INDUCTION

1. *Soit A l'alphabet {(,)}, soit L le sous ensemble de A* formé des mots dont tous les préfixes contiennent au moins autant de (que de)*
a) Donnez une définition inductive de L et la prouver.
b) Montrez que L n'est pas égal à l'ensemble des mots bien parenthésés. Comment peut-on associer à un mot de L, un mot bien parenthésé.
c) Prouvez soit que le schéma donné en a) est libre soit qu'il est ambigu.

PREMIERE SOLUTION
Une définition possible est
Base : ε est dans M
Règles :Si m et m' sont dans M alors (m et (m)m' sont dans M

M est inclus dans L par induction structurelle, en effet ε appartient à L et si tout préfixe de m et de m' comprennent au moins autant de (que de), alors il en est de même de (m et de (m)m', les préfixes de (m)m' étant de la forme (p_m ou (m)$p_{m'}$, p_m étant un préfixe de m et $p_{m'}$ un préfixe de m'.

Réciproquement, soit m un mot de longueur n, soit p_i le préfixe de m composé des i premières lettres, et soit diff(m,i)= le nombre de (dans p_i moins le nombre de).
Notons que m appartient à L si et seulement si diff(m,i) ≥ 0, pour tout i, 1≤ i ≤ n. En particulier tout mot de L commence par la lettre (.

Montrons par récurrence sur n que tout mot de L appartient à M.

Base Si n=0, m=ε et donc m appartient à M

Etape inductive
Supposons que tout mot de L de longueur strictement inférieure à n appartient à M

Soit u un mot de L, de longueur n
Premier cas : diff(u,i)>0 pour tout i $1 \le i \le n$
Si u n'est pas le mot vide, alors u = (u', et comme diff(u,i) = diff(u',i-1)+1, diff(u',j) ≥ 0, pour tout j $1 \le j \le n-1$, et donc u' appartient à L. Comme u' est de longueur n-1, par hypothèse de récurrence u' appartient à M. Donc u appartient à M par définition de M.

Deuxième cas : il existe k tel que diff(u,k)=0
Soit j le plus petit entier tel que diff(u,j)=0. On a donc diff(u,i) > 0, pour tout i $1 \le i \le j-1$. La $j^{ième}$ lettre de u est nécessairement un). Soit m tel que p_j=(m). Comme diff(u,k) = 1+diff(m,k-1), m appartient à L, et par hypothèse de récurrence à M. Soit m' le mot éventuellement vide tel que m=p_jm', on a diff(m,k)=diff(m',k-i), et donc m' aussi appartient à L et par récurrence à M. On a donc u=(m)m', avec m et m' dans M, donc u appartient à M.

DEUXIEME SOLUTION
Une autre définition possible est
Base : ε et (sont dans M
Règles :Si m et m' sont dans M alors (m) et mm' sont dans M

M est inclus dans L par induction structurelle, en effet ε et (sont dans L et si tout préfixe de m et de m' comprennent au moins autant de (que de), alors il en est de même de (m) - dont les préfixes non vides sont de la forme (p_m, et de mm' - dont les préfixes sont de la forme p_m ou $mp_{m'}$

En utilisant les mêmes notations que pour la première définition, **montrons par récurrence sur la longueur des mots que tout mot de L est dans M.**

Base : le mot vide est bien dans M
Hypothèse de récurrence : Tout mot de L de longueur inférieure à n est dans M

Soit u un mot de L de longueur n.
Premier cas diff(u,i)>0, pour tout i $1 \leq i \leq n$
Alors u = (m', où m' est un mot de L. Si m' est le mot vide alors u = (appartient à M. Sinon

- Ou bien la dernière lettre de m' est un (. Dans ce cas u = (u'(, et (u' est dans L et par hypothèse d'induction il est aussi dans M. Par définition de M, u = (u'(est donc dans M.
- Ou bien la dernière lettre de m' est un). Dans ce cas u = (u') et u' est dans L et par hypothèse d'induction il est aussi dans M. Par définition de M u = (u') est donc aussi dans M.

Deuxième cas il existe k tel que diff(u,k)=0,
Choisissons pour k, le plus petit entier tel que diff(u,k) = 0. Soit m=p_k et m' tel que u=mm'. m et m' sont dans L.

- Si m' n'est pas le mot vide alors la longueur de m et de m' est inférieur à n et donc par hypothèse d'induction ils sont tous les deux dans M et donc u aussi appartient à M.
- Si m' est le mot vide (k=n), alors u=(m), avec m dans L et donc dans M. En conséquence, u est dans M.

Question b)

Le mot (est dans M mais n'est pas bien parenthésé. En fait il suffit d'ajouter en fin d'un mot de M le nombre de) nécessaires pour équilibrer le nombre de) et de (pour rendre ce mot bien parenthésé.

Question c)

Le premier schéma donné en a) n'est pas libre, en effet le mot (() peut être dérivé soit avec la règle (m et m=(), soit avec la règle (m)m' avec m=(et m' vide.
Le second schéma n'est pas libre non plus, le mot (((peut être dérivé par la règle mm' avec m=(m'=((, soit avec m'=(, m=((.

2. *Soient Var et Op deux alphabets disjoints.*
On pose A= Var U Op.
On appelle langage des expressions polonaises préfixées le langage L sur A défini par le schéma :
Base $Var \subset L$
Règle Si $\omega \in Op$, $u,v \in L$, alors $\omega uv \in L$
En supposant que Var={0,1,2,3,4,5,6,7,8,9}
et Op={+,-,/,}, le mot*
*+ + * 2 4 - 5 7 - 4 + 3 2 est-il dans L?*

Montrez qu'un mot w de A appartient à L si et seulement si il vérifie les deux conditions suivantes :*
i)w contient une variable de plus que d'opérateurs
ii) tout préfixe propre p de w contient au moins autant d'opérateurs que de variables
Montrez que le schéma définissant L est libre.

Le mot est dans L, on peut l'obtenir de la manière suivante

3,2	⇒	+ 3 2
4, +3 2	⇒	-4 + 3 2
2 4	⇒	* 2 4
5 7	⇒	- 5 7
* 2 4, - 5 7	⇒	+* 2 4 - 5 7
+* 2 4 - 5 7, -4 + 3 2	⇒	++* 2 4 - 5 7 -4 + 3 2

Montrons par induction structurelle sur L que tout mot m de L vérifie les 2 propriétés.
Pour la suite de l'exercice nous introduisons les notations suivantes :

- Pour un mot m, var(m) désignera le nombre de variables dans m.
- Pour un mot m, op(m) désignera le nombre d'opérateurs dans m.
- Pour un mot m, diff(m) = op(m) – var(m).

Avec cette notation les deux propriétés deviennent:

i. diff(w) = -1
ii. pour tout préfixe propre p de w diff(p) ≥ 0.

Si m est dans la base, alors var(m)=1 et op(m)=0 et m n'a aucun préfixe propre, donc les deux propriétés sont vérifiées.

Supposons que u et v vérifient les deux propriétés, alors ωuv vérifie aussi les deux propriétés.
En effet par hypothèse :
var(u) = op(u)+1 et var(v) = op(v)+1, donc var (ωuv) = var(u)+var(v) = op(u)+1+op(v)+1 = op(ωuv)+1.
Et donc ωuv vérifie la première propriété

Pour montrer que ωuv vérifie la seconde propriété, examinons p un préfixe propre quelconque de ωuv.
Cas 1, p= ω, alors p vérifie bien var(p) = 0 ≤ 1 = op(p).
Cas 2 $p=\omega p_u$ où p_u est un préfixe propre de u.
Par hypothèse d'induction $var(p_u) \leq op(p_u)$, et donc var(p) ≤ op(p).
Cas 3 $p=\omega u p_v$ où p_v est un préfixe de v ($p_v \neq v$).
Par hypothèse d'induction var(u) = op(u)+1 et $var(p_v) \leq op(p_v)$, et donc var(p) ≤ op(p).

Réciproquement, montrons par induction sur la longueur du mot que si un mot vérifie les deux propriétés, alors il appartient à L.

Soit w un mot vérifiant les deux propriétés, c'est à dire tel que diff(w)=-1 et diff(p) ≥ 0 pour tout préfixe propre p de w.

Si w est de longueur 1, alors w est une variable (à cause de la propriété 1) et w appartient à L.

Sinon supposons que tout mot de longueur inférieure où égale à n vérifiant les deux propriétés est dans L.

Soit w un mot de longueur n+1, vérifiant les deux conditions, alors nécessairement ce mot commence par un opérateur : w=ωp (remarque : on ne peux pas dire ici que p vérifie les propriétés i et ii parce que ce n'est pas vrai, on va chercher deux mots u et v qui vérifient les propriétés (et qui donc par hypothèse de récurrence seront dans L, tels que p =uv)

Appelons p_i le préfixe de p comportant i lettres.
Puisque ωp_i est un préfixe de w, diff(ωp_1) ≥ 0, d'autre part puisque ωp_n =w, on a diff(ωp_n)=1. Donc il existe i, 1≤ i tel que pour tout j<i, diff(ωp_j)>0 et diff(ωp_i) =0 - i est le plus petit entier tel que diff(ωp_i) =0.
Puisque ω est un opérateur, on a donc pour tout j<i, diff(p_j) ≥ 0 et diff(p_i) = -1.

Donc p_i vérifie les deux propriétés, comme il est de longueur strictement inférieure à n, il est donc dans L.
Soit r tel que $w = \omega p_i r$. Puisque $diff(\omega p_i) = 0$, r lui aussi vérifie les deux conditions. Comme r est de longueur strictement inférieure à n, il appartient à L, il en est donc de même pour w.

Montrons que le schéma est non ambigu

Soit w un mot de L, ayant n lettres, et supposons qu'il existe deux opérateurs o_1 et o_2 et quatre mots de L u_1, v_1, u_2, v_2 tels que $w = o_1 u_1 v_1 = o_2 u_2 v_2$.

Nécessairement $o_1 = o_2$

Si u_1 et u_2 sont de la même longueur, alors ils doivent être égaux.
Sinon, supposons $u_2 = u_1 s$. Alors u_1 étant un mot de L , $\delta(u_1) = 1$, mais par ailleurs u_1 est un préfixe propre de u_2 donc $\delta(u_2) < 0$, contradiction.

Donc nécessairement u_1 et u_2 sont de la même longueur.
On a donc $u_1=u_2$ et $v_1=v_2$.

3. *Comme pour la fonction factorielle, donnez des définitions inductives des fonctions:*
Add_m
Multiply_by_m

Add_m(0)=m
Add_m(n+1)=Add_m(n)+1

Ou

```
public int addM(int n){
     if (n==0) return 1
     else return 1+addM(n-1)
}
```

Multiply_by_m(0)=0
Multiply_by_m(n+1)= Multiply_by_m(n)+m

Ou

```
public int Multiply_by_M(int n){
     if (n==0) return 0
     else return m+ Multiply_by_M (n-1)
}
```

4. *On défini les ensemble E,F,G et H par*

E : Base 0 et 1 sont dans E ; Règle Si n est dans E, alors n+2 est dans E
*F : Base 0 est dans F ; Règle Si n est dans F, alors 2*n est dans F*
*G : Base 0 est dans G ; Règle Si n est dans G, alors 2*n+1 est dans G*
*H : Base 0 est dans H ; Règles Si n est dans H, alors 2*n est dans H. Si n est dans H, alors 2*n+1 est dans H*
a) A quoi sont égaux ces 4 ensembles ? Les schémas sont ils libres?

b) En vous appuyant sur une définition inductive de N, donnez une définition inductive des fonctions n modulo 2, division entière de n par 2 et écriture de n en base deux.

E) L'ensemble E est égal à N.
Tout élément de E est dans N, par induction structurelle sur E (ajouter 2 à un entier donne un entier)
Tout élément de N est dans E, par récurrence sur N:

0 et 1 sont dans E.

Supposons que tout entier < k soit dans E

Soit l'entier k, on peut le supposer au moins égal à 2 (les autres cas sont réglés dans la base) et donc k-2 est en entier qui par hypothèse de récurrence est dans E, donc par définition de E, k est lui aussi dans E.

Le schéma est libre : 0et 1 sont dans la base et ne peuvent être le résultat de la règle. Tout entier ≥ 2 peut être fabriqué par LA règle à partir de n-2 uniquement.

F) L'ensemble F est réduit au nombre 0, ce qui se voit aisément par induction structurelle sur F. Le schéma n'est pas libre 0 est dans la base et peut être engendré par la règle.

G) L'ensemble G, est égal au sous ensemble de N formé des entiers qui sont égaux à une puissance de 2 moins un. Notons G' ce sous-ensemble.

Clairement G est inclus dans G' par induction structurelle (il suffit de vérifier que 1 = 2-1 et que si $n=2^k-1$ alors $2n+1 =2(2^k-1)+1 =2^{k+1}-1$).

Réciproquement, on peut montrer que G' est inclus dans G, en montrant par récurrence sur k que 2^k-1 est dans G

Si k=1, c'est vrai.

Supposons le résultat vrai pour k, soit l'entier $2^{k+1}-1$, par hypothèse de récurrence l'entier 2^k-1 est dans G, donc définition de G, il est de même de $2(2^k-1)+1 =2^{k+1}-1$

Le schéma est libre.

H) L'ensemble H est égal à N

H est inclus dans N par induction structurelle.

N est inclus dans H.

Montrons par récurrence sur k que k appartient à H.

Si k=0, c'est vrai car 0 est dans la base de H.

Soit k un entier non nul, supposons que tous les entiers inférieur à k soit dans H.

Si k est pair, k=2k', et k'<k, donc par hypothèse de récurrence k' est dans H, donc par définition de H, k=2k' est aussi dans H.

Si k est impair, k=2k'+1, et par hypothèse de récurrence k' est dans H, donc par définition de H, k=2k'+1 est aussi dans H.

Le schéma n'est pas libre tel que car n est dans la base et est aussi résultat de la règle un appliqué à n=0. On peut modifier le schéma pour le rendre libre :

Base 0 est dans H

Règles *Si n non nul est dans H, alors 2*n est dans H*

*Si n est dans H, alors 2*n+1 est dans H*

---

b) Pour donner une définition inductive de la fonction n modulo 2, on peut utiliser le fait que N=E .
On définira alors la fonction modulo 2 par

0 mod 2 = 0
1 mod 2 = 1
n+2 mod 2 = n mod 2

Ce qui pourrait se programmer sous la forme

```
Public int mod2 (int n) {
     (if n==0 | n==1)  {return n}
               else return (mod2(n-2))}
}
```

Pour définir n / 2 , on peut aussi utiliser N=E,
On définira alors la fonction division entière par deux par

0/2 =0
1/2 =0
(n+2)/2 = n/2 +1

Ce qui pourrait se programmer sous la forme

```
Public int div2 (int n) {
     (if n==0 | n==1)  {return 0}
               else return (div(n-2)+1 )}
}
```

Pour définir la fonction écriture en base deux de n, on peut utilise le fait que N=H,
On définira alors a fonction écriture en base deux par

Ecriture(0) = 0
Ecriture(1) = 1
Si n > 0, Ecriture(2n) = Ecriture(n).0
Si n > 0, Ecriture(2n+1) = Ecriture(n).1

5. *Définir inductivement les fonctions de N^2 dans N :*

Addition de deux entiers
Multiplication de deux entiers
Calcul de m^n.

Add(0,0=0
Add(n+1,0)=n+1
Add(m,n+1)=Add(m,n)+1

ou

```
public int add (int m, int n) {
     if (n==0) return m
          else return add (m,n-1)+1
}
```

Mult(0,0)=0
Mult(n+1,0)=0
Mult(m,n+1)=Mult(m,n)+m

ou

```
public int mult (int m, int n) {
     if (n==0) return 0
          else return mult (m,n-1)+m
}
```

Puiss(0,0)=0
Puiss(n+1,0)=1
Puiss(m,n+1)=Puiss(m,n)*m

ou

```
public int puiss (int m, int n) {
     if (n==0) {if (m==0) return 0 else return 1}
          else return puiss (m,n-1)*m
}
```

6. *Définir inductivement la fonction* μ *de* A^* ----> A^* *telle que* $\mu(x_1x_2\ldots x_n)=x_n\ldots x_2x_1$

Base $\mu(\varepsilon) = \varepsilon$

Règle Si $u \in A^*$ et $x \in A$, $\mu(xu) = \mu(u)x$

Preuve : Montrons par induction structurelle sur A^* que

$\forall\ m \in A^*$, $\mu(m) = inv(m)$ où inv désigne l'inverse.

Base : $\mu(\varepsilon) = \varepsilon = inv(\varepsilon)$.

Supposons $\mu(m) = inv(m)$, alors $\mu(am)= \mu(m)a=inv(m)a=inv(am)$.