

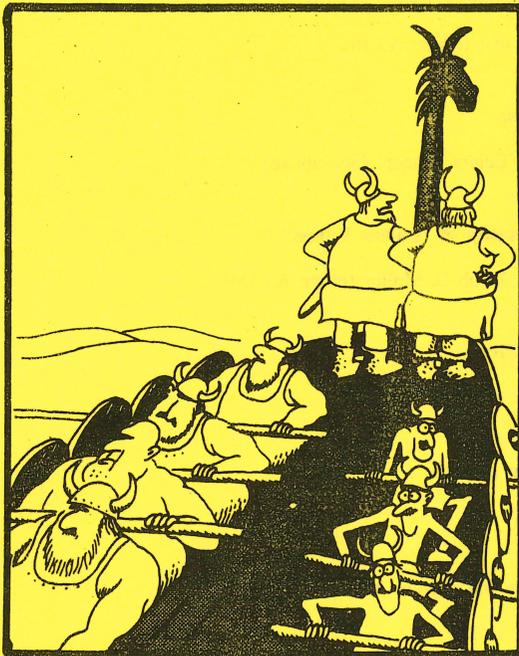


# Q.E.D.



**Special Edition.**

9. september 1992



"I've got it, too, Omar . . . a strange feeling like  
we've just been going in circles."



# EULERS VENNER

Foreningen af Matematikere - Aarhus Universitet

Matematisk Institut - Aarhus Universitet

8000 Aarhus C Giro: 5 87 58 97

**Editors:**

Gorm Salomonsen (office B4.29)

Bernd Rühlicke (office A3.16)

Henrik Just (office A3.16)

**Address:**

As for 'Eulers venner' (See above)

**Membership of 'Eulers Venner'**

Contact Jacob S. Møller (office A3.16)

**Printed by**

Institute of mathematics

**Number printed**

200

**Deadline for edition 9:**

October 1, 1992

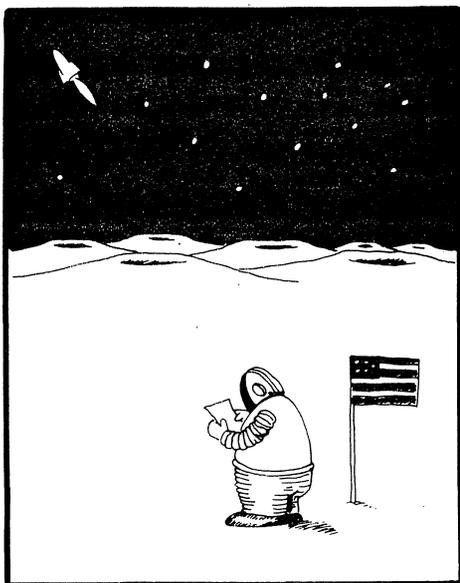
## About this edition of QED.

(by Gorm Salomonsen)

This edition of QED is, as one can see on the front page, a special edition. The occasion is the visit of a group of Russian students. In order to make it readable for them, we have decided to write everything in English. The ordinary editions, which is to come in this semester, will continue to be in Danish.

I will use this place to ask all members of Eulers Venner to consider whether they want to take more active part in its work. At the present time we need one or two more of the editorial board of QED, the Friday Bar could use one or two people, and it seems that there will be rather few candidates to the election for the executive committee of the society in February. The reason for this is that some of the most active members of the society has finished their studies or have gone abroad to finish their studies there. If you are interested in one or more of these things, please contact me at office B.4.29.

Q.E.D.



"Dear Henry: Where were you? We waited and waited but finally decided that . . ."



"Wouldn't you know!!! . . . There goes our market for those things!"

## WELCOME! VELKOMMEN!

Finally after almost eleven months of planing we are able to welcome our Russian friends here in Århus, and half of the exchange program of Eulers Venner<sup>1</sup> and ILIP<sup>2</sup> has become reality. Eulers Venner has some experience regarding planing and conducting studie-tours — as you may be able to read somewhere else in this little lampoon Eulers Venner was born in connection with a studie-tour — but this is the most extensive project in Eulers Venner's short life. We have never before been involved in an exchange but we believe to have found a good co-operation with ILIP.

Many an application has been written and sent to finance the program and luckily not all has been in vain: The Danish Foreign Ministry's Foundation for Democracy will pay almost all expences regarding the Russian students' travel to and activities in Denmark, and the Tuborg Foundation, the Svend Bundgaard Foundation, The family Hede-Nielsens Foundation and the Mathematical Institute of the University of Aarhus have supported the Danish students' trip to St. Petersburg. We are of course all very pleased and thankful that so many have been willing to contribute and make all this possible.

The role of Eulers Venner at the Institute of Mathematics here in Århus is to function as catalyst for social activities and thereby help to provide a good atmosphere at the institute, but a no lesser role is to arrange professional events of a different kind than "those of the classroom". This can for instance be seminars by mathematicians from the industry, the gymnasium (high-school) or elsewhere, or it can be talks given by local people on subjects out of the usual educational context and many other things. Studie-tours are obviously an effective way of widening the social and professional horizon.

The reason for choosing St. Petersburg as our next goal was probably a general interest for this *new* world combined with the coincident that Thomas K. Christensen got in contact with ILIP during a trip to St. Petersburg last autum. And after all St. Petersburg *is* a cultural diamond and it *is* and *has been* the home of many great mathematicians — Leonhard Euler to name one that is closely associated with our society. To conduct an exchange with St. Petersburg was preferred because we believe that both parties would gain the most in this manner. And it

---

<sup>1</sup>You may have been wondering what *Eulers Venner* actually means: It means *Friends of Euler* (and I don't expect *he* needs any presentation).

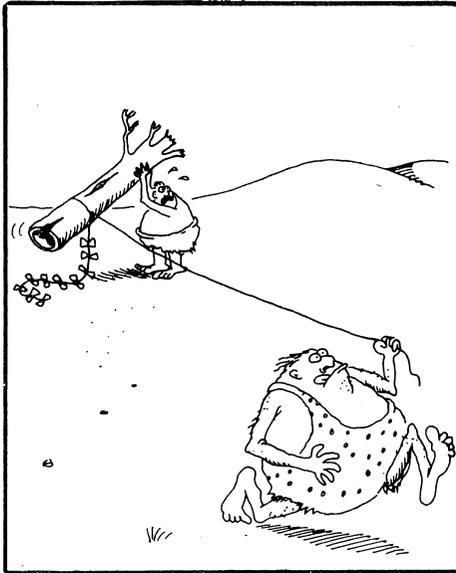
<sup>2</sup>There may be some Danes who do not know of *ILIP*: Well, *ILIP* is short for *Joint Stock Enterprise ILIP* and it is an organisation probably very much like our *International Secretariat*.

would give us in Eulers Venner an opportunity in a modest way to reach out a hand to at least a few fellow students in a troubled country.

We have all — teachers as well as students — been looking very much forward to the visit of the 28 from St. Petersburg. And we sincerely hope that we are able to provide you/them with a very instructive experience and a good and comfortable staying in Denmark. And those of us who are so lucky that we are going there, are looking very much forward to see you/them in St. Petersburg in October.

On behalf of the executive committee of Eulers Venner

Jakob Grove, president.



"Okay, Bob! Go! Go!"

The program for the Russian students in mathematics' visit in Aarhus, autumn 1992 in connection with the exchangeprogram of ILIP and Eulers Venner:

**Sunday September 13:**

16.00: Arrival in Aarhus, where the Russian participants will be informed about practical issues regarding their stay in Aarhus and meet the Danish students they will be staying with during the week. (Staff Lounge)

**Monday September 14:**

9.15–10.00: Welcome by the head of the mathematical Institute of Aarhus, Hans Anton Salomonsen, followed by a little sightseeing around the institute and parts of the university. (AUD G1)

10.00–10.30: Light Lunch. (Mat. Kant.)

11.00–14.30: Visit at the City Hall where there will be given a talk on the structure of the Danish democracy, and the history of Aarhus.

14.30–?: A walk through the city and a visit at the Cathedral.

20.00– : Visit at the wine club of the International Student Center (ISC, Niels Juuls gade 84).

**Tuesday September 15:**

8.45: We meet in front of the Information Office.

9.00–10.30: Guided tour in the Science Park and a lecture by managing director, Erik Jantsen, regarding the relationship between university research and industry and the role of the Science Park. — The Science Park, is an institution, whose role is to make scientific know-how from the University accessible to the industry.

10.30–12.00: Visit at “Cryptomatics” which is a little company situated in the Science Park. It is driven by three mathematicians from the University of Aarhus, and is leading in data security. There will be given lectures on cryptology, and university scientists' role in businesslife.

12.00–13.00: Lunch. (Mat. Kant.)

13.15–15.00: Faculty Council: Dean Karl Pedersen, teachers and students from the Faculty Council will give talks on the democratic system of the Danish Universities, and the potentials of “free faculties”. (AUD G1)

15.15- : Visit at the Art Museum of Aarhus where there is an exhibition in connection with the project Welcome Europe which covers the twelve EEC countries.

### **Wednesday September 16:**

This day will be spent at "JTAS"; look for separate program elsewhere.

19.00- : Visit at Aarhus theatre where we will see the musical "Aspects of Love" by Andrew Lloyd Webber. (Those that don't participate in the visit at JTAS must meet at the theatre at 18.30 at the latest)

### **Thursday September 17:**

9.15-11.00: Lectures by Jørgen Tornehave: Knots (AUD G1).

11.15-13.00: Lectures by Jørgen Hoffman Jørgensen: Games theory and optimal strategies (AUD G1).

13.00-14.00: Lunch. (Mat. Kant.)

14.00- : Visit at "Moesgaard Museum". They have a standard exhibition on Danish history and culture and a special exhibition called "Asian accords" which is about the travels of Verner Jakobsen in East Asia from 1938 to 1963. (We will as usual meet in front of the Information Office)

### **Friday September 18:**

8.15-10.00: Lectures by Johan Dupont: Scissors congruences and homology (AUD G1).

10.15-12.00: Lectures by Johan P. Hansen: Algebraic geometry (AUD G1).

12.15-13.15: Seminar by Konstantin M. Dyakonov: Division by Inner Factors and Embedding Theorems for Star-Invariant Subspaces of Hardy Spaces. (Seminar on high level for all interested. Not an obligatory part of the exchange tour) (AUD G1).

13.00-14.00: Lunch. (Mat. Kant.)

14.15-16.00: Student movements in Denmark. Talks, arranged by two political student organisations, regarding history, structure and purpose of the organisations (AUD G1).

16.15- : Evaluation of the week in Aarhus. (To be announced)

18.00- : Party time. (To be announced)

**Saturday September 19:**

9.15–12.00: Shopping tour and sightseeing in the center of Aarhus.

12.00–13.00: Lunch. (That's your own problem)

13.30– : Visit at "The Old City"— an openair museum of historical Denmark. (We meet at the main entrance)

**Sunday September 20:**

12.00–14.00: Lunch. (To be announced)

14.00: Departure. (From parkinglot nr. 530 at the main entrance of the institute)

## Page 9 Theorem.

We have decided to reserve page 9 of the next (countable) infinitely many numbers of Q.E.D. for theorems of especially sweet and/or sexy character. Here is the first one, which I spotted a few days ago in a course in operator algebras.

**Theorem:** Let  $I$  be a closed ideal in a  $C^*$ -algebra  $A$ , then  $I$  is selfadjoint and therefore a  $C^*$ -subalgebra of  $A$ . If  $\{u_\lambda\}_{\lambda \in \Lambda}$  is an approximate unit for  $I$ , then for each  $a \in A$ :

$$\|a + I\| = \lim_{\lambda} \|a - u_\lambda a\| = \lim_{\lambda} \|a - a u_\lambda\|$$

The reason why I have chosen this theorem is that it gives a nice parallel to the case where  $A$  is a Hilbert space and  $I$  is a closed subspace. In this case the identity on  $I$  can be considered as the projection in  $A$  on  $I$  through the natural inclusion of  $B(I)$  into  $B(A)$ .

Gorm Salomonsen

References: Gerald J. Murphy: "C\*-algebras and operator theory" page 79. Academic press INC.



# Program for the visit at JTAS

## September 16.

- 8.15 Departure from the Mathematical Institute
- 9.00–9.15 Welcome
- 9.15–10.00 Implementation of cryptoalgorithms by Holger Orup
- 10.15–11.00 Neural networks by Per Rosenbek
- 11.00–11.45 The job of a mathematician at JTAS by Henrik Karstoft
- 12.00–12.45 Possible use of mathematics in network planning by Jens Rasmussen
- 13.00–14.00 Lunch
- 14.00–14.30 Introduction to JTE A/S and Personaledvikling
- 14.30–17.00 Exercise in management training
- 17.00 Dinner

### Implementation of cryptoalgorithms

Holger Orup  
Udviklingsafdelingen  
Jydsk Telefon

In recent years there has been a growing interest in introducing cryptography in communication systems. Hereby you can obtain secrecy of transmitted data and you can apply data with a "digital signature". Up till now the best proposal for a cryptosystem is RSA (Rivest, Shamir & Adleman), though this is very slow.

For the cryptograing not to become a bottleneck in the communication system the expression  $M^E \bmod N$ , where the operands has a length of 500 bit!, must be computed sufficiently fast. We therefore developed efficient algorithms which are suitable for implementation in hardware. Some of the technics are the use of redundant number representations which make it possible to add arbitrary large numbers in constant time. Furthermore we are constructing a VLSI processor which can encrypt an ISDN communication channel with the speed of 64 Kbit/sec. This is twice as fast as the previously fastest implementation.

## Some notes about Eulers Venner

Eulers Venner (The friends of Euler) is an association for mathematician at University of Aarhus.

The association was established in 1988. During that year 4 students of mathematics decided to plan a study tour for the mathematicians at the University. 20 students and 1 professor participated at the tour. They went to West Germany and Austria to visit several universities and companies. The goal of the tour was to get a taste of how mathematics is applied in industry. The tour was a success as regards the purpose of the tour as well as the social benefit. But the experience showed it would have been easier to plan such a tour if there has been an association behind. As a consequence "The friends of Euler" was founded in December 1988.

The object of the association is to make arrangements which disseminate the knowledge of topics which have connection with mathematics, especially among the students of mathematics at the University of Aarhus. This has been done by arranging study tours and lectures.

The association has since 1988 organised study tours to Copenhagen (1989), England (1990), Roskilde-Copenhagen-Lund (1991) and this year the exchange programme with Sct. Petersburg. A list of the arranged lectures would be too long to be included here.

Other more social activities have been added. Twice a year a party is made to celebrate the mathematicians who have finished their study and a bar every Friday afternoon has been organised.

Today most of the students of mathematics and a lot of the staff of the Mathematical Institute are members. The Mathematical Institute supports the activities of the association. For example the Institute gives economical support to the study tours and last year it extended the "Staff Lounge" (the "coffee-room of the Institute), which have stimulated the social life at the Institute.

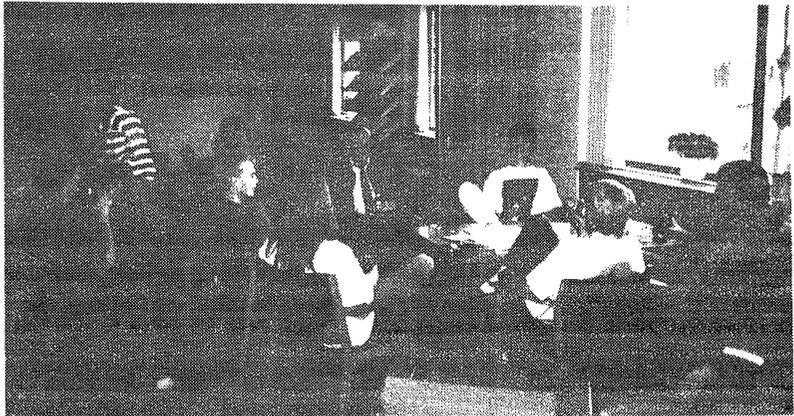
Kurt Ramskov

## Visit by the Tuborg Foundation.

Thursday, september 3, a representative for the Tuborg Foundation showed up to deliver a cheque of 12.500 Dkr. to support Eulers Venners study tour to St. Petersburg — from Sunday October 18 to Sunday October 25. After the presentation, the representative from Tuborg gave us a crate of beer, and we had a nice time. (When we bought the beer, we had the bad luck that there was no Tuborg in the canteen. People (read first year students and their tutors) had simply drunk all the Tuborg's that day. Fortunately the canteen was not out of stock, and we found a crate in the bag premises).



The delivery of the cheque.



People enjoy the divine liquid.

## Reception for the new students on part II in mathematics.

Friday September 4, the mathematical institute held a reception for the new students on part II in Staff Lounge. The occasion was that the study on part II has been changed — from now on part II starts after two years of study, and each student get a supervisor among the teachers at the start of part II. Further the number of new students on part II was exceptionally high, not only because two year groups was taken in because of the change, but also because there was exceptionally many from each who had chosen mathematics as their main subject. It was the plan that the reception should be a means for the students for talking informally with their new supervisor, other teachers and other students in the same situation. As an 'old boy' on part II, I was not directly involved, and might therefore not be the right person to tell about the reception, but it seemed that it worked out well.

It should be mentioned that the new supervisors in the start of the study does not play the same role as the traditional supervisors at the end of the study. Their role is to give some advise about courses and so on, not to specialize the students in their own speciality that early in the study.

After the reception Eulers Venners bar was open — and with some more customers than usual.



Eulers Venner took advantage of the reception to get quite a lot of new members. Here Jacob Schach is selling memberships.

# **The Russians are coming!! Wine Club Strikes!!**

It's our own democratic fault. Since we crumbled the Wall their way was open, but who thought they ever would come to this corrupt capitalistic west? They are even coming to Denmark of all places. To be somewhat more specific; they are coming to the ISC!! Who is coming and how are we to retaliate? Well, since they are 28 students of the mathematical institute of the University of st.Petersborg, I have to decided that, after a brief briefing with my *vice-president* Dan (*Qualey*) Otzen, the only appropriate option would be to revitalise the ISC Wine Club. The evening we have planned our counter attack will be

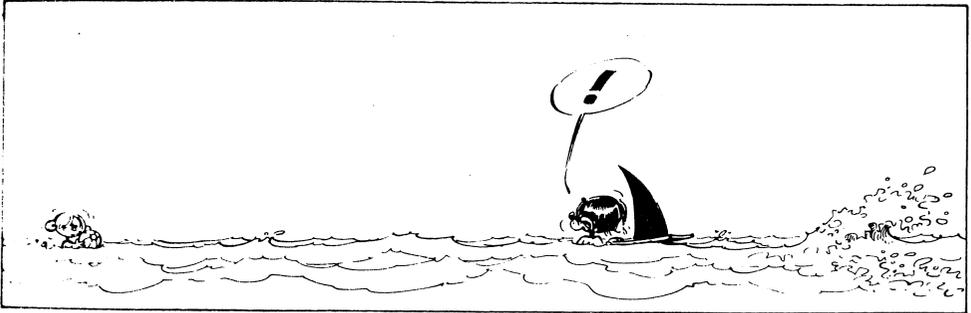
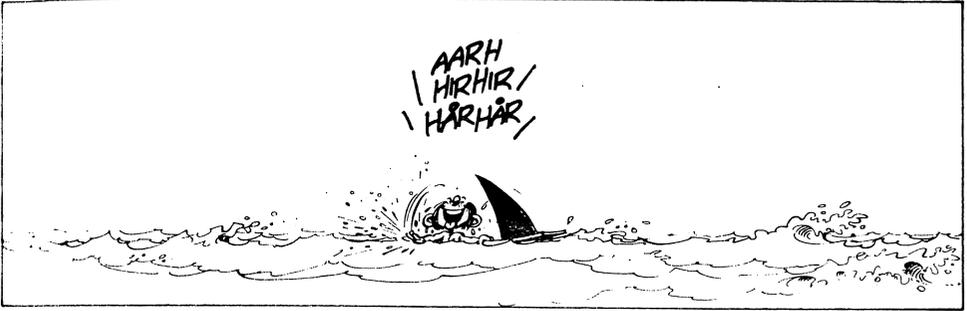
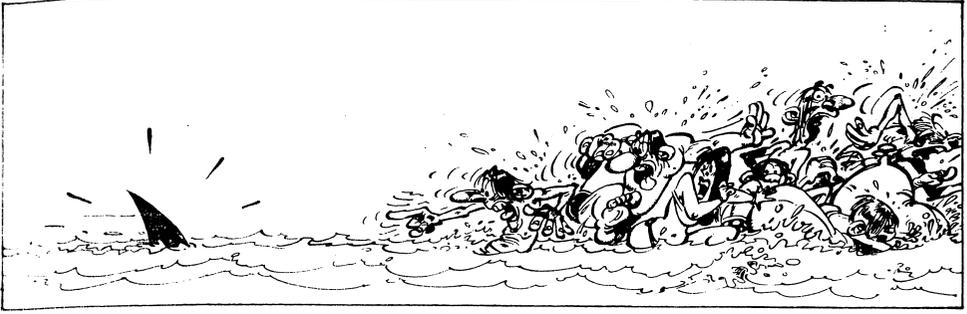
**Monday 14<sup>th</sup> of September 1992 AD  
at 20.00 (after the foodclub)**

The plans are to let the *vice-president* explain something about the formal, dry as dust and terribly boring, theoretical principles of wine making, while yours truly will cut to the essence of the matter and inform the amassed crowds about the delicate and noble art of homebrewing, which the capitalistic Occidental governments have forced their subjects to perfect.

Even though we will be sampling some Danish elderberry pettle- and an applewine of undefined species afterwards, we encourage you to bring some more of the right spirit with you. Since we all know about the abhorring price of a bottle of wine around this place you should try and find a friend who'll help you share the initial investment. In order to make this event the customary great success any other Wine Club evening so far has been, we encourage you, dear reader, to bring your friend along to help you share your bottle's content.

Pieter van de Griend  
President of the ISC Wine Club.  
Århus 250892 AD.

# JAWS



# Games and optimal strategies

J. Hoffmann-Jørgensen

When you are joining a series of random games, you are faced with the problem of when to stop. Of course the best thing is to stop at the time, when your winnings reaches its maximum, but in a random environment you will never know, if you could increase your winnings by continuing. However you may hope to find stopping strategies, which maximizes your expected winnings. To handle this problem we need three basic notions:

- (1) **Information:** It turns out that the cardinal point in gambling is information. As the games evolves your learn more and more about the game, and it is this increasing information, which is used to construct the optimal strategy. Thus we need a precise mathematical formulation of the notion of information and increasing information. This will be done in terms of “ $\sigma$ -algebras” and “filters”
- (2) **Conditional expectations:** Having defined information we need to be able to compute the expectation of our future winnings given all the information available at present. This will done in terms of “conditional expectations”
- (3) **Stopping times:** Suppose that you are visiting a gambling house, and that you have decided to play at most 100 games. Let  $X_n$  be the your net winnings after the first  $n$  games for  $n = 1, 2, \dots, 100$  ( $X_n$  may negative, meaning that you have lost money). Let  $M = \max(X_1, \dots, X_{100})$  be your maximal winnings. Then the best you can do is to stop the first time that  $X_n = M$ . However this stopping strategy has a serious drawback: You never know if  $X_n = M$  before you have played all the 100 games, and then it is too late stop. Thus we need a precise mathematical definition of the kind of stopping strategies, which actually can be carried out without clairvoyance. This will done in terms of “stopping times”

In the lecture I shall introduce the three notions above. With these notions at hand I shall give a general formula for the optimal stopping strategy in case of a finite number of games, and a formula for the optimal stopping strategy for a certain class of an unlimited number of games. And I shall give a series of examples of such optimal stopping strategies, for instance for “quits or doubles”, “black jack”, “hazard”, “auction” etc.

## Abstract

Johan Dupont: *Scissors congruences and homology.*

Two polyhedra in Euclidean 3-space are called *scissors congruent* if they can be subdivided into finitely many pairwise congruent pieces. In particular they have the same volume. *Hilbert's third problem* was to prove that there exist two polyhedra with the same volume which are not scissors congruent. This was actually solved in the same year as it was stated (1900) by Max Dehn who introduced another invariant for scissors congruence of polyhedra. But the general problem of finding necessary and sufficient conditions for scissors congruences of polytopes in higher dimensions and in the other classical geometries (spherical or hyperbolic) is still open. In the lecture we shall reformulate the problem in terms of modern homological algebra and sketch a recent homological proof of the difficult theorem of J. P. Sydler (1965) that, in Euclidean 3-space, the scissors congruence class of polyhedra is determined by volume and the Dehn invariant.

September 4, 1992

## **ANALYSIS SEMINAR**

Konstantin M. Dyakonov (Institute of Electrical Engineering, St. Petersburg) :

*Division and Multiplication by Inner Factors and Embedding Theorems for Star-Invariant Subspaces in Hardy Spaces..*

Date : Friday, September 18, 1992.

Time : 12.15 – 13.15.

Place : Aud. G1.

Henrik Stetkær

FRIDAYBAR!

- NATURALLY

