to the Bulletin either as TEX input files, or as typewritten manuscripts. Handwritten manuscripts are not acceptable.

Manuscripts prepared with TEX

The Bulletin is typeset with TEX, and authors who have access to TEX are encouraged to submit articles in the form of TEX input files. Plain TEX, AMS–TEX and LATEX are equally acceptable. The TEX file should be accompanied by any non-standard style files which have been used.

The input files can be transmitted to the Editor either by electronic mail to:

EARN/BITNET: MATRYAN@VAX1.UCG.IE,

or on an IBM $5\frac{1}{4}$–inch diskette, or a Macintosh diskette.

Two printed copies of the article should also be sent to the Editor.

Typed Manuscripts

Typed manuscripts should be double-spaced, with wide margins, on numbered pages. Commencement of paragraphs should be clearly indicated. Handwritten symbols should be clear and unambiguous. Illustrations should be carefully prepared on separate sheets in black ink. Two copies of each illustration should be submitted: one with lettering added, and the other without lettering. Two copies of the manuscript should be sent to the Editor.