MATHÉMATIQUES DE L'INFORMATIQUE

PRÉLIMINAIRES

Les candidats sont priés de respecter les notations de l'énoncé et la numérotation des questions.

Le but du problème est d'étudier les ensembles de mots définis par certaines propriétés de leurs sous-mots. Dans la première partie, on établit quelques résultats élémentaires sur les monoïdes reconnaissant un langage. La deuxième partie décrit un algorithme pour construire un automate reconnaissant l'ensemble des sous-mots d'un mot donné. On caractérise les langages reconnus par un monoïde ordonné dans les parties III et IV et ceux reconnus par un p-groupe dans la partie V. La partie II est indépendante du reste du problème et la partie V est indépendante des parties III et IV.

RAPPELS ET DÉFINITIONS GÉNÉRALES

Relations.

On appelle *relation de préordre* une relation réflexive et transitive. Si $\leqslant$ est une relation de préordre, la relation $\sim$ définie par $x \sim y$ si et seulement si $x \leqslant y$ et $y \leqslant x$ est une relation d'équivalence, appelée *relation d'équivalence associée à* $\leqslant$.

Monoïdes.

On appelle *monoïde* un ensemble M muni d'une loi de composition interne $(x, y) \mapsto xy$, associative et admettant un élément neutre, noté 1. Soit x un élément de M. On pose $x^0 = 1$ et, pour tout entier $n \geqslant 0$, $x^{n+1} = x^n x$.

Soit M un monoïde. Un *sous-monoïde* de M est une partie N de M contenant 1 et telle que si $x, y \in$ N alors $xy \in$ N.

Soient M et N deux monoïdes. Une application φ de M dans N est un *morphisme de monoïdes* si $\varphi(1) = 1$ et si, pour tout x, y dans M, $\varphi(xy) = \varphi(x)\varphi(y)$. Si de plus φ est surjectif, on dit que N est un *quotient* de M. Si φ est bijectif on dit que φ est un *isomorphisme.*

Soient M_1 et M_2 deux monoïdes. Le produit cartésien $M_1 \times M_2$, muni de la loi de composition interne $(m_1, m_2)(n_1, n_2) = (m_1 n_1, m_2 n_2)$ est un monoïde, appelé *produit* de M_1 et M_2.

On appelle *congruence* sur un monoïde M une relation d'équivalence R sur M telle que pour tout x, y, z da M, x R y entraîne xz R yz et zx R zy. On appelle *index de la congruence* le cardinal de l'ensemble quotient M/R.

Monoïde libre.

Soit A un ensemble fini appelé *alphabet*. On note A* l'ensemble des mots sur l'alphabet A. On appelle *lettr* les éléments de A, et on note 1 le mot vide. Tout mot s'écrit de façon unique sous la forme $u = a_1 a_2 \dots a_n$ av $n \geqslant 0$ et où $a_1, a_2, \dots, a_n$ sont des lettres.

Le produit des mots $a_1 a_2 \dots a_n$ et $b_1 b_2 \dots b_m$ est le mot $a_1 a_2 \dots a_n\, b_1 b_2 \dots b_m$. Muni de cette loi de compositio A* est un monoïde. On admettra la propriété « universelle » suivante :

« toute application φ de A dans un monoïde M se prolonge de façon unique en un morphisme de monoïde de A* dans M. Ce prolongement est défini par les formules $\varphi(1) = 1$ et, pour tout mot non vide $u = a_1 \dots a_n$ par $\varphi(u) = \varphi(a_1) \dots \varphi(a_n)$. »

Mots.

On dit qu'un mot u est *facteur* d'un mot v s'il existe des mots x et y (éventuellement vides) tels que $v = xuy$.

On dit qu'on mot $u = a_1 \dots a_n$ est *sous-mot* d'un mot v s'il existe une suite $v_0, v_1, \dots, v_n$ de mots (éventuellement vides) telle que $v = v_0 a_1 v_1 a_2 \dots a_n v_n$. Ainsi le mot *aba* est un sous-mot de *caccbac* mais n'est pas facteur de ce mot.

La longueur d'un mot u est notée $| u |$.

Langages.

On appelle *langage* tout sous-ensemble de A*. Une *algèbre de Boole de langages* (sur A*) est un ensemble $\mathcal{B}$ de langages tel que :

i) $\varnothing \in \mathcal{B}$.

ii) Si $L_1 \in \mathcal{B}$ et $L_2 \in \mathcal{B}$, alors $L_1 \cap L_2 \in \mathcal{B}$.

iii) Si $L \in \mathcal{B}$ alors $A^* \backslash L \in \mathcal{B}$.

Automates.

On appelle automate sur l'alphabet A un quintuplet $\mathcal{A} = (Q, A, \delta, q_0, F)$, où

Q est un ensemble fini, appelé ensemble des états,

δ est une application de $Q \times A$ dans Q,

q_0 est un élément de Q (l'état initial),

F est un sous-ensemble de Q (l'ensemble des états finaux).

L'application δ se prolonge en une application $(q, u) \mapsto q \cdot u$ de $Q \times A^*$ dans Q en posant, pour tout $q \in Q$, $u \in A^*$ et $a \in A$, $q \cdot 1 = q$ et $q \cdot (ua) = \delta(q \cdot u, a)$.

Le langage reconnu par $\mathcal{A}$ est le langage $L = \{ u \in A^* \mid q_0 \cdot u \in F \}$.

Idéaux.

Soit I un idéal d'un anneau et soit n un entier positif. On note I^n l'idéal engendré par les éléments de la forme $x_1 x_2 \dots x_n$, où $x_1, x_2, \dots, x_n$ sont des éléments de I.

I

1° Soit $\sim$ une congruence sur un monoïde M et soit $\pi : M \to M/\sim$ l'application canonique de M sur l'ensemble quotient $M/\sim$. Montrer qu'il existe une unique structure de monoïde sur $M/\sim$ telle que π soit un morphisme de monoïdes.

2° Soient $\sim_1$ et $\sim_2$ deux congruences sur un monoïde M telles que, pour tout x, y dans M, $x \sim_1 y$ entraîne $x \sim_2 y$. Démontrer qu'il existe un morphisme de monoïdes surjectif de $M/\sim_1$ sur $M/\sim_2$.

3° On dit qu'un langage L de A^* est reconnu par un monoïde M s'il existe un morphisme de monoïdes η de A^* dans M et une partie P de M telle que $L = \eta^{-1}(P)$.

a. Montrer que si M est quotient d'un monoïde N, N reconnaît également L (on pourra utiliser la propriété universelle de A^* pour construire un morphisme de monoïdes de A^* dans N).

b. Montrer que M reconnaît également le langage $A^* \backslash L$.

c. Montrer que si un monoïde M_1 (respectivement M_2) reconnaît un langage L_1 (respectivement L_2), le monoïde $M_1 \times M_2$ reconnaît $L_1 \cap L_2$.

4° Soit $\mathcal{A} = (Q, A, \delta, q_0, F)$ un automate sur l'alphabet A et soit L le langage de A^* reconnu par $\mathcal{A}$. On note $\mathcal{C}(Q)$ le monoïde des applications de Q dans lui-même muni de la loi de composition $(f, g) \to fg = g \circ f$. À chaque mot u de A^*, on associe l'application $\overline{u} \in \mathcal{C}(Q)$ définie par $\overline{u}(q) = q.u$.

a. Montrer que l'application $u \to \overline{u}$ définit un morphisme de monoïdes de A^* dans $\mathcal{C}(Q)$.

b. Montrer que $\mathcal{C}(Q)$ reconnaît L.

5° Soit η un morphisme de monoïdes de A^* dans un monoïde fini M et soit P une partie de M. On pose $L = \eta^{-1}(P)$.

a. Montrer que l'automate $\mathcal{A} = (M, A, \delta, 1, P)$ — où δ est définie par $\delta(m, a) = m\eta(a)$ — reconnaît le langage L.

b. Montrer qu'un langage est rationnel (ou « régulier ») si, et seulement si, il est reconnu par un monoïde fini.

II

On donne ci-dessous l'en-tête et deux procédures du programme « sous-mots ».

```
program sous_mots (input, output);

const

    taille_max = 25;      (* taille maximum de l'alphabet *)

    long_max = 100;       (* longueur maximum des mots *)

type
    mot = array [1...long_max] of integer;
var

    k, m : integer;

    t : array [1...taille_max] of integer;

    u : mot;

    procedure entree;
```

```
var
    i : integer;
begin
    write ('Donnez le nombre de lettres de l''alphabet : ');
    readln(k);
    begin
        write( 'Donnez la longueur du mot : ');
        readln(m);
        for i := 1 to m do begin
            write( 'Donnez la lettre numero ', i , ' : a ');
            readln(u[i])
        end
    end
end;
procedure automate (k, m: integer; u: mot);
var
    i, j: integer;
begin
    writeln( 'L' 'ensemble des etats est (0,..., ', m + 1, ') ');
    for j := 1 to k do begin
        writeln( 'delta( ', m + 1, ', a ', j, ')= ', m + 1);
        writeln( 'delta( ', m, ', a ',j , ')= ', m + 1);
        t[j] := m + 1
    end;
    for i := m - 1 downto 0 do
        for j := 1 to k do begin
            if j = u[i + 1] then
                t[j] := i + 1;
            writeln( 'delta( ', i, ', a ', j, ')= ', t[j])
    end;
writeln( 'L' 'etat initial est 0; ');
writeln( 'Tous les etats sauf ', m + 1, 'sont des etats finaux. ')
end;
```

La procédure « entree » permet de fixer la taille k de l'alphabet, puis de donner un mot u sur l'alphabet $\{ a_1, ..., a_k \}$ en précisant d'abord sa longueur m. Le mot u est représenté en fait par une suite finie d'entiers de l'ensemble $\{ 1, ..., k \}$. Ainsi, pour $k = 3$, le mot $a_1a_3a_2a_1$ est représenté par la suite 1,3,2,1. Dans la suite, on ne fera plus la distinction entre un mot et sa représentation par une suite d'entiers.

1° Donner sans démonstration le résultat de l'exécution de la procédure « automate » lorsque $k = 2$, $m = 4$ et lorsque u est le mot $a_1a_2a_1a_1$.

2° De façon générale, si u est un mot de longueur m sur l'alphabet $\{a_1, ..., a_k\}$, l'exécution de la procédure « automate » permet de définir un automate $\mathcal{A}(k, m, u) = (Q, A, \delta, q_0, F)$ où $Q = \{0,1, ..., m+1\}$, $A = \{a_1, ..., a_k\}$, $q_0 = 0$, $F = \{0,1, ..., m\}$ et où δ est l'application « delta » décrite lors de l'exécution de la procédure.

a. Démontrer que pour tout entier i tel que $0 \leqslant i \leqslant m$, et pour tout $a \in A$, $i + 1 \leqslant \delta(i, a) \leqslant \delta(i + 1, a)$.

b. On pose $u = b_1 ... b_m$ (où $b_1, ..., b_m \in A$). Démontrer que pour tout entier i tel que $0 \leqslant i < m$, $\delta(i, b_{i+1}) = i + 1$.

3° *a.* Démontrer que si i et j sont des entiers tels que $0 \leqslant i < j \leqslant m + 1$, alors $\delta(i, b_j) \leqslant j$.

b. Démontrer que l'automate $\mathcal{A}(k, m, u)$ reconnaît l'ensemble des sous-mots de u.

4° Calculer en fonction de k et de m le nombre d'exécutions de l'instruction « writeln » lors de l'exécution de la procédure « automate ».

III

Soit n un entier positif ou nul. On définit une relation $\leqslant_n$ sur A^* par $u \leqslant_n v$ si et seulement si tout sous-mot de longueur inférieure ou égale à n de u est sous-mot de v.

1° Montrer que $\leqslant_n$ est une relation de préordre. On notera $\sim_n$ la relation d'équivalence associée à $\leqslant_n$.

a. Montrer que $\sim_n$ est une congruence d'index fini sur A^*.

b. On suppose (pour cette question uniquement) que A est un alphabet de 2 lettres. Calculer l'index de $\sim_1$ et montrer que pour $n \geqslant 2$, l'index de $\sim_n$ est supérieur ou égal à 2^{n+1}.

2° Pour tout mot u, on pose $S(u) = \{v \in A^* \mid u \text{ est un sous-mot de } v\}$, et on note $\mathcal{J}_n$ l'algèbre de Boole engendrée par les langages $S(u)$ tels que $|u| \leqslant n$. Montrer qu'un langage L est dans $\mathcal{J}_n$ si et seulement si L est union de classes d'équivalence de $\sim_n$.

3° On dit qu'un monoïde M est ordonné s'il existe une relation d'ordre $\leqslant$ définie sur M et telle que :

pour tout $x \in M$, $x \leqslant 1$, et,

pour tout x, y, z dans M, $x \leqslant y$ entraîne $xz \leqslant yz$ et $zx \leqslant zy$.

a. Montrer que le monoïde $S_n(A) = A^*/\sim_n$ est ordonné.

b. Soit M un monoïde ordonné et soit η un morphisme de monoïdes surjectif de A^* dans M. On suppose que toute suite strictement décroissante d'éléments de M est de longueur inférieure ou égale à $n + 1$. Montrer que si $u \sim_n v$ alors $\eta(u) = \eta(v)$.

c. En déduire que M est quotient de $S_n(A)$ et que tout langage reconnu par M est élément de $\mathcal{J}_n$.

IV

Soit M un monoïde. On définit une relation $\leqslant_J$ sur M en posant $x \leqslant_J y$ si, et seulement si, il existe des éléments s et t de M tels que $x = syt$. Le monoïde M est dit J-trivial si la relation $\leqslant_J$ est une relation d'ordre.

1° *a.* Montrer que dans tout monoïde M, $\leqslant_J$ est une relation de préordre mais pas nécessairement une relation d'ordre (on donnera un contre-exemple explicite).

b. Soit E un ensemble fini. Si R et S sont deux relations sur E, on définit une relation RS en posant, pour tout $x, y \in E$:

x RS y si, et seulement si, il existe $z \in E$ tel que x R z et z S y.

On note $\mathcal{R}(E)$ l'ensemble des relations réflexives sur E. Montrer que $\mathcal{R}(E)$, muni de la loi de composition (R,S) $\to$ RS, est un monoïde J-trivial.

c. Montrer qu'un monoïde ordonné est J-trivial.

d. Soit M l'ensemble de matrices à coefficients entiers suivant :

$$M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

Montrer que M muni de la multiplication usuelle des matrices est un monoïde J-trivial non ordonné.

2° Soit M un monoïde *fini*. Démontrer l'équivalence des conditions i), ii) et iii). (On pourra montrer successivement l'équivalence de i) et ii) puis celle de i) et iii).)

i) Il existe un entier n tel que, pour tout x, y dans M, $(xy)^n x = (xy)^n = y(xy)^n$.

ii) Il existe un entier n tel que, pour tout x, y dans M, $(xy)^n = (yx)^n$ et $x^n = x^{n+1}$.

iii) M est J-trivial.

3° Soit M un monoïde fini J-trivial.

a. Montrer que tout sous-monoïde et tout quotient de M sont également J-triviaux.

b. Montrer que le produit de deux monoïdes finis J-triviaux est J-trivial.

4° Soit M un monoïde fini J-trivial.

a. Montrer que M contient un élément minimum pour l'ordre $\leqslant_J$, qui sera noté 0. Vérifier que, pour tout $x \in M$, $0 \leqslant_J x \leqslant_J 1$ et $0x = 0 = x0$.

b. On note N(M) l'ensemble des éléments minimaux de $M \setminus \{0\}$ pour l'ordre $\leqslant_J$. Montrer que pour tout $n \in N(M)$, l'ensemble $M \setminus \{n\}$, muni de la loi de composition interne $*$ définie par

$$x * y = \begin{cases} xy & \text{si } xy \neq n \\ 0 & \text{sinon} \end{cases}$$

est un monoïde, que l'on notera M_n. Montrer que l'application π_n de M dans M_n, définie par $\pi_n(x) = x$ si $x \neq n$ et $\pi_n(n) = 0$, est un morphisme de monoïdes.

c. On suppose que $N(M) = \{n_1, n_2, \ldots, n_r\}$ avec $r \geqslant 2$. Montrer que l'application π de M dans $M_{n_1} \times M_{n_2} \times \ldots \times M_{n_r}$ définie par $\pi(m) = (\pi_{n_1}(m), \pi_{n_2}(m), \ldots, \pi_{n_r}(m))$ est un morphisme de monoïdes injectif.

5° Pour tout entier positif n, on note P(n) la propriété suivante :

« si M est un monoïde J-trivial tel que Card M $\leqslant n$, alors M est quotient d'un monoïde ordonné fini ».
On se propose d'établir P(n) par récurrence sur n. P(1) étant trivialement vérifiée, on suppose que P(n) est vraie pour un certain entier $n > 0$ et on considère un monoïde J-trivial M tel que Card M $= n + 1$.

a. Montrer que si Card N(M) $\geqslant 2$, M est quotient d'un monoïde ordonné fini.

b. On suppose désormais $N(M) = \{n\}$. Montrer que si $n^2 = n$, $M \setminus \{0\}$ est un sous-monoïde de M. En déduire que M est quotient d'un monoïde ordonné fini.

6° On suppose maintenant $n^2 \neq n$.

a. Démontrer que $n^2 = 0$.

b. Montrer qu'il existe un alphabet fini A, un monoïde ordonné fini T et des morphismes de monoïdes surjectifs, φ de A^* sur M, α de A^* sur T et β de T sur M_n, tels que $\pi_n \circ \varphi = \beta \circ \alpha$.

7° Soit $\leqslant_A$ la relation définie sur A^* par $u \leqslant_A v$ si et seulement si

(*) $\alpha(u) \leqslant \alpha(v)$, et

(**) pour toute factorisation du type $u = u_0 a u_1$ avec $u_0 \in A^*$, $u_1 \in A^*$ et $a \in A \cup \{1\}$, il existe une factorisation du type $v = v_0 b v_1$ avec $v_0 \in A^*$, $v_1 \in A^*$ et $b = a$ ou $b = 1$, telle que :

$$\alpha(u_0) \leqslant \alpha(v_0) \text{ et } \alpha(u_1) \leqslant \alpha(v_1)$$

a. Établir que $\leqslant_A$ est une relation de préordre sur A^* et que pour tout mot u de A^*, $u \leqslant_A 1$.

b. Montrer que si u, v et w sont des mots tels que $u \leqslant_A v$, alors $uw \leqslant_A vw$ et $wu \leqslant_A wv$.

8° Soit $\sim_A$ la relation d'équivalence associée au préordre $\leqslant_A$.

a. Montrer que $\sim_A$ est une congruence d'index fini.

b. Montrer que pour tout $u, v \in A^*$, $u \sim_A v$ entraîne $\varphi(u) = \varphi(v)$.

c. En déduire que M est quotient d'un monoïde ordonné fini.

9° On note $\mathcal{J}$ la réunion des ensembles $\mathcal{J}_n$ définis au III-2°.

a. Vérifier que $\mathcal{J}$ est une algèbre de Boole.

b. Démontrer que, pour tout langage L, les conditions suivantes sont équivalentes :

i) L est reconnu par un monoïde J-trivial fini,

ii) L est reconnu par un monoïde ordonné fini,

iii) $L \in \mathcal{J}$.

V

Soit k un corps commutatif et M un monoïde. On note k[M] l'ensemble des sommes formelles de la forme $\alpha = \sum_{m \in M} \alpha_m m$, où $(\alpha_m)_{m \in M}$ est une famille presque nulle d'éléments de k (c'est-à-dire telle que $\alpha_m = 0$ sauf pour un nombre *fini* d'éléments de M). On admettra que k[M], muni des trois opérations suivantes :

$$\sum_{m \in M} \alpha_m m + \sum_{m \in M} \beta_m m = \sum_{m \in M} (\alpha_m + \beta_m) m$$

$$\left(\sum_{m \in M} \alpha_m m\right)\left(\sum_{m \in M} \beta_m m\right) = \sum_{m \in M} \sum_{st = m} (\alpha_s \beta_t) m$$

$$\lambda \left(\sum_{m \in M} \alpha_m m\right) = \sum_{m \in M} (\lambda \alpha_m) m \text{ (où } \lambda \text{ désigne un élément de } k)$$

est une k-algèbre unitaire.

Étant donné deux mots u et v, on note $\binom{v}{u}$ le nombre de façons distinctes d'écrire u comme sous-mot de v. Plus formellement, si $u = a_1 \dots a_n$,

$$\binom{v}{u} = \text{Card } \{ (v_0, v_1, \dots, v_n) \in A^* \times \dots \times A^* \mid v = v_0 a_1 v_1 \dots a_n v_n \}.$$

Par exemple, $\binom{abab}{ab} = 3$ et $\binom{aabbaa}{aba} = 8$.

1° Soit a une lettre. Montrer que si n et m sont des entiers tels que $0 \leqslant m \leqslant n$, on a $\binom{a^n}{a^m} = \binom{n}{m}$.

2° Soient u et v deux mots et soient a et b deux lettres. Établir les formules

(*) $\binom{va}{ub} = \binom{v}{ub} + \delta_{a,b} \binom{v}{u}$ où $\delta_{a,b} = 1$ si $a = b$ et $\delta_{a,b} = 0$ si $a \neq b$.

(**) $\binom{v}{1} = 1$.

(***) $\binom{1}{u} = 0$ si $u \neq 1$

et montrer que ces trois formules suffisent à déterminer $\binom{v}{u}$ pour tous les mots u et v.

3° On prend $M = A^*$. Dans ce cas, un élément de $k[A^*]$ est appelé polynôme en variables non commutative à coefficients dans k. Montrer qu'il existe un unique automorphisme d'algèbre μ (respectivement σ) sur $k[A^*]$ te que $\mu(a) = 1 + a$ (respectivement $\sigma(a) = 1 - a$) pour tout $a \in A$. Calculer $\mu(aba)$.

4° On prend $k = Q$, le corps des rationnels.

a. Vérifier que pour tout mot v

$$\mu(v) = \sum_{u \in A^*} \binom{v}{u} u$$

$$\sigma(v) = \sum_{u \in A^*} (-1)^{|u|} \binom{v}{u} u$$

b. En déduire que pour tous mots u, v, w

$$\binom{uv}{w} = \sum_{w_1 w_2 = w} \binom{u}{w_1}\binom{v}{w_2}$$

5° Soit p un nombre premier et w un mot. On définit une relation $\equiv_w$ sur A^* en posant $u \equiv_w v$ si, et seulement si, pour tout facteur x de w, $\binom{u}{x} \equiv \binom{v}{x} \bmod p$.

a. Montrer que $\equiv_w$ est une congruence d'index fini sur A^*.

b. Montrer que pour tout mot u, $u^{p^{|w|}} \equiv_w 1$.

c. En déduire que le monoïde quotient $A^*/\equiv_w$ est un p-groupe (c'est-à-dire un groupe fini dont l'ordre est une puissance de p).

6° Soit w un mot et soit i un entier tel que $0 \leqslant i < p$. On pose

$$L_{w,i} = \left\{ v \in A^* \mid \binom{v}{w} \equiv i \bmod p \right\}$$

a. Montrer que $L_{w,i}$ est union de classes d'équivalence de la congruence $\equiv_w$.

b. En déduire que $L_{w,i}$ est reconnu par un p-groupe.

c. Soit $\mathcal{G}_p$ l'algèbre de Boole engendrée par les langages de la forme $L_{w,i}$ (où $w \in A^*$ et $0 \leqslant i < p$). Montrer que si $L \in \mathcal{G}_p$, alors L est reconnu par un p-groupe.

7° Soit n un entier positif ou nul. On définit une relation $\equiv_n$ sur A^* en posant $u \equiv_n v$ si et seulement si $u \equiv_w v$ pour tout mot w tel que $|w| \leqslant n$.

a. Montrer que $\equiv_n$ est une congruence et que le monoïde quotient $G_n = A^*/\equiv_n$ est un p-groupe.

b. Décrire G_0 et G_1.

8° Soit l'ensemble des éléments $\alpha = \sum_{u \in A^*} \alpha_u u$ de $\mathbb{Z}/p\mathbb{Z}\,[A^*]$ tels que $\sum_{u \in A^*} \alpha_u = 0$.

a. Montrer que I est un idéal engendré par les éléments de la forme $(1 - a)$ avec $a \in A$.

b. En déduire que $\sigma(I^{n+1})$ est l'idéal engendré par les éléments de la forme w où $|w| > n$.

c. Soient u et v deux mots. Montrer que $u \equiv_n v$ si et seulement si $u - v \in I^{n+1}$.

9° Soit G un p-groupe non trivial.

a. Démontrer qu'il existe un élément x de G, différent de 1, tel que $x^p = 1$ et tel que, pour tout $g \in G$, $xg = gx$.

b. Soit G' le sous-groupe de G engendré par x et soit $H = G/G'$. On note γ l'homomorphisme de groupe canonique de G sur H. Montrer que γ se prolonge de façon unique en un homomorphisme d'algèbre de $\mathbb{Z}/p\mathbb{Z}[G]$ dans $\mathbb{Z}/p\mathbb{Z}[H]$.

c. On pose $K = \gamma^{-1}(0)$. Montrer que K est égal à l'idéal engendré par $(1 - x)$.

d. Montrer que $(1 - x)^p = 0$ et en déduire que $K^p = 0$.

10° Soit I_G (respectivement I_H) l'idéal de $\mathbb{Z}/p\mathbb{Z}[G]$ (respectivement de $\mathbb{Z}/p\mathbb{Z}[H]$) engendré par les éléments de la forme $1 - g$ où $g \in G$ (respectivement $g \in H$).

a. Montrer que $\gamma(I_G) = I_H$.

b. Montrer par récurrence sur r que si G est un p-groupe d'ordre p^r, alors $I_G^{p^r} = 0$.

11° Soit G un p-groupe d'ordre p^r et soit η un morphisme de monoïdes surjectif de A^* dans G. On pose $n = p^r - 1$.

a. Montrer que si $u \equiv_n v$, alors $\eta(u) = \eta(v)$.

b. En déduire que G est quotient de G_n.

12° Soit L un langage de A^* reconnu par un p-groupe.

a. Montrer qu'il existe un entier positif n tel que G_n reconnaisse L.

b. En déduire que $L \in \mathcal{G}_p$ si et seulement si L est reconnu par un p-groupe.