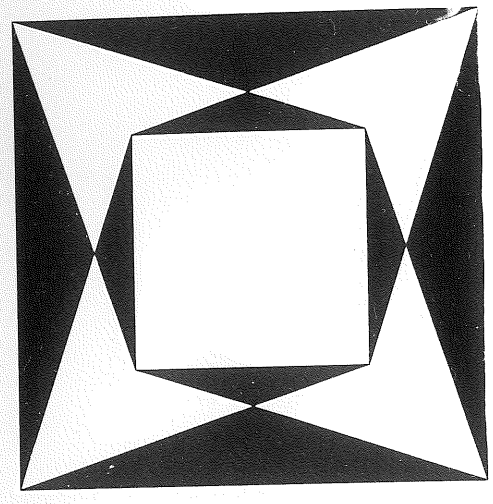
IRISH MATHEMATICAL SOCIETY



BULLETIN

NUMBER 24 MARCH 1990
ISSN 0790-1690

IRISH MATHEMATICAL SOCIETY BULLETIN

EDITOR: Ray Ryan

ASSOCIATE EDITOR: Ted Hurley

PROBLEM PAGE EDITOR: Phil Rippon

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 is supplied free of charge to to members by Local Representatives, or by surface mail abroad. Libraries may subscribe to the Bulletin for IR£20 per annum.

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 the form of typed manuscripts will be given the same consideration as articles in TEX.

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	Dr. Fergus Gaines	Department of Mathematics University College Dublin
Vice-President	Dr. Richard Timoney	School of Mathematics Trinity College Dublin
Secretary	Dr. Graham Ellis	Department of Mathematics University College Galway
Treasurer	Dr. David A. Tipple	Department of Mathematics University College Dublin

Committee Members: P. Barry, G.M. Enright, B. Goldsmith, R. Ryan, M. O'Reilly, A.G. O'Farrell, M. Ó Searcóid, D.J. Simms, R.O. Watson.

LOCAL REPRESENTATIVES

Cork	RTC	Mr. D. Flannery
	UCC	Dr. M. Stynes
Dublin	DIAS	Prof. J. Lewis
	Kevin St.	Dr. B. Goldsmith
	NIHE	Dr. M. Clancy
	St. Patrick's	Dr. J Cosgrave
	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
Belfast	QUB	Dr. D.W. Armitage

IMS MEMBERSHIP

Ordinary Membership

Ordinary of the Irish Mathematical Society is open to all persons interested in the activities of the Society. Application forms are available from the Treasurer and from Local Representatives. Special reciprocity rates apply to members of the Irish Mathematics Teachers Association and of the American Mathematical Society.

Institutional Membership

Institutional Membership is a valuable support to the Society. Institutional members receive two copies of each issue of the Bulletin and may nominate up to five students for free membership.

Subscriptions rates

The rates are listed below. The membership year runs from 1st October to 30th September. Members should make payments by the end of January either direct to the Treasurer or through Local Representatives. Members whose subscriptions are more than eighteen months in arrears are deemed to have resigned from the Society.

Ordinary Members	IR£10
Student Members	IR£5
Reciprocity Members from IMTA	IR £5
Reciprocity Members from AMS	US$10
Institutional Members	IR£50

IRISH MATHEMATICAL SOCIETY

Annual Meeting

December 22, 1989

The Annual General Meeting of the Irish Mathematical Society was held at 12.15 pm on Friday, 22-12-89, in the DIAS.

There were 16 members present. The President, F. Gaines, was the chair.

1. The **minutes** of the meeting of 7-8th September 1989 and 24th November 1989 were read, approved, and signed.

2. **Elections.** D.A. Tipple was proposed and seconded and elected Treasurer of the Society.

   G. Ellis was proposed and seconded and elected Secretary of the Society.

   The following were proposed and seconded and elected to the Committee:

   G. Enright, A.G. O'Farrell, D. Simms, R.O. Watson.

   (P. Barry, B.G. Goldsmith, M. O'Reilly and M. Ó Searcóid continue on the Committee, together with the co-opted member R. Ryan).

   The co-option of a person from Cork was suggested to the Committee.

   The President expressed the Society's gratitude to G. Enright for his seven years' service as Treasurer to the Society, during which time the financial affairs of the Society were admirably organised and conducted. He also thanked A.G. O'Farrell for his service as Secretary. A vote of thanks was passed.

3. The Treasurer presented his **accounts** for the session 1988-89. He pointed out the encouraging growth shown by the Society during his period in office. The number of members has gone from 145 to 267, and the cash turnover has tripled.

   A suggestion by T.T. West that the Society's funds were large enough that the Treasurer should consider how best to invest them was noted.

   The adoption of the accounts was proposed, seconded, and passed.

4. It was agreed to revise the **membership fees**, as follows: Ordinary members: £10; AMS reciprocity members: $10; IMTA reciprocity members: £4; (It was noted that the IMTA has raised its fee to IMS members, under the agreement, to £3).; Institutional Members: £50; Student members: £4.

5. R. Timoney presented an account of progress on the EUROMATH project. He outlined proposed arrangements for setting up a Database of European Mathematicians, to be made available on the EUROMATH system. It was agreed that information for this database was best collected directly from mathematicians, and that people should have the option of refusing to participate.

6. **MSI Project.** R. Timoney tabled a questionnaire prepared by himself and Donal O'Donovan, for circulation to TCD Maths graduates. He expressed the hope that a similar questionnaire could be sent out by all the institutions, and could form the basis for completing the first task of the project on the situation, potential and requirements of the Mathematical Sciences in Ireland. The questionnaire, which had been already vetted by the committee, was subjected to some further criticism. It was agreed that this kind of survey was best carried out by the institutions, and that the IMS could not dictate to the institutions. However, it was felt desirable that the institutions that participated should use as uniform a format as possible. R. Timoney and D. O'Donovan will circulate the final form of their questionnaire to the institutions for their consideration.

7. It was reported that unavoidable delays had caused the **Bulletin** editorial staff to miss the printer's deadline. It is hoped to have the December Bulletin by the end of January.

8. Members were reminded that the **September Meeting** in 1990 will be held at Dublin City University, and that proposals to host the 1991 September Meeting should reach the Society in good time for the Easter Meeting 1990.

Anthony G. O'Farrell

NEWS

Report on the Participation of the Irish Team in the 31st International Mathematical Olympiad

Fergus Gaines

The International Mathematical Olympiad is an annual mathematics competition, the most prestigious of its kind, for pre-university students, and in 1990 it was held in Beijing, China. This was the third year that Ireland was involved in the competition, after Australia in 1988 and West Germany in 1989 and it was by far our most successful performance. The competition consists of two four-and-a-half hour examinations, with three problems to be solved in each examination. Each country taking part is invited to send a team of up to six students, each student competing as an individual. The benefits of the competition are many; it enables talented students to test their skill against the best people of their own age in the world; it stimulates an interest in problem-solving; it enables budding young mathematicians to make contacts with their peers in other countries, contacts that, in many cases, are maintained over the years; it reflects the trends in mathematical education worldwide.

Choosing the Team

Last November letters were sent out to most secondary and vocational schools in the catchment areas of the training centres in University College Dublin, University College Galway and Limerick University inviting them to send their three most mathematically talented students in the post Intermediate Certificate classes to the training sessions in the three centres. It was intended to have training sessions in University College Cork also but due to unforseen

circumstances they did not take place. In the case of a number of schools mathematically talented students had already been identified from information supplied by the Department of Education, from the results of the Irish National Mathematics Contest, etc., and these were invited to take part. About three hundred students were involved in the initial stages.

Training sessions were held in the three venues — as well as discussing techniques of problem-solving it was also necessary to teach some areas of mathematics that are not covered in the school syllabus — number theory, aspects of combinatorics and aspects of Euclidean geometry.Because the work of training is purely voluntary it was necessary to have some elimination tests which, as well as whittling down the numbers, also helped to identify the most talented of the students. It was noticeable that students who had been involved in the training in previous years had a distinct advantage over newcomers. Even students who were eliminated at the earlier stages were exposed to (for them) new mathematics which will serve them well when they compete next time, as well as stimulating their interest in mathematics.

The Third Irish Mathematical Olympiad took place on 5 May 1990. The top scorers in this competition were, in order,

1. Aidan Hollinshead, Blackrock College, Dublin.
2. Cian Dorr, Ashton School, Cork.
3. David Galvin, St. Fintan's College, Ennis.
4. Andrew McMurray, The High School, Dublin.
5. Patrick Connolly, Blackrock College, Dublin.
6. Julian McCrae, The High School, Dublin.
7. Stephen McInerney, Gonzaga College, Dublin.
8. Eoghan Burns, Blackrock College, Dublin.
9. Adrian Colley, O'Connell School, Dublin.
   Ken Humborg, CBS, Roscommon.
10. Edmund Roche Kelly, Ard Scoil Rís, Limerick.
    Charles von Schmieder, The King's Hospital School, Dublin.

The first three candidates were invited to take part in the IMO in Beijing, with Fergus Gaines of UCD as leader of the team and Gordon Lessels of Limerick University as deputy leader. At this point there was only sufficient sponsorship money to fund a team of three. Subsequently, further sponsorship was obtained and the candidates in the fourth, fifth and sixth places were invited to join the team. All six candidates accepted the invitation.

As there were insufficient funds to run a final training session the Dublin based students came to three afternoon sessions in UCD and Gordon Lessels gave some further training to David Galvin in Limerick.

The Competition

The team, accompanied by the leader and deputy leader, left Dublin on Sunday 8 July, and arrived in Beijing on the morning of Monday 9 July, after a ten-hour flight from Frankfurt. On arrival they were met by representatives of the organisers and by Mr. Éamonn Robinson of the Irish Embassy. The students were then interviewed by Chinese television. The team leader, F. Gaines, was taken to a hostel on the outskirts of Beijing, while G. Lessels and the students were accomodated more centrally. The leaders from all 54 countries taking part formed the jury whose task it was to select the six final questions, from those shortlisted by the organisers from the questions submitted by the countries concerned. Two of the questions submitted by Ireland were shortlisted, but did not make it to the final six. The work of selection, rewording and translation into the various languages took a little over two days. The formal opening took place on the afternoon of Wednesday, 11 July.

The first examination took place on Thursday, 12 July and the second one on Friday the 13th. F. Gaines and G. Lessels marked each of the Irish students' work, according to the marking scheme laid down by the hosts. On the Saturday and Sunday they went to a team of Chinese "coordinators", a separate team for each question, to agree the final marks that each student should get.

From the comments of the leaders of the teams taking part it was felt that the competition was one of the more difficult IMO's and thus the relatively good performance of the Irtish team was all the more commendable. Andrew McMurray won a bronze medal, a magnificent achievement, as it was the first time Ireland had won a medal in the IMO. Cian Dorr was one point short of a bronze medal and this, in its own way, was quite remarkable as Cian was

not involved in the training programme at all — he was specially invited to take part in the Irish Mathematical Olympiad on the basis of his getting first place in the Irish National Mathematics Competition. When the team scores were totted up the final (unofficial) placings, by country, were: first, China, second, the Soviet Union, third, USA, and ...fortieth, Ireland. Out of 308 competitors 23 won gold medals, 56 silver and 76 bronze.

The questions in the competition were graded by the organisers, "easy", "moderate" and "difficult". (These are purely relative terms!). Question 1 was judged to be "easy", but proved very difficult for many of the students. This, perhaps, reflects the modern trend away from Euclidean geometry. It was interesting to note that two of our students had exactly the same idea for doing this question: pick AB and CD to be perpendicular diameters, work out the required ratio in this case, and this gives the correct answer! — this got 4 marks out of 7. Three of the students also had the same idea for doing Question 2 — they considered a maximal "bad" colouring. Question 5 proved our most successful question, as it did for most countries, and Question 4 our worst. By far the hardest question on the exam was Question 6. Thus, for example, one of the Chinese students who has a perfect score (7) on each of the first five questions, could only manage to get one point on Question 6. Thus Cian Dorr's score of 5 on this question was all the more commendable.

Acknowledgements

The organisors are extremely grateful to our sponsors for so generously supporting our participation. The sponsors were an Roinn Oideachais, EOLAS, Bank of Ireland, the ESB, the Irish National Mathematics Competition, and three corporate sponsors who wish to remain anonymous.

Two of the parents of team members, Mrs. Hilary McCrae and Professor Brian McMurray, were extremely helpful in raising sponsorship and sincere thanks go to them.

The Department of Education and the Depatment of Foreign Affairs gave their expert assistance which we wish to acknowledge.

Special thanks goes to Mr. Éamonn Robinson of the Irish Embassy for his assistance while the team was in China.

The Trainers

The mathematicians who helped with training were:

In UCD:
F. J. Gaines, T. J. Laffey, M. Ó Searcóid, R. M. Timoney (TCD).

In UCG:
G. Ellis, J. J. Ward.

In Limerick:
Mark Burke (University of Limerick), Gerard Enright (Mary Immaculate College), Alan Hegarty (University of Limerick), John Kinsella (University of Limerick), Jim Leahy (Thomond College), Gordon Lessels (University of Limerick), Marian Morrin (Ballynanty National School), Eamonn Murphy (University of Limerick), Pat O'Sullivan (Mary Immaculate College).

The Chairman of the Irish Participation Committee is Mr. C. C. Ó Caoimh of the Department of Education.

The Results

Each question scores 7 points and thus the maximum possible score is 42. Only four students in the whole competition scored 42. The top Irish scores were Andrew McMurray, 16; Cian Dorr, 15 and Julian McCrae, 13; The team scored a total of 65 points, which was almost double the previous year's score.

To put this in perspective, China scored 230, the USSR 193 and the USA 177 to get first, second and third places respectively.

The Problems

FIRST DAY
Beijing, July 12, 1990

1. Two chords AB, CD of a circle intersect at a point E inside the circle. Let M be an interior point of the segment EB. The tangent line at E to the circle through D, E, M intersects the lines BC, AC at F, G respectively. If $\frac{AM}{AB} = t$, find $\frac{EG}{EF}$ in terms of t.

2. Let $n \geq 3$ and consider a set E of $2n-1$ distinct points on a circle. Suppose that exactly k of these points are to be coloured black. Such a colouring is "good" if there is at least one pair of black points such that the interior of one of the arcs between them contains exactly n points from E. Find the smallest value of k so that every such colouring of k points of E is good.

3. Determine all integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

TIME: 4.5 Hours
Each problem is worth 7 points.

SECOND DAY
Beijing, July 13, 1990

4. Let $\mathbf{Q}^+$ be the set of positive rational numbers. Construct a function $f : \mathbf{Q}^+ \to \mathbf{Q}^+$ such that $f(xf(y)) = \frac{f(x)}{y}$ for all x, y in $\mathbf{Q}^+$.

5. Given an initial integer $n_0 > 1$, two players A and B choose integers n_1, n_2, n_3, ... alternately according to the following rules.

   Knowing n_{2k}, A chooses any integer n_{2k+1} such that $n_{2k} \leq n_{2k+1} \leq n_{2k}^2$. Knowing n_{2k+1}, B chooses any integer n_{2k+2} such that $\frac{n_{2k+1}}{n_{2k+2}}$ is a positive power of a prime.

   Player A wins the game by choosing the number 1990, player B wins by choosing the number 1.

   For which n_0 does

   (a) A have a winning strategy,

   (b) B have a winning strategy,

   (c) neither player have a winning strategy?

6. Prove that there exists a convex 1990-gon with the following two properties:

   (a) all angles are equal,

(b) the lengths of the sides are the numbers

$$1^2, 2^2, 3^2, \ldots, 1989^2, 1990^2$$

in some order.

TIME: 4.5 Hours
Each problem is worth 7 points.

Subscription, IMTA Reciprocity

New subscription rates for IMS members come into effect in from 1990/91 (the standard rate is now £10).

In addition, the reciprocity agreement with the Irish Mathematics teachers Association has been renegotiated. The new agreement provides for members of each Society to join the other at half price. The previous system where IMS members paid their reduced IMTA subscription through the IMS treasurer (and vice-versa for IMTA members) has been discontinued, and subscriptions will be now be paid directly to each society.

CONFERENCES

1991 September Meeting

It will be held at University College Galway on September 5th and 6th. The details of the programme are not yet fully settled.

Operator Theory and Operator Algebras

The fifth international conference in the Cork series will be held at University College Cork from Wednesday May 15 to Friday May 17, 1991. The principal speaker will be Professor R.G. Douglas (SUNY, Stonybrook) and his title will be *Operator theory and algebnaic geometry.* Further information from G.J. Murphy, Mathematics Dept., UCC.

European Mathematics Congress

The European Mathematical Society (EMS) was recently inaugurated at a meeting in Warsaw, and the Irish Mathematical Society will become a corporate member. Individual members of the IMS will have the possibility of becoming EMS members through the IMS, but detailed arrangements have not yet been made for this. B. Goldsmith is the Society's representative for EMS business.

The EMS is organising a congress in Paris in 1992, probably July 6–10, 1992.

13th IMACS World Congress on Computation and Applied Mathematics

It will be held at Trinity College, Dublin July 22–26, 1991. Further details from JJH Miller, IMACS '91, 26 Temple Lane, Dublin 2.

ARTICLES

Some properties and uses of the discriminant of a polynomial

R. Gow

Let K be a field and let $K[x]$ denote the ring of polynomials over K. Let $f = f(x)$ be a monic polynomial in $K[x]$ of degree $n \geq 1$ and let the roots of f in some splitting field L over K be $\alpha_1, \ldots, \alpha_n$. Put

$$\delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j),$$

so that δ is an element of L. Clearly, if f has a repeated root, $\delta = 0$. Otherwise, $\delta \neq 0$ and then $L : K$ is a normal separable extension of finite degree. Recall that the Galois group G of f over K is the group of all automorphisms of L that fix K elementwise. The elements of G permute the roots of f and G may naturally be considered as a subgroup of the symmetric group of degree n. The following basic result is proved in any standard text on Galois theory.

1.1 Lemma. *Let $\sigma \in G$. Consider σ as a permutation on the n roots of f. Then*

$$\sigma(\delta) = \epsilon_\sigma \delta$$

where ϵ_σ is the sign of the permutation determined by σ.

We now set $D = \delta^2$ and call D the *discriminant* of the polynomial f. It follows from Lemma 1.1 that D is fixed by all elements of G and thus, by the Galois correspondence, $D \in K$. Indeed, using the notation just introduced, the following result holds.

1.2 Theorem. *Suppose that K has characteristic different from 2 and let D be the discriminant of f. Let G be the Galois group of f over K.*

(i) If $D = 0$, f has a repeated root.

(ii) If $D \neq 0$ and D has a square root in K, G is naturally a subgroup of A_n, the alternating group of degree n.

(iii) If $D \neq 0$ and D has no square root in K, $G \cap A_n$ has index 2 in G and $K(\sqrt{D})$ is a quadratic extension of K contained in the splitting field of f over K.

It should be clear that the restriction on the characteristic of K is not required for part (i) above. We will discuss substitutes for parts (ii) and (iii) when the characteristic of K is 2 later in the paper.

It is the purpose of this paper to discuss some properties of the discriminant of a polynomial. While the discriminant may seem to be rather a weak invariant, we hope to show how it may be used quite effectively when investigating a number of problems. Our results are drawn from various parts of the literature and contain nothing new.

The discriminant of a polynomial f is expressible as a polynomial in the coefficients of f. However, the number of terms involved tends to be ineffably large. For example, the discriminant of the quartic $x^4 + ax^3 + bx^2 + cx + d$ is

$$256(I^3 - 27J^2)$$

where

$$I = d - \frac{ac}{4} + \frac{b^2}{12}, \quad J = \frac{bd}{6} - \frac{c^2}{16} - \frac{a^2 d}{16} + \frac{abc}{48} - \frac{b^3}{216}.$$

This involves 16 terms. The discriminant of a quintic involves 59 terms. The interested reader should consult the article by J. McKay, [2], to see some explicit formulae and references on this topic.

One of the most useful formulae for calculating the discriminant involves the formal derivative of a polynomial.

1.3 Lemma. *Let $f \in K[x]$ be a monic polynomial of degree $n \geq 1$ and let the roots of f in some splitting field over K be $\alpha_1, \ldots, \alpha_n$. Then the discriminant of f is*

$$(-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\alpha_i).$$

If we take $f = x^m - 1$, we find from this formula that the discriminant D of f is $(-1)^{\epsilon(m)} m^m$, where $\epsilon(m) = m(m-1)/2 + (m-1)^2$. Taking m equal to an odd prime p, we obtain $D = p^p$ if $p \equiv 1 (\mathrm{mod} 4)$ and $D = -p^p$ if $p \equiv 3 (\mathrm{mod} 4)$. This provides us with a convenient proof of the fact that if ϵ is a primitive p–th root of unity in $\mathbb{C}$, $\sqrt{p} \in \mathbb{Q}(\epsilon)$ if $p \equiv 1 (\mathrm{mod} 4)$ and $\sqrt{-p} \in \mathbb{Q}(\epsilon)$ if $p \equiv 3 (\mathrm{mod} 4)$.

There is a formula, due to R. G. Swan, [4], for the discriminant of a trinomial, that is, a polynomial having only three non–zero terms. Let $f = x^n + ax^k + b$, where $0 < k < n$. The discriminant D of f is given by

$$D = (-1)^{n(n-1)/2} b^{k-1} (n^N b^{N-K} - (-1)^N (n-k)^{N-K} k^K a^N)^d$$

where $d = \gcd(n,k), N = n/d, K = k/d$. This formula is quite useful, as trinomials are frequently employed for various field–theoretic constructions. We remark that when $k = 1$, the result above is easily proved using Lemma 1.3.

As an example of the use of this formula, let $f = x^n + ax + b$, with a and b both non–zero and let D be the discriminant of f. If $n \equiv 1 (\mathrm{mod}\, 4)$, it is not hard to see that D is a non–zero square in K if and only if

$$a = \lambda^2 - n^n \mu^{n-1}, \quad b = (n-1)a\mu,$$

for non–zero elements λ and μ in K. If $n \equiv 3 (\mathrm{mod}\, 4)$, the general solution for square D is

$$a = -\lambda^2 - n^n \mu^{n-1}, \quad b = (n-1)a\mu.$$

Suppose now that n is a prime p with $p \equiv 3 (\mathrm{mod}\, 4)$. Take

$$a = -1 - p^p \mu, \quad b = (p-1)a\mu,$$

where μ is an integer not divisible by p. Then we have

$$f = x^p - (1 + p^p \mu)x - (p-1)(1 + p^p \mu)\mu.$$

As the reduction of f modulo p is well known to be irreducible in $\mathbf{F}_p[x]$, f is irreducible in $\mathbf{Q}[x]$. The classification of finite simple groups now implies that the Galois group of f over $\mathbf{Q}$ is the alternating group A_p for $p > 23$ (and presumably this holds good for $p = 7, 11, 19, 23$). See, for example, Corollary 4.4 of [5]. Perhaps this can be proved purely by field–theoretic methods.

Consider now a polynomial f of degree $n \geq 1$ with real coefficients. Suppose that f has exactly r real roots. The Galois group of f over $\mathbf{R}$ is generated by the complex conjugation involutory mapping, σ, say. In its action on the roots of f, σ is represented by the product of $(n-r)/2$ transpositions and hence the sign of σ is $(-1)^{(n-r)/2}$. Since the discriminant of f is a non–zero square in $\mathbf{R}$ if and only if it is positive, we obtain the following result from Lemma 1.1.

1.4 Theorem. *Let $f \in \mathbf{R}[x]$ have degree n and exactly r real roots. Suppose that the discriminant of f is positive. Then $n \equiv r (\mathrm{mod}\, 4)$.*

The discriminant of a monic integral polynomial has an interesting congruence property modulo 4, as the next result indicates.

1.5 Theorem. *Let $f \in \mathbf{Z}[x]$ be a monic integral polynomial of degree $n \geq 1$. Let D be the discriminant of f. Then $D \equiv 0$ or $1 (\mathrm{mod}\, 4)$.*

Proof. Let the roots of f be $\alpha_1, \ldots, \alpha_n$. As f is monic, the α_i are algebraic integers. Put

$$\Delta = \prod_{1 \leq i < j \leq n} (\alpha_i + \alpha_j).$$

It should be clear that Δ is fixed by all elements of the Galois group of f and hence it is a rational number. However, Δ is also an algebraic integer and thus it is a rational integer. We have now

$$D = \prod \left((\alpha_i + \alpha_j)^2 - 4\alpha_i \alpha_j \right) = \Delta^2 + 4E,$$

where E is an algebraic integer. As E is clearly rational, E is a rational integer. Finally, the square of a rational integer is congruent mod 4 to 0 or 1 and since $D \equiv \Delta^2 (\mathrm{mod}\, 4)$, the result follows.

This result is a special case of a result of Stickelberger, [3], on the discriminant of an algebraic number field.

One of the nicest applications of the discriminant concerns irreducibility questions for polynomials over finite fields. Let q be a power of a prime p and let $\mathbf{F}_q$ denote the finite field of order q. For the sake of simplicity, we first prove a special case of another result of Stickelberger, [3].

1.6 Theorem. *Suppose that q is odd and let f be a polynomial in $\mathbf{F}_q[x]$. If f has even degree ≥ 2 and the discriminant of f is a square in $\mathbf{F}_q$, f is reducible in $\mathbf{F}_q[x]$. If f has odd degree and the discriminant of f is a non– square in $\mathbf{F}_q$, f is also reducible.*

Proof. Suppose that f is irreducible of even degree $2m$. Then it is known from the theory of finite fields that $\mathbf{F}_{q^{2m}}$ is a splitting field for f over $\mathbf{F}_q$ and the Galois group of f is cyclic of order $2m$, being generated by the Frobenius mapping σ that sends a root α to α^q. Thus, as a permutation of the roots, σ is represented by the cycle

$$(\alpha, \sigma(\alpha), \ldots, \sigma^{2m-1}(\alpha)).$$

But it is well known that a cycle of even length has sign -1 and thus we deduce from Theorem 1.2 that the discriminant of f must be a non–square in $\mathbf{F}_q$. Similar reasoning gives the corresponding result when f has odd degree.

Before giving the generalization of this result, we mention an application that is occasionally useful. Let $f \in K[x]$ be a monic polynomial of degree $n \geq 1$ and let $g = f(x^2)$. It is quite straightforward to show that if D and D_1 are the discriminants of f and g, respectively, then

$$D_1 = (-1)^n f(0) 2^{2n} D^2.$$

Now we can prove a simple irreducibility criterion for g when K is a finite field.

1.7 Theorem. *Let $f \in \mathbf{F}_q[x]$ be a monic irreducible polynomial of degree $n \geq 1$ and suppose that q is odd. Let $g = f(x^2)$. Then g is irreducible if and only if $(-1)^n f(0)$ is a non–square in $\mathbf{F}_q$.*

Proof. Suppose that g is irreducible over $\mathbf{F}_q$. As g has even degree it follows from Theorem 1.6 that the discriminant of g must be a non–square in $\mathbf{F}_q$. The formula above for D_1 implies that $(-1)^n f(0)$ is a non–square.

We consider the converse part of the theorem. Given a polynomial h of degree $r \geq 1$, define h^* by

$$h^* = (-1)^r h(-x).$$

It should be clear that $(hh_1)^* = h^* h_1^*$ for polynomials h and h_1 and that $h^{**} = h$. Moreover, suppose that $h = h^*$. Then if r is even, h is a polynomial in x^2, whereas, if r is odd, x divides h and $x^{-1}h$ is a polynomial in x^2. Let h be a monic irreducible factor of g. Then we have $g = hw$ for some polynomial w. As g is a polynomial in x^2, we have $g = g^*$ and thus by our remarks above, $g = h^* w^*$. We see that h^* is a monic irreducible factor of g. Thus we either have $h = h^*$ or else h and h^* are relatively prime, in which case hh^* divides g.

Suppose that $h = h^*$. We can obviously assume that x does not divide f by the irreducibility of f (this only excludes the possibility that $f = x$, for which the result is obvious) and it follows that x does not divide h. We conclude that h is a polynomial in x^2, say $h = a(x^2)$, for some irreducible monic polynomial a. But we see that w above must also be a polynomial in x^2, say $w = b(x^2)$ and thus

$$g = f(x^2) = a(x^2)b(x^2).$$

But this entails a factorization $f = ab$ and it follows that as f is irreducible, $f = a$. Hence g is irreducible in this case.

Suppose now that $h \neq h^*$. Then hh^* divides g and as hh^* is fixed by *, it is a polynomial in x^2, say $hh^* = a(x^2)$. Repeating the argument above we must have $f = a$ and hence $g = hh^*$. We obtain

$$g(0) = f(0) = h(0)h^*(0) = (-1)^n h(0)^2.$$

It follows that if g is reducible, $(-1)^n f(0)$ is a square and thus the converse statement is proved.

We note that the second part of this argument applies to any field of characteristic not equal to 2. Either g is irreducible or else $g = hh^*$ for some monic irreducible polynomial h. If the characteristic of K is 2, we can argue that g is either irreducible or else $g = h^2$ for some irreducible h. This latter condition holds if and only if each coefficient of f is a square in K. The first part of the argument applies only to finite fields.

We now give the generalization of Theorem 1.6, due to Stickelberger.

1.8 Theorem. *Let q be a power of an odd prime and let f be a polynomial of degree $n \geq 1$ in $\mathbf{F}_q[x]$ without repeated roots. Let r be the number of irreducible factors of f in $\mathbf{F}_q[x]$ and let D be the discriminant of f. Then we have $n \equiv r \pmod 2$ if D is a square in $\mathbf{F}_q$ and $n \equiv r + 1 \pmod 2$ if D is a non–square in $\mathbf{F}_q$.*

Proof. Let $f_1, \ldots, f_r$ be the irreducible factors of f in $\mathbf{F}_q[x]$ and let $D_1, \ldots, D_r$ be the discriminants of the f_i. Elementary properties of the discriminant show that $D = D_1 \ldots D_r$ modulo squares in $\mathbf{F}_q$. Let s be the number of irreducible factors of even degree. If D is a square, Theorem 1.6 implies that s must be even. Thus if t is the number of factors of odd degree, $r \equiv t \pmod 2$. But we clearly have $n \equiv t \pmod 2$ and the result follows in this case. The corresponding result when D is a non–square is proved similarly.

There remains the problem of finding an analogue of these results for fields of characteristic 2. We begin by discussing Swan's approach to this problem. For the sake of simplicity, we restrict our attention to the field $\mathbf{F}_2$. Let f be a polynomial in $\mathbf{F}_2[x]$ without repeated roots. We can find a monic polynomial g in $\mathbf{Z}[x]$ such that $\overline{g} = f$, where the bar denotes reduction modulo 2. The discriminant of g is then an odd integer. For the discriminant of f must be 1 in $\mathbf{F}_2$, since f has no repeated roots, and it is easily proved that the discriminant of f is the reduction modulo 2 of that of g (because the discriminants are given

by the same integral polynomial in the coefficients of the polynomials). We now consider g as a polynomial in $\mathbf{Z}_2[x]$, where $\mathbf{Z}_2$ denotes the ring of 2–adic integers. Hensel's Lemma shows that as the discriminant of g is a 2–adic unit, if f has r irreducible factors in $\mathbf{F}_2[x]$, g has r irreducible factors in $\mathbf{Z}_2[x]$ having the same degree as those of f. Furthermore, the splitting field of g over the field of 2–adic numbers is an unramified extension (uniquely determined up to isomorphism by its degree) whose Galois group is cyclic. Thus g has a cyclic Galois group when considered as a 2–adic polynomial. Finally, it is well known that a 2–adic unit u is a 2–adic square if and only if $u \equiv 1(\mathrm{mod}8)$. Thus, the Galois group of g over the 2–adic numbers is contained in A_n if and only if $D \equiv 1(\mathrm{mod}8)$, where D is the discriminant of g, and it follows from Theorem 1.8 that $n - r$ is even if and only if $D \equiv 1(\mathrm{mod}8)$. (Notice that we already know that $D \equiv 1(\mathrm{mod}4)$, by Theorem 1.5.) Taking into account the correspondence discussed above between the factorizations into irreducibles of f and g, we obtain a result of Swan, [4].

1.9 Theorem. *Let $f \in \mathbf{F}_2[x]$ be a polynomial of degree $n \geq 1$ without repeated roots and suppose that f has exactly r irreducible factors in $\mathbf{F}_2[x]$. Let $g \in \mathbf{Z}[x]$ be a monic polynomial such that $\overline{g} = f$. Then $n - r$ is even if and only if $D \equiv 1(\mathrm{mod}8)$, where D is the discriminant of g.*

This result is quite useful, as we are able to obtain a factorization criterion again by means of the discriminant. Swan applied his discriminant formula for trinomials and Theorem 1.9 to obtain information about the factorization of trinomials over $\mathbf{F}_2$. This information was helpful in the compilation of tables of data about such trinomials. See, for example, [1]. It is apparently possible to obtain Theorem 1.9 without the intermediary of the 2–adic numbers but it seems to us that this provides a good conceptual framework. If we replace $\mathbf{F}_2$ by $\mathbf{F}_q$, where q is a power of 2, we must work in the ring of integers of an appropriate unramified extension of the field of 2–adic numbers to obtain an analogue of Theorem 1.9.

Finally, we describe an intrinsic invariant of a polynomial over a field of characteristic 2 that plays the role of the discriminant over fields of characteristic different from 2. Let K be a field of characteristic 2 and let $f \in K[x]$ be a non–constant polynomial of degree n without repeated roots. Let the roots of f be $\alpha_1, \ldots, \alpha_n$ in a splitting field over K. Define $\beta = \beta(f)$ by

$$\beta = \sum_{i<j} \frac{\alpha_i}{\alpha_i + \alpha_j}.$$

Then we find that $\beta + \beta^2 = C$, where

$$C = \sum_{i<j} \frac{\alpha_i \alpha_j}{\alpha_i^2 + \alpha_j^2}.$$

It is found that for a transposition σ permuting the roots, $\sigma(\beta) = \beta + 1$. Thus, β is invariant under A_n but not S_n. The quantity C is invariant under all permutations of the roots and hence lies in K. Moreover, the Galois group of f is contained in A_n if and only if $C = \lambda + \lambda^2$ for some λ in K. If K is the finite field $\mathbf{F}_{2^m}$, C is expressible in the form above if and only if $\mathrm{Tr}(C) = 0$, where Tr is the trace function, defined by

$$\mathrm{Tr}(C) = \sum_{i=0}^{m-1} C^{2^i}.$$

Of course, if $K = \mathbf{F}_2$, C satisfies this condition if and only if $C = 0$. This provides an alternative approach to Theorem 1.9. We could say that C is a second discriminant of f, which is used once we know that the original discriminant of f is non–zero. The introduction of C and discussion of its properties are due to Berlekamp, [1]. We remark that we have not seen any formula for calculating C from, say, the coefficients of f.

References

[1] E. R. Berlekamp, An analog of the discriminant over fields of characteristic two, J. Algebra 38 (1976), 315–317.

[2] J. McKay, On computing discriminants, Amer. Math. Monthly 94 (1987), 523–527.

[3] L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Verhandl. Ersten Intern. Math. Kongresses, Zürich 1897, Leipzig 1898, 182–193.

[4] R. G. Swan, Factorization of polynomials over finite fields, Pac. J. Math. 12 (1962), 1099–1106.

[5] W. Feit, Some consequences of the classification of finite simple groups, Proc. Symp. Pure Math. 37 (1980), 175–181.

Department of Mathematics,
University College,
Belfield,
Dublin 4.

Taylor Exactness and The Apostol Jump

Robin Harte

Abstract
The middle exactness condition of Joseph Taylor is related to the zero-jump condition of Constantin Apostol and used to derive Kaplansky's lemma.

0. If $T : X \to Y$ and $S : Y \to Z$ are linear operators between complex spaces we shall call the pair (S,T) *exact* iff

0.1 $$S^{-1}(0) \subseteq T(X),$$

whether or not the *chain condition*

0.2 $$ST = 0$$

is satisfied. For example if $T = 0$ this means that S is *one-one*; if $S = 0$ this means that T is *onto*. When S and T are bounded operators between normed spaces we shall call the pair (S,T) *weakly exact* if

0.3 $$S^{-1}(0) \subseteq \text{cl } T(X),$$

and *split exact* if there are bounded $T' : Y \to X$ and $S' : Z \to Y$ for which

0.4 $$S'S + TT' = I.$$

It is clear at once that

0.5 (S,T) split exact $\implies$ (S,T) exact $\implies$ (S,T) weakly exact;

conversely if S and T are both *regular* in the sense that there are bounded $T^\wedge : Y \to X$ and $S^\wedge : Z \to Y$ for which

0.6 $$T = TT^\wedge T \text{ and } S = SS^\wedge S$$

then there is implication

0.7 (S,T) weakly exact $\implies$ (S,T) split exact :

indeed if (0.3) and (0.6) both hold then ([10] Theorem 10.3.3)

0.8 $$(I - TT^\wedge)(I - S^\wedge S) = 0,$$

giving two candidates for T' and S' to satisfy (0.4).

Lemma 1 *If $U : W \to X$, $T : X \to Y$ and $V : Y \to Z$ are linear there is implication*

1.1 (V,TU) *exact*, (T,U) *exact* $\implies$ (VT,U) *exact*

and

1.2 (VT,U) *exact*, (V,T) *exact* $\implies$ (V,TU) *exact.*

If U, T and V are bounded there is implication

1.3 (V,TU), (T,U) *split exact* $\implies$ (VT,U) *split exact*

and

1.4 (VT,U), (V,T) *split exact* $\implies$ (V,TU) *split exact.*

Proof. These are beefed up versions of parts of Theorem 10.9.2 and Theorem 10.9.4 of [10]: for example if $V^{-1}(0) \subseteq TU(W)$ and $T^{-1}(0) \subseteq U(W)$ then

$$VTx = 0 \implies Tx \in V^{-1}(0) \subseteq TU(W) \implies x - Uw \in T^{-1}(0) \subseteq U(W) \bullet$$

Lemma 1 does not extend to weak exactness: to violate the weak analogue of (1.2) take $U = 0$, T dense but not onto and $V^{-1}(0) = \mathbf{C}e$ with $e \in Y \backslash T(X)$.

Lemma 2 *If $U : W \to X$ and $V : Y \to Z$ are bounded and linear, and $T = TT^\wedge T : X \to Y$ is regular, then*

2.1 $$V^{-1}(0) \subseteq T(X) \implies T^\wedge V^{-1}(0) \subseteq (VT)^{-1}(0)$$

and

2.2 $$T^{-1}(0) \subseteq U(W) \Longrightarrow T\hat{}TU(W) \subseteq U(W).$$

Also

2.3 $$V'V + TT' = I \Longrightarrow VTT\hat{} = V''V$$

and

2.4 $$T'T + UU' = I \Longrightarrow T\hat{}TU = UU''.$$

Proof. The first part of this is essentially given by Mbekhta ([16] Proposition 2.4): to see (2.1) argue

$$Vy = 0 \Longrightarrow VTT\hat{}y = VTT\hat{}Tx = VTx = Vy = 0.$$

For (2.3) take $V'' = VTT\hat{}V' + I - VV'$•

It is familiar that the product of regular operators need not be regular ([10](7.3.6.17);[3]§2.8), and that regularity of the product need not imply regularity of the factors ([10](7.3.6.16);[3]§2.8):

Theorem 3 *If $T : X \to Y$ and $S : Y \to Z$ are bounded and linear and (S, T) is split exact then*

3.1 $$ST \text{ regular} \iff S,\ T \text{ regular}.$$

Proof. If $ST = STUST$ and $S'S + TT' = I$ then

$$(I - TT')T(I - UST) = 0 = (I - STU)S(I - S'S).$$

Conversely if $S = SS\hat{}S$ and $T = TT\hat{}T$ and $S^{-1}(0) \subseteq \text{cl } T(X)$ then ([10] Theorems 3.8.3, 2.5.4)

$$STT\hat{}S\hat{}ST = S(TT\hat{} + S\hat{}S - I)T = ST$$•

When $T : X \to X$ and $S : X \to X$ are complex linear operators on the same space X we shall call the pair (S, T) *left non-singular* if

3.2 $$S^{-1}(0) \cap T^{-1}(0) = \{0\},$$

right non-singular if

3.3 $$S(X) + T(X) = X,$$

and *middle non-singular* if, in matrix notation,

3.4 $$(-S \quad T)^{-1}(0) \subseteq \begin{pmatrix} T \\ S \end{pmatrix}(X).$$

This last condition means of course that whenever $Sy = Tx$ there is z for which $y = Tz$ and $x = Sz$, and is a special case of (0.1). Each of these conditions is symmetric in S and T, and not restricted to pairs (S, T) which are *commutative* in the sense that

3.5 $$ST = TS.$$

Gonzalez ([7] Proposition) has essentially shown

Theorem 4 *Necessary and sufficient for middle non-singularity of (S, T) are the following three conditions:*

4.1 $$S^{-1}(0) \subseteq T\ S^{-1}(0);$$

4.2 $$T^{-1}(0) \subseteq S\ T^{-1}(0);$$

4.3 $$S(X) \cap T(X) \subseteq (ST)\ (TS - ST)^{-1}(0).$$

If (4.1) *and* (4.2) *hold then also*

4.4 $$(ST)^{-1}(0) + (TS)^{-1}(0) \subseteq S^{-1}(0) + T^{-1}(0).$$

Proof. Suppose first that middle non-singularity (3.4) holds: then

$$Sy = 0 \Longrightarrow (-S \quad T)\begin{pmatrix} y \\ 0 \end{pmatrix} = 0 \Longrightarrow \begin{pmatrix} y \\ 0 \end{pmatrix} = \begin{pmatrix} T \\ S \end{pmatrix} x,$$

giving $y = Tx$ with $x \in S^{-1}(0)$; this proves (4.1), and similarly (4.2). Also

$$w = Tx = Sy \Longrightarrow \begin{pmatrix} y \\ x \end{pmatrix} = \begin{pmatrix} T \\ S \end{pmatrix} z \Longrightarrow w = STz = TSz,$$

giving (4.3). Conversely if these conditions hold then, using first (4.3),

$$\begin{pmatrix} y \\ x \end{pmatrix} \in (-S \quad T)^{-1}(0) \Longrightarrow Sy = Tx = STz = TSz,$$

giving $y - Tz \in S^{-1}(0) \subseteq T\,S^{-1}(0)$ and $x - Sz \in T^{-1}(0) \subseteq S\,T^{-1}(0)$, so that there are u and v for which

$$y - Tz = Tu \quad \text{with} \quad Su = 0 \quad \text{and} \quad x - Sz = Sv \quad \text{with} \quad Tv = 0:$$

but now $\begin{pmatrix} T \\ S \end{pmatrix}(z+u+v) = \begin{pmatrix} y \\ x \end{pmatrix}$, as required by (3.4). Towards the last part we assume only (4.1), and claim

4.5 $$(ST)^{-1}(0) \subseteq S^{-1}(0) + T^{-1}(0):$$

for if $(ST)x = 0$ then $Tx \in T\,S^{-1}(0)$, giving $Tx = Tz$ with $Sz = 0$, and hence

$$x = (x - z) + z \in T^{-1}(0) + S^{-1}(0)\bullet$$

The conditions (4.3) and (4.4) are not together sufficient for either (4.1) or (4.2), even in the presence of commutivity: if for example

4.6 $$S = T = P = P^2 \neq I$$

is a non-trivial idempotent then both (4.3) and (4.4), and of course also (3.5), hold, while neither (4.1) nor (4.2) are satisfied. The conditions (4.1) and (4.2) are not together sufficient for (4.3): for example take $S = T$ to be one-one with $T(X) \neq T^2(X)$. Specifically if $X = \ell_2$ we can take $S = T = U$ the forward shift with $(Ux)_{n+1} = x_n$ and $(Ux)_0 = 0$. Curto ([5] pp 71-72) has shown essentially that, in the presence of commutivity (3.5), middle non-singularity (3.4) is equivalent to (4.1) together with

4.7 $$T^{-1}S(X) \subseteq S(X),$$

and therefore also (4.2) together with

4.8 $$S^{-1}T(X) \subseteq T(X).$$

"Duality" considerations then suggest that (4.7), (4.8) and (4.4) might together be equivalent to (3.4). This however fails without commutivity : if for example $X = \ell_2$ we can take $T = V$, the backward shift with $(Vx)_n = x_{n+1}$, and $S = W$ with $(Wx)_n = (1/n)x_n$, to satisfy both (4.7) and (4.8), and also (4.4), but not (3.4). Sufficient for the non-singularity conditions (3.2)-(3.4) are the corresponding invertibility conditions: we call the pair (S,T) *left invertible* if there is another pair (S',T') for which

4.9 $$S'S + T'T = I,$$

right invertible if there is another pair (S'',T'') for which

4.10 $$SS'' + TT'' = I,$$

and *middle invertible* if there are pairs (S',T') and (S'',T'') for which, in matrix notation,

4.11 $$\begin{pmatrix} -S'' \\ T'' \end{pmatrix}(-S \quad T) + \begin{pmatrix} T \\ S \end{pmatrix}(T' \quad S') = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}.$$

In the context of pure linear algebra it is clear that "invertibility" and "non-singularity" are equivalent, by the argument for (0.7); for bounded linear operators between normed spaces we require that the "left", "right" and "middle" inverses be made out of bounded operators. When the operators S and T commute and the space X is a Hilbert space then non-singularity implies invertibility; for Banach spaces this question appears to be still open ([9] pp 73-74). In general it is sufficient for left, right and middle invertibility that (4.9) holds for a pair (S',T') such that

4.12 $(S',S),(S',T),(T',T),(T',S)$ are commutative.

The reader may suspect that there is an analogue for Theorem 4 with "invertibility" in place of "non-singularity": the author has been unable to find it. The invertible analogues of the conditions (4.1) and (4.2), and of (4.7) and (4.8), are not hard to find - each consists of either a column or a row from (4.11): the reader is invited to think up invertible analogues for (4.3) and (4.4). Theorem 4 should also have an analogue for "weak exactness": thus (3.2) is equivalent to implication

4.13 $$SU = TU = 0 \Longrightarrow U = 0,$$

the weakly exact analogue of (3.3) is

4.14 $$VS = VT = 0 \Longrightarrow V = 0,$$

and the weakly exact analogue of (3.4) is

4.15 $$(-S \quad T)\begin{pmatrix} -U' \\ U \end{pmatrix} = (V \quad V')\begin{pmatrix} T \\ S \end{pmatrix} = 0 \Longrightarrow (V \quad V')\begin{pmatrix} -U' \\ U \end{pmatrix} = 0.$$

It is not hard, starting from the "invertible" versions of (4.1) and (4.2), and of (4.7) and (4.8), to write down corresponding weak versions of these four conditions .

The next observation is again based on Gonzalez ([7] Theorem), and has also been noted by Curto ([5] p 72):

Theorem 5 *If (S_1, S_2, T) is commutative then there is equivalence*

5.1 (S_1S_2, T) *non-singular* $\Longleftrightarrow (S_1, T)$ *and* (S_2, T) *non-singular*

and equivalence

5.2 (S_1S_2, T) *invertible* $\Longleftrightarrow (S_1, T)$ *and* (S_2, T) *invertible.*

Proof. Consider first invertibility : if $S_1'S_1 + T_1'T = I = S_2'S_2 + T_2'T$ then

$$I = S_2'(S_1'S_1 + T_1'T)S_2 + T_2'T = (S_2'S_1')S_1S_2 + (S_2'T_1'S_2 + T_2')T;$$

conversely if $S_{12}'S_1S_2 + T_{12}'T = I$ then

$$(S_{12}'S_2)S_1 + T_{12}'T = I = (S_{12}'S_1)S_2 + T_{12}'T.$$

This proves (5.2) for left invertibility, and similarly for right invertibility . Towards middle invertibility, suppose that

5.3 $\mathbf{R'S' + SR = I}$ with $\mathbf{S'U = U'T'}$ and $\mathbf{W'T' + WU = I}$:

then

$$\mathbf{U = R'S'U + SRU = R'U'T' + UTRU}$$

giving

$$\mathbf{WR'U'T' = WU(I - TRU) = (I - W'T')(I - TRU)}$$

and hence

5.4 $$\mathbf{(WR'U' + W')T' + T(RU) = I.}$$

The implication (5.3)$\Longrightarrow$(5.4), which we have just proved, gives forward implication in (5.2) for middle invertibility if we take

5.5 $$\mathbf{T} = \begin{pmatrix} T \\ S_1 \end{pmatrix}, \mathbf{T'} = (-S_1 \quad T), \mathbf{S} = \begin{pmatrix} T \\ S_1S_2 \end{pmatrix} \quad \text{and} \quad \mathbf{S'} = (-S_1S_2 \quad T)$$

with

5.6 $$\mathbf{U} = \begin{pmatrix} I & 0 \\ 0 & S_2 \end{pmatrix}, \quad \mathbf{U'} = S_2, \quad \mathbf{W} = \begin{pmatrix} I & 0 \\ T_{12}'S_1 & S_{12}'S_1 \end{pmatrix},$$

$$\mathbf{W'} = \begin{pmatrix} 0 \\ T_{12}' \end{pmatrix}, \quad \mathbf{R} = (T_{12}' \quad S_{12}'), \quad \mathbf{R'} = \begin{pmatrix} -S_{12}'' \\ T_{12}'' \end{pmatrix}.$$

Conversely if

5.7 $$\begin{pmatrix} -S_1' \\ T_1' \end{pmatrix}(-S_1 \quad T) + \begin{pmatrix} T \\ S_1 \end{pmatrix}(S_1'' \quad T_1'') = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}$$

then since again

$$\begin{pmatrix} T \\ S_1S_2 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & S_2 \end{pmatrix}\begin{pmatrix} T \\ S_1 \end{pmatrix}$$

we have

$$\begin{pmatrix} I & 0 \\ 0 & S_2 \end{pmatrix} = \begin{pmatrix} -S_1' \\ S_2T_1' \end{pmatrix}(-T \quad S_1) + \begin{pmatrix} T \\ S_1S_2 \end{pmatrix}(T_1'' \quad S_1'')$$

giving

$$\begin{pmatrix} 0 \\ S_2 \end{pmatrix} = \begin{pmatrix} -S_1' \\ S_2T_1' \end{pmatrix}T + \begin{pmatrix} T \\ S_1S_2 \end{pmatrix}S_1''$$

and hence

$$5.8 \qquad \begin{pmatrix} T \\ S_1S_2 \end{pmatrix} S_1'' = \begin{pmatrix} S_1' & 0 \\ -S_2T_1' & I \end{pmatrix} \begin{pmatrix} T \\ S_2 \end{pmatrix}$$

and also

$$5.9 \qquad \begin{pmatrix} I \\ 0 \end{pmatrix} = \begin{pmatrix} -S_1' \\ S_2T_1' \end{pmatrix} (-S_1) + \begin{pmatrix} T \\ S_1S_2 \end{pmatrix} T_1''.$$

Combining (5.8) with

$$5.10 \qquad \begin{pmatrix} -S_2' \\ T_2' \end{pmatrix} (-S_2 \quad T) + \begin{pmatrix} T \\ S_2 \end{pmatrix} (T_2'' \quad S_2'') = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}$$

gives

$$5.11 \quad \begin{pmatrix} S_1'' & 0 \\ -S_2T_1' & I \end{pmatrix} = \begin{pmatrix} S_1'S_2' \\ S_2T_1'S_2' + T_2' \end{pmatrix} (-S_2 \quad T) + \begin{pmatrix} T \\ S_1S_2 \end{pmatrix} S_1'' (T_2'' \quad S_2''),$$

which combines with (5.9) to give

$$5.12 \qquad \begin{pmatrix} I \\ 0 \end{pmatrix} = \begin{pmatrix} T \\ S_1S_2 \end{pmatrix} (T_1'' + S_1''T_2S_1) + \begin{pmatrix} S_1'S_2' \\ S_2T_1'S_2 + T_2' \end{pmatrix} (-S_2S_1).$$

From (5.11) and (5.12) we get

$$5.13 \qquad \begin{pmatrix} S_1' & 0 & I \\ -S_2T_1' & I & 0 \end{pmatrix} = \begin{pmatrix} S_1'S_2' \\ S_2T_1'S_2' + T_2' \end{pmatrix} (-S_2 \quad T \quad -S_2S_1)$$

$$+ \begin{pmatrix} T \\ S_1S_2 \end{pmatrix} (S_1''T_2'' \quad S_1''S_2'' \quad T_1'' + S_1''T_2''S_1),$$

from which we can read off

$$5.14 \qquad \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}$$

$$= \begin{pmatrix} S_1'S_2' \\ S_2T_1'S_2' + T_2' \end{pmatrix} (-S_1S_2 \quad T) + \begin{pmatrix} T \\ S_1S_2 \end{pmatrix} (T_1'' + S_1''T_2''S_1 \quad S_1''S_2'').$$

This is backward implication in (5.2) for middle invertibility, and completes the proof of (5.2). With the information displayed in the proof of (5.2), the argument for (5.1) can be left to the reader •

For bounded linear operators between Banach spaces, (5.1) follows from the spectral mapping theorem for the Taylor spectrum, and then (5.2) from the corresponding theorem for the "Taylor split spectrum" ([10] Theorems 11.9.10,11.9.11). Our derivation of forward implication in (5.2) is based on the corresponding argument for non-singularity ([9] Theorem 4.3; [6]); our derivation of backward implication in (5.2) also follows from the corresponding argument for non-singularity, which is what is given by Gonzalez [7]. The reader may find it entertaining to try and carry out the matrix juggling in terms of operator calculations; he may also like to try and do the non-singularity argument (5.1) in a general ring, using conditions (4.13)-(4.15).

If $T : X \to X$ is linear then its *hyperrange* and *hyperkernel* are the subspaces

$$5.15 \qquad T^{\infty}(X) = \bigcap_{n=1}^{\infty} T^n(X)$$

and

$$5.16 \qquad T^{-\infty}(0) = \bigcup_{n=1}^{\infty} T^{-n}(0);$$

when T is continuous on a normed space X neither of these need be closed. If we write

$$5.17 \qquad \mathrm{comm}(T) = \{S \in BL(X,X) : ST = TS\}$$

for the *commutant* of T and

$$5.18 \qquad \mathrm{comm}^{-1}(T) = \mathrm{comm}(T) \cap BL^{-1}(X,X)$$

for the *invertible commutant* of T, then we can collect the following

Lemma 6 *If $T \in BL(X,X)$ is arbitrary then*

$$6.1 \qquad T^{-1}T^{-\infty}(0) \subseteq T^{-\infty}(0)$$

and

6.2 T essentially one $-$ one $\Longrightarrow T^{\infty}(X) \subseteq T\,T^{\infty}(X)$.

If $S \in \mathrm{comm}(T)$ *then*

6.3 $S\,T^{-\infty}(0) \subseteq T^{-\infty}(0)$ *and* $S\,T^{\infty}(X) \subseteq T^{\infty}(X)$.

If $S \in \mathrm{comm}^{-1}(T)$ *then*

6.4 $(T-S)^{-1}(0) \subseteq T^{\infty}(X)$ *and* $T^{-\infty}(0) \subseteq (T-S)(X)$.

Proof. This is Theorem 7.8.3 of [10]•

We shall call the operator $T : X \to X$ *self-exact* if the pair (T,T) satisfies (0.1):

6.5 $$T^{-1}(0) \subseteq T(X),$$

n-exact if (T,T^n) satisfies (0.1):

6.6 $$T^{-1}(0) \subseteq T^n(X),$$

and *hyperexact* if

6.7 $$T^{-1}(0) \subseteq T^{\infty}(X).$$

There are various equivalent forms of these conditions:

Theorem 7 *If* $T : X \to X$ *is linear and* $n \in \mathbf{N}$ *and* $m+k = n+1$ *then*

7.1 $T^{-1}(0) \subseteq T^n(X) \Longleftrightarrow T^{-k}(0) \subseteq T^m(X) \Longleftrightarrow T^{-n}(0) \subseteq T(X)$

and

7.2 $T^{-1}(0) \subseteq T^{\infty}(X) \Longleftrightarrow T^{-\infty}(0) \subseteq T(X) \Longleftrightarrow T^{-\infty}(0) \subseteq T^{\infty}(X)$.

If $T = TT^{\wedge}T$ *is regular then*

7.3 $T^{\wedge}T^{\infty}(X) \subseteq T^{\infty}(X)$ *and* $T^{\wedge}T^{-\infty}(0) \subseteq T^{-\infty}(0)$.

If $S \in \mathrm{comm}^{-1}(T)$ *then*

7.4 $(T-S)^{-\infty}(0) \subseteq T^{\infty}(X)$ *and* $T^{-\infty}(0) \subseteq (T-S)^{\infty}(X)$

and

7.5 $$T^{-\infty}(0) \cap (T-S)^{-\infty}(0) = \{0\}$$

and for each $m,n \in \mathbf{N}$

7.6 $$T^m(X) + (T-S)^n(X) = X.$$

Proof. Most of this comes from Lemma 1 and Lemma 2, taking U and V to be powers of T. For the last part factorise $(T^m - S^m)^n$ in two ways to see that $((T-S)^n, T^n)$ satisfies (4.9)-(4.11) for each n:

7.7 $$S^{mn} - r_{m,n}(T,S)T^n = (T-S)^n q_m(T,S)^n$$

for certain polynomials q_m and $r_{m,n}$•

We cannot replace m and n by ∞ in (7.6): for a counterexample take $T = U$ to be the forward shift on $X = \ell_2$ and $S = I$.

Definition 8 *Call* $T \in BL(X,X)$ *hyper-regular if it is regular and hyper-exact. We shall say that* T *is "consortedly regular" if there are sequences* (S_n) *in* $\mathrm{comm}^{-1}(T)$ *and* $(T_n^{\wedge})$ *in* $BL(X,X)$ *for which*

8.1 $\|S_n\| + \|T_n^{\wedge} - T^{\wedge}\| \longrightarrow 0$ *and* $T - S_n = (T-S_n)T_n^{\wedge}(T-S_n)$,

and "holomorphically regular" if there is $\delta > 0$ *and a holomorphic mapping* $T_z^{\wedge} : \{|z| < \delta\} \longrightarrow BL(X,X)$ *for which*

8.2 $T - \lambda I = (T-\lambda I)T_{\lambda}^{\wedge}(T-\lambda I)$ *for each* $|\lambda| < \delta$.

Mbekhta ([16] Theorem 2.6) has essentially proved

Theorem 9 *If* X *is complete and* $T \in BL(X,X)$ *then*

9.1

T *consortedly regular* $\Longrightarrow T$ *hyper* $-$ *regular* $\Longrightarrow T$ *holomorphically regular.*

Proof. If T is consortedly regular then, using (6.4), there is inclusion $T^{-k}(0) \subseteq (T - S_n)(X)$ for arbitrary k and n, where S_n satisfies (8.1), and hence if $T^k x = 0$ then $x = (T - S_n)T_n^{\wedge} x$ giving

$$(I - TT^{\wedge})x = ((T - S_n)T_n^{\wedge} - TT^{\wedge})x \longrightarrow 0 \text{ as } n \longrightarrow 0,$$

and hence $x = TT^{\wedge}x \in T(X)$. This gives, without completeness, the first implication of (9.1). Conversely suppose $T = TT^{\wedge}T$ is hyper-regular and $S \in \text{comm}(T)$ with $\|S\|\|T^{\wedge}\| < 1$: using (6.3) and (7.3) and expanding $(I - T^{\wedge}S)^{-1}$ in the geometric series gives

$$S(I - T^{\wedge}S)^{-1}T^{-1}(0) \subseteq \text{cl } T^{-\infty}(0) \subseteq \text{cl } T(X)$$

and hence

$$(I - TT^{\wedge})S(I - T^{\wedge}S)^{-1}(I - T^{\wedge}T) = 0,$$

which by (3.8.4.3) from the proof of Theorem 3.8.4 [10] says

9.2 $$T - S = (T - S)(I - T^{\wedge}S)^{-1}T^{\wedge}(T - S).$$

Specialising to scalar $S = \lambda I$ gives the second implication of (9.1)•

The derivation of (9.2) is based on Caradus [4]; cf also Theorem 3.9 of Nashed [18]. If we observe

9.3 $$T^{\wedge}(T - S) + (I - T^{\wedge}T) = I - T^{\wedge}S$$

that $I - T^{\wedge}S$ sends the null space of $T - S$ into the null space of T, then we can see that for Fredholm T and one-one $I - T^{\wedge}S$ we have $\dim(T - S)^{-1}(0) \leq \dim T^{-1}(0)$ ([10] Theorem 6.4.5). Conversely if $T = TT^{\wedge}T$ is hyperregular and $S \in \text{comm}(T)$ has small enough norm,

9.4
$$(T-S)^{\wedge}T+I-(T-S)^{\wedge}(T-S) = I+(T-S)^{\wedge}S \text{ with } (T-S)^{\wedge} = (I-T^{\wedge}S)^{-1}T^{\wedge},$$

furnishing an invertible operator which sends the null space of T into the null space of $T - S$. In the Fredholm case this is the Apostol *zero jump* condition [1],[22],[19].

Theorem 9 says that the hyper-regular operators form an open subset of $BL(X, X)$, and hence that a certain kind of "spectrum" is closed in C We

may also observe that the topological boundary of the spectrum is contained in this "hyper-regular spectrum":

9.5 $$\{T \in \text{cl}_{\text{comm}} BL^{-1}(X, X) : T \text{ hyper} - \text{regular}\} \subseteq BL^{-1}(X, X).$$

We are claiming that if hyper-regular T is the limit of a sequence $T - S_n$ of invertible operators which commute with T then T must also be invertible. It follows from (9.4) that if $(T - S)^{\wedge}$ and $I - T^{\wedge}S$ are both invertible then so is $T^{\wedge}$; since this argument extends to $T^{\wedge}TT^{\wedge}$ this also makes T invertible.

The spectral mapping theorem for polynomials extends to the "hyper-regular spectrum":

Theorem 10 *If $ST = TS$ then*

10.1 $$ST \text{ self} - \text{exact} \Longrightarrow S,\ T \text{ self} - \text{exact}$$

and

10.2 $$ST \text{ hyper} - \text{regular} \Longrightarrow S,\ T \text{ hyper} - \text{regular}$$

If $ST = TS$ and (S, T) is middle exact then

10.3 $$S,\ T \text{ self} - \text{exact} \Longrightarrow ST \text{ self} - \text{exact}$$

and

10.4 $$S,\ T \text{ hyper} - \text{regular} \Longrightarrow ST \text{ hyper} - \text{regular}.$$

Proof. The first part is an extension of Mbekhta ([17] Lemma 4.15): if $(ST)^{-1}(0) \subseteq (ST)(X)$ then

$$T^{-1}(0) \subseteq (ST)^{-1}(0) \subseteq (ST)(X) = (TS)(X) \subseteq T(X),$$

and similarly for S and powers T^n and S^m. This gives (10.1) and most of (10.2): the regularity of S and T come from (3.1). Conversely, for (10.3), use (4.1)-(4.4):

$$(ST)^{-1}(0) \subseteq S^{-1}(0) + T^{-1}(0) \subseteq S(X) \cap T(X) \subseteq (ST)(X).$$

This gives (10.3) and most of (10.4): the regularity of ST is (3.1) again•

One situation in which all the invertibility and non-singularity conditions for (S,T) are satisfied is when we can write

10.5 $$S = q(A), T = r(A)$$

for an operator $A : X \to X$ and polynomials q and r without non-trivial common factor. In general polynomials q and r have a unique "highest common factor" $\mathrm{hcf}(q,r)$ determined by the logical equivalence

10.6 $$\{q,r\} \subseteq (\mathrm{Poly})p \Longleftrightarrow p \in (\mathrm{Poly})\mathrm{hcf}(q,r),$$

together with the requirement that it be "monic" (unless either q or r is 0, in which case also $\mathrm{hcf}(q,r) = 0$). It is now familiar that, by the Euclidean algorithm,

10.7 $$\mathrm{hcf}(q,r) \in (\mathrm{Poly})q + (\mathrm{Poly})r,$$

so that there are polynomials q' and r' for which $\mathrm{hcf}(q,r) = q'q + r'r$. If in particular $\mathrm{hcf}(q,r) = 1$, so that q and r have no common non-trivial common factors, then (in the algebra *Poly*) the pair (q,r) satisfies all the invertibility conditions (4.9)-(4.11) (since the analogue of (4.12) holds). This extends to the pair $(S,T) = (q(A), r(A))$, with $(S',T') = (q'(A), r'(A))$ whenever $A : X \to X$ is an operator: thus if (10.5) holds then the non-singularity conditions (3.2)-(3.4) are satisfied.

Lemma 11 *If $A : X \to X$ is linear there is equality*

11.1 $$\sum_{\lambda \in \mathbf{C}} (A - \lambda I)^{-\infty}(0) = \bigcup_{0 \neq p \in \mathrm{Poly}} p(A)^{-1}(0)$$

and

11.2 $$\bigcap_{\lambda \in \mathbf{C}} (A - \lambda I)^{\infty}(X) = \bigcap_{0 \neq p \in \mathrm{Poly}} p(A)(X).$$

Proof. The left hand side of (11.1) is obviously included in the right; conversely if $p = qr \in \mathrm{Poly}$ with $\mathrm{hcf}(q,r) = 1$ then by (4.4)

11.3 $$p(A)^{-1}(0) = q(A)^{-1}(0) + r(A)^{-1}(0).$$

More generally if $p = q_1 q_2 \dots q_n$ is a finite product of factors q_j of which no pair has any common factors then the null space of $p(A)$ is the sum of the null spaces $q_j(A)^{-1}(0)$; but by the fundamental theorem of algebra p is a product of polynomials of the form $(z - \lambda)^k$ for distinct complex numbers λ. This proves (11.1). Similarly, the right hand side of (11.2) is included in the left, and the opposite inclusion follows by the inductive extension of equality (4.3):

11.4 $$p(A)(X) = q(A)(X) \cap r(A)(X)$$

if $p = qr$ with $\mathrm{hcf}(q,r) = 1$•

The operator $A : X \to X$ is described as *algebraic* if there exists a non-trivial polynomial $p \in \mathrm{Poly}$ for which

11.4 $$p(A)^{-1}(0) = X,$$

and as *locally algebraic* if

11.5 $$\bigcup_{0 \neq p \in \mathrm{Poly}} p(A)^{-1}(0) = X.$$

The intermediate notion is that A is *boundedly locally algebraic* if there is $k \in \mathbf{N}$ for which

11.6 $$X = \bigcup \{p(A)^{-1}(0) : 0 \neq p \in \mathrm{Poly}, \mathrm{degree}(p) \leq k\}.$$

For bounded linear operators between Banach spaces, an application of Baire's theorem says that (11.5)$\Longrightarrow$ (11.6) ([13] Theorem 15; [20] Theorem 4.8 ; [21] (3.4)); our interest here is to expound *Kaplansky's lemma* ([13] Lemma 14; [20] Theorem 4.8; [21](3.5)), which says that (11.6)$\Longrightarrow$ (11.4):

Theorem 12 *If $A : X \to X$ is boundedly locally algebraic then it is algebraic.*

Proof If A is locally algebraic in the sense of (11.5) then by (11.1) there is equality

12.1 $$\sum_{\lambda \in \mathbf{C}} (A - \lambda I)^{-\infty}(0) = X;$$

for a locally algebraic operator to be algebraic it is necessary and sufficient that it have a finite set of *eigenvalues*

12.2
$$\pi^{\text{left}}(A) = \{\lambda \in \mathbf{C} : (A-\lambda I)^{-1}(0) \neq \{0\}\} = \{\lambda \in \mathbf{C} : (A-\lambda I)^{-\infty}(0) \neq \{0\}\}.$$

We claim that if the set $\pi^{\text{left}}(A)$ is infinite then the condition (11.6) must fail: for if $\lambda_1, \lambda_2, \ldots, \lambda_m$ are pairwise distinct eigenvalues of A, with corresponding eigenvectors $x_1, x_2, \ldots, x_m$, and $p \in \text{Poly}$ is a polynomial, we claim that there is implication

12.3
$$p(A)(\sum_{j=1}^{m} x_j) = 0 \Longrightarrow \{x_1, x_2, ..., x_m\} \subseteq p(A)^{-1}(0)$$

$$\Longrightarrow \{\lambda_1, \lambda_2, ..., \lambda_m\} \subseteq p^{-1}(0),$$

forcing degree$(p) \geq m$. To see why the first part of (12.3) holds argue that

12.4 $\quad \text{hcf}(q,r) = 1, q(A)y = r(A)z = 0, y+z = 0 \Longrightarrow y = z = 0$:

this is because the pair $(S,T) = (q(A), r(A))$ satisfies the condition (3.2) so that equality $y+z=0$ puts $y=-z$ in $q(A)^{-1}(0) \cap r(A)^{-1}(0) = \{0\}$. To apply (12.4) to the first part of (12.3) take

$$y = x_j, z = \sum_{i \neq j} x_i, q = z - \lambda_j, r = \prod_{i \neq j} z - \lambda_i.$$

To see why the second part of (12.3) holds observe that

12.5 $\quad p(\lambda_j) \neq 0 \Longrightarrow \text{hcf}(p, z-\lambda_j) = 1 \Longrightarrow p(A)^{-1}(0) \cap (A-\lambda_j I)^{-1}(0) = \{0\}\bullet$

When the operator A is algebraic then (12.1) becomes a finite direct sum decomposition of the space X : this decomposition makes it clear, as is observed by Aupetit [2], that if $k \in \mathbf{N}$ satisfies the condition (11.6) then (11.4) can be satisfied with degree$(p) \leq k$. When A is algebraic then each existing inverse $(A-\lambda I)^{-1}$ is expressible as a polynomial in A : when X is finite dimensional this is one of the familiar applications of the Cayley-Hamilton theorem. We may also observe, as in the finite dimensional case [12], that when $(A-\lambda I)^{-1}$ does not exist, then all the eigenvectors $x \in (A-\lambda I)^{-1}(0)$ lie in the range

of a related polynomial in A : the simple observation is that if $p(A) = 0$ and $p = qr$ with $\text{hcf}(q,r) = 1$ then

12.6
$$q(A)^{-1}(0) = r(A)(X).$$

We conclude by expounding another generalization of Kaplansky's lemma; the unpublished argument is due to Laffey ([15] Lemma 1; [20] (3.5)):

Theorem 13 *If the operator $A : X \to X$ is boundedly locally algebraic modulo a finite dimensional subspace $Y \subseteq X$, then it is algebraic.*

Proof The assumption is that there is $k \in \mathbf{N}$ for which, for each $x \in X$, there is a non-trivial polynomial $p_x \in \text{Poly}$ for which

13.1
$$\text{degree}(p_x) \leq k \quad \text{and} \quad p_x(A)x \in Y.$$

We are not assuming that the finite dimensional subspace Y is "invariant" under A in the sense that $A(Y) \subseteq Y$, but immediately replace it with the (possibly infinite dimensional) invariant subspace

13.2
$$\hat{Y} = \bigcup_{p \in \text{Poly}} p(A)(Y) = Y + \sum_{n \in \mathbf{N}} A^n(Y)$$

generated by it, together with the induced quotient operator $\hat{A} : X/\hat{Y} \longrightarrow X/\hat{Y}$. Applying Kaplansky's lemma (Theorem 12) to $\hat{A}$ gives a non-trivial polynomial (of degree $\leq k$) $p_0 \in \text{Poly}$ for which

13.3
$$p_0(A)(X) \subseteq \hat{Y}.$$

If Y is of dimension m , with basis $y = (y_1, y_2, \ldots, y_m)$, then again by assumption there are non-trivial polynomials $q_1, q_2, \ldots, q_m$ (of degree $\leq k$) for which

13.4
$$q_i(A)Ay_i \in Y \ (i = 1, 2, \ldots, m),$$

and hence complex numbers $(\lambda_{ij}) = B$ for which

13.5
$$q_i(A)Ay_i = \sum_{j=1}^{m} \lambda_{ij} y_j \quad (i = 1, 2, \ldots, m).$$

This gives

13.6 $$Q(A)y = 0 \in Y^m,$$

treating the basis $y \in Y^m$ as a column matrix, where $Q(A) \in L(X,X)^m$ is the "operator matrix"

13.7 $$Q(A) = B \otimes I - q(A)(I \otimes A)$$

$$= \begin{pmatrix} \lambda_{11}I - q_1(A)A & \lambda_{12}I & \dots & \lambda_{1m}I \\ \lambda_{21}I & \lambda_{22}I - q_2(A)A & \dots & \lambda_{2m}I \\ \dots & \dots & \dots & \dots \\ \lambda_{m1}I & \lambda_{m2}I & \dots & \lambda_{mm}I - q_m(A)A \end{pmatrix}.$$

It follows ([8] Problem 70; [11](2.0.4)p.108)

13.8 $q_0(A)y_j = 0 \quad (j = 1, 2, \dots, m)$ with $q_0(A) = \det Q(A) \in L(X,X)$:

since all the entries of $Q(A)$ commute we can write $\mathrm{adj}Q(A).Q(A) = q_0(A) \otimes I$, exactly as in the numerical case. It now follows

$$q_0(A)Y = 0 \quad \text{and hence} \quad q_0(A)\mathrm{Poly}(A)Y = \{0\}$$

and hence

13.9 $$q_0(A)p_0(A)X \subseteq q_0(A)\hat{Y} = \{0\}.$$

Our final observation explains why (13.5) was not replaced by something simpler : by construction

13.10 $$\mathrm{degree}(q_0) \geq m,$$

which ensures $0 \neq q_0 p_0 \in \mathrm{Poly}\bullet$

References

[1] C. Apostol, The reduced minimum modulus, *Michigan Math. Jour.* 32 (1985) 279–294.

[2] B. Aupetit, An improvement in Kaplansky's lemma for locally algebraic operators, *Studia Math.* 88 (1985) 275–278.

[3] S.R. Caradus, *operator theory of the pseudo-inverse*, Queen's papers in pure and applied mathematics 38, Queen's University, Kingston Ontario (1978).

[4] S.R. Caradus, Perturbation theory for generalized Fredholm operators II, *Proc. Amer. Math. Soc.* 62 (1977) 72–76.

[5] R.E. Curto, Applications of several complex variables to multiparameter spectral theory, *Pitman Research Notes in Mathematics* 192, *Surveys of some recent results in operator theory II* pp 25–90 (Longmans 1988).

[6] A.S. Fainstein, Towards a spectral mapping theorem for the Taylor spectrum, *Spectral theory of operators and applications* no. 8, Azerbaidzan SSR Academy of Sciences pp 212–236 (Baku 1987).

[7] M. Gonzalez, Null spaces and ranges of polynomials of operators, *Publicacions Matematiques Universitat Barcelona* 32 (1988) 167–170.

[8] P.R. Halmos, *A Hilbert space problem book* (Springer 1982).

[9] R.E. Harte, Invertibility, singularity and Joseph L. Taylor, *Proc. Royal Irish Acad.* 81A (1981) 71–79.

[10] R.E. Harte, *Invertibility and singularity for bounded linear operators* (Dekker 1988).

[11] R.E. Harte, Invertibility and singularity for operator matrices, *Proc. Royal Irish Acad.* 88A (1989) 103–108.

[12] R.E. Harte, Cayley-Hamilton for eigenvalues, *Bull. Irish Math. Soc.* 22 (1989) 66–68.

[13] I. Kaplansky, *Infinite abelian groups* (University of Michigan Press, Ann Arbor Mich. 1954).

[14] T. Kato, Perturbation theory for nullity, deficiency and other quantities for linear operators, *J. Analyse Math.* 6 (1958) 261–322.

[15] T.J. Laffey and T.T. West, Fredholm commutators, *Proc. Royal Irish Acad.* 82A (1982) 129–140.

[16] M. Mbekhta, Generalization de la decomposition de Kato aux operateurs paranormeaux et spectraux, *Glasgow Math. Jour.* 29 (1987) 159–175.

[17] M. Mbekhta, Resolvant generalise et theorie spectrale, *Jour. Operator theory* 21 (1989) 69–105.

[18] M.Z. Nashed, Perturbations and approximations for generalized inverses and linear operator equations, *Generalized inverses and applications* (ed. M.Z. Nashed, Academic Press 1976), pp 325–396.

[19] M. O'Searcoid and T.T. West, Continuity of the generalized kernel and range of semi-Fredholm operators, *Math. Proc. Cam. Phil. Soc.* 105 (1989) 513–522.

[20] H. Radjavi and P. Rosenthal, *Invariant subspaces* (Ergebnisse der Math. 77, Springer 1973).

[21] A.Sinclair, *Automatic continuity of linear operators* (Cambridge University Press, UK 1976).

[22] T.T. West, A Riesz-Schauder theorem for semi-Fredholm operators, *Proc. Royal Irish Acad.* 87A (1987) 137–146.

University of Fairbanks,
Alaska, AK 99775

Dimension Theory and Stable Rank

Gerard J. Murphy

1. Topological Dimension Theory

The theory of dimension in topology grew from attempts to establish the topological invariance of the dimension of Euclidean spaces. The first proof that the spaces $\mathbf{R}^n$ and $\mathbf{R}^m$ are homeomorphic only if n and m are equal was given by Brouwer in 1911. His proof did not explicitly involve a property that might serve as a topological definition of n, but in the same year Lebesgue suggested an approach which led to the covering dimension. If I is the closed unit interval of $\mathbf{R}$ it was observed by Lebesgue that the cube I^n can be covered by arbitrarily small closed sets in such a manner that not more than $n+1$ of them meet (in a common point). This is illustrated in the 2-dimensional case by the usual pattern of brickwork, where a maximum of 3 bricks can meet.

To define the covering dimension we introduce a preliminary concept. If $\Phi = (U_\lambda)_{\lambda\in\Lambda}$ is a family of subsets of a topological space X and $x \in X$ the *order* of Φ at x, denoted $ord_x(\Phi)$, is defined to be the number of elements λ of Λ such that U_λ contains x (if there are infinitely many such elements λ then $ord_x(\Phi) = +\infty$). The *order* of Φ is defined to be the supremum of all $ord_x(\Phi)$ where x runs over X. Thus for the brickwork family of sets mentioned above the order is 3. If X is a topological space the *(covering) dimension* of X, denoted $dim(X)$, is the least integer n such that every finite open covering of X has an open refinement of order not greater than $n+1$. If no such integer n exists then we set $dim(X) = +\infty$. Here is an alternative, very useful, formulation: For any topological space X, the inequality $dim(X) \leq n$ holds if and only if for each open covering $U_1, \ldots, U_{n+2}$ of X there is an open covering $V_1, \ldots, V_{n+2}$ such that $V_j \subseteq U_j$ for $j = 1, \ldots, n+2$ and $V_1 \cap \ldots \cap V_{n+2} = \emptyset$. For the classical spaces such as $\mathbf{R}^n$, I^n and S^n (the n-sphere) the covering dimension is the number one would expect. It is however non-trivial to show that $dim(\mathbf{R}^n) = n$. The proof involves the well known theorem of Brouwer which asserts that for all n the sphere S^{n-1} is not a retract of the closed unit

ball of $\mathbf{R}^n$. There is a nice easily-stated criterion to determine if a subspace X of a Euclidean space $\mathbf{R}^n$ has dimension n. This is true if and only if X contains a non-empty open set of $\mathbf{R}^n$.

The case where the covering dimension is zero is easy to interpret in direct topological terms. If X is Hausdorff and $dim(X) = 0$ then X is necessarily normal and totally disconnected. For compact Hausdorff spaces being zero-dimensional is equivalent to being totally disconnected, but this is not true for arbitrary spaces, as we shall see in an example below.

Incidentally, there are other concepts of dimension, such as the large and small inductive dimensions. For metric spaces the large inductive dimension is the same as the covering dimension, and all three dimensions agree on separable metric spaces. The covering dimension appears to be preferred for the analysis of general topological spaces.

There is a very nice connection between dimension theory and the problem of the existence of continuous extensions of certain continuous functions:

1.1. Theorem. *If X is a normal space then $dim(X) \leq n$ if and only if for each closed set A of X and continuous function $f: A \to S^n$ there exists a continuous extension $f': X \to S^n$.*

Dimension theory also has useful applications to topological K-theory. The latter topic can be viewed as the algebraic aspect of the theory of vector bundles, and one of the questions it investigates is the extent to which the cancellation property holds for (Whitney) direct sums of bundles. This is controlled in part by the dimension of the base space.

Although the covering dimension gives the expected answer in many classical situations, it has a number of paradoxical and even pathological features. For instance, the set $X = \{1, 2, 3, 4\}$ can be endowed with a non-Hausdorff topology making it a topological space of covering dimension 1. This illustrates the point that dimension theory does not work too well for "strange" topological spaces. A mininum assumption appears to be normality to get some kind of reasonable theory. But even for compact Hausdorff spaces and metric spaces unexpected things can happen. For instance, the "logarithmic product rule"

$$(*) \qquad dim(X \times Y) = dim(X) + dim(Y)$$

fails spectacularly. To illustrate this denote by Q the separable metric space of all square-summable sequences of rational numbers with the metric defined

by

$$d((x_n), (y_n)) = (\sum_{n=1}^{\infty} (x_n - y_n)^2)^{1/2}.$$

One can show that $dim(Q) = 1$ and that Q is homeomorphic to $Q \times Q$, so $(*)$ fails for $X = Y = Q$. (We promised above an example of a totally disconnected space not of dimension zero. The space Q is such an example.) The logarithmic product rule fails even for compact spaces. Pontryagin has exhibited an example of a pair of compact metrisable spaces of dimension 2 whose product has dimension 3. In a number of important cases one gets a useful inequality instead of $(*)$. If X and Y are arbitrary compact Hausdorff spaces then

$$dim(X \times Y) \leq dim(X) + dim(Y).$$

This inequality also holds in the case that X and Y are metric spaces.

Perhaps one should not really be surprised by these paradoxes of dimension theory. After all, as is well known, one can continuously map I onto I^2!

There are many more aspects to dimension theory, a full account of which can be found in [5] and [6]. We turn now to the problem of defining the "dimension" of a C*-algebra. We shall see there a number of possible candidates for the position, and all have connections with the classical topological dimension.

2. The Bass Stable Rank and the Real Rank

One of the great sucesses in recent years in operator algebra theory has been the development of K-theory of C*-algebras (for an introductory exposition see [3]). Recall that a *C*-algebra* is a Banach algebra A together with an isometric involution $a \mapsto a^*$ such that $\|a^*a\| = \|a\|^2$ for all $a \in A$. If H is a Hilbert space and $B(H)$ denotes the algebra of all bounded linear operators on H then $B(H)$ is a C*-algebra, as is every norm-closed self-adjoint subalgebra. A theorem of Gelfand and Naimark asserts that up to isomorphism these are all the C*-algebras.

There is an important connection with topology given as follows: If X is a locally compact Hausdorff space then $C_0(X)$, the set of all continuous complex-valued functions on X that vanish at infinity, is a commutative C*-algebra (the operations are pointwise-defined and the norm is the supremum norm). Conversely every commutative C*-algebra is of this form up to isomorphism.

This correspondence between commutative C*-algebras and locally compact Hausdorff spaces has inspired an approach to the theory of C*-algebras which regards it as "non-commutative topology", with the finitely-generated projective modules being the appropriate generalisation of vector bundles (based on a theorem of Swan). This point of view has been very fruitful and was the motivation for introducing K-theory into C*-algebra theory. From this perspective it is natural to try to develop some concept of "dimension" for a C*-algebra analogous to the dimension of a topological space. This was attempted by Rieffel [10], who introduced the concept of the topological stable rank of a C*-algebra. This was soon seen to be identical with the Bass stable rank already known to algebraists. Rieffel was led to investigate the stable rank by a question concerning a certain class of C*-algebras. If θ is an irrational number in [0,1] then there is (up to isomorphism) a unique C*-algebra A_θ generated by a pair of unitaries u, v such that $uv = e^{i2\pi\theta}vu$ (u is a *unitary* means that $u^* = u^{-1}$). These algebras, called *irrational rotation algebras*, are the motivating examples in the non-commutative differential geometry being developed by the Fields' medalist Alain Connes. The question that interested Rieffel is whether the cancellation property for projective modules holds for the irrational rotation algebras. This can be reformulated in more concrete terms: if two projections in A_θ have equal trace are they necessarily unitarily equivalent? The answer turns out to be affirmative, as was shown by Rieffel using the stable rank. He was led to his notion of topological stable rank by the following theorem of classical dimension theory:

2.1. Theorem. *If X is a compact Hausdorff space then its dimension is the least integer n such every continuous function from X to $\mathbf{R}^{n+1}$ can be uniformly approximated arbitrarily closely by continuous functions which never vanish.*

Interpreting this in terms of the algebra $C_0(X)$, and then slightly reformulating, one arrives at the definition of stable rank. Let A be a unital C*-algebra, and for each integer n let $L_n(A)$ be the set of n-tuples $(a_1, \ldots, a_n)$ generating A as a left ideal, that is, such that

$$Aa_1 + \cdots + Aa_n = A.$$

The *stable rank* $sr(A)$ of A is the least integer n such that $L_n(A)$ is dense in A^n for the product topology. If no such integer exists $sr(A) = +\infty$. If

$A = C_0(X)$ where X is a compact Hausdorff space, and if $[t]$ denotes the integer part of t, then $sr(A) = [dim(X)/2] + 1$.

Except in the lowest rank case, it is not easy to interpret the stable rank directly in terms of properties of the algebra A. It can however be proved without difficulty that a unital C*-algebra A is of stable rank 1 if and only if the set of invertible elements of A is dense in A. The question of whether this is true for the irrational rotation algebras was open for a number of years, and has only recently been determined (in the affirmative) [9].

As in classical dimension theory, there are a number of surprising results in the theory of the stable rank. For instance, stable C*-algebras can have rank either 1 or 2 only. (A C*-algebra A is *stable* if it is isomorphic to the C*-tensor product $A \otimes_* \mathbf{K}$, where $\mathbf{K}$ is the C*-algebra of all compact operators on the Hilbert space ℓ^2. These algebras occur frequently in C*-theory.) If A is an arbitrary C*-algebra and $M_n(A)$ denotes the set of square matrices of size n having entries in A, then $M_n(A)$ is a C*-algebra in a natural way. If $sr(A) = 1$ then $sr(M_n(A)) = 1$, that is, if the invertible elements of A are dense in A then the invertible elements of $M_n(A)$ are dense in $M_n(A)$. If $sr(A) = +\infty$ then $sr(M_n(A)) = +\infty$ also. If $1 < sr(A) \leq n + 1$ then $sr(M_n(A)) = 2$.

Following along lines set down by Rieffel, Brown and Pedersen [1] introduced another concept of rank for C*-algebras. If A is a unital C*-algebra then its *real rank* is defined to be the smallest integer, $RR(A)$, such that for each n-tuple $(a_1, \ldots, a_n)$ of self-adjoint elements of A for which $n \leq RR(A)+1$ and each $\varepsilon > 0$ there is an n-tuple of self-adjoint elements $(b_1, \ldots, b_n)$ in A such that $\sum_{k=1}^n b_k^2$ is invertible and

$$\| \sum_{k=1}^{n} (a_k - b_k)^2 \| < \varepsilon.$$

(The element a is *self-adjoint* if $a^* = a$.) If X is a compact Hausdorff space and $A = C_0(X)$ then it is easy to show that $RR(A) = dim(X)$. For an arbitrary unital C*-algebra A the real and stable ranks are related by the inequality

$$RR(A) \leq 2sr(A) - 1.$$

However these two ranks can be very far apart. There is a C*-algebra A such that $RR(A) = 0$ and $sr(A) = +\infty$. Based on previous experience one would expect the lowest real rank case to be easiest to interpret directly in terms of the algebra, and this is indeed true. One has $RR(A) = 0$ if and only if every

self-adjoint element of A is the limit of a sequence of such elements having finite spectra. Algebras satisfying this condition had already been extensively analysed by Pedersen [8], and have some very interesting properties.

3. The Analytic Rank

Motivated by results in classical dimension theory the author has introduced a third concept of rank. If A is a unital C*-algebra a C*-subalgebra B is defined to be *analytic* if B contains the unit 1 of A and $a^2 \in B$ implies $a \in B$ for all self-adjoint elements $a \in A$. If S is an arbitrary subset of A then there is a smallest analytic subalgebra of A containing it, and if this is A itself and the elements of S are self-adjoint then S is called an *analytic base* of A.

Every analytic subalgebra contains all the elements with finite spectrum, in particular all the projections. If A is of real rank zero then its only analytic subalgebra is A itself. The field $\mathbf{C}$ is an analytic subalgebra of an arbitrary C*-algebra A if and only if the only projections of A are 0 and 1. In particular if $A = C_0(X)$ then $\mathbf{C}$ is an analytic subalgebra if and only if X is connected.

The *analytic rank*, $ar(A)$, of a C*-algebra A is defined to be $+\infty$ if A has no finite analytic base, and to be n if A has an analytic base of this (finite) cardinality but none of smaller cardinality. If X is a compact metric space then by classical dimension theory results one has $ar(A) = dim(X)$. The analytic rank, considered purely as a C*-algebra invariant, seems to behave better in a number of respects than the stable rank and the real rank, although like these it has some paradoxical properties.

Here is an example of nice behaviour. Associated with each locally compact group G there is a C*-algebra $C^*(G)$ having the same representation theory as G (thus the representation theory of these groups is contained in the representation theory of C*-algebras). If $\mathbf{F}_n$ is the (discrete) free group on $n > 1$ generators then the stable rank of $C^*(\mathbf{F}_n)$ is $+\infty$, so the stable rank is unable to distinguish between these algebras. However $ar(C^*(\mathbf{F}_n)) = n$.

There are a number of properties that one would like a "rank" function to have. For instance, if $A \mapsto r(A)$ is a rank function it is desirable that it should satisfy the following conditions:

(1) If $A = A_1 \oplus A_2$ then $r(A) = \max\{r(A_1), r(A_2)\}$.
(2) If B is a quotient algebra of A then $r(B) \leq r(A)$.
(3) If $A = A_1 \otimes_* A_2$, that is, A is the (spatial) C*-tensor product of A_1 and A_2, then $r(A) \leq r(A_1) + r(A_2)$.
(4) If $A = B \times_\alpha G$, that is, A is the C*-crossed product of the unital C*-algebra B and the countable discrete abelian group G, then $r(A) \leq r(B) + dim(\hat{G})$, where $\hat{G}$ is the Pontryagin dual group of G.

The analytic rank satisfies all four conditions, and the proofs involved in showing this are not difficult. However, some of these conditions are difficult, or unknown, for the stable and real ranks.

The analytic rank seems to be a natural invariant. However the concept of analytic C*-subalgebra is rather mysterious, and it would be useful to be able to reformulate the definition of analytic rank in terms of better understood C*-algebraic ideas.

It appears that (at least some of) these various concepts of rank may be of great future importance. As yet however the theory is only in its initial stages. It is desirable to compute the ranks of many more examples, and to be able to interpret the ranks more directly in terms of properties of the algebras.

References

[1] L.G. Brown and G.K. Pedersen, C*-algebras of real rank zero, preprint (1989).

[2] R.H. Herman and L.N. Vaserstein, The stable range of C*-algebras, *Inventiones Math.* **77** (1984), 553–555.

[3] G.J. Murphy, Extensions and K-Theory of C*-algebras, *Bull. Irish Math. Soc.* **18** (1987), 18–29.

[4] G.J. Murphy, The analytic rank of a C*-algebra, submitted.

[5] J. Nagata, *Modern Dimension Theory.* Heldermann Verlag, Berlin, 1983.

[6] A.R. Pears, *Dimension Theory of General Spaces.* Cambridge Univ. Press, Cambridge, 1975.

[7] G.K. Pedersen, *C*-Algebras and their Automorphism Groups.* Academic Press, New York-London, 1979.

[8] G.K. Pedersen, The linear span of projections in simple C*-algebras, *J. Operator Theory* **4** (1980), 289–296.

[9] I.F. Putnam, The invertible elements are dense in the irrational rotation C*-algebras, preprint (1989).

[10] M.A. Rieffel, Dimension and stable rank in the K-theory of C*-algebras, *Proc. London Math. Soc.* (3) **46** (1983), 301–333.

Department of Mathematics,
University College, Cork.

MATHEMATICAL EDUCATION

Mathematics at Third Level — How We Teach

F.D.T. Dickenson, E.S. Gillespie & S.K. Houston

Courses combining mathematics, statistics and computing at the University of Ulster are described. Innovative methods of teaching, learning and assessment are discussed.

Introduction

This paper describes degree and sub-degree courses combining mathematics, statistics and computing at the University of Ulster and discusses the non-traditional approaches taken to teaching, learning and assessment. It has been written in response to a recent article in the Bulletin by Maurice O'Reilly [1] which questions how we teach mathematics at third level.

The University is required by its Charter to offer courses at degree and at sub-degree level. Hence we offer an honours degree, an ordinary degree and a Higher National Diploma (which is validated by the University and by the Business and Technician Education Council). These are linked courses which means that students enter the course most appropriate to their entrance qualifications (usually A levels, but about 10% offer the Irish Leaving Certificate) but can subsequently transfer between courses if their progress so dictates.

The suite of courses was designed only after an extensive market research exercise. All U.K. firms known to advertise regularly for graduates of combined degrees in mathematics, statistics and computing were contacted in an attempt to assess their needs as regards knowledge and skills, the desirability of a sandwich year, and the potential availability of sandwich placements. Detailed information was received from 100 of the 246 firms contacted.

Each course comprises applicable mathematics, statistics, computing and operational research, and aims principally to produce graduates (or diplo-

mates) prepared for a mathematical career in industry, commerce or the public sector. The topics studied are there because they are useful in the solution of practical problems. Students are encouraged to look as much at the problem and its context as at the mathematical methods they will use to solve it. The non-traditional methods of teaching, learning and assessment which the courses embrace include:

(i) an emphasis on the development of enterprise,

(ii) group project work,

(iii) a unifying theme of mathematical modelling,

(iv) an industrial placement year.

These are discussed below together with details of the course units in which they especially feature.

1 Enterprise

Business today calls increasingly for enterprising employees, that is, lively, resourceful, adaptable people able to recognise and exploit opportunities, to take risks and respond to challenges, to innovate, to communicate well, to work effectively either alone or as a member of a team, and to organise and motivate others.

This suite of courses aims to develop these personal and interpersonal skills through the various group project based units and in the case of the degrees through conventional final year individual projects and through sandwich placement. Industry and commerce clearly make a major contribution to this process during the placement year. From October 1990 financial support from the U.K. Enterprise in Higher Education Initiative will enable them also to make a contribution during the college- based years of the degree courses. Each year students will attend about a dozen seminars given by visiting industrialists. These will both address selected aspects of enterprise in business and serve to introduce particular firms to prospective placement students and prospective graduate employees.

2 Group Project Work

Group project work plays a key role in the following units of these courses.

(i) A workshop unit, (HND Year 1).

(ii) An introductory unit in mathematical modelling and models, (common to Year 2 of the HND and Year 1 of both degrees).

(iii) A more advanced unit in mathematical modelling case studies, (common to Year 2 of both degrees).

(iv) A final year group project unit, (HND Year 2).

The first three of these units share a common organisational feature as regards group project content. The class is initially divided into small groups, (four students per group seems to work best), and each group is assigned a project involving the solution of a practical real-life problem. Different groups are usually, but not necessarily, assigned different projects. The members of each group then have a few hours per week for a few weeks in which to investigate the background to the problem, analyse the problem systematically, find one or more solutions, and then present their results in the form of individually or jointly written reports to the supervisor and (usually) a seminar delivered jointly to the rest of the class. They are assessed on their technique, results and reporting. Marks are awarded typically for method and organisation, content, understanding, oral and written clarity and presentation, and initiative. The reports are expected to exhibit conclusions in a form comprehensible by non-specialists. The class is then reorganised into different groups of four and the process is repeated using a different set of projects. One or more further reorganisations and sets of group projects then follow.

A final written examination is involved only in the case of the introductory unit in mathematical modelling and models.

2.1 HND Workshop Unit

This unit comprises only group project work, albeit very closely supervised. It aims to integrate all components of the HND course, that is, analytical and numerical mathematics, statistics, computing and operational research. Computing plays an important role in every project and practical guidance

is given in the use of mainframe and microcomputers in the solution of real-life problems. However, only later will the students be introduced to the methodology of mathematical modelling,and so here the emphasis is on the systematic analysis of the problem rather than a detailed investigation of its background. Each student participates in several projects but only delivers one (joint) seminar. The audience for this usually includes a visiting industrialist.

2.2 Introductory Unit in Mathematical Modelling and Models

This unit looks at the philosophy and methodology of mathematical modelling and is taught by a single member of staff. It is essentially a unit about applying mathematics. After an introductory lecture on the modelling process each student takes part in several group projects designed to emphasise and give practical experience of this process. The problems posed can be tackled reasonable satisfactorily using the students' existing mathematical knowledge. Each student writes an individual report and jointly delivers a seminar on each project undertaken.

The "models" section of this unit is a study of some standard mathematical models such as Newtonian mechanics and population dynamics. Emphasis is placed on the development and understanding of the models. This section is assessed both by coursework and by a final written examination.

Students are encouraged to read mathematical articles and comprehend them to the extent that they can satisfactorily explain them to others and answer questions about them. To help achieve this objective an article on some aspect of applied mathematics is copied and given to the students in advance of a timed written comprehension test relating to it. An example of such a test is given by Houston [2]. (It is worth noting that in Northern Ireland a comprehension test also forms part of the assessment for a Further Mathematics A-level examination [3].)

2.3 Mathematical Modelling Case Studies

This unit aims further to develop interpersonal skills and expertise in mathematical modelling, and to integrate the various components of the degree courses. It consists almost entirely of group project work. The problems differ from those of the introductory modelling unit in length and difficulty, in

the breadth of skills needed to solve them, in the standard of reporting required, and in the extent to which the groups are expected to work without close supervision. By the end of this unit the students should be confident public speakers and ready within reason to make worthwhile contributions to their sandwich placements no matter what tasks they are given.

The unit commences with a short lecture course in communication skills. This includes, for example, instruction in the preparation of formal written reports and a detailed comparative study of well written and poorly written articles taken from mathematical research journals.

Each student then participates in three group projects in mathematical modelling. The first of these requires only first year mathematical methods, the second is a case study in applied statistics, and the final one is based on operational research and computer simulation. Different groups are always assigned different projects. Each problem is posed by a different member of staff who both plays the role of an industrial client and acts as supervisor and assessor. Most probably the case-study has been designed by him. He simulates problems of communication, (for example by feigning a total ignorance of mathematics), and probably withholds some essential facts initially. It is up to the group to seek further information from him as they think necessary. The group then has one full day per week for four weeks in which to solve the problem and produce a single written report. Throughout this period the supervisor monitors progress and intervenes with guidance if necessary but otherwise the group is left to its own devices. Each case-study involves about the same amount of work as a conventional final year degree project. This places fairly severe pressure on each group as regards time, and forces the four members properly to plan their schedule of work and share out the various tasks. After submitting their written report the group members deliver a joint seminar on the project during which they are subjected both to a viva-voce examination of content and to a critical appraisal of their oral and visual communication skills, the rest of the class being encouraged to contribute to both of these exercises. Finally the group members meet with the supervisor to receive detailed feedback on all aspects of their performance.

Two important questions have arisen in connection with the organisation of this unit.

(i) How does one distribute the students between groups, (and later redistribute them twice), so that all groups have as nearly as possible the same overall academic ability?

(ii) How does one design and implement a monitoring, assessment and marking scheme which is as objective as possible, which properly discriminates between different members of the same group, and which ensures uniformity of marking of case-studies of differing length and difficulty by different assessors?

Both these matters are the subject of ongoing research, the final results of which will be reported in a subsequent article. To date two quite different assessment schemes have been tried. Neither has proved entirely satisfactory and a third will be used in the academic year 1990-91.

2.4 HND Final Year Group Project

Final year HND students are unlikely to have fully developed enterprise skills. So rather than undertaking an individual final year project each student takes part in a group project. This lasts for the entire academic year, but in all other respects is similar to the group projects discussed above. The unit aims to ensure that HND students, particularly those without relevant work experience, are given the opportunity to learn how theory is applied in the solution of realistic large-scale problems.

3 Industrial Placement

Both degree courses are of four years duration. Years 1, 2 and 4 are spent on campus and Year 3 in industrial placement. The aims and advantages of sandwich placement as regards both students and employers are too well known to need reiterating here. Nevertheless, placement is still very much a non-traditional component as far as combined degrees in mathematics, statistics and computing are concerned. This is possibly due to three widely held beliefs.

(i) Employers place no value on the sandwich element when hiring graduates of such degrees.

(ii) Undergraduates of such courses are very hard to place.

(iii) Those placements which are available involve experience only in computing.

Our experience at the University of Ulster seems to dispel these beliefs except for the case of employment in the finance and commerce sector.

Overall, a majority of the firms who responded to our market research survey placed great value on the sandwich component and were keen to consider students of degrees such as these for placement. But in the finance and commerce sector, (about 32% of the firms contacted and 33% those who responded), the opposite was true and a majority never accepted students for sandwich placement.

At the time of writing of this article our first cohort of 23 students are just completing their sandwich year. All were placed with relative ease and all have reported in glowing terms on the value of the experience obtained. Of these 23 placements: 4 (17%) were in finance and commerce, 8 (35%) involved extensive use of mathematics, 10 (43%) involved extensive use of statistics, and 7 (30%) involved extensive use of operational research. All 23 placements naturally involved some computing, but in only 6 cases (26%) was it the principal element.

4 Conclusion

In his paper O'Reilly [1] poses 22 questions. We hope that our experiences at the University of Ulster, described in this paper, will help him find answers.

References

[1] Maurice O'Reilly, Mathematics at Third Level - Questioning How we Teach, Bulletin Irish Math Soc, No 22, (1989), 50-54.

[2] S. K. Houston, Mathematical Comprehension, in M S Arora, F. Mina and A Rogerson, editors, Mathematical Education: The Present State of the Art, to appear (1990).

[3] J. R. McCartney, A Comprehension Paper in A-level Mathematics, Teaching Mathematics and its Applications, 9, No 1 (1990), 6-14.

Department of Mathematics
University of Ulster
Jordanstown

Use of MACSYMA and MAPLE in Mathematics teaching in UCG

Raymond A. Ryan

Introduction

Several years ago the Honours Mathematics program in UCG began to undergo major reform. At the centre of the changes which our courses are still undergoing was the introduction of modern computing techniques, and in particular the use of symbolic computation software. There were a number of reasons for this reform; two in particular stand out — a desire to reverse a trend of falling numbers of good Mathematics students, and a process of reeducation among members of the Mathematics Department themselves.

The number of students taking honours degrees in Mathematics in UCG had been decreasing through the late '70's and early '80's. Departments like Electronic Engineering and Medicine were full of frustrated mathematicians, but it was not just the distorting effects of the points system that robbed us of students. There was — and still is — an image problem associated with Mathematics. This problem has several facets. On the one hand, most school leavers could picture themselves in the role of an Engineer or Accountant or Solicitor, but few could imagine themselves as a Mathematician. Also, the divorce between Mathematics and Computer Science meant that many Mathematics programs were frozen in outdated modes of content and presentation, lacking the vital interplay with computing which would have ensured growth and change.

The second factor was the changing attitudes of the members of the Mathematics Department. Of course, computers had been used, and taught, for the past 25 years or so, but "Pure" Mathematics had remained largely untouched. Then, over the course of a few years, people became acquainted with Pascal, Lisp, electronic mail, TEX, CAYLEY, REDUCE, MACSYMA, and so on. The

computer had really arrived in Mathematics! And as computing techniques began to find a place in our own research, it became clear that all our courses would eventually have to reflect this new fact of mathematical life. One read constantly of the reform of Calculus in the USA, and if one was still sceptical, there was the spectacle of seeing our own students with calculators which could sketch graphs and compute derivatives and invert matrices. Primitive though these devices were, they were clearly a sign of things to come. Questions began to be asked that wouldn't have made sense five years previously, such as: why should I spend several weeks teaching methods of integration when my students are going to get their integrals from a computer or calculus calculator in "real life"? or: if I use CAYLEY to help me understand the structure of this group, shouldn't my students have the same opportunity?

The response to these stimuli took place at various levels. In this account we look mainly at the introduction of symbolic computation in first year courses.

MACSYMA and MAPLE

MACSYMA was introduced in the first year Analysis course in 1987. While REDUCE was also available, the manuals were so cryptic as to be unusable. MACSYMA was somewhat better in this respect, but it was still necessary for us to write our own introductory manual.

Software such as this can be taught at two levels. The first is to view it as a sort of symbolic supercalculator. The second is as a full programming language, in which the user will write their own procedures, define their own environments etc. At the first year level we concentrated mainly on the first level. Our aim was to make it possible for the student to be able to interact with MACSYMA with sufficient ability to be able to carry out the manipulations that they would be likely to meet in their courses. Initially we dealt with Calculus applications only; in our second year we brought MACSYMA into the Algebra course as well, dealing mainly with matrix-related computations.

The effect on the students was remarkable. Mathematics suddenly became something immediate, rather than a sequence of theorems alternating with daunting examples. The ability to cut quickly through tedious, repetetive calculations meant that more time could be spent exploring the ideas behind the calculations. To give one simple example, consider the partial fraction expansion of a rational function. This can be taught in a formal lecture situation, the various tricky cases outlined and so on, but such knowledge is

best absorbed when acquired actively. It was in precisely such a situation that MACSYMA came to the fore. The student could now compute these expansions at will, and could experiment freely with changes in the structure of the function to see how they would affect the expansion. Similarly, it became possible to deal with more interesting problems in Linear Algebra. No longer were we confined to 3×3 matrices! The courses themselves began to change to reflect the new presence of the computer, and the effect of this has been invigorating for all concerned. Our first year Analysis and Algebra are, in their philosophy and content, and in the way they are taught, quite different from what they were in 1986. There are also implications for the way courses are examined. The traditional three-hour written exam is giving way to a combination of written and computer work.

Unfortunately, it was not all plain sailing, as those who have experience of MACSYMA in a multi-user environment will understand. Each user essentially loads a full copy of the program when MACSYMA is invoked, and this places great strains on the computer. Our experience was that once seven or eight students had started to do computations in MACSYMA, the whole system (a VAX 11/785 in this case) was reduced to a snail's pace, leading to great frustration on the part of our own students and other users. The following year, we tried working with smaller groups of students. This still did not eliminate the problem with speed of response, and the additional supervisory burden created its own problems.

MACSYMA is an excellent program, but is not suitable for simultaneous use by groups of students. Alternatives were sought. MATHEMATICA looks very promising, but the cost, under present circumstances, is prohibitive. MAPLE was acquired instead, and installed on the same computer, alongside MACSYMA (and REDUCE). Its outstanding advantage is its adaptability to a multi-user situation. Each user is given only those parts of the program which are required at the time, other modules being loaded as needed. The capabilities at the level at which we use this software seem to be at least as good as those of MACSYMA, and the level of documentation is also good. So, within the next year or two, we foresee a situation in which all our Honours students will learn to use MAPLE in their first year, and will continue to develop their skills in its use in succeeding years, and will come to take it for granted as a normal mathematical skill which is available when needed.

Conclusions

As a result of these and other changes, enrolment in the honours Mathematics programs began to increase sharply in recent years, and the first year numbers are now three times their previous levels. Although there are other factors at work here, the introduction of symbolic computation in first year has certainly contributed to this development. There is a noticeable improvement in the attitude of the students to Mathematics. The computer is clearly acting as a bridge for them into an area that they otherwise would not feel they could reach.

Finally, the Mathematics courses themselves are changing, and the use of software such as MAPLE is driving this change. New types of problems are now accessible which could not be tackled by hand. Some parts of our courses have become obsolete, and must be ruthlessly pruned. New branches of Mathematics are emerging. The long-term effect of this will be interesting to see. One thing is clear: if we are not preceived by our students as leading in this revolution rather than being dragged along, then Mathematics will, by the turn of the century, be a neglected backwater.

NOTES

A public key cryptosystem as hard as factorisation

M. Christopher W. Jones

1 Introduction

The idea of a public-key cryptosystem was first put forward by Diffie & Hellman in their 1976 paper [7]. Since then various descriptions of it have appeared [3,11,14,24,27] including a recent Bulletin article [10]. The idea behind a public-key cryptosystem is that it allows secret messages to be sent across an open channel without it being necessary for some additional piece of information to be previously exchanged between sender and receiver.

Briefly, the idea is this. If Mr. X wishes to receive secret communications he constructs an *encryption function* E and a *decryption function* D. These should possess the following properties: (i) $D(E(m)) = m$ for all messages m, (ii) both E and D should be easily computable, (iii) it should not be possible to determine D from a knowledge of E alone, (iv) $E(D(m)) = m$ for all messages m. (Actually property (iv) is not absolutely essential, but is useful for purposes of authentication - for more details consult the above references.)

Mr. X then publishes the encryption function E (the *public key*) and keeps the decryption function D to himself (the *secret key*). Anyone wishing to send him a message m then transmits the encrypted message $E(m)$. On receiving this, Mr. X is able to recover the original message using D and property (i). However any eavesdropper who intercepts $E(m)$ is unable, because of property (iii), to discover m, even if he knows the encryption function E.

In order to put the above scheme into practice it is necessary to construct suitable encryption/decryption functions. One way this has been attempted is by the use of a "trapdoor" function f: this is a function for which it is easy to compute $f(x)$ but very difficult to compute $f^{-1}(x)$ without some additional

"trapdoor" information. However with the knowledge of the "trapdoor" information $f^{-1}(x)$ should be easy to compute.

Most attempts to construct "trapdoor" functions consist of putting some computationally hard problem between f and f^{-1}. Then to quote from [10], "... solving the hard problem implies breaking the cryptosystem and *it is hoped* that ... the cryptosystem cannot be broken *without* solving the hard problem. In no case has this been proved ..."

It is the purpose of this note to describe a cryptosystem, due to Rabin [16], which has the property that breaking it *is* equivalent to solving a computationally hard problem, specifically that of integer factorisation. In this respect, Rabin's scheme bears certain similarities to the well-known RSA scheme [10,20,27]. However Rabin's scheme possesses the important difference that breaking it is known to be *equivalent* to factorising an integer; whereas in the case of the RSA scheme, all that is known is that no-one has yet been able to devise a method of breaking it which does not involve factorisation.

The problem of factorisation of large integers has received much attention in the last twenty years, ever since the use of computers became commonplace. At present the most efficient algorithms for factorising a number n have average running times of order $\exp(\log n \log\log n)^{1/2}$ (see [8,9,26]). Riesel [18,19] states that the present upper limit for factorisation is 10^{75} and he estimates that with the most sophisticated technology available, factorisation of a hundred digit number would take one year. However, it may be noted that few theoretical results above the difficulty of factorisation are known - it is not, for instance, known whether the factorisation problem is NP-hard (see [12,23,27]).

To conclude, perhaps we should note that the *factorisation* problem should not be confused with the *primality* problem which is to determine whether a given integer is prime or not. This problem is much easier and there are algorithms ([2,5,9,15,17,25]) by means of which a computer can determine the primality of a 200 digit number in ten minutes. Indeed, as we shall see, in order to implement the Rabin cryptosystem it is essential that we can easily generate large (say 100 digit) primes. In passing, readers might be interested to learn that a new largest known prime has recently been discovered. The largest known prime is now $391581 \times 2^{216193} - 1$, and was discovered by a group working in the Amdahl Corporation, Sunnyvale, California [4,6]. (This compares with the previous largest known prime which was $2^{216091} - 1$, a record which has stood since 1985.)

2 Number Theoretic Preliminaries

In this section we give a brief account of the number theory necessary for a description of Rabin's method. For proofs of the results stated, see almost any book on number theory, for instance [13,21,22].

Let n be a positive integer greater than 1 and let y be an integer which is non-zero (mod n). Then if the congruence $x^2 \equiv y \pmod{n}$ is soluble, y is said to be a *quadratic residue* (mod n). Given y and n, it is straightforward to discover whether or not y is a quadratic residue (mod n) by means of the celebrated *law of quadratic reciprocity*. Now suppose $n = p$, an odd prime. Then exactly half of the non-zero integers (mod p) are quadratic residues in which case the congruence $x^2 \equiv y \pmod{p}$ has precisely two incongruent (mod p) solutions which may be written x_0 and $p - x_0$. In the special case when p is of the form $4k + 3$, we have the result that $x_0 \equiv y^{\frac{p+1}{4}} \pmod{p}$. (This follows from *Euler's criterion* which states that y is a quadratic residue (mod p) if and only if $y^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.)

In the case when $n = pq$, a product of two primes, it may be shown that y is a quadratic residue (mod n) if and only if y is a quadratic residue (mod p) *and* y is a quadratic residue (mod q). When this is true, and in the particular case when p and q both have the form $4k + 3$, there is a straightforward procedure for solving $x^2 \equiv y \pmod{n}$ (*provided* the factorisation of n is known).

To find the solutions, first determine integers a and b such that $ap - bq = 1$. (Such integers must exist because the greatest common divisor of p and q is 1 and they can easily be found by the Euclidean algorithm.) Now denote the solutions of $x^2 \equiv y \pmod{p}$ by u and $p - u$ and the solutions of $x^2 \equiv y \pmod{q}$ by v and $q - v$. Then it is a routine calculation to verify that the four solutions of the original congruence are

$$x_1 = bqu + apv, \quad x_2 = bq(p - u) + apv,$$

$$x_3 = bq(p - u) + ap(q - v), \quad x_4 = bqu + ap(q - v).$$

These four solutions are clearly incongruent (mod n) and it is not hard to show that they are the only solutions (mod n) of $x^2 \equiv y \pmod{n}$.

We may now give a description of the Rabin cryptosystem, the security of which depends essentially on the fact that solving $x^2 \equiv y \pmod{n}$ is *equivalent* to factorising n.

3 The Rabin Cryptosystem

A user of the Rabin system who wishes to receive messages first picks two primes p and q both of which are of the form $4k+3$. He also picks a positive integer $a < n = pq$. Then the integers n and a are made public while the primes p and q are kept secret. In order to encrypt a message m, which must be an integer between 0 and $n-1$, a sender calculates

$$E(m) = m(m+a) \pmod{n}.$$

If the resulting encrypted message is e, the receiver, who knows the factorisation of n, can easily decipher it by means of the following procedure:

It is required to find m which satisfies

$$m^2 + am \equiv e \pmod{n}.$$

Multiplying through by 4 this becomes

$$4m^2 + 4am \equiv 4e \pmod{n},$$

which may be written

$$(2m+a)^2 \equiv 4e + a^2 \pmod{n}.$$

Now, since the factorisation of n is known, it is straightforward to solve $x^2 \equiv 4e + a^2 \pmod{n}$ by means of the method outlined in §2. When this has been done m may be determined by solving the linear congruence $2m \equiv x - a \pmod{n}$. Note that there will be, in general, four values of x and hence four possible messages m. This illustrates a weakness of the Rabin scheme in that the deciphering process does not lead back to a unique value of m. However, assuming the original message was written in English, it will normally be obvious which of the different possibilities for m is the correct one.

(It may be noted here that property (iv) of the list given in §1, that $E(D(m)) = m$ for all messsages m, does hold in the Rabin system, whichever value is taken for $D(m)$.)

It is clear from the description given above that breaking the Rabin system cannot be *harder* than factorisation. To show that it is in fact equivalent it will be sufficient to show that if there were an efficient algorithm for solving $x^2 \equiv y \pmod{n}$, where $n = pq$, then it would be possible to factorise n. To

see that this is indeed so, suppose that it were possible to solve $x^2 \equiv y \pmod{n}$. Then by §2 the solutions are:

$$x_1 = bqu + apv, \qquad x_2 = bq(p-u) + apv,$$
$$x_3 = bq(p-u) + ap(q-v), \qquad x_4 = bqu + ap(q-v).$$

(Note that $x_1 \equiv -x_3 \pmod{n}$ and $x_2 \equiv -x_4 \pmod{n}$.) Then $x_1 + x_2 = p(bq + 2av)$ and so p is the greatest common divisor of $x_1 + x_2$ and n. Since g.c.d.'s can be found easily using the Euclidean algorithm, this factorises n.

Rabin's original cryptosystem was rather more sophisticated than the simplified version given here. He relaxed the condition that p and q have the form $4k+3$. This means that another more complicated method, due to Adleman *et al*, for solving quadratic congruences has to be used. For more details see [1,15,16].

4 An example

We illustrate this system with an example. Let $p = 59, q = 47, n = 2773$ and $a = 1371$. Now suppose we wish to send the message

TRINITY COLLEGE

The first step is to convert this into numerical form using the scheme $A = 00, B = 01 \ldots Z = 25$, space $= 26$. The message then becomes, divided into blocks of four,

1917 0813 0819 2426 0214 1111 0406 0426.

To encipher the first block, we calculate

$$E(1917) = 1917(1917 + 1371) \equiv 0067 \pmod{2773}.$$

In this way the whole message enciphers as

0067 0872 2252 2389 0884 1140 0482 0174.

To decipher this, it is required to find m such that

$$m^2 + 1371m \equiv 0067 \pmod{2773}.$$

Completing the square this becomes

$$(2m + 1371)^2 \equiv 2588 \pmod{2773}.$$

The next step is to solve $u^2 \equiv 2588 \pmod{59}$, which simplifies to $u^2 \equiv 51 \pmod{59}$. By a result contained in §2, $u \equiv (51)^{15} \pmod{59}$. This can be calculated more quickly by writing it as $u \equiv ((51^2)^2)^2(51^2)^2 51^2 51 \pmod{59}$ and hence we obtain that $u \equiv 46$ or $13 \pmod{59}$. Similarly the solutions of $v^2 \equiv 2588 \equiv 3 \pmod{47}$ are $v \equiv 35$ or $12 \pmod{47}$.

Now, the Euclidean algorithm yields that 4.59-5.47=1 and so the solutions of
$(2m + 1371)^2 \equiv 2588 \pmod{1773}$ are

$$2m + 1371 \equiv 5.47 \begin{Bmatrix} 46 \\ 13 \end{Bmatrix} + 4.59 \begin{Bmatrix} 35 \\ 12 \end{Bmatrix} \equiv \begin{cases} 341 \\ 1724 \\ 2432 \\ 2550 \end{cases} \pmod{2773}.$$

Hence $2m \equiv 1743, 353, 1061$ or $1179 \pmod{2773}$ and so $m \equiv 2258, 1563, 1917$ or $1976 \pmod{2773}$. The only value of m which corresponds to a pair of letters is 1917 which leads back to TR. The rest of the decryption is accomplished similarly.

References

[1] L. Adleman, K. Manders and G. Miller, *On taking roots in finite fields*, 20th IEEE FOCS **20** (1977), 175-178.

[2] L.M. Aldeman, C. Pomerance and R.S. Rumely, *On distinguishing prime numbers from composite*, Annals of Math. **117** (1983), 173-206.

[3] Gilles Brassard, *Modern Cryptology*, Springer-Verlag Lecture Notes in Computer Science **325**, 1988.

[4] Barry A. Cipra, *Math. team vault over prime record*, Science (25 Aug. 1989), p.815.

[5] H. Cohen and H.W. Lenstra, *Primality testing and Jacobi sums*, Math. Comp. **42** (1984), 297-330.

[6] A. Coyle, *Computer finds largest prime number*, The London Independent (31 Aug. 1989), p.3.

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

[8] J.D. Dixon, *Asymptotically fast factorization of integers*, Math. of Computation **36** (1981), 255-260.

[9] J.D. Dixon, *Factorization and primality tests*, Amer. Math. Monthly (June 1984), 333-352.

[10] Patrick Fitzpatrick, *Asymmetric Cryptography*, IMS Bulletin **20** (1988), 21-31.

[11] M. Gardner, *Mathematical games, a new kind of cipher that would take millions of years to break*, Scientific American (Aug. 1977), 120-4.

[12] M. Garey and D.S. Johnson, *Computers and intractability; a guide to the theory of NP-completeness*, W.H. Freeman & Co., San Francisco, 1979.

[13] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford U.P., 1979.

[14] M.E. Hellman, *The mathematics of public key cryptography*, Scientific American (Aug. 1977), 130-9.

[15] Evangelos Kranakis, *Primality and Cryptography*, Wiley-Teubner, 1987.

[16] M.O. Rabin, *Digitalized signature and public key functions as intractable as factorization*, MIT Lab. for Comp. Sci. Technical Report **LCS/TR-22**, Cambridge, Mass. 1979.

[17] M.O. Rabin, *Probabilistic algorithms for testing primality*, J.Numb. Thy. **12** (1980), 128-138.

[18] Hans Riesel, *Modern factorization methods*, BIT **25** (1985), 205-222.

[19] Hans Riesel, *Prime numbers and computer methods for factorization*, Birkhauser, Boston, 1985.

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

[21] H.E. Rose, *A course in number theory*, Oxford U.P., 1988.

[22] Kenneth H. Rosen, *Elementary Number Theory and its Applications*, Addison-Wesley, 1988.

[23] J. Seberry and J. Pieprzyk, *Cryptography: an introduction to computer security*, Prentice Hall, 1989.

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

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

[26] H.C. Williams, *Factoring on a Computer*, Math. Intelligencer **6** (1984), 29-36.

[27] Dominic Welsh, *Codes and Cryptography*, Oxford U.P., 1988.

Department of Pure Mathematics,
The Queen's University of Belfast.

An Elementary proof that periodicity and generalized-periodicity are equivalent in nilpotent groups

Gary J. Sherman

Let S be a non-empty subset of the group G. An element x of G is said to be S-periodic if there are elements $g_1, \ldots, g_n$ in S for which

$$\prod_{i=1}^{n} g_i^{-1} x g = e.$$

If $S = \{e\}$, then S-periodicity is the usual notion of group periodicity. If $S = G$, then S-periodicity is referred to as generalized-periodicity, a concept which occurs naturally in the theory of partially ordered groups. Indeed, a group admits a partial ordering relation compatible with the group operation if, and only if, the group contains an element which is not generalized-periodic [1]. Another case of special interest is when $S = P(G)$, the set of periodic elements of G. It was shown in [5] that $P(G)$ is a subgroup of G if, and only if, each $P(G)$-periodic element of G is periodic.

If G is abelian, then generalized-periodicity and $P(G)$-periodicity are equivalent to periodicity. Thus, when presented the class of nilpotent groups as a natural generalization of the class of abelian groups one asks: "Is generalized-periodicity equivalent to periodicity in the class of nilpotent groups?" Hollister [3] has shown that the answer to this question is yes. His proof makes use of a deep result from the theory of partially ordered groups and the fact that the periodic elements of a nilpotent group form a subgroup [4]. In this paper we give an elementary proof of Hollister's result and obtain, as a corollary, the fact that $P(G)$ is a subgroup for nilpotent G.

To this end the following two observations are useful. Let x and y be elements of the group G.

Fact 1. If x and y are periodic then xy is generalized-periodic.

Proof. Let x and y be of orders m and n, respectively. Then

$$\prod_{i=0}^{mn-1} x^{-i} x y x^i = x y^{mn} x^{mn-1} = e.$$

Notice that if generalized-periodicity is equivalent to periodicity, then $P(G)$ is closed with respect to taking products and inverses; i.e., $P(G)$ is a subgroup.

Fact 2. If a non-trivial power of x commutes with y, then the commutator $[x,y] = x^{-1}y^{-1}xy$ is a generalized-periodic element of the subgroup generated by x and $[x,y]$.

Proof. Let $x^n y = yx^n$ for some positive integer n. Then

$$\begin{aligned}\prod_{i=1}^{n} x^{-n+i}[x,y]x^{n-i} &= x^{-n}(y^{-1}xy)^n \\ &= x^{-n}y^{-1}x^n y \\ &= e.\end{aligned}$$

Notice that $[x,y]$ is conjugated by powers of x.

Theorem. *Generalized-periodicity is equivalent to periodicity in a nilpotent group.*

Proof. Recall that a group, G, is nilpotent of class n if it possesses a series of normal subgroups, $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$, in which G_i/G_{i+1} is the center of G/G_{i+1}. Such a series is referred to as the upper central series of G. We proceed by induction on the class of the nilpotent group G.

If G is of class one, then G is abelian and the result is obvious.

Now suppose that G is nilpotent of class n and that generalized-periodicity is equivalent to periodicity in nilpotent groups of class less than n. Let x be a generalized-periodic element of $G - G_{n-1}$ (Each generalized-periodic element of G_{n-1} is periodic since G_{n-1} is the center of G.). For some positive integer k there are $y_1, \ldots, y_k$ in G for which

$$\prod_{i=1}^{k} y_i^{-1}xy_i = e. \tag{i}$$

Applying the identity $y_i^{-1}xy_i = x[x,y_i]$ to (i) we obtain

$$\prod_{i=1}^{k} x[x,y_i] = e. \tag{ii}$$

It also follows from (i) that

$$\prod_{i=1}^{k}(y_i^{-1}G_{n-1})(xG_{n-1})(y_iG_{n-1}) = G_{n-1}$$

in the factor group G/G_{n-1}. Since G/G_{n-1} is a nilpotent group of class less than n the induction hypothesis implies that xG_{n-1} is periodic in G/G_{n-1}. Thus there exists a positive integer m for which $x^m \in G_{n-1}$, the center of G. Fact 2 implies that each of $[x,y_1], \ldots, [x,y_k]$ is generalized-periodic so for $i = 1, \ldots, k$ there is a positive integer s_i and there are $z_{i_1}, \ldots, z_{i_{s_i}}$ in G such that

$$\prod_{j=1}^{s_i} z_{i_j}[x,y_i]z_{i_j} = e; \tag{iii}$$

$$\text{i.e.,} \quad \prod_{j=1}^{s_i}[x,y_i][[x,y_i],z_{i_j}] = e. \tag{iv}$$

Reasoning with (iii) as with (i), we find $[[x,y_i],z_{i_j}]$ to be generalized-periodic in the subgroup generated by $[x,y_i]$ and $[[x,y_i],z_{i_j}]$. But $[x,y_i] \in G_1$ and $[[x,y_i],z_{i_j}] \in G_2$ so $[[x,y_i],z_{i_j}]$ is generalized-periodic as an element of G_1. By the induction hypothesis and Fact 1, $[[x,y_i],z_{i_j}] \in P(G_2) = P(G) \cap G_2$ which is a normal subgroup of G . From (iv) we have $[x,y_i]^{s_i}P(G_2) = P(G_2)$ in the factor group $G_1/P(G_2)$. Thus, since $[x,y_i]^{s_i}$ is periodic, $[x,y_i]$ must be periodic; i.e., $[x,y_i] \in P(G_1) = P(G) \cap G_1$, which i s a normal subgroup of G. From (ii) it follows that $x^kP(G_1) = P(G_1)$ in the factor group $G/P(G_1)$. We conclude that x is periodic since x^k is periodic.

Corollary. The periodic elements of a nilpotent group form a subgroup.

References

[1] Fuchs, L., *Partially Ordered Algebraic Systems*, Pergamon Press, London, 1963.

[2] Hall, M., *The Theory of Groups*, The Macmillan Company, New York, 1959.

[3] Hollister, H.A., On a condition of Onishi, Proc. Amer. Math. Soc., 19 (1968), 1337-1340.

[4] Kurosh, A.G., *The Theory of Groups*, Second English Edition, Chelsea Publishing Company, New York, 1960.

[5] Sherman G.J., When do the periodic elements of a group form a subgroup?, Math. Mag., 47 (1974), 279-281.

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute
Indiana 47803
USA

Note on the Diophantine Equation

$$x^x y^y = z^z$$

James J. Ward.

In a letter to the Editor of the Irish Times, Dr. Des McHale issued the challenge of finding any solution (x, y, z), with none of x, y, $z = 1$, of the Diophantine equation

$$x^x y^y = z^z.$$

This had appeared as a problem in the first Irish Universities Mathematical Olympiad and apparently none of the contestants found a non–trivial solution. The purpose of this note is to indicate a method for generating solutions to this equation.

Lemma: Suppose X, Y, Z, φ are natural numbers such that

(i) $X + Y - Z = 1$ and

(ii) $\varphi \geq 2$ and

(iii) $\varphi = Z^Z/(X^X Y^Y)$;

then $x = \varphi X, y = \varphi Y, = \varphi Z$ have the property that

$$x^x y^y = z^z.$$

Proof: Consider $x^x y^y$: this equals

$$(\varphi X)^{\varphi X}(\varphi Y)^{\varphi Y} = \varphi^{\varphi(X+Y)}(X^X Y^Y)^\varphi.$$

On the other hand z^z equals

$$\varphi^{\varphi Z}(Z^Z)^\varphi$$

So $x^x y^y = z^z$ if and only if

$$\begin{aligned} & \varphi^{\varphi(X+Y)}(X^X Y^Y)^\varphi = \varphi^{\varphi Z}(Z^Z)^\varphi \\ \Leftrightarrow \quad & \varphi^{\varphi(X+Y-Z)}(X^X Y^Y)^\varphi = (Z^Z)^\varphi \\ \Leftrightarrow \quad & \varphi^\varphi (X^X Y^Y)^\varphi = (Z^Z)^\varphi \quad \text{since} \quad X+Y-Z=1 \\ \Leftrightarrow \quad & \varphi X^X Y^Y = Z^Z \quad \text{which follows from (iii).} \end{aligned}$$

Now suppose $X = 2^{2\alpha}$ and $Y = p^{2\beta}$ where p is odd and $\alpha, \beta \geq 1$. Consider $(2^\alpha - p^\beta)^2$. This is

$$2^{2\alpha} + p^{2\beta} - 2^{\alpha+1}p^\beta = X + Y - Z$$

say for $Z = 2^{\alpha+1}p^\beta$. In this case one has $X + Y - Z = 1$ if and only if

$$(2^\alpha - p^\beta) = \pm 1. \qquad (*)$$

Subject to this we want to ensure that $Z^Z/X^X Y^Y$ is an integer ≥ 2. Now $\varphi := Z^Z/X^X Y^Y$ in this case can be written as

$$\varphi = \frac{2^{(\alpha+1)[2^{\alpha+1}p^\beta]} \cdot p^{\beta(2^{\alpha+1}p^\beta)}}{2^{\alpha 2^{2\alpha+1}} \cdot p^{2\beta p^{2\beta}}}.$$

The power of 2 in φ equals

$$(\alpha+1)[2^{\alpha+1} \cdot p^\beta] - \alpha 2^{2\alpha+1} \qquad (1)$$

The power of p in φ equals

$$\beta 2^{\alpha+1}p^\beta - 2\beta p^{2\beta} \qquad (2)$$

Equation (2) is $\geq 0 \Leftrightarrow 2^\alpha - p^\beta \geq 0$ (on dividing (2) by $2\beta p^\beta$). Therefore in (*) we shall require $2^\alpha - p^\beta = +1$. Inserting this condition into (1) we get

$$(\alpha+1)[2^{\alpha+1}(2^\alpha - 1)] - \alpha 2^{2\alpha+1} \qquad (3)$$

Dividing by $2^{\alpha+1}$, for (1) to be non–negative we require

$$(\alpha+1)[2^\alpha - 1] - \alpha 2^\alpha \geq 0$$

$$\Leftrightarrow 2^\alpha - 1 \geq \alpha.$$

However this holds for all $\alpha \geq 1$. Using $2^\alpha - p^\beta = 1$, (2) becomes $2\beta p^\beta$ and (3) simplifies to $2^{\alpha+1}(p^\beta - \alpha)$. From this, it is apparent that $\varphi \geq 2$.

Since $2^1 - p = 1$ implies $\varphi = 1$ we shall now assume $\alpha \geq 2, \beta \geq 1$.

Examples:

(i) Choose $\alpha = 2$, then $2^2 - p^\beta = 1$ gives $p = 3, \beta = 1$.

Then $X = 2^{2\alpha} = 16, Y = 3^{2\beta} = 9$ and $Z = 2^{\alpha+1}p^\beta = 8.3 = 24$. Note that $X + Y - Z = 1$.

Letting $\varphi = Z^Z/X^X Y^Y$, the power of 2 in φ equals $2^{\alpha+1}(p^\beta - 2)$ which in this example is 8. The power of p in φ equals $2\beta p^\beta$ which equals $2.1.3 = 6$, so

$$\varphi = 2^8 3^6.$$

Hence

$$x = 2^{12} \cdot 3^6, y = 2^8 \cdot 3^8 \quad \text{and} \quad z = 2^{11} \cdot 3^7$$

is a solution of the Diophantine equation

$$x^x y^y = z^z.$$

(ii) Choose any power of 2, say 2^k where $k \geq 2$. Then $p = 2^k - 1$ is always odd and clearly $2^k - p = 1$. So we can take

$$X = 2^{2k}, Y = p^2 \quad \text{and} \quad Z = 2^{k+1}p$$

and compute φ as before. For instance if we take 2^4 then $p = 15$ and we get

$$\begin{array}{llll} X = 2^8, & Y = 225 & \text{and} & Z = 480 \\ \varphi = & 2^{352}(15)^{30} & & \text{etc.} \end{array}$$

Department of Mathematics
University College
Galway

THE SUBGROUP STRUCTURE OF THE FINITE CLASSICAL GROUPS

London Mathematical Society Lecture Note Series 129

By PETER KLEIDMAN and MARTIN LIEBECK: Cambridge University Press, 1990, pp.313. £17.50 stg. LMS members' price £13.10, ISBN 0521 35949 X.

The classification of finite simple groups revealed that non–abelian finite simple groups fall into three distinct families:

(1) the alternating groups A_n, with $n \geq 5$;

(2) the simple groups of Lie type;

(3) 26 sporadic simple groups.

The alternating groups are well known to anyone who has studied group theory at the most elementary level but the sporadic groups are less accessible to non–specialists. Chevalley showed in 1955 how certain simple groups (including finite simple groups) can be constructed as automorphism groups of Lie algebras over arbitrary fields. Chevalley's construction was modified by Steinberg, Ree, Hertzig and others to provide further simple groups (so–called twisted groups). The groups obtained by these procedures are called simple groups of Lie type. While certain of the finite simple groups of Lie type were unknown until these constructions were introduced in the 1950's and early 1960's others turned out to be versions of groups that had been well known since the work of C. Jordan in 1870 and L. E. Dickson in 1901. These are the finite classical simple groups, which are derived from certain groups of automorphisms of vector spaces over finite fields. The groups of automorphisms in question fall into four families: special linear, symplectic, unitary, orthogonal. It may be argued that these four families of linear groups provide the best introduction to the study of finite simple groups and to finite groups in general. Certainly, the techniques of linear algebra, field theory and permutation groups learnt in most undergraduate courses find wide application in the analysis of the classical groups.

The term finite classical group encompasses various groups derived from certain progenitors that we shall now try to describe. Let V be a vector space of dimension $n \geq 2$ over the finite field $\mathbf{F}_q$ of order q, where q is a power of a prime. The group of all automorphisms of V is called the *general linear group* of degree n over $\mathbf{F}_q$ and is denoted by $GL(n,q)$. The normal subgroup of $GL(n,q)$ consisting of all automorphisms of determinant 1 is called the *special linear group* of degree n over $\mathbf{F}_q$ and is denoted by $SL(n,q)$. The centre Z of

$SL(n,q)$ consists of all scalar matrices of determinant 1 and the factor group $SL(n,q)/Z$ is a non–abelian simple group unless $n = 2$ and $q = 2$ or 3. This group is called the *projective special linear group* of degree n over $\mathbf{F}_q$ and is denoted by $PSL(n,q)$. Suppose now that f is a non–degenerate alternating form defined on $V \times V$. In this case, n must be even, say $n = 2m$. An *isometry* of f is an automorphism σ of V that satisfies

$$f(\sigma u, \sigma v) = f(u,v)$$

for all u and v in V. The set of all isometries of f forms a group called the *symplectic group* of degree $2m$ over $\mathbf{F}_q$ and it is denoted by $Sp(2m,q)$. Since all non–degenerate alternating forms defined on $V \times V$ are equivalent, different choices of f lead to conjugate groups of isometries. The centre of $Sp(2m,q)$ has order 2 if q is odd and order 1 if q is even and the group obtained by factoring out the centre is called the *projective symplectic group* of degree $2m$ over $\mathbf{F}_q$. It is denoted by $PSp(2m,q)$ and it is a non–abelian simple group unless $n = 2$ and $q = 2$ or 2 or $n = 4$ and $q = 2$. As $Sp(2,q) = SL(2,q)$, the exceptions to simplicity when $n = 2$ are explained by the results for $PSL(2,q)$. $Sp(4,2)$ is isomorphic to the symmetric group S_6, which contains the simple group A_6 as a subgroup of index 2. Suppose we now replace $\mathbf{F}_q$ by $\mathbf{F}_{q^2}$ and let f be a non–degenerate hermitian form defined on $V \times V$. We may define isometries of f as in the alternating case and the group of all isometries of f is called the *unitary group* of degree n over $\mathbf{F}_{q^2}$. It is denoted by $U(n,q)$ or $U(n,q^2)$ (the differences are occasionally confusing). We define the special unitary group $SU(n,q)$ to be those isometries of determinant 1 and the *projective special unitary group* $PSU(n,q)$ is obtained from $SU(n,q)$ by factoring out its centre. As $SU(2,q)$ is isomorphic to $SL(2,q)$, we have the usual exceptions to simplicity for $PSU(2,q)$. If $n \geq 3$, $PSU(n,q)$ is a non–abelian simple group unless $n = 3$ and $q = 2$.

Finally we turn to the orthogonal groups. Let Q be a non–degenerate quadratic form defined on V. An isometry of Q is an automorphism σ of V that satisfies $Q(\sigma v) = Q(v)$ for all v in V. If $n = 2m$, there are two inequivalent classes of quadratic forms defined on V and their corresponding isometry groups are denoted by $O^+(2m,q)$ and $O^-(2m,q)$. The groups have different orders. $O^+(2m,q)$ is called the *split orthogonal group* of degree $2m$ over $\mathbf{F}_q$ and $O^-(2m,q)$ is called the *non–split orthogonal group* of degree $2m$ over $\mathbf{F}_q$. Suppose now that $n = 2m+1$ is odd. If q is a power of 2, there is a single equivalence class of non–degenerate quadratic forms defined on V and

the corresponding isometry groups turn out to be isomorphic to $Sp(2m, q)$. If q is odd, there are two equivalence classes of non–degenerate quadratic forms defined on V, but their corresponding isometry groups are isomorphic and are denoted by $O(2m+1, q)$. Suppose now that n is arbitrary but q is odd. It can be shown that the commutator subgroup $\Omega^{\pm}(2m, q)$ or $\Omega(2m+1, q)$ of a finite orthogonal group has index 4 in the group and the centre of the Ω subgroup has order 1 or 2 if $\dim V \geq 3$. On factoring out the centre, we obtain projective groups $P\Omega^{\pm}(2m, q)$ and $P\Omega(2m+1, q)$. If $\dim V \geq 5$, the groups so obtained are non–abelian simple groups. Suppose next that $n = 2m$ is even and q is a power of 2. It can be shown that $O^{\pm}(2m, q)$ has a subgroup $SO^{\pm}(2m, q)$ of index 2. If $2m \geq 6$, $SO^{\pm}(2m, q)$ is a non–abelian simple group. It might be added that if q is a power of 2, both orthogonal groups $O^{\pm}(2m, q)$ are $Sp(2m, q)$ and there is a rich interplay between orthogonal and symplectic geometry in this case. Unfortunately, this material is often omitted from standard texts, such as 'Geometric Algebra' by Artin, although it is not intrinsically harder than the odd characteristic theory. The book 'Linear Groups' by L. E. Dickson (1901) develops most of this theory and indeed a significant number of results concerning classical groups are due to Dickson. The proofs in Dickson's book are rather computational for modern tastes, and some of his nomenclature has become obsolete, but the book still remains a remarkable source of information on the finite classical groups.

After this rather long introduction, we turn now to the book under review. The aim of the book is to determine the maximal subgroups of the finite classical simple groups. This is clearly an extremely difficult problem, especially when one observes that every finite group must occur eventually as a subgroup of some finite classical group. Indeed, it does not seem likely that the problem is even approachable without invoking the classification of finite simple groups. In an analogous piece of work, E. B. Dynkin (1952) classified the maximal subgroups of the classical complex linear groups $SL(n, \mathbf{C})$, $Sp(2m, \mathbf{C})$ and $O(n, \mathbf{C})$. Dynkin's work made essential use of the classification of simple Lie groups over $\mathbf{C}$ and of the theory of their irreducible finite dimensional complex representations. While some analogies with Dynkin's technique may be drawn for the finite classical groups, the finite problem seems to be considerably harder. Dickson's book made a first inroad into the classification of maximal subgroups of finite classical groups by including a chapter listing all subgroups of $PSL(2, q)$. H. H. Mitchell (1911, 1914) and R. W. Hartley (1926) extended these investigations to certain three and four dimensional classical groups.

The authors' starting point is a paper of Aschbacher (On the maximal subgroups of the finite classical groups, Invent. Math. 76 (1984), 469–514). In this paper, Aschbacher introduces a natural collection of geometrically defined subgroups $\mathcal{C}(G)$ of a finite simple classical group G. These fall into eight families, $\mathcal{C}_1 - \mathcal{C}_8$, which include maximal parabolic subgroups (well known from permutation actions), certain classical groups of smaller degree over extension fields of $\mathbf{F}_q$, tensor products of classical groups acted on by symmetric groups (related to wreath products) and extensions of symplectic–type r–groups (r being a prime) by symplectic groups. Aschbacher also introduces a family $\mathcal{S}$ of almost simple groups that have an irreducible projective representaion on the underlying vector space V. His main result is that if H is a subgroup of G, then either H is contained in $\mathcal{C}(G)$ or in $\mathcal{S}$. Moreover, the great majority of subgroups lie in $\mathcal{C}(G)$. The authors undertake an intricate analysis of the collection $\mathcal{C}(G)$ and their main theorem is as follows:

(A) the group–theoretic structure of each member of $\mathcal{C}(G)$ is known;
(B) the conjugacy amongst members of $\mathcal{C}(G)$ is known;
(C) for $H \in \mathcal{C}(G)$, all overgroups of H in $\mathcal{C}(G) \cup \mathcal{S}$are known.

In fact, a more general result is proved, as G is allowed to be a group satisfying $G_0 \lhd G \leq \mathrm{Aut}(G_0)$, where G_0 is a classical group and $\mathcal{C}(G)$ is a collection of subgroups of G obtained from $\mathcal{C}(G_0)$. The precise details of the main theorem are difficult to summarize and Chapter 3 is devoted to explanation. Various tables are required to present the information. Because of the complexity of the solution to the problem, it requires a certain amount of effort to interpret these tables and some instructive examples are provided. Determination of the maximal subgroups of the classical groups still requires the knowledge of when a subgroup in $\mathcal{S}$ is maximal in G. This is an area where much work is in progress. However, it does not seem at present that a non–specialist can expect a quick answer to such questions as whether the Conway group is a maximal subgroup of $SO^{\pm}(24, 2)$.

The second chapter of the book provides an introduction to the classical groups and their properties. This material might prove useful to someone wishing to have a rapid survey of these groups. Chapter 5 is a particularly welcome summary of less familiar properties of finite simple groups. There are tables giving information on the minimal degree of a non–trivial permutation representation of a finite classical group, the containment of alternating and classical groups in sporadic simple groups and lower bounds for the degree of a non–trivial irreducible projective representation of a group of Lie type over a field of characteristic coprime to the underlying characteristic of the group.

There is also substantial information about representations in the defining characteristic, with special emphasis on spin modules for orthogonal groups. Chapters 6, 7 and 8 are concerned with finding the maximal overgroups of the subgroups in $\mathcal{C}(G)$. These chapters are densely written and are probably of interest mainly to specialists.

I feel that this book would be a valuable asset for anyone interested in finite groups, geometry over finite fields or linear algebra. The book contains a substantial body of new results, and constitutes a major research achievement for the authors. It also fulfils a valuable encyclopedic role, which may be its main function for the majority of readers. Considering the quantity of writing, I did not detect an excessive number of typos. I noticed a confusion over a reference to a paper of McLaughlin, two papers being mixed up. I can thoroughly recommend this book to anyone who needs to know about finite classical groups, and its price makes it accessible to virtually everyone.

Roderick Gow
Mathematics Department
University College
Belfield
Dublin 4

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 on an IBM or Macintosh diskette, or by electronic mail to the following Internet address:

MATRYAN@CS8700.UCG.IE

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

Authors who prepare their articles with word processors other than TEX can expedite the typesetting of their articles by submitting the input file in the same way, along with the printed copies of the article. The file should be sent as an ASCII file.

Typed Manuscripts

Typed manuscripts should be double-spaced, with wide margins, on numbered pages. Commencement of paragraphs should be clearly indicated. Hand-written symbols should be clear and unambiguous. Ilustrations 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.