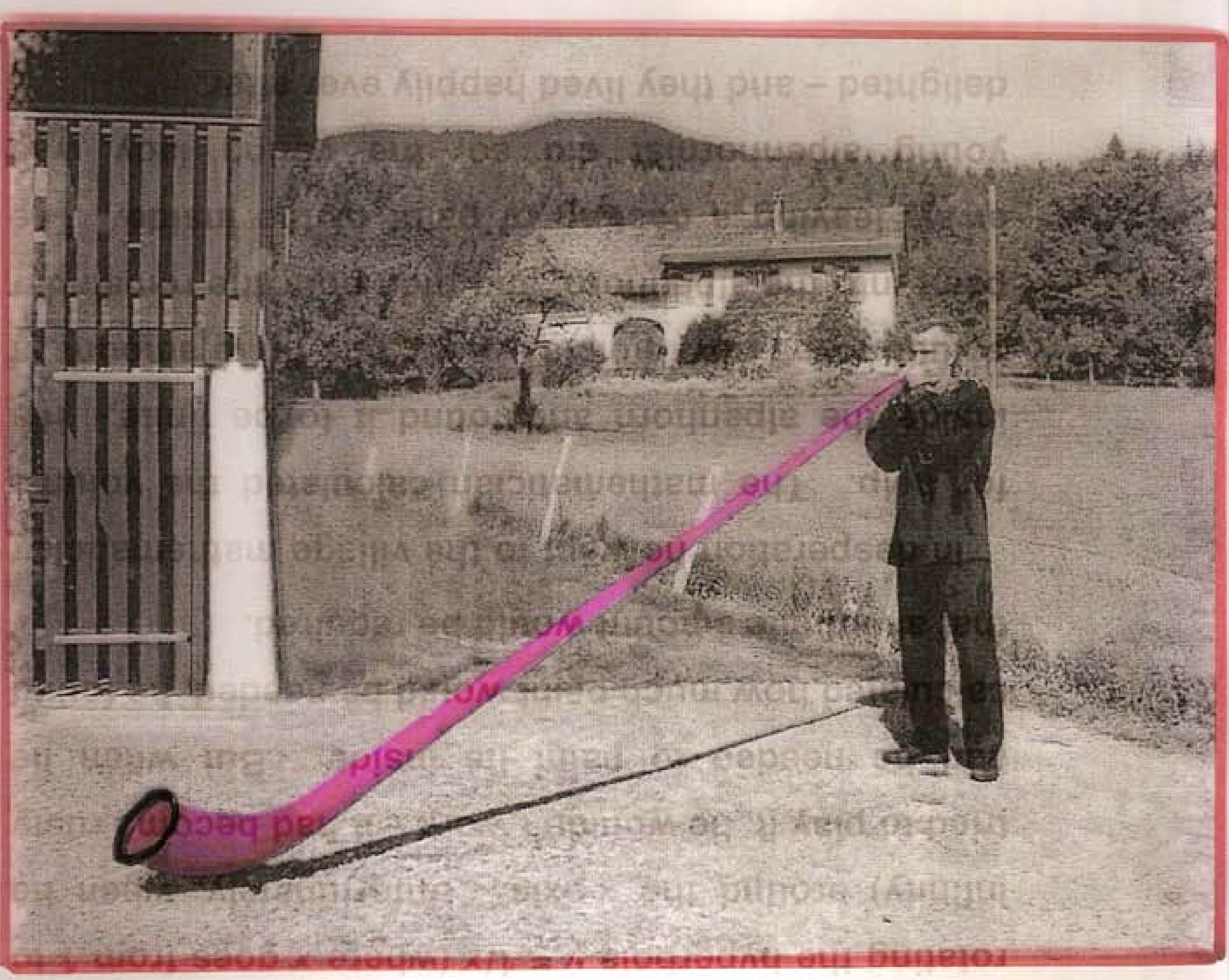
The 20th Century:

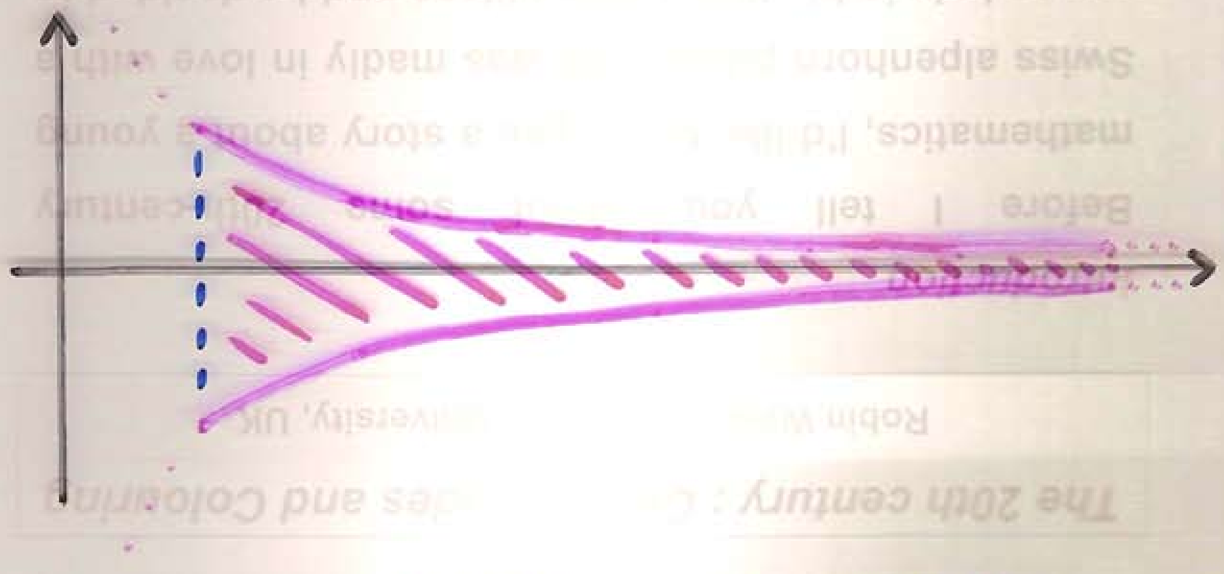
Chaos, codes and colouring

Robin Wilson
The Open University

Painting Swiss alpenhorns

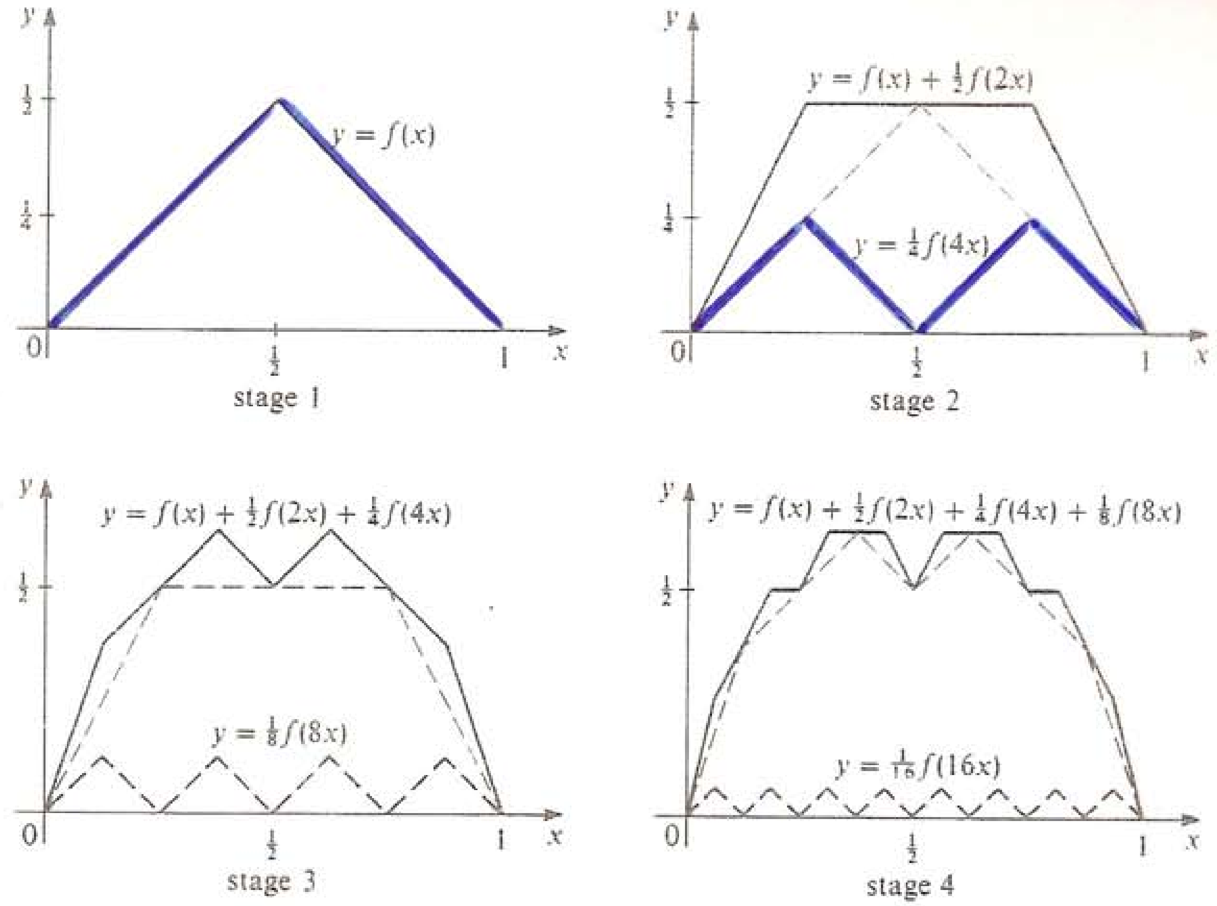


$y = 1/x$ for $x \geq 1$:

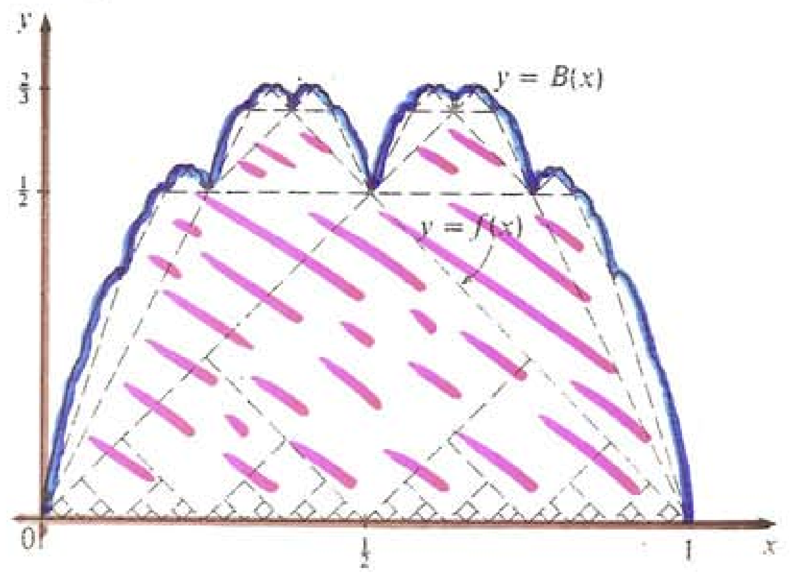


surface area infinite : volume finite

The blancmange function

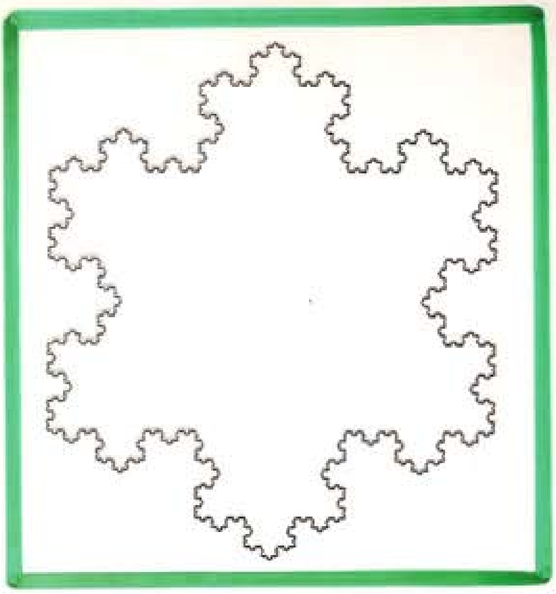


Eventually we obtain the following graph of B:



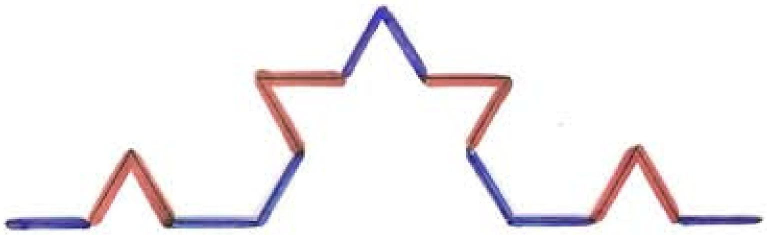
von Koch's Snowflake Curve

finite area – infinite length

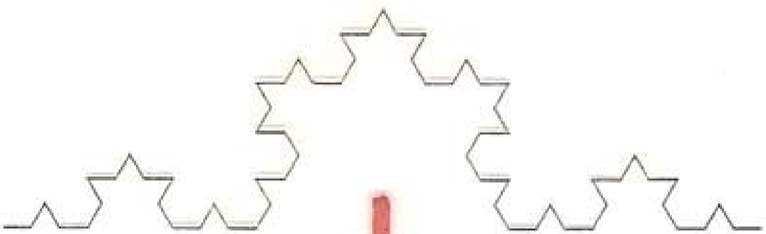


step 1

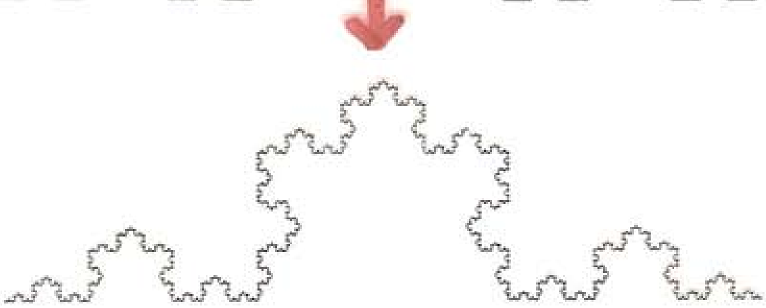
step 2



step 3



step 4



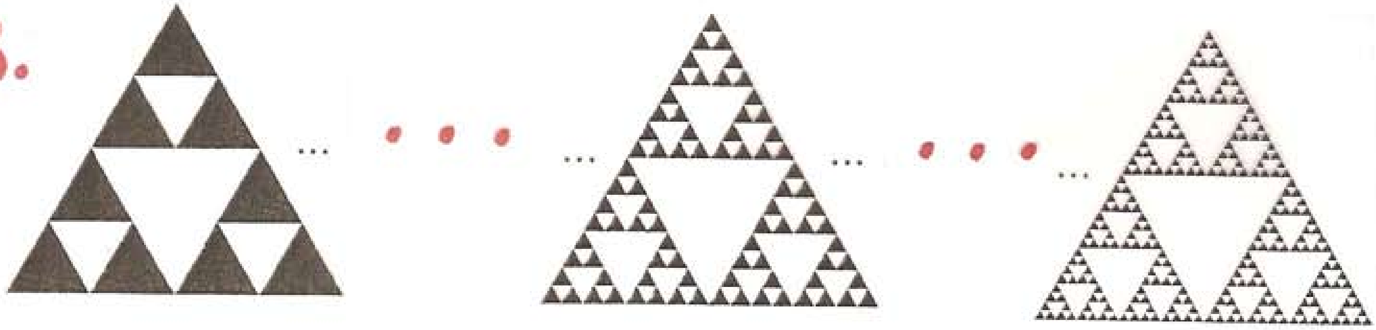
⋮

Sierpinski gasket

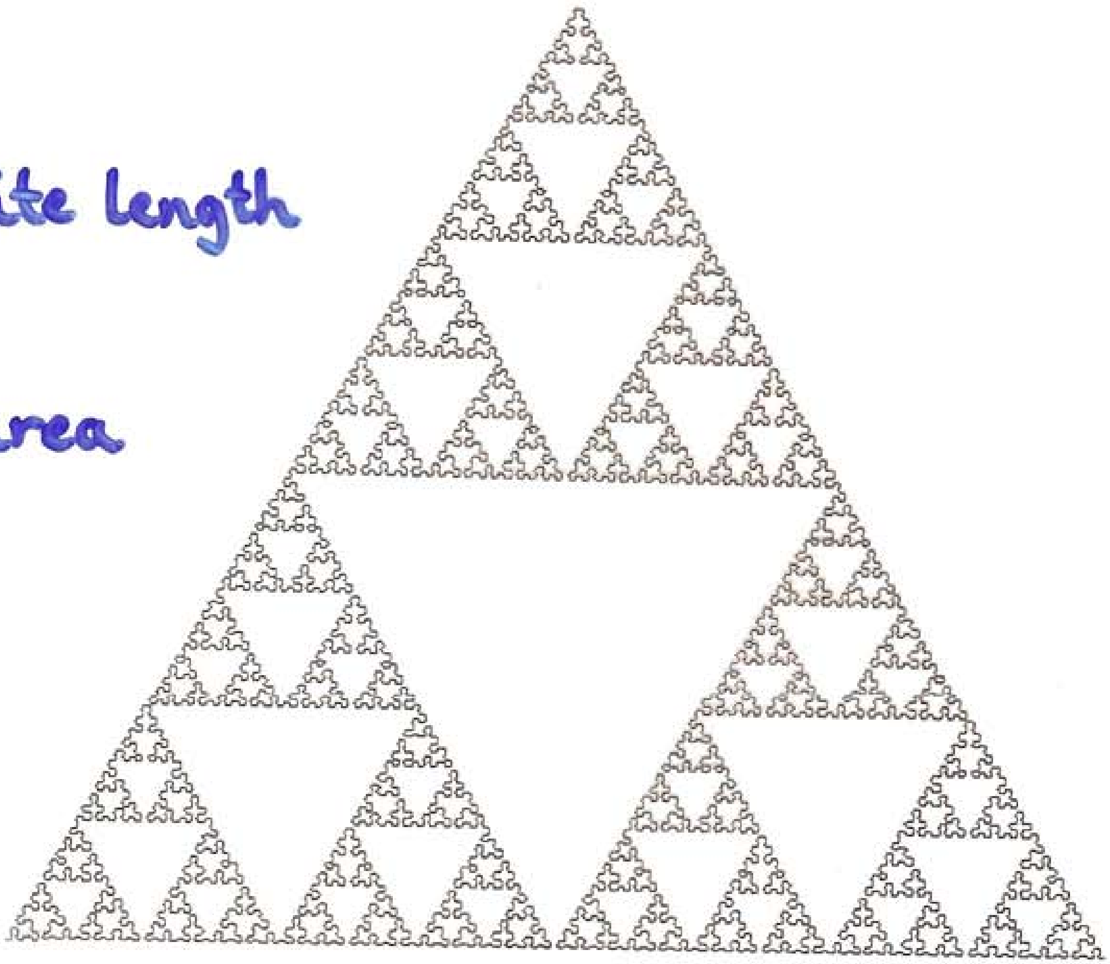
1.

2.

3.



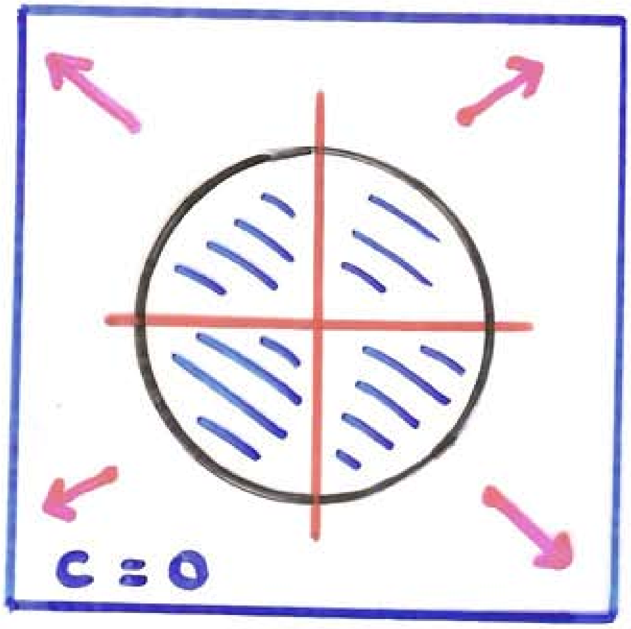
infinite length
-
zero area



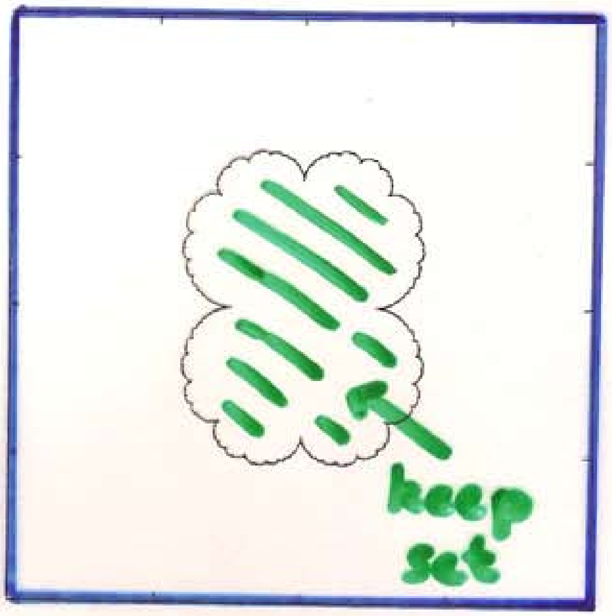
The map $z \to z^2 + c$

Do this over and over again:

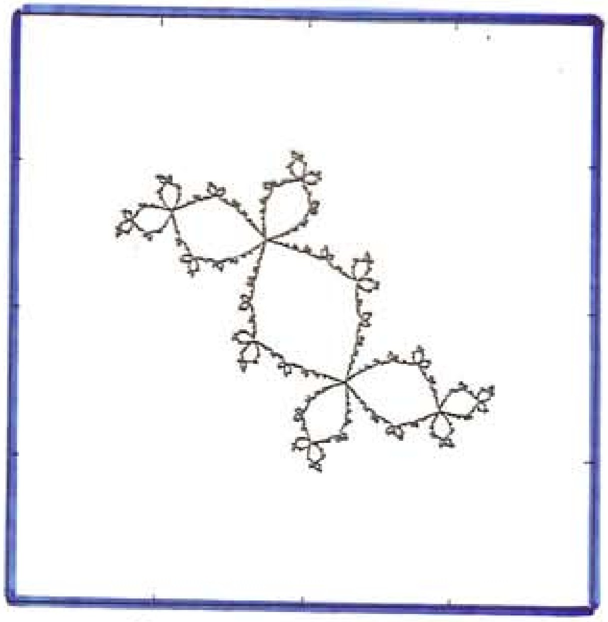
which points go off to infinity?



boundary = 'Julia set'



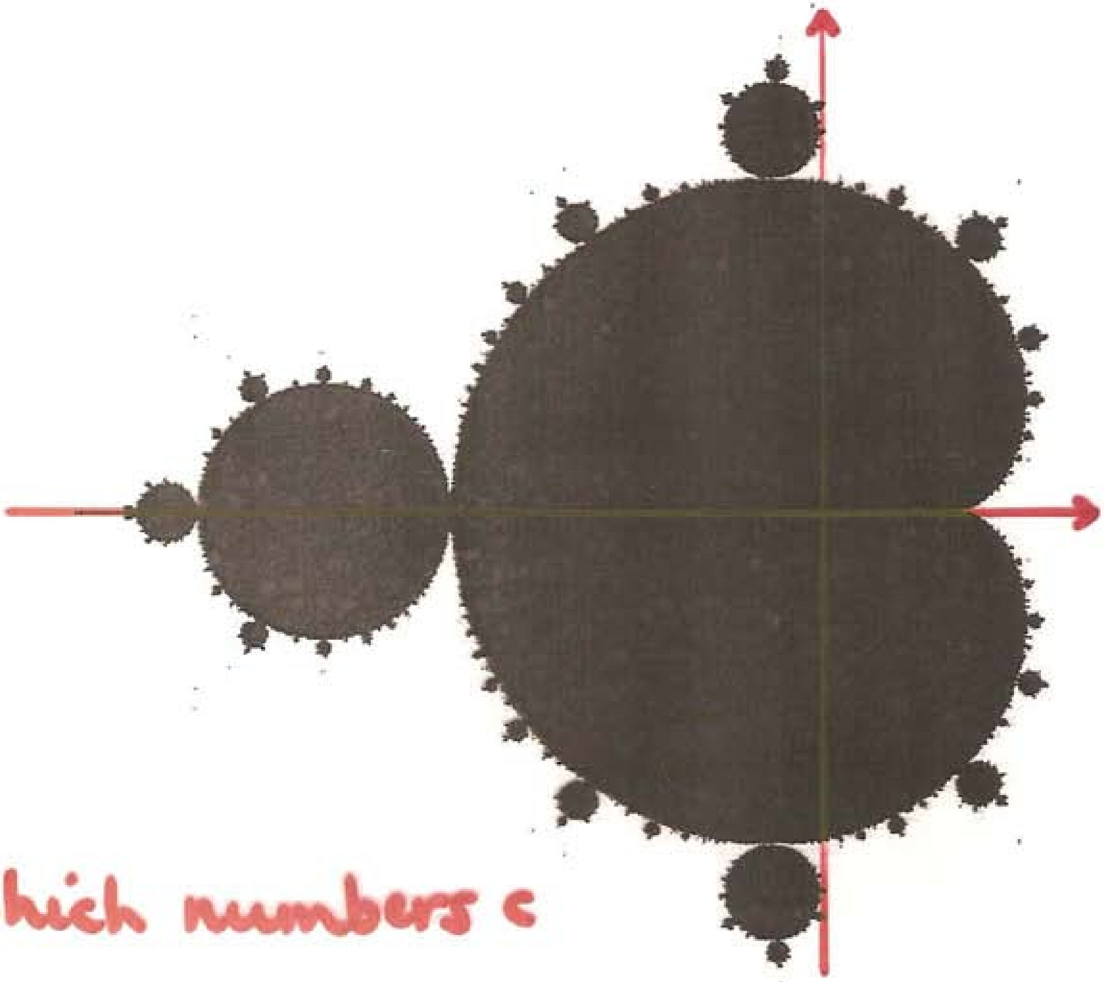
$J_c : c = 0.25$ (cauliflower)



$J_c : c = -0.123 + 0.745i$ (rabbit)

$J_c : c = -0.75 + 0.25i$ (sea-horse)

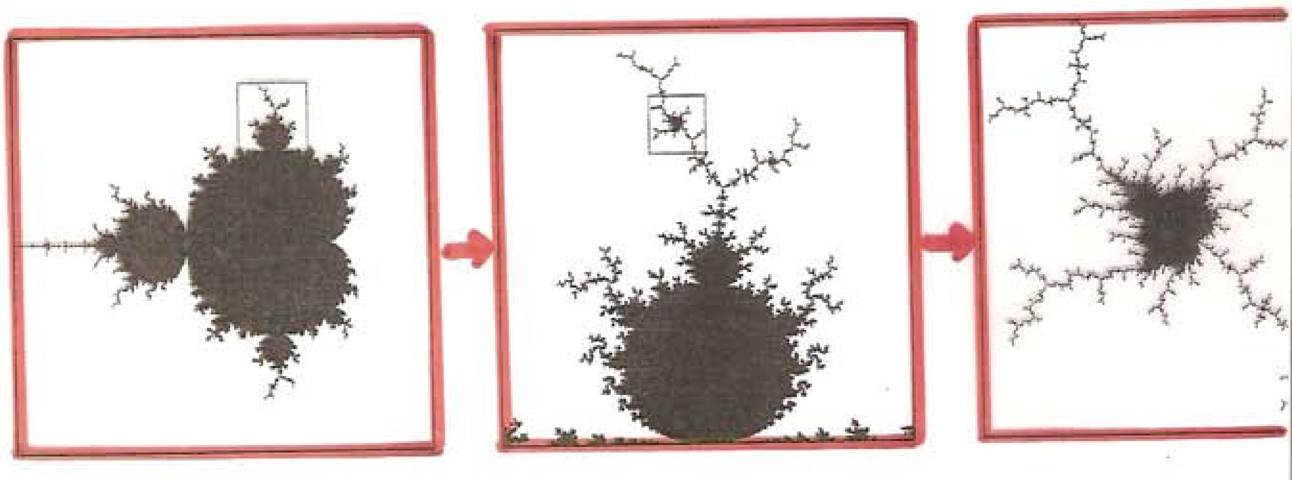
The Mandelbrot set



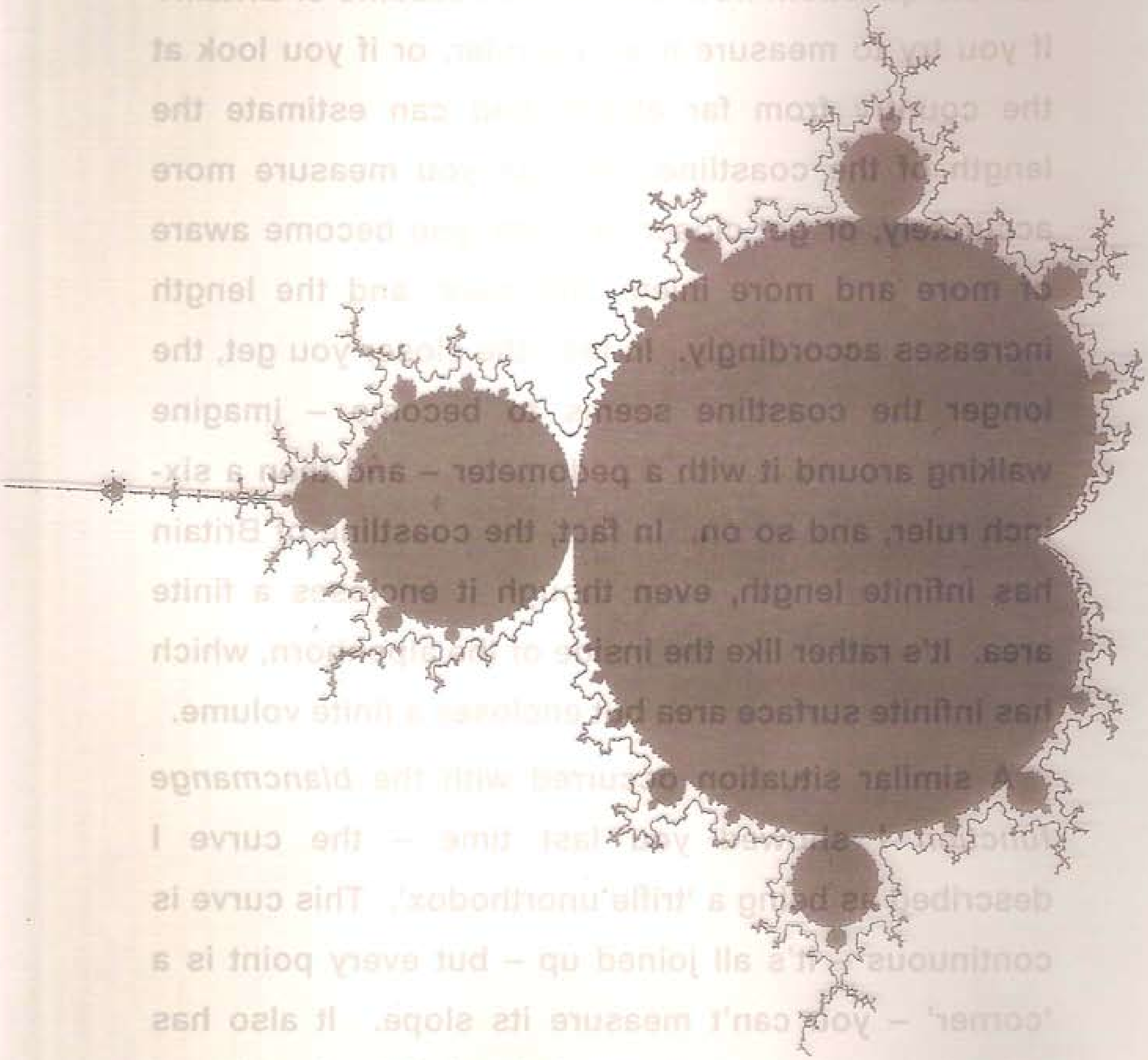
For which numbers c

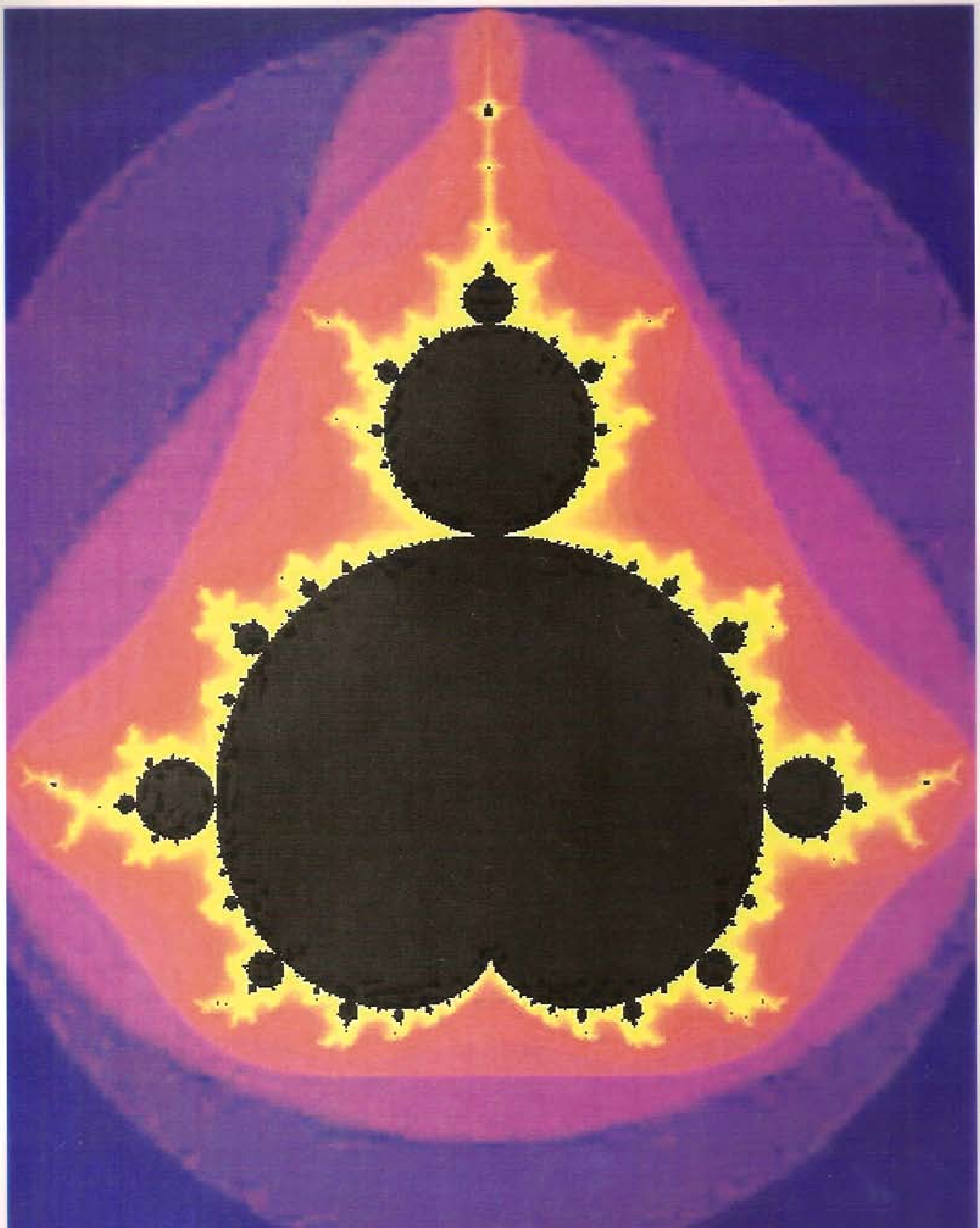
is the 'keep set' in one piece?

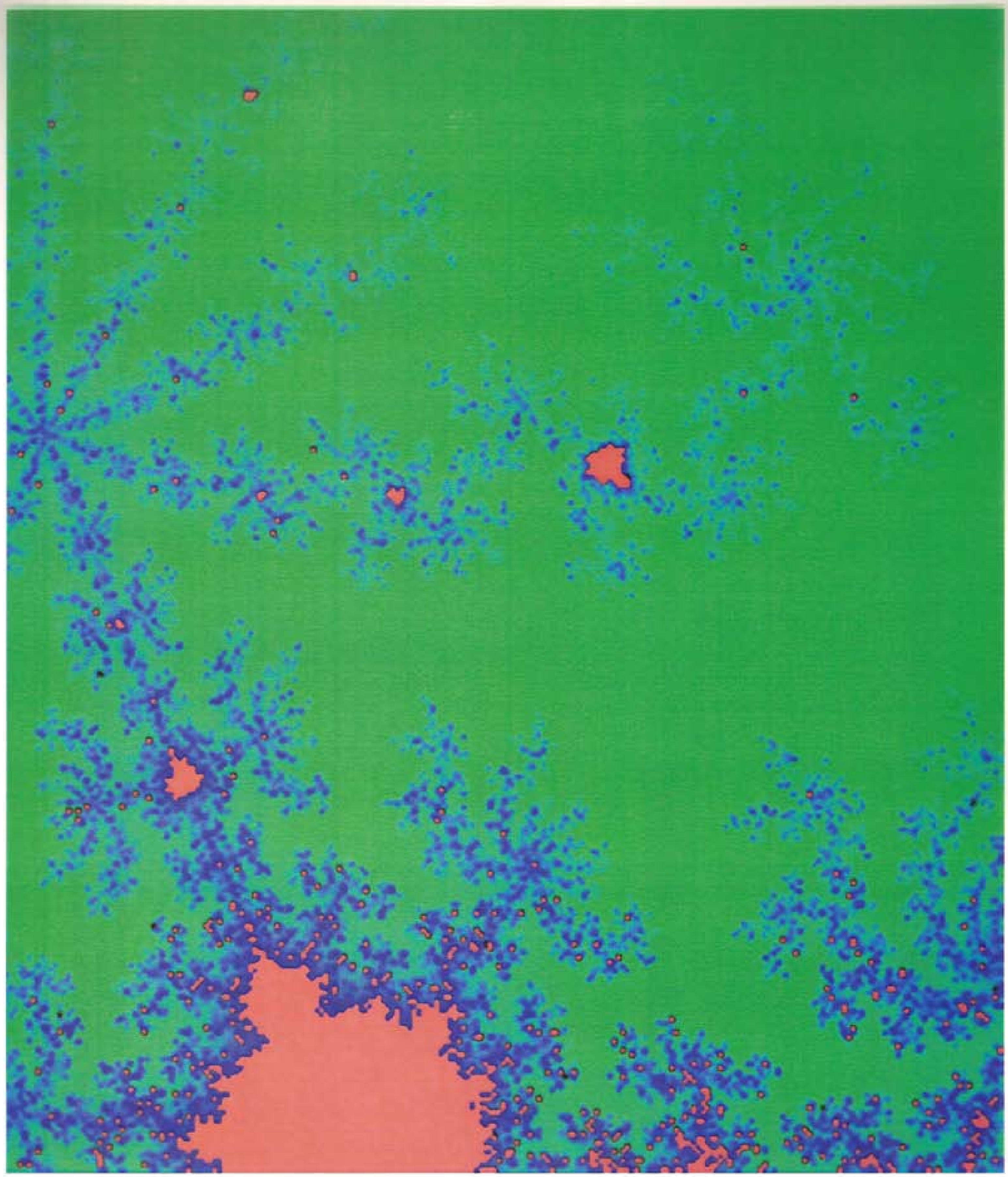
For which c is 0 in the keep set?

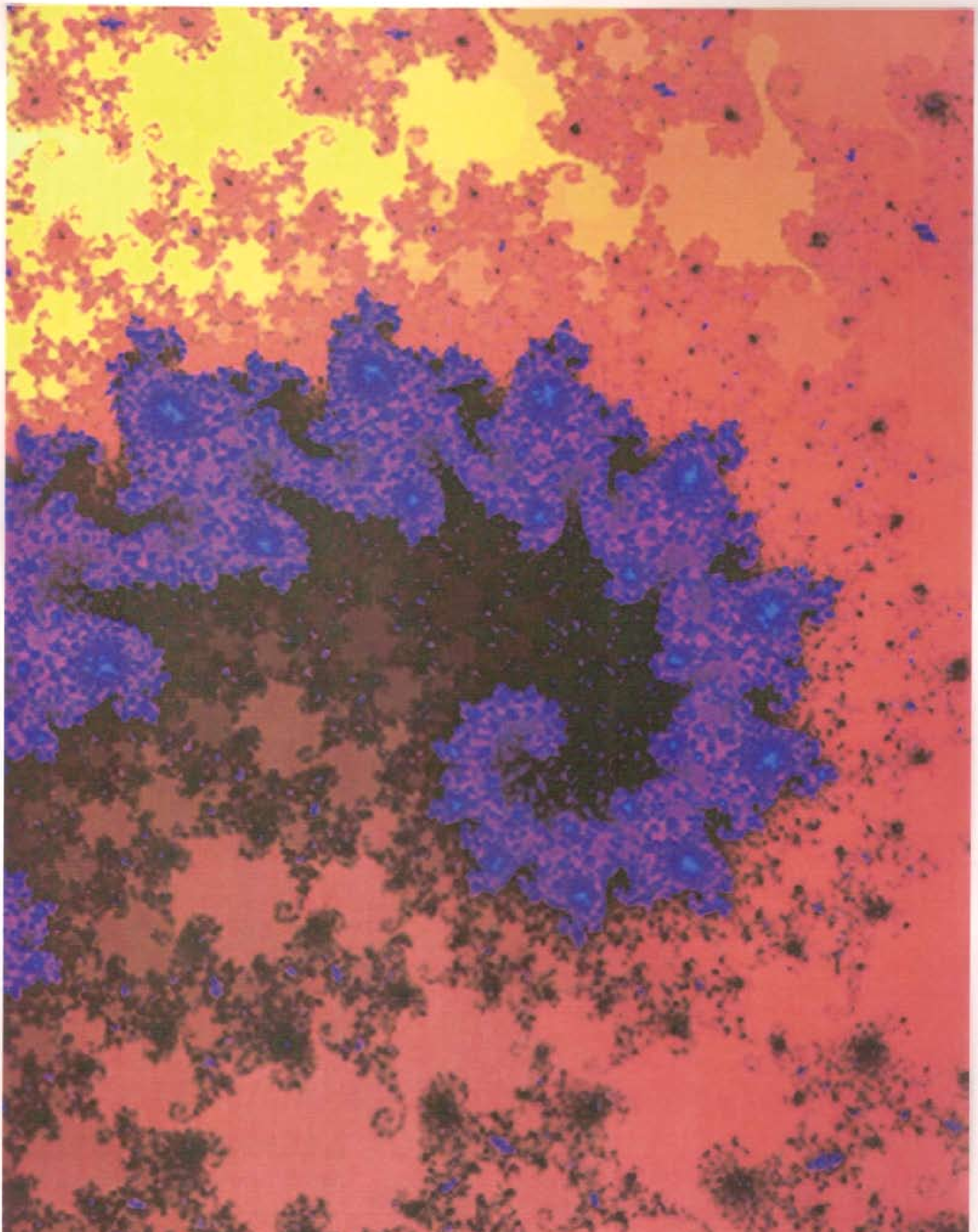


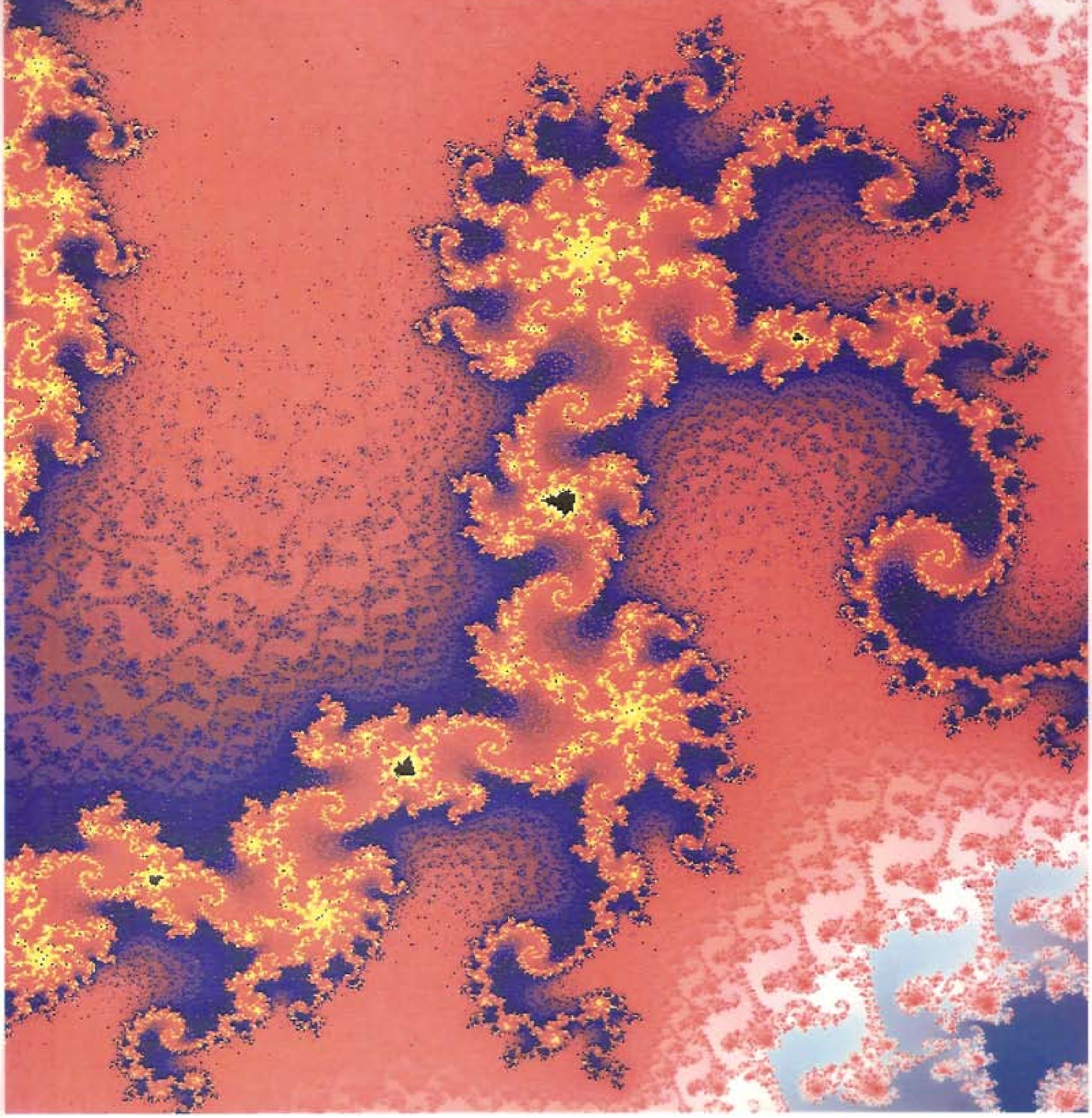
The Mandelbrot set

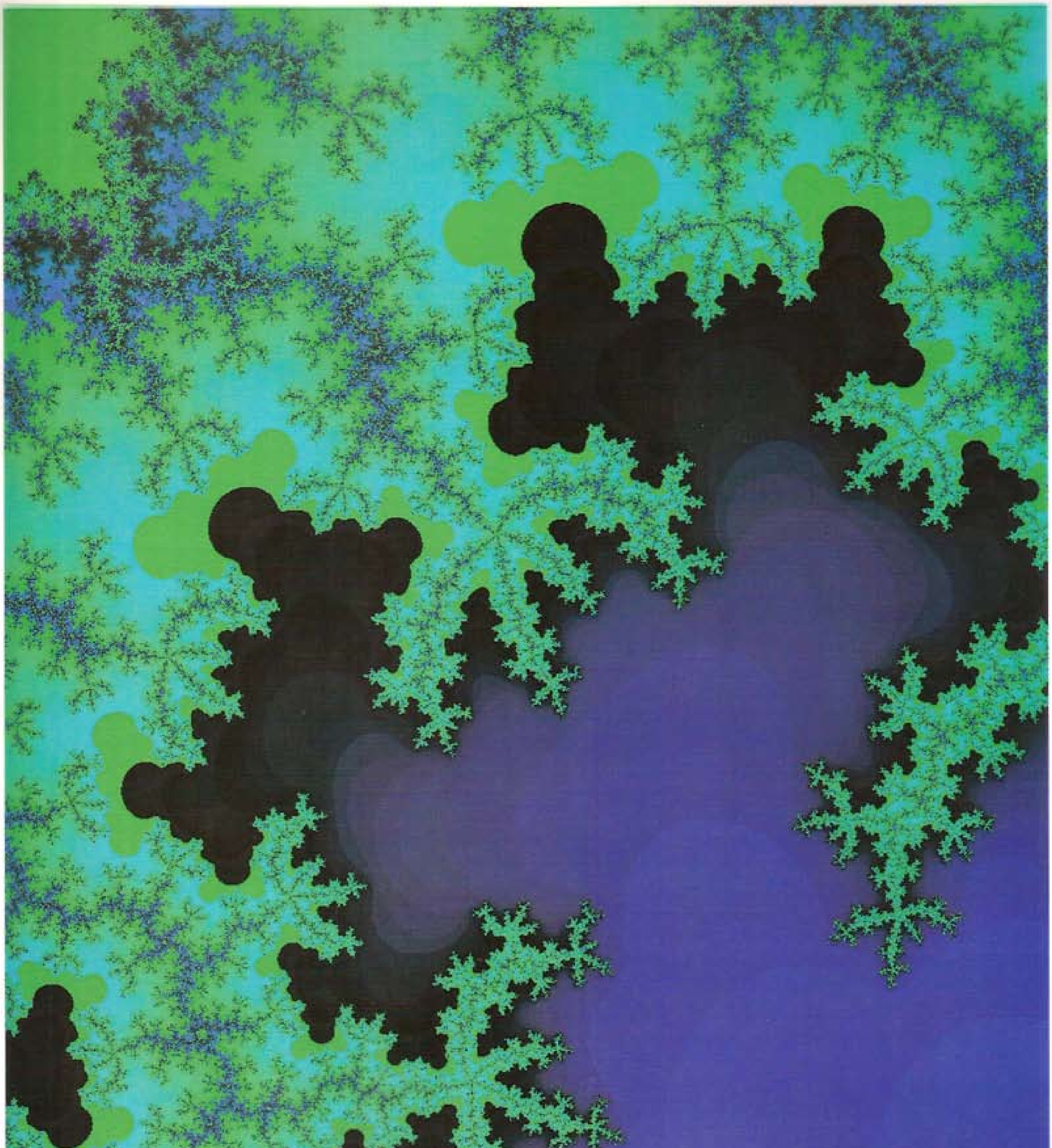












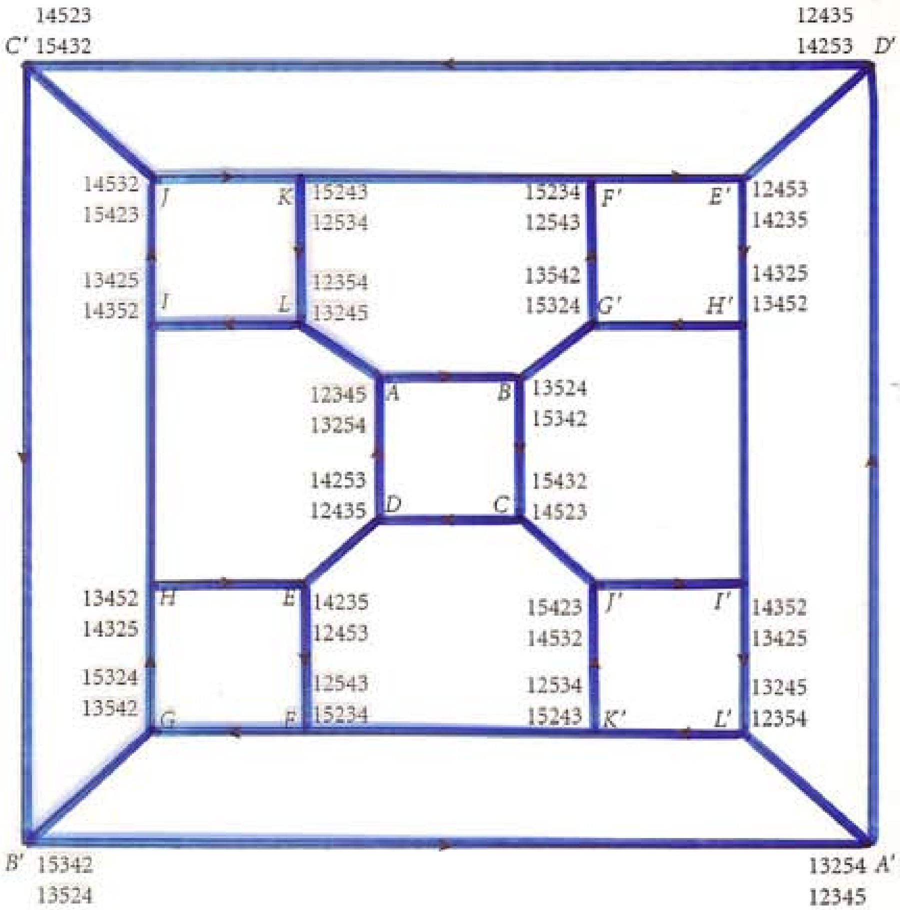
Four bells: Plain Bob Minimus

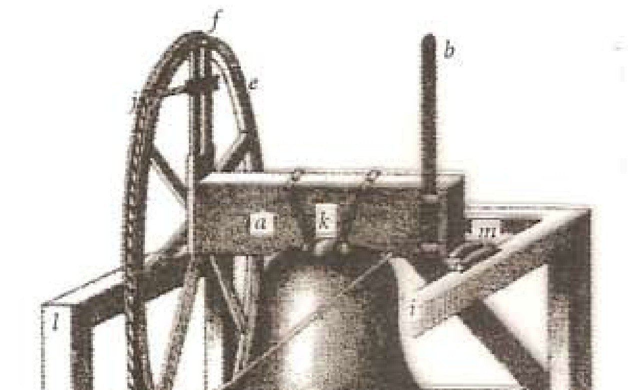
1 2 3 4
2 1 4 3
2 4 1 3
4 2 3 1
4 3 2 1
3 4 1 2
3 1 4 2
1 3 2 4
1 3 4 2
3 1 2 4
3 2 1 4
2 3 4 1
2 4 3 1
4 2 1 3
4 1 2 3
1 4 3 2
1 4 2 3
4 1 3 2
4 3 1 2
3 4 2 1
3 2 4 1
2 3 1 4
2 1 3 4
1 2 4 3
1 2 3 4

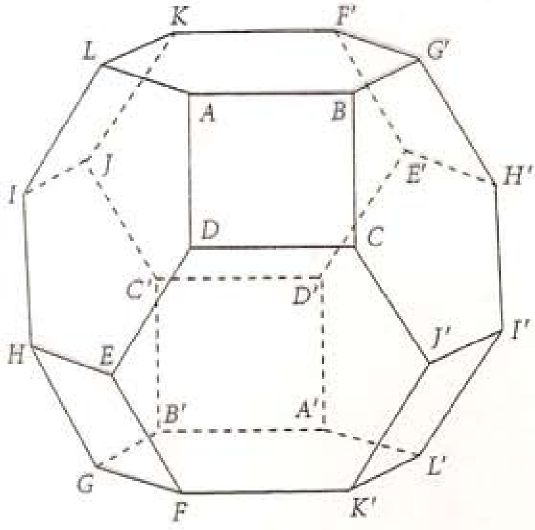
Interchange consecutive bells :

1 2 3 4
(even)
2 1 4 3
(odd)
2 4 1 3
. . .

Five bells : Plain Bob Doubles

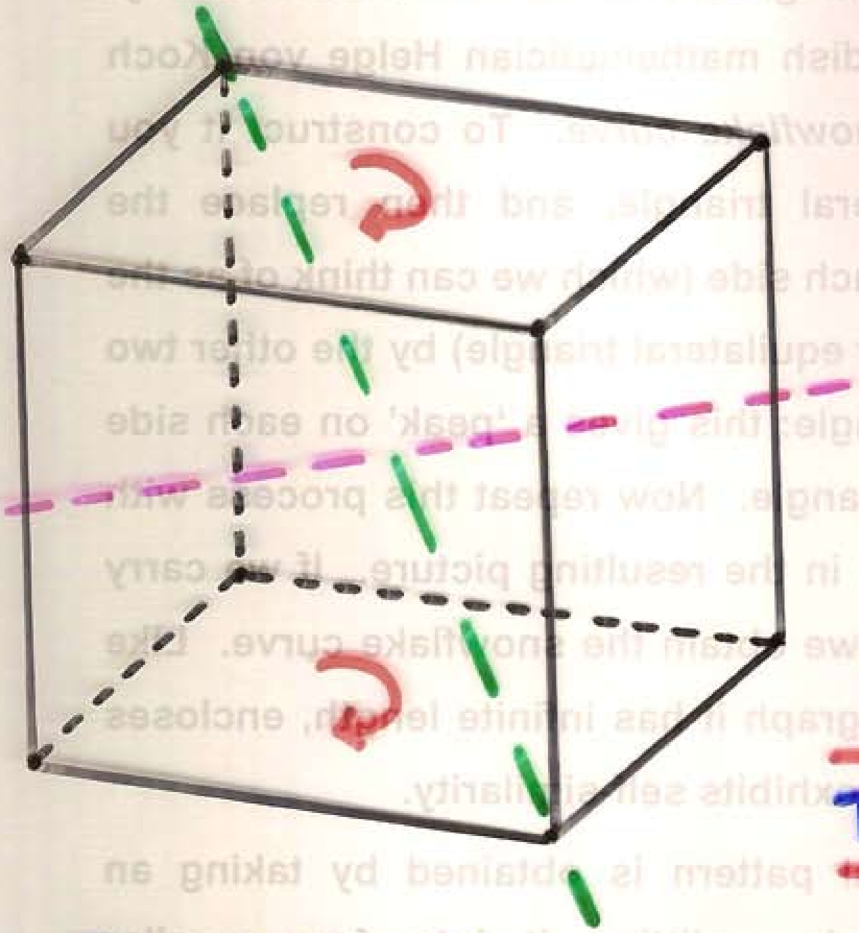






truncated octahedron

Symmetries of a Cube



Rotations

1 identity

9 face rotations

8 vertex rotns

6 edge rotns

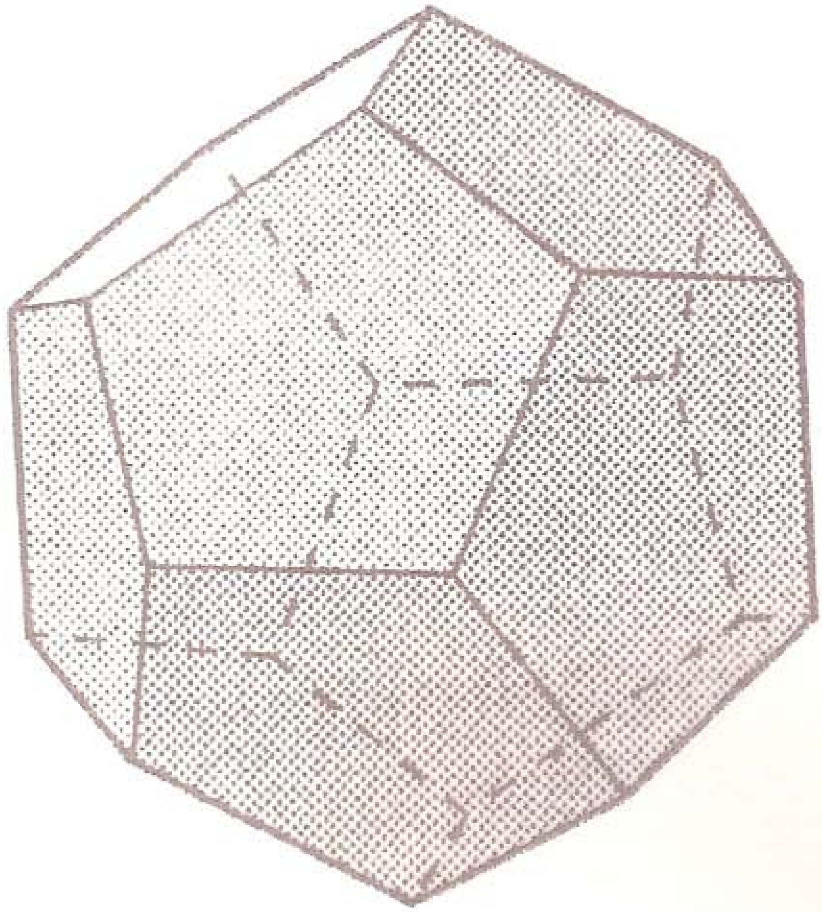
Total : 24

24 rotations

24 'indirect' symmetries

(reflection + rotation)

Rotations of a Dodecahedron



60 rotations

Abstract Groups

Take a set G of elements, and a rule for combining them ($*$). For a **group**, we have:

(1) **Closure**: if a and b are in G, then so is $a * b$.

(2) **Associativity**: if a, b, c are in G, then $(a * b) * c = a * (b * c)$

(3) **Identity**: there is an element e such that $a * e = e * a = a$ for all a.

(4) **Inverses**: for each a in G, there is an inverse a^{-1} such that $a * a^{-1} = e$.

[(5) **Abelian**: if a and b are in G, then $a * b = b * a$.]

Remembering the group axioms

C losure

A ssociative

I nverses

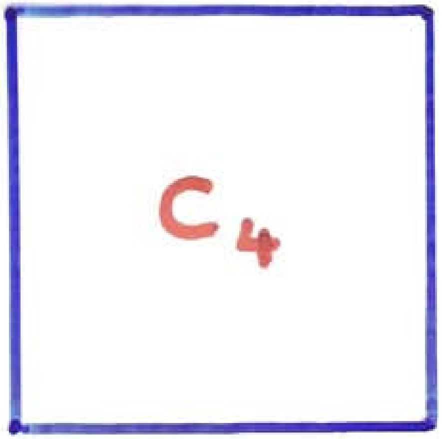
N eutral element

not necessarily **ABEL**ian

Examples :

- permutations of 4 bells
- symmetries of a cube
- rotations of a dodecahedron
- addition of integers
- multiplying positive real numbers

Cyclic Groups



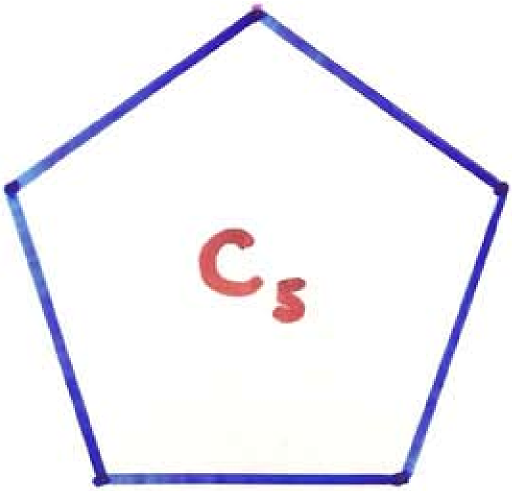
rotations of a square through 0, 1, 2, 3 right angles:

$1 + 3 = 0, \quad 3 + 2 = 1, \ldots$

(arithmetic 'mod 4')

rotations of a pentagon through 0, 1, 2, 3, 4 turns:

$2 + 3 = 0, \quad 3 + 4 = 2, \ldots$



Classification theorem: Every abelian group is obtained by combining cyclic groups.

Simple groups

- 'building blocks' for groups in general
- groups that 'contain no other groups inside them' – they have no proper normal subgroups

- cyclic groups with a prime number of elements: C_5, C_7, C_{101}, ...
- rotations of a dodecahedron (A_5)
- A_n ($n \geq 5$): even permutations of $\{1, 2, \ldots, n\}$
- groups of 'Lie type' (related to matrices)
- 26 'sporadic groups'

[Monster group: rotations in 196883-dimensional space]

How big is a set?

- $\{100, 101\}$ $\quad$ $\{1, 2, 3, 4\}$
- $\{1, 2, 3, 4, 5, 6, \cdots\}$

  $\{1, 4, 9, 16, 25, 36, \cdots\}$
- $\{\frac{1}{2}, 1, 1\frac{1}{2}, 2, 2\frac{1}{2}, 3, \cdots\}$
- $\{0, 1, -1, 2, -2, 3, \cdots\}$

A set is <u>countable</u> if we can list them all – for example, the <u>rationals</u>:

1	2	3	4	5	6 ...
1/2	~~2/2~~	3/2	~~4/2~~	5/2	...
1/3	2/3	~~3/3~~	4/3	5/3	...
1/4	~~2/4~~	3/4	4/4	5/4	...
1/5	2/5	3/5	4/5	5/5	...

The real numbers are not countable

Suppose that the real numbers between 0 and 1 are countable: let's list them all –

$$0 \cdot a_1\, a_2\, a_3\, a_4\, a_5 \cdots$$

$$0 \cdot b_1\, b_2\, b_3\, b_4\, b_5 \cdots$$

$$0 \cdot c_1\, c_2\, c_3\, c_4\, c_5 \cdots$$

$$0 \cdot d_1\, d_2\, d_3\, d_4\, d_5 \cdots$$

$$\cdots$$

Now choose numbers $x_1, x_2, x_3, \cdots$ so that

$$x_1 \neq a_1,\ x_2 \neq b_2,\ x_3 \neq c_3,\ x_4 \neq d_4, \cdots$$

Then the number $0 \cdot x_1 x_2 x_3 x_4 \cdots$ is not in the above list – contradiction

So they are NOT countable.

The Continuum Problem

Let $\aleph_0$ be the (infinite) number of integers (or rationals):

$\aleph_0 + 1 = \aleph_0, \ \aleph_0 + \aleph_0 = \aleph_0, \ldots$

Let $\aleph_1$ be the number of reals:

so $\aleph_1 > \aleph_0, \ \aleph_1 + \aleph_0 = \aleph_1, \ldots$

Is there a number between $\aleph_0$ and $\aleph_1$?

P. Cohen (1963): Using the 'usual' axioms of set theory, this problem is undecidable.

Cryptography

Old method:

Alice and Bob both have the key. Alice encodes a message and sends it to Bob who decodes it.

Public-key cryptography

Uses prime numbers:

- we can test whether a large number (≤ 300 digits) is prime
- but we cannot find a prime factor

(e.g. $2047 = 23 \times 89$)

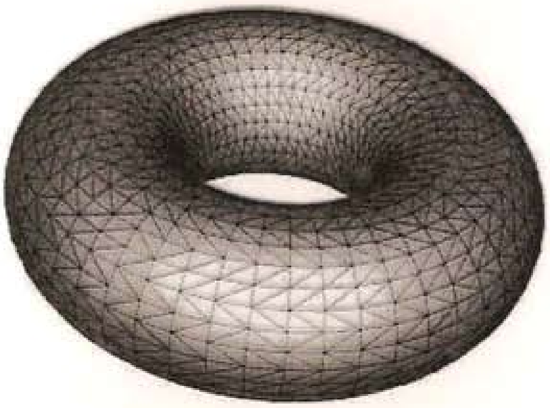
An example

Alice chooses two large primes p and q, and makes $n = pq$ public.	Alice chooses $p = 5$, $q = 11$, and announces $n = 55$.
Alice chooses v (public) and calculates s (private) so that $sv \equiv 1 \pmod{(p-1)(q-1)}$	Alice announces $v = 3$ and calculates $s = 27$: $(81 \equiv 1 \bmod 40)$
Alice takes her message b, calculates $h = b^s \pmod{n}$, and sends h and b to Bob.	If $b = 49$, then $h \equiv 49^{27} \pmod{55} = 14$. Alice sends 49 and 14.
Bob receives h and b, looks up n and v, and calculates $h^v \pmod{n}$, obtaining the message b.	Bob calculates $14^3 \pmod{55}$ and obtains 49.

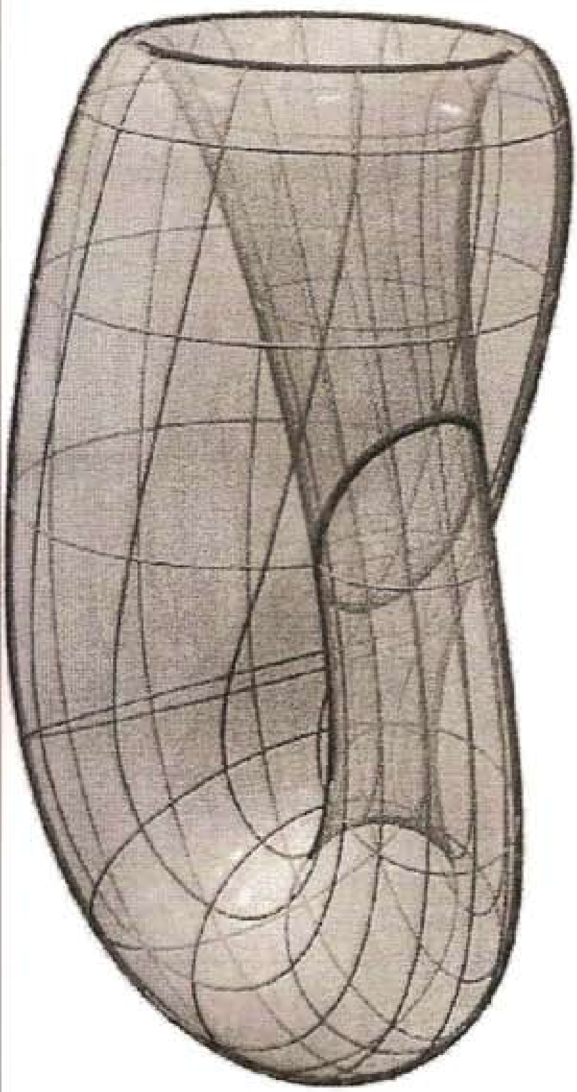
[Reason: $b^{sv} \equiv b \pmod{n}$
if b is not divisible by p or q]

Classification of surfaces

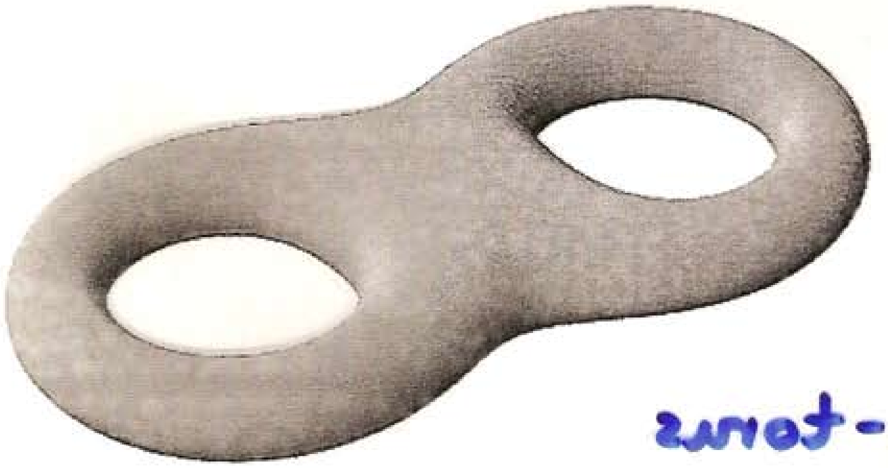
sphere



torus



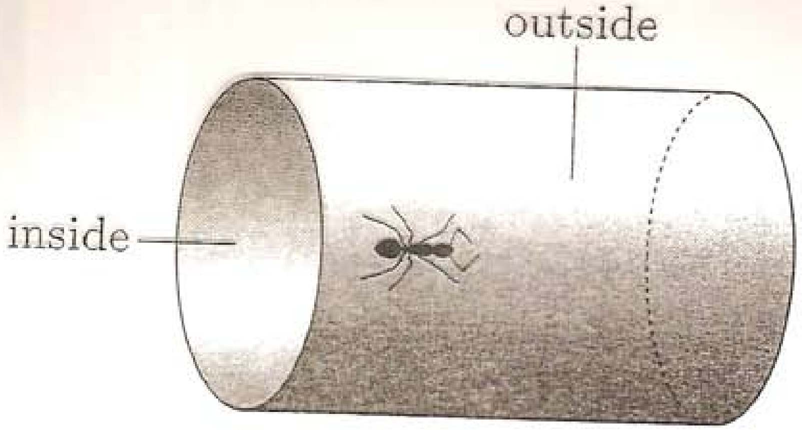
Klein bottle



double-torus

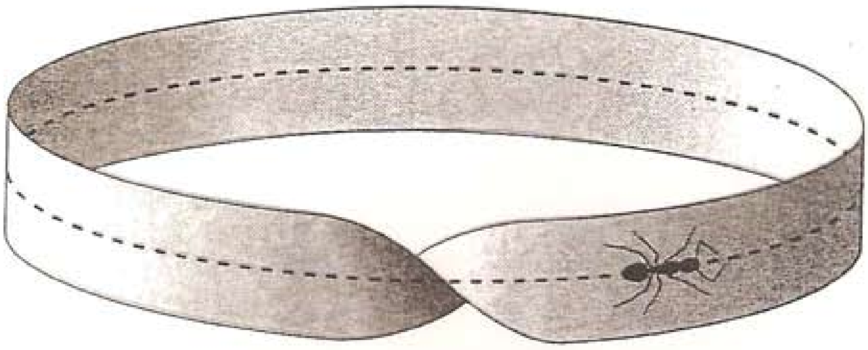
(sphere with two handles)

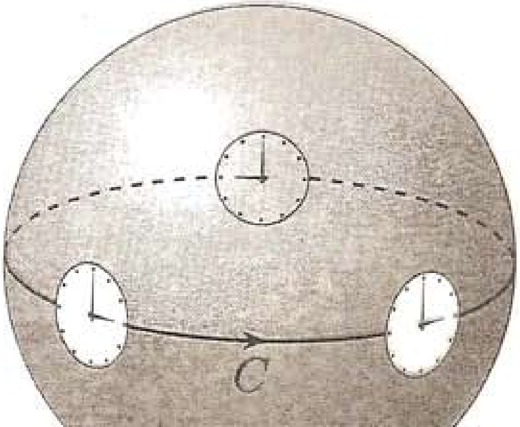
Orientable surfaces

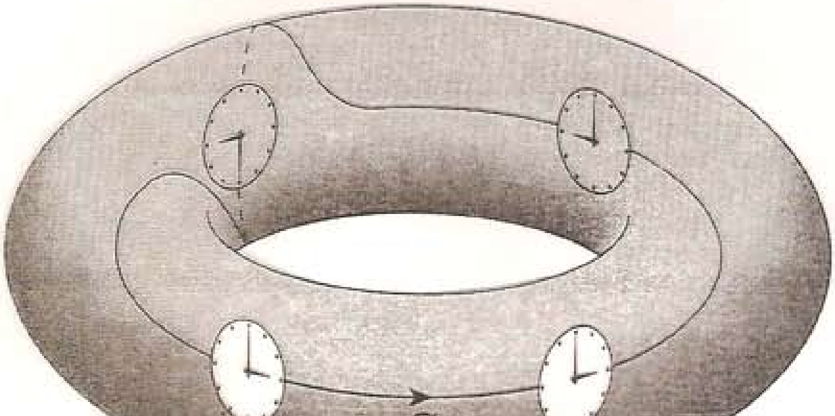


cylinder
(orientable)

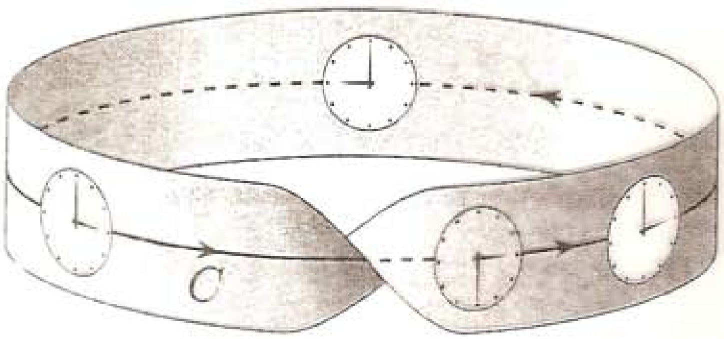
Möbius strip
(non-orientable)







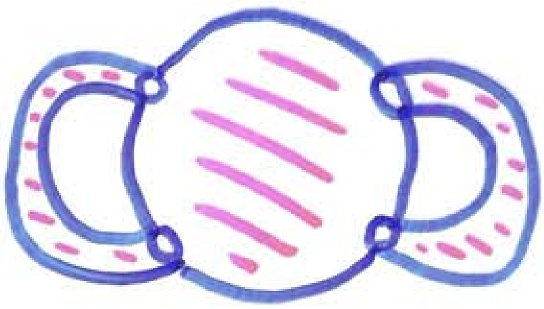
orientable



non-
orientable

Classifying Surfaces

Every orientable surface is either equivalent to a sphere, or can be obtained by adding handles to a sphere.



adding a handle

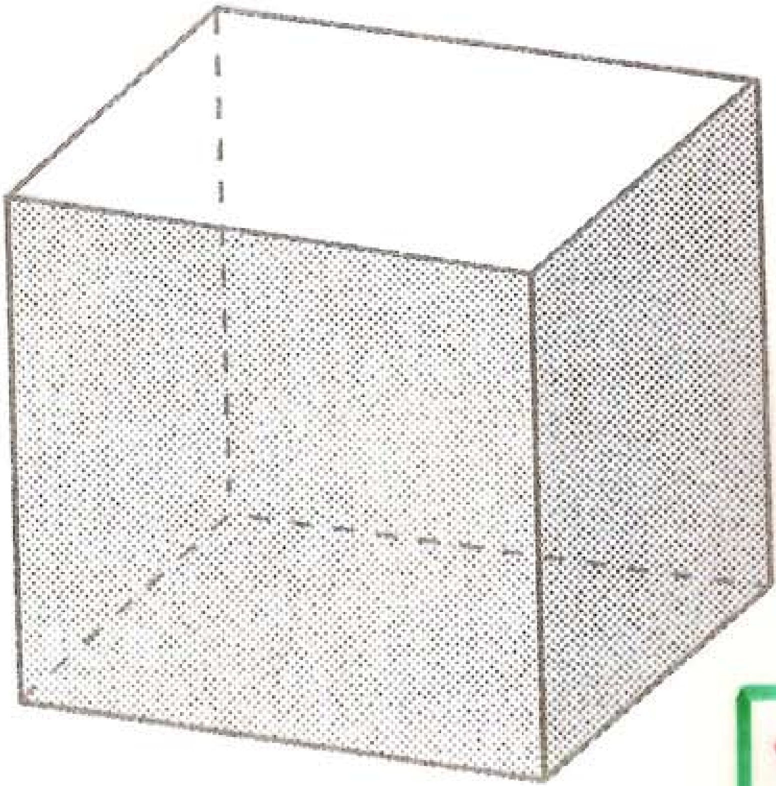
adding a cross-cap

Every non-orientable surface can be obtained by adding cross-caps to a sphere.

2 handles : double-torus

2 cross-caps : Klein bottle

Euler's Polyhedron Formula



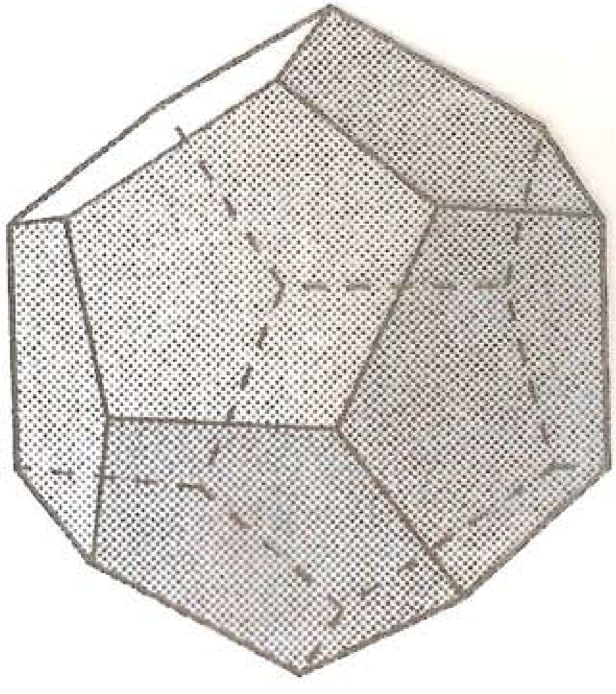
8 vertices

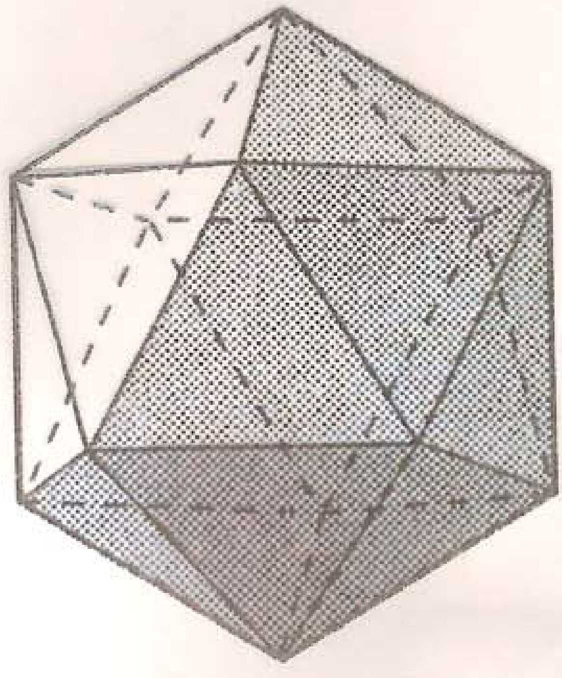
6 faces

12 edges

8 + 6 = 12 + 2

$$\boxed{V + F = E + 2}$$





20 + 12 = 30 + 2

12 + 20 = 30 + 2

Euler's formula for surfaces

Sphere : $V - E + F = 2$

Torus : $V - E + F = 0$

Double-torus : $V - E + F = -2$

Sphere with h handles : $2 - 2h$

Projective plane : $V - E + F = 1$

Klein bottle : $V - E + F = 0$

Sphere with k cross-caps : $2 - k$

Classification Theorem : knowing the following classifies a surface uniquely:

- the value of $V - E + F$
- how many pieces of boundary there are
- whether it is orientable

The Heawood Conjecture

For a surface with h holes $(h \geq 1)$

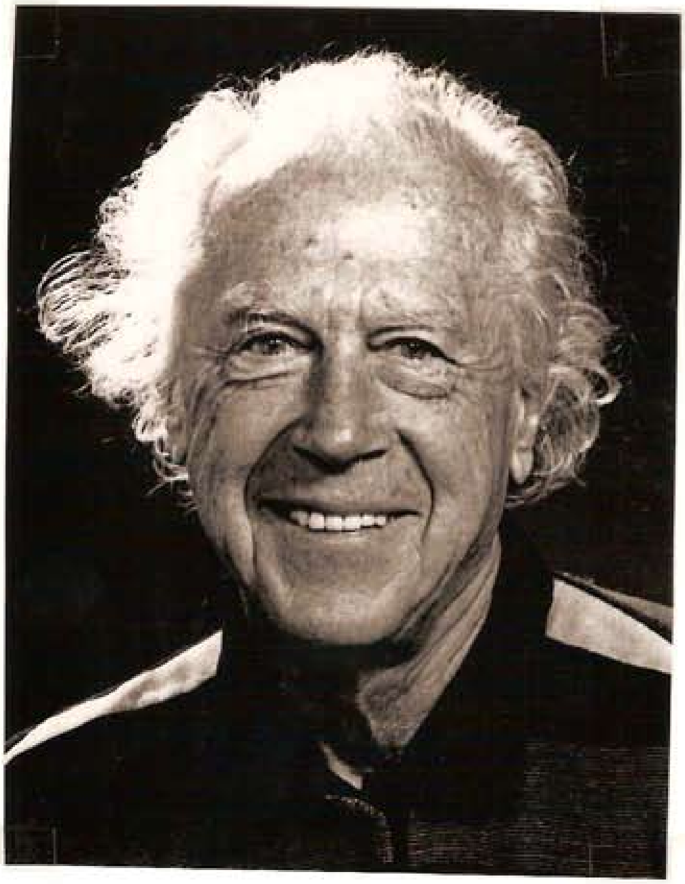
$\left[\frac{1}{2}\left(7+\sqrt{1+48h}\right)\right]$ colours suffice.

$h = 1$: $\left[\frac{1}{2}\left(7+\sqrt{49}\right)\right] = \left[\frac{1}{2}(7+7)\right] = 7$

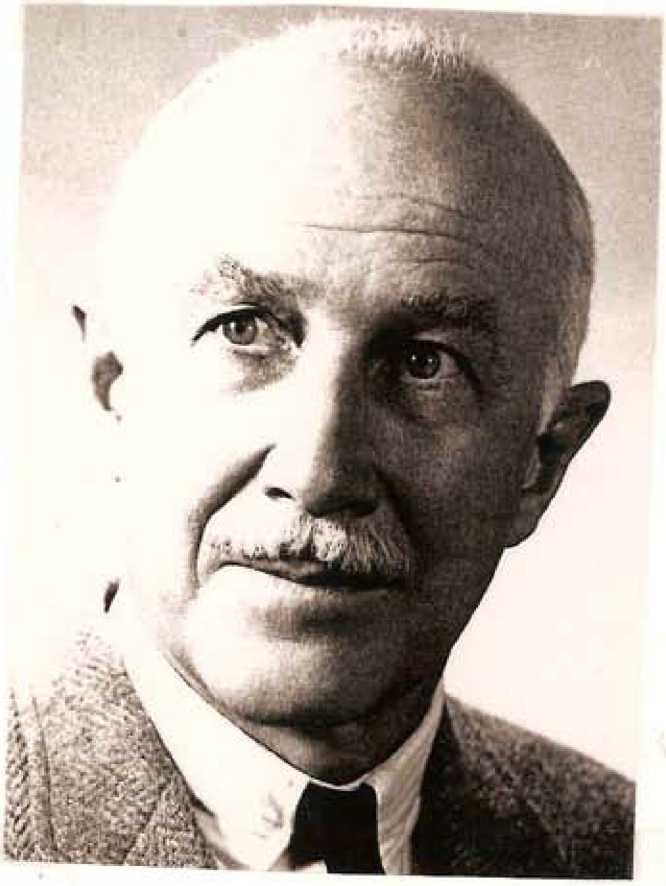
$h = 2$: $\left[\frac{1}{2}\left(7+\sqrt{97}\right)\right] = [8 \cdot 42 \ldots] = 8$ ...

Is this best possible?

Yes: G. Ringel & J.W.T. Youngs (1967-8)

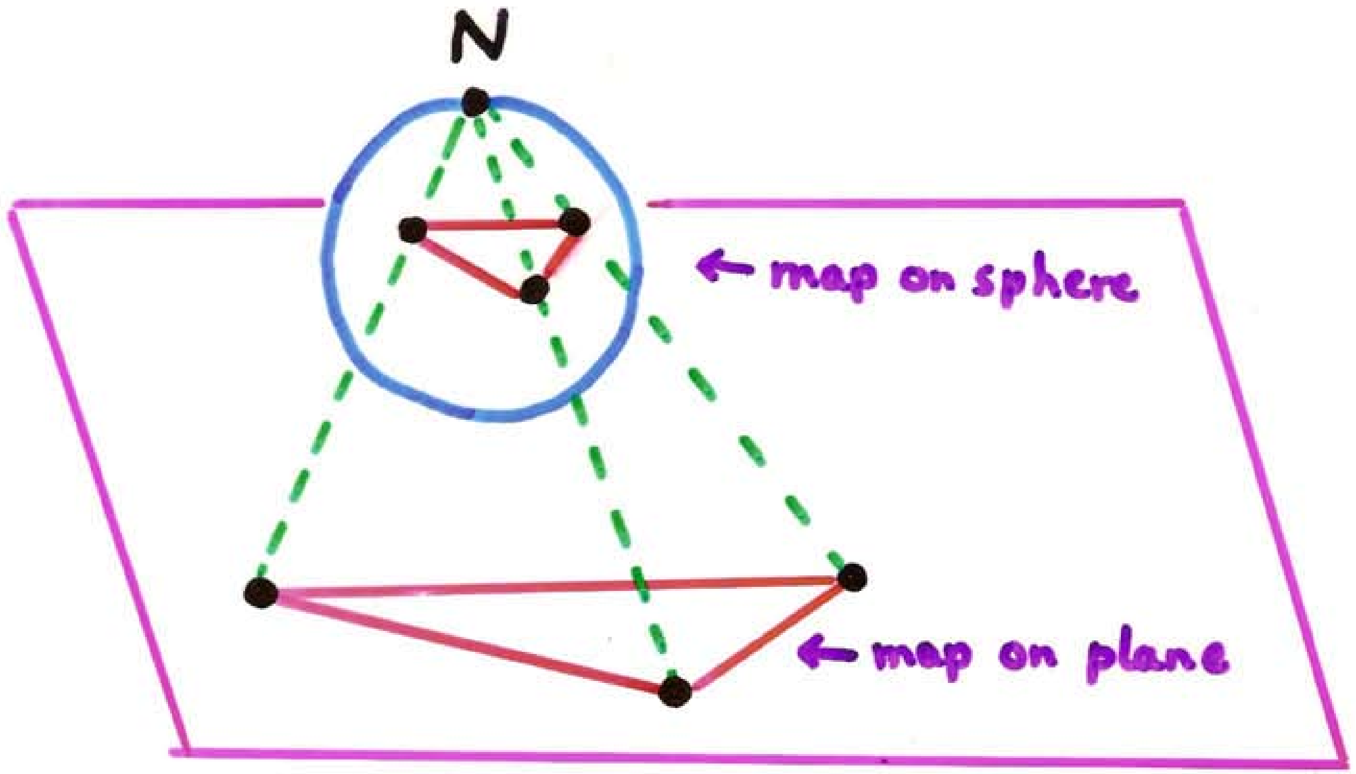


Gerhard Ringel



Ted Youngs

Maps on other surfaces



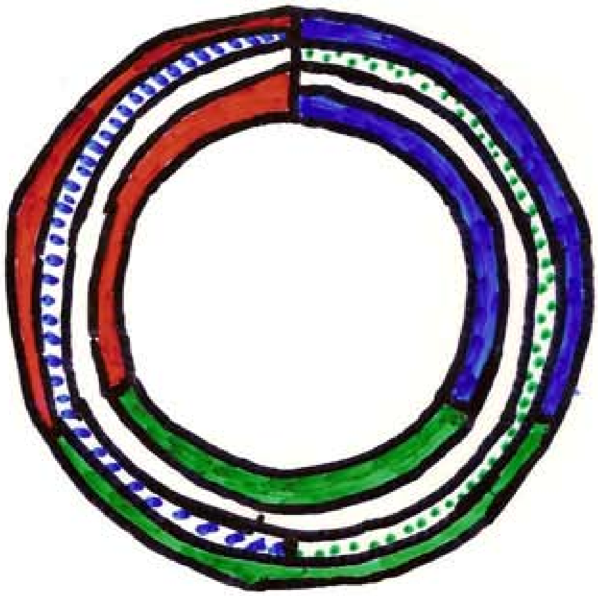
So the four-colour problem concerns maps on a sphere ...

What about other surfaces?

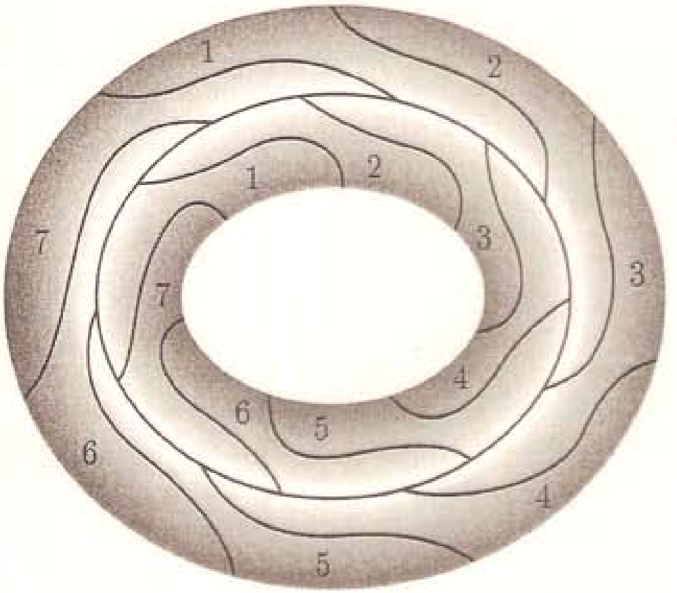
TORUS

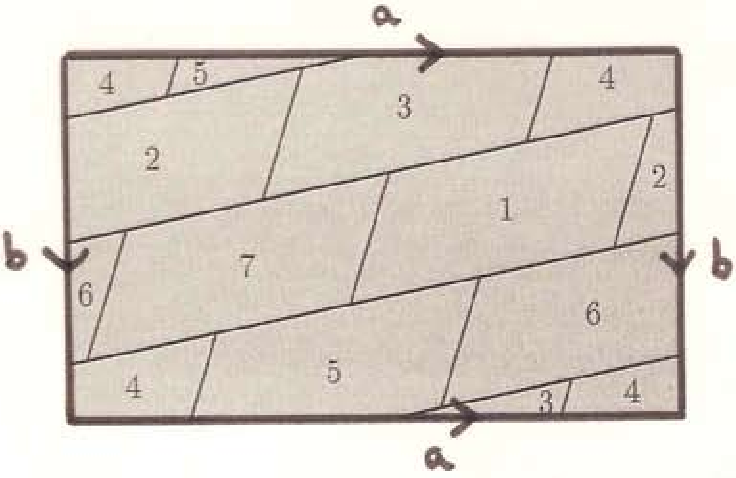
7 colours sufficient

– and sometimes necessary

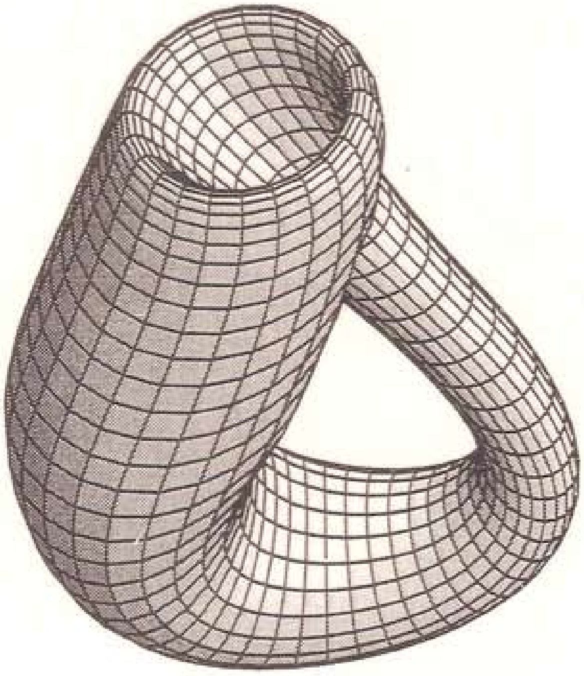


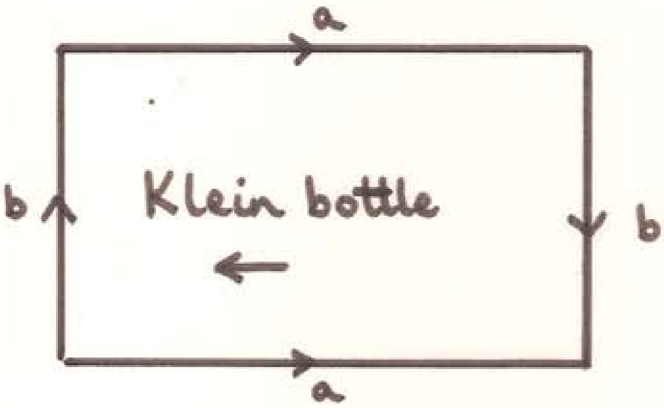
Maps on Surfaces

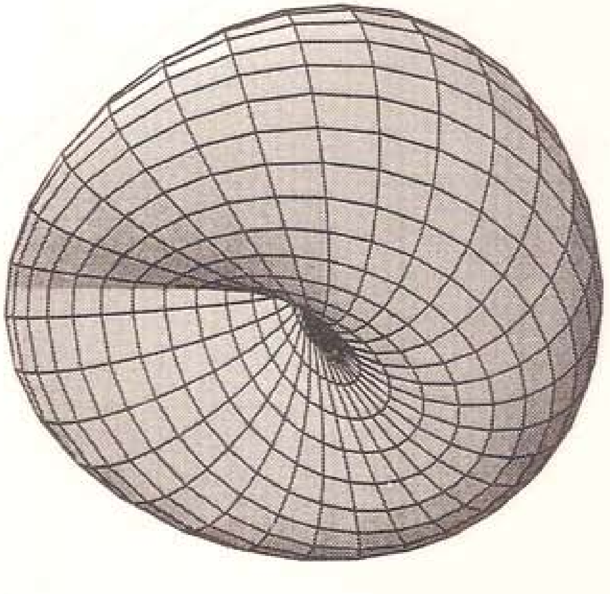




torus



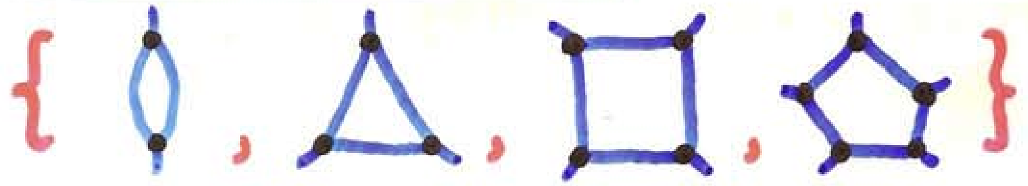




Kenneth Appel and Wolfgang Haken solved the four-colour problem by finding an unavoidable set of 1936 (later 1482) reducible configurations.

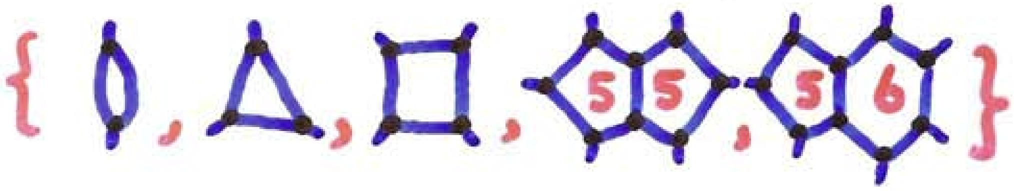
Proving the Four-Colour Theorem

Unavoidable sets



is an unavoidable set – every map contains at least one of them...

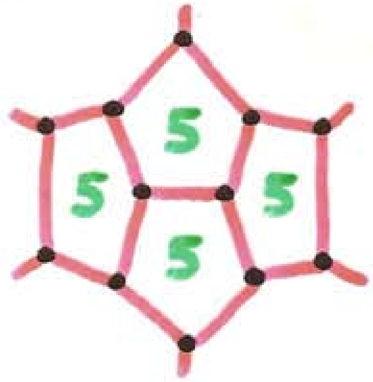
and so is :



Reducible configurations

are reducible

so is



'Birkhoff diamond' (1913)

Aim (Heinrich Heesch): solve the problem by finding an unavoidable set of reducible configurations.

FOUR COLOURS SUFFICE