Lamps, Factorizations and Finite Fields

BARTHOLDI, Laurent

Abstract
I answer a question from the 1993 International Mathematical Olympiads by constructing an equivalent algebraic problem, and unearth a surprising behaviour of some polynomials over the two-element field.


DOI : 10.2307/2695298
arxiv : math/9910056v1
LAMPS, FACTORIZATIONS AND FINITE FIELDS

LAURENT BARTHOLDI

1. Introduction

The origin of this study is the 1993 International Mathematical Olympiads, held at Istanbul, Turkey. Problem # 6, which occurred on day 2, reads:

Let \( n > 1 \) be an integer. There are \( n \) lamps \( L_0, \ldots, L_{n-1} \) arranged in a circle. Each lamp is either ON or OFF. A sequence of steps \( S_0, S_1, \ldots, S_j, \ldots \) is carried out. Step \( S_j \) affects the state of \( L_j \) only (leaving the state of all others lamps unaltered) as follows:

- if \( L_{j-1} \) is ON, \( S_j \) changes the state of \( L_j \) from ON to OFF or from OFF to ON;
- if \( L_{j-1} \) is OFF, \( S_j \) leaves the state of \( L_j \) unchanged.

The lamps are labeled mod \( n \), that is, \( L_{j-1} = L_{n-1}, L_0 = L_{n}, L_1 = L_{n+1}, \ldots \).

Initially all lamps are ON. Show that

(a) there is a positive integer \( M(n) \) such that after \( M(n) \) steps all the lamps are ON again;
(b) if \( n \) has the form \( 2^k \) then all the lamps are ON after \( n^2 - 1 \) steps;
(c) if \( n \) has the form \( 2^k + 1 \) then all the lamps are ON after \( n^2 - n + 1 \) steps.

In this note we answer the Olympiads question using elementary algebra over finite fields, and exhibit an interesting phenomenon when \( n \) is one less than a power of two. More generally, we are interested in the minimal time \( t(n) \geq 1 \) such that after repeating \( t(n) \) times the above instructions all lamps are again lit.

It turns out this question is tightly related to the factorization of the polynomial \( \Phi_n = X^n + X + 1 \) over the field \( \mathbb{F}_2 \). For \( n = 2^k \) or \( 2^k + 1 \) it has only small factors, and there is a surprising connection between the factorization of \( \Phi_n \) and that of \( \Phi_{2^n - 1} \).

Only undergraduate abstract algebra knowledge is assumed from the reader; however unsolved problems appear, for instance in Conjecture 2.5. It would be interesting to know by what means pre-university students solved this Olympiad problem.

2. An Algebraic Reformulation

We let a lamp’s state be represented by \( 0, 1 \in \mathbb{F}_2 \) for unlit and lit respectively, and number the lamps counterclockwise from 0 to \( n - 1 \) in such a way that we are about to alter the lamp at position \( n - 2 \). We denote by \( (a_0, \ldots, a_{n-1}) \) the lamps’ state. One step of evolution amounts then to the following: replace \( a_{n-2} \) by \( a_{n-2} + a_{n-1} \), and move to position \( n - 3 \). The process is invariant under rotation of the circle, so we may renumber the lamps so that we are again at position \( n - 2 \), and describe one step of evolution as the operation

\[
(a_0, \ldots, a_{n-1}) \mapsto (a_{n-1}, a_0, \ldots, a_{n-3}, a_{n-2} + a_{n-1}).
\]

In turn, the lamps’ state \( (a_0, \ldots, a_{n-1}) \) is conveniently encoded as a polynomial,

\[
f = \sum_{i=0}^{n-1} a_i X^i \in \mathbb{F}_2[X]/(X^n + X^{n-1} + 1).
\]

The reason \( f \) is represented as a polynomial in this peculiar ring is that one step of evolution described in [1] translates, in terms of polynomials, to the operation \( f \mapsto X \cdot f \). Indeed the direct translation of \( f \) in the polynomial ring is

\[
f \mapsto Xf + a_{n-1}(1 + X^{n-1} + X^n);
\]

Date: February 1, 2008.
or, in other words: the conversion from the list representation to the polynomial one is linear; a lit lamp at position $i$ corresponds to $X^i$, which evolves to $X^{i+1}$, and $i + 1$ is the new position of the lamp; and a lit lamp at position $n - 1$ corresponds to $X^{n-1}$, which evolves in $X^n = X^{n-1} + 1$, which maps back to the lamp at position 0 and a switched lamp at position $n - 1$.

Note now that $X$ is invertible: $1/X = X^{n-1} + X^{n-2}$. The ring in (2) is naturally isomorphic, via the map $X \mapsto X^{-1}$, to

$$R_n \overset{\text{def}}{=} \mathbb{F}_2[X]/(X^n + X + 1).$$

We shall consider the evolution \( 'f := X \cdot f' \) occurring in $R_n$; this amounts to consider the original question with time moving backwards.

We denote by $R_n^\times$ the group of invertible elements of $R_n$. The initial position corresponds to

$$f_0 = \sum_{i=0}^{n-1} X^i = \frac{X^n + 1}{X + 1} = X^{1-n} \in R_n^\times.$$

Thus

$$t(n) = \min\{t \geq 1 | X^t = 1 \text{ in } R_n\} = |\langle X \rangle|,$$

where $\langle X \rangle$ is viewed as a subgroup (not an ideal!) of $R_n^\times$. We have proved the

**Proposition 2.1.**

$$t(n) < \infty.$$

More precisely, $t(n) < 2^n$, and divides $|R_n^\times|$.

**Proof.** $t(n)$ is the order of a subgroup of $R_n^\times$, and $R_n^\times$ is a finite group of order at most $2^n - 1$. \( \square \)

We shall later give more details about the structure of $R_n^\times$; for now explicit values of $t(n)$ can be given in a few special cases:

**Proposition 2.2.** If $n$ is a power of two (say $n = 2^k$), then

$$t(n) = n^2 - 1.$$

**Proof.** We compute

$$X^{n^2} = (X^n)^n = (X + 1)^n = X^n + 1 = X,$$

so $X^{n^2-1} = 1$. Conversely, if $n \leq t < n^2 - n$, write $t = ni + j$ with $1 \leq i < n - 1$ and $0 \leq j < n$, and note that the polynomial $X^t = X^{ni+j} = (X + 1)^iX^j$ has degree at most $2n - 3$ and span $i$; write it as $f + X^n g$ with $f$ and $g$ of degree less than $n$. It is equal, in $R_n$, to $f + (X + 1)g$ where the two summands don’t overlap, and therefore cannot equal $X$. If $2 \leq t < n$, it is clear that $X^t \neq X$, and if $n^2 - n \leq t < n^2$ the same holds by symmetry. \( \square \)

**Proposition 2.3.** If $n$ is one more than a power of two (say $n = 2^k + 1$), then

$$t(n) = n^2 - n + 1.$$

**Proof.** We compute

$$X^{n^2} = (X^n)^n = (X + 1)^n = X^n + X^{n-1} + X + 1 = X^{n-1},$$

so $X^{n^2-n+1} = 1$. The argument in the proof of the previous proposition shows that no smaller value satisfies this equation. \( \square \)

In case $k$ is one less than a power of two, say $k = 2^n - 1$, there is a peculiar phenomenon:

**Proposition 2.4.** For all $n \geq 2$, \( t(2^n - 1) | 2^{t(n)} - 1 \).
Proof. In \( R_{2n-1} \), we may consider a subset

\[
Q_n = \{ \sum_{i=0}^{n-1} a_i X^{2i} \mid a_i \in \mathbb{F}_2 \}.
\]

It is a vector subspace of dimension \( n \), as the \( X^i \) are linearly independent for \( 0 \leq i < 2^n - 1 \). Elements of \( R_{2^n-1} \) are polynomials and therefore can be composed, an operation we denote by \( \circ \). This operation is internal to \( Q_n \), and endows \( Q_n \) with an \( \mathbb{F}_2 \)-algebra structure: \( f(g(X) + h(X)) = f(g(X)) + f(h(X)) \) as soon as all the monomials of \( f \) have degree a power of 2. Moreover, \( Q_n \) is Abelian (on the basis \( \{ X^i \} \) we have \( X^i \circ X^j = X^{ij} = X^j \circ X^i \)), and \( Q_n \cong R_n \) through the natural map \( X^i \mapsto X^{2^i} \) extended by linearity. Indeed

\[
X^{i+j} = X^i \cdot X^j \mapsto X^{2^i} \circ X^{2^j} = X^{2^{i+j}},
\]

and for any \( f \in \mathbb{F}_2[X] \)

\[
0 = f \cdot (X^n + X + 1) \mapsto \hat{f} \circ (X^{2^n} + X^2 + X),
\]

where \( \hat{f} \) is a polynomial divisible by \( X \). It follows that any polynomial representing 0 in \( Q_n \) maps to a multiple (for \( \circ \)) of \( X^{2^n} + X^2 + X \), which in turn represents 0 in \( R_{2^n-1} \).

Now the evolution \( 'f := X \cdot f' \) is mapped in \( Q_n \) to \( 'g := X^2 \circ g = g^2' \); thus for all \( t \) such that \( X^t = 1 \) in \( R_n \), one has \( X^{2t} = X \) in \( Q_n \), and \( X^{2^{t-1}} = 1 \) in \( R_{2^n-1} \).

The following conjecture relies on numerical evidence. It has been checked for \( n \leq 16 \) using GAP [3] and PARI-GP [4] and their finite field algorithms.

**Conjecture 2.5.** For all \( n \geq 2 \),

\[
t(2^n - 1) = 2^{t(n)} - 1.
\]

Recall that a polynomial \( f \in \mathbb{F}_2[X] \) is **primitive** if \( (\mathbb{F}_2[X]/f) \) is generated by \( X \). A striking consequence of Conjecture 2.5 is the following

**Conjecture-Corollary 2.6.** Let \( n_0 = 2 \) and define recursively \( n_{i+1} = 2^{n_i} - 1 \) for \( i \geq 0 \). Then \( X^{n_i} + X + 1 \) is irreducible and primitive in \( \mathbb{F}_2[X] \) for all \( i \geq 0 \).

**Proof.** \( \Phi_n \) is irreducible and primitive if and only if \( R_n \) is a field and \( R_n^{\times} \) is generated by \( X \); this is equivalent to \( t(n) = 2^n - 1 \), its maximal possible value. We have

\[
t(n_{i+1}) = 2^{t(n_i)} - 1 = 2^{2^{n_i} - 1} - 1 = 2^{n_{i+1}} - 1,
\]

the first and third equalities following from Conjecture 2.5 and the second from induction.

\[
3. \text{More Results on the Factorization of } X^n + X + 1
\]

We now turn to a more thorough study of the polynomial \( \Phi_n = X^n + X + 1 \) over \( \mathbb{F}_2 \). The behaviour of \( t(n) \) is closely related to the structure of the algebra \( R_n \), which in turn is determined by the factorization of \( \Phi_n \).

We denote by \( \chi \) the Frobenius automorphism [5, page 9] of \( R_n \). Recall that any algebra \( A \) over \( \mathbb{F}_2 \) has an endomorphism defined by \( \chi(g) = g^2 \); if \( A \) is a finite field of degree \( d \), then \( \chi \) is invertible, of order \( d \), and generates the Galois group \( \text{Gal}(A/\mathbb{F}_2) \).

We show first that \( \chi \) is invertible in \( R_n \). For this purpose, suppose \( g \in \mathbb{F}_2[X] \) satisfies \( g^2 \equiv 0 \mod \Phi_n \). It then follows that \( g \equiv 0 \mod \Phi_n \), by the

**Lemma 3.1.** The \( \Phi_n \) do not have repeated factors.

**Proof.** It suffices to show that \( \langle \Phi_n, \Phi'_n \rangle = 1 \); if \( n \) is even, then \( \Phi'_n = 1 \), while if \( n \) is odd, then \( \Phi'_n = X^{n-1} + 1 \) and

\[
\langle \Phi_n, \Phi'_n \rangle \mid \Phi_n - X \Phi'_n = 1.
\]
Table 1. Factorizations of $X^n + 1$ in $\mathbb{F}_2$ and corresponding $t(n)$ and $u(n)$ (see Lemma 3.2)

| $n$ | $(t(n) = |X|)/u(n)$ |
|-----|---------------------|
| 2   | 1                    |
| 3   | 1                    |
| 4   | 1                    |
| 5   | 1                    |
| 6   | 1                    |
| 7   | 1                    |
| 8   | 1                    |
| 9   | 1                    |
| 10  | 1                    |
| 11  | 1                    |
| 12  | 1                    |
| 13  | 1                    |
| 14  | 1                    |
| 15  | 1                    |
| 16  | 1                    |
| 17  | 1                    |
| 18  | 1                    |
| 19  | 1                    |
| 20  | 1                    |
| 21  | 1                    |
| 22  | 1                    |
| 23  | 1                    |
| 24  | 1                    |
| 25  | 1                    |
| 26  | 1                    |
| 27  | 1                    |
| 28  | 1                    |
| 29  | 1                    |
| 30  | 1                    |
| 31  | 1                    |
| 32  | 1                    |
| 33  | 1                    |
| 34  | 1                    |
| 35  | 1                    |
| 36  | 1                    |
| 37  | 1                    |
| 38  | 1                    |
| 39  | 1                    |
| 40  | 1                    |
| 41  | 1                    |
| 42  | 1                    |
| 43  | 1                    |
| 44  | 1                    |
| 45  | 1                    |
| 46  | 1                    |
| 47  | 1                    |
| 48  | 1                    |
| 49  | 1                    |
| 50  | 1                    |

As a consequence, $R_n$ is semisimple, i.e. decomposes as a direct sum of fields. Let $\Phi_n$ factor as $f_{n,1} \cdots f_{n,r_n}$, with $f_{n,i}$ irreducible polynomials of degree $d_{n,i}$. Then $R_n$ splits as

$$R_n = F_{n,1} \oplus \cdots \oplus F_{n,r_n},$$

where the $F_{n,i}$ are field extensions of $\mathbb{F}_2$ of degree $d_{n,i}$. Note then that the order of the Frobenius automorphism $\chi$ is $d_{n,i}$ in $F_{n,i}$ and, therefore is $\text{lcm}\{d_{n,i}\}_{1 \leq i \leq r_n}$ in $R_n$. The following lemma is straightforward:

Lemma 3.2. For $i \in \{1, \ldots, r_n\}$, let $\pi_i$ be the natural map $R_n \rightarrow F_{n,i}$. Then

$$t(n) = \text{lcm}\{(|\pi_i(X)|)\}_{1 \leq i \leq r}.$$

In particular, $t(n)$ divides $u(n) = \text{lcm}\{2^{d_{n,i}} - 1\}_{1 \leq i \leq r_n}$ (see Table 3).

Proposition 3.3. $\mathbb{F}_2[X]/\Phi_{2k} \overset{df}{=} A$ splits as a direct sum of fields of degree dividing $2k$.

$\mathbb{F}_2[X]/\Phi_{2k+1} \overset{df}{=} B$ splits in factors of degree dividing $3k$. 

Proper. Let us denote by $\psi : g \mapsto g^2$ the $k$-th power of the Frobenius automorphism. We must show that $\psi^2 = 1$ in $A$, and $\psi^3 = 1$ in $B$; but in $A$ we have $\psi(X) = 1 + X$ of order 2, and in $B$ we have $\psi(X) = \frac{1 + X}{X}$ of order 3.

This is in accordance with the results in the previous section: $t(n = 2^k) = n^2 - 1 = 2^{2k} - 1$, and $t(n = 2^k + 1) = n^2 - n + 1 | 2^{2k} - 1$. Remark that the two transformations $X \mapsto 1 + X$ and $X \mapsto \frac{1 + X}{X}$ of $R_n$ lift to $PGL_2(\mathbb{F}_2) = \text{Aut}(\mathbb{F}_2(X))$. These are the only possible “systematic lifts”, and explains the special behaviour of $R_{2^k}$ and $R_{2^k+1}$.

For any polynomial $f = \sum a_iX^i \in \mathbb{F}_2[X]$, let us denote by $\hat{f} = \sum a_iX^{2i} \in \mathbb{F}_2[X]$ the hat-polynomial of $f$. (Sometimes $\hat{f}$ is called a linearized polynomial or a 2-polynomial; see [3.4] or [8.3.4].) Hat-polynomials can be multiplied, but also composed as in the proof of Proposition 2.4. The composition operation $\circ$ is linear thanks to the fact that all monomials in hat-polynomials have degree a power of the field’s characteristic, 2; indeed

$$\hat{f} \circ \hat{g} = f(\chi)(\hat{g}) = \hat{f} \cdot \hat{g}.$$ 

Let us note $S_n \stackrel{\text{def}}{=} \mathbb{F}_2[X]/\hat{\Phi}_n = \mathbb{F}_2[X]/(X \cdot \Phi_{2^n-1})$; then for any $f \in R_n$ we may naturally see $\hat{f} \in \hat{R}_n \subset S_n$, and there is a natural embedding of $R_n$ in $\text{End}(\hat{R}_n)$ given by $f \mapsto f(\chi)$, with $f(\chi)(X) = \hat{f}$. Note that under this embedding $X$ maps to the Frobenius automorphism of $S_n$.

While $R_n$ decomposes as a direct sum, $S_n$ decomposes naturally as a tensor product. Recall that the tensor product of two algebras $A$ and $B$ with bases $\{a_i\}$ and $\{b_j\}$ respectively is the algebra with basis $\{a_i \otimes b_j\}$ and multiplication $(a_i \otimes b_j)(a_i' \otimes b_j') = a_i a_i' \otimes b_j b_j'$. If $A = \mathbb{F}_2[X]/f(X)$ and $B = \mathbb{F}_2[Y]/g(Y)$, one may take as bases $\{a_i = X^i\}$ and $\{b_j = Y^j\}$, whence $A \otimes B = \mathbb{F}_2[X,Y]/(f(X), g(Y))$.

**Proposition 3.4.** $S_n$ decomposes as

$$S_n = R_{2^n-1} \oplus \mathbb{F}_2 = \bigotimes \mathbb{F}_2[X]/f_{n,i} = \bigotimes \mathbb{F}_2[X]/(f_{n,i}/X) \oplus \mathbb{F}_2$$.

**Corollary 3.5.** If $\Phi_n$ factors in $r_n > 1$ factors, then $\Phi_{2^n-1}$ factors in at least $2^n - 1 > 1$ factors; if $f$ is a factor of $\Phi_n$, then $\hat{f}/X$ is a factor of $\Phi_{2^n-1}$.

Proof. The factors $f_{n,i}$ of $\Phi_n$ are irreducible, but the $f_{n,i}$ have at least two factors, one of them being $X$. According to the proposition,

$$S_n = R_{2^n-1} \oplus \mathbb{F}_2 = \bigotimes \mathbb{F}_2[X]/f_{n,i} = \bigotimes \mathbb{F}_2[X]/(f_{n,i}/X) \oplus \mathbb{F}_2.$$

If we distribute the $r_n$ direct sums over the tensor products, we obtain an expression of $S_n$ as a direct sum of $2^n$ algebras. Among these is $\mathbb{F}_2 = \mathbb{F}_2 \otimes \cdots \otimes \mathbb{F}_2$; all the $2^n - 1$ others are summands of $R_{2^n-1}$. Among these others are the $\mathbb{F}_2 \otimes \cdots \otimes \mathbb{F}_2[X]/(f_{n,i}/X) \otimes \cdots \otimes \mathbb{F}_2$.

**Proof of Proposition 3.4.** By Lemma 3.1, $\Phi_n$ factors as claimed. By induction, it suffices to consider a factorization $\Phi_n = fg$, with $f$ and $g$ coprime, and to show that in that case

$$S_n = \mathbb{F}_2[X]/\bar{\Phi}_n \cong \mathbb{F}_2[X]/\bar{f} \otimes \mathbb{F}_2[X]/\bar{g} = \mathbb{F}_2[Y,Z]/(\bar{f}(Y), \bar{g}(Z)).$$

As $f$ and $g$ are coprime, apply Bézout’s theorem to decompose the identity $1 = \alpha f + \beta g$, for $\alpha$ and $\beta$ polynomials. Apply the “hat” operator:

$$X = \hat{\alpha}(\hat{f}(X)) + \hat{\beta}(\hat{g}(X)).$$

We may now define the two mutually inverse maps

$$\mathbb{F}_2[X]/(\hat{f} \circ \hat{g}) \cong \mathbb{F}_2[Y,Z]/(\hat{f}(Y), \hat{g}(Z))$$

$$X \mapsto \hat{\beta}(Y) + \hat{\alpha}(Z)$$

$$\hat{g}(X) \mapsto Y, \quad \hat{f}(X) \mapsto Z.$$

$\square$
Really, this proposition is a dual version of the Chinese Remainder Theorem, and its proof draws largely on this fact: we constructed natural injections $F_2[X]/f_{n,i} \hookrightarrow S_n$ dual to the natural projections $R_n \twoheadrightarrow F_2[X]/f_{n,i}$.

The decomposition stated in Corollary 3.5 need not be complete, though, as the tensor product of fields need not be a field:

**Proposition 3.6.** Let $f$ and $g$ be two irreducible polynomials, so that $A = F_2[X]/f(X)$ and $B = F_2[Y]/g(Y)$ are fields. Then $A \otimes B = F_2[X,Y]/(f(X), g(Y))$ is a direct sum of gcd($\deg f, \deg g$) fields of degree lcm($\deg f, \deg g$); in particular, $A \otimes B$ is a field if and only if $\deg f$ and $\deg g$ are coprime.

**Proof.** $A \otimes B$ is semisimple and commutative whenever both $A$ and $B$ are, so $A \otimes B$ is a direct sum of fields. Let $\chi_A$ and $\chi_B$ be the Frobenius automorphisms of $A$ and $B$; then the Frobenius automorphism of $A \otimes B$ is $\chi = \chi_A \otimes \chi_B$, so is of order exactly lcm($\deg f, \deg g$), and all subfields of $A \otimes B$ are of degree at most lcm($\deg f, \deg g$). On the other hand, $A \otimes B$ splits as a sum of fields each containing $A$ and $B$ (see [2, page 54]).

We give an example of Corollary 3.5 in the first non-trivial case, $n = 5$: then $\Phi_5 = X^5 + X + 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$, so

$$R_n = F_2[X]/(X^2 + X + 1) \oplus F_2[Y]/(Y^3 + Y^2 + 1).$$

Let us note $f = X^2 + X + 1$, $g = Y^3 + Y^2 + 1$, and for convenience $F = \widehat{f}/X = X^3 + X + 1$ and $G = \widehat{g}/Y = Y^7 + Y^3 + 1$. Then

$$S_n = F_2[X]/\widehat{f} \otimes F_2[Y]/\widehat{g} = (F_2 \oplus F_2[X]/F) \otimes (F_2 \oplus F_2[Y]/G) = F_2 \oplus F_2[X]/F \oplus F_2[Y]/G \oplus F_2[X,Y]/(F,G) \oplus F_2[Z]/H,$$

where $H(Z) = \Phi_{31}(Z)/F(Z)/G(Z)$. This in turn factors

$$\Phi_{31} = \widehat{f}/X \cdot \widehat{g}/X \cdot \left( X \widehat{\circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \circ \c
References


Section de Mathématiques
Université de Genève
CP 240, 1211 Genève 24
Switzerland
E-mail address: Laurent.Bartholdi@math.unige.ch