Correction - ENS Maths/Info 2012

Merci de signaler les erreurs à l'adresse suivante : mickaelpechaud (arobase) gmail (point) com.

Partie 1 : Algèbre des séries formelles

1. $(X_F)^0 = 1_F$, le neutre pour la multiplication.
   On montre par récurrence que pour tout $n \in \mathbb{N}^*$, la suite associée à $(X_F)^n$ est la suite $(0, 0, \dots, 0, 1, 0, 0, \dots)$ constituée de zéros et d'un unique 1 en position n.
   L'initialisation est triviale.
   Supposons le résultat vrai pour $n \in \mathbb{N}^*$. On note s_n la suite associée à $(X_F)^n$, t_n celle associée à X_F, et u_n celle associée à $(X_F)^{n+1}$.
   Par définition, $(X_F)^{n+1} = (X_F)^n X_F$, d'où $\forall k \in \mathbb{N}$, $u_k = \displaystyle\sum_{j=0}^{k} s_j t_{k-j}$.
   Un terme de cette somme est non-nul Ssi $j = n$ (par hypothèse de récurrence) et $k - j = 1$, ce qui impose $k = n + 1$. On a donc $u_{n+1} = 1$, et $u_k = 0$ pour tout $k \neq n + 1$, d'où l'hérédité.

2. - Soit $f : \mathbb{R}[X] \to \mathbb{R}[[X]]$, définie par $f(\displaystyle\sum_{k=0}^{n} a_k X^k) = \sum_{k=0}^{n} a_k (X_F)^k$.
     f est trivialement une application linéaire, et par définition, on a bien $\forall n \in \mathbb{N}$ $f(X^n) = (X_F)^n$.
   - Montrons qu'il s'agit d'un morphisme d'algèbre. On a déjà $f(1) = f(X^0) = X_F^0 = 1_F$ d'après la question précédente.
     Soit $P = \sum_{k=0}^{n} a_k X_k$ et $Q = \sum_{k=0}^{p} b_p X_p$. Par linéarité de f, et en utilisant la question précédente, on a
     $f(PQ) = f(\displaystyle\sum_{k=0}^{n+p}(\sum_{j=0}^{k} a_j b_{k-j}) X^k) = \sum_{k=0}^{n+p}(\sum_{j=0}^{k} a_j b_{k-j}) f(X^k) = \sum_{k=0}^{n+p}(\sum_{j=0}^{k} a_j b_{k-j})(X_f)^k$ – qui est la série formelle de terme général $\sum_{j=0}^{k} a_j b_{k-j}$, c'est-à-dire $f(P)f(Q)$.
   - L'injectivité est triviale : par définition de f, l'unique antécédent de O_F est le polynôme nul.
   - L'unicité est triviale : si $g(X^n) = (X_F)^n$ pour tout $n \in \mathbb{N}$, alors par linéarité de f et de g, pour tout polynôme $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$, on a , $g(P) = g(\sum_{k=0}^{n} a_k X^k) = \sum_{k=0}^{n} a_k g(X^k) = \sum_{k=0}^{n} a_k f(X^k) = f(P)$.

3. (a) Oh, la belle erreur d'énoncé... On utilisera plutôt $\frac{1}{\nu(S-T)+1}$ pour éviter les divisions par 0.
   - Par définition, $d(S, T) = 0 \Leftrightarrow S = T$.
   - Toujours par définition, $d(S, T) \geq 0$.
   - Soient S, T, U trois séries formelles. Si au moins deux séries parmi les trois sont égales, on a trivialement $d(S, U) \leq d(S, T) + d(T, U)$. Sinon, $\nu(S, T)$ est le plus petit indice tel que $s_i \neq t_i$, et $\nu(T, U)$ est le plus petit indice tel que $t_i \neq u_i$. Pour tout $i < \min\{\nu(S, T), \nu(T, U)\}$, on a $s_i = t_i = u_i$. On en déduit que $\nu(S, U) \geq \min\{\nu(S, T), \nu(T, U)\}$, d'où $\frac{1}{\nu(S,U)+1} \leq \frac{1}{\min\{\nu(S,T),\nu(T,U)\}+1}$.
     Si $\nu(S, T) \leq \nu(T, U)$, alors $d(S, U) = \frac{1}{\nu(S,U)+1} \leq \frac{1}{\min\{\nu(S,T),\nu(T,U)\}+1} = \frac{1}{\nu(S,T)+1} \leq \frac{1}{\nu(S,T)+1} = d(S, T) \leq d(S, T) + d(T, U)$, et de même dans le cas symétrique.
     d est donc bien une distance sur $\mathbb{R}[[X]]$.

(b) On considère 1_F et 2.1_F. Si d dérivait d'une norme $\|.\|$, on aurait $d(0_F, 1_F) = \|1_F\| = \frac{1}{2}\|2.1_F\| = \frac{1}{2}d(0_F, 2.1_F)$.
Or $d(0_F, 1_F) = 1$, et $d(0_F, 2.1_F) = 1$ – donc d ne dérive pas d'une norme.

4. On suppose $S.T = 0_F$. On raisonne par l'absurde, et l'on suppose que $S \neq 0$ et $T \neq 0$. On note $i = \nu(S)$ et $j = \nu(T)$ (par définition, on a donc $s_i = t_j = 0$).
Si l'on note $U = S.T$, on a donc $u_{i+j} = \sum_{k=0}^{i+j} s_k t_{i+j-k} = s_i.t_j \neq 0$: absurde (tous les autres termes de la somme sont nuls par minimalité de i et j).

5. (a) • Supposons que $P_n(X)$ converge vers P_∞.
Par définition, $\lim \nu(P_n(X), P_\infty) = +\infty$. Pour n_0 assez grand, $\nu(P_n(X), P_\infty) \geq 2$, d'où les 2 premiers termes de P_∞ sont 1 et $(1/n_0)$. Mais alors, pour tout $n > n_0$, $1/n \neq 1/n_0$, d'où $\nu(P_n(X), P_\infty) = 1$, ce qui est en contradiction avec la divergence de cette quantité vers $+\infty$.
• Sur $\mathbb{R}[X]$, P_n converge vers 1 au sens par exemple de la norme $\|P\|_\infty = \max_{x\in[0,1]} |P(x)|$.

(b) • **Condition nécessaire** : si $U^{(n)}$ converge vers U, alors par définition, $\lim \nu(U^{(n)} - U) = +\infty$. Si $k \in \mathbb{N}$, pour n assez grand, on a $\nu(U^{(n)} - U) > k$, d'où $u_k^{(n)} = u_k$.
• **Condition suffisante** : supposons que pour tout $k \in \mathbb{N}$, $(u_k^{(n)})_n$ soit ultimement constante et égale à u_k.
On fixe $k \in \mathbb{N}$. Soit n_0 assez grand pour que $\forall n \geq n_0\ \forall j \in [\![0, k]\!]$, $u_j^n = u_k$ (un tel n_0 existe, car il y a un nombre fini de suites $(u_j^n)_n$ considérées).
Alors, pour tout $n \geq n_0$, on a $d(U^{(n)}, U) > k$.
On en déduit que $(U^{(n)})$ converge vers U.

(c) Notons $U^{(n)} = \displaystyle\sum_{k=0}^{n} V^{(k)}$. On a donc $U^{(n+1)} - U^n = V^{(n+1)}$ pour $n \geq 0$ et $V^{(0)} = U^{(0)}$.
$(U^n)_n$ converge Ssi $(\sum_{k=0}^n V^{(k)})_k$ Ssi pour tout $j \in \mathbb{N}$ $\sum_{k=0}^n v_j^{(k)}$ est ultimement constante Ssi pour tout $j \in \mathbb{N}$, $(v_j^{(k)})_k$ est ultimement nulle Ssi pour tout $j \in \mathbb{N}$ $(U^{(k)} - U^{k-1})_j$ est ultimement nulle Ssi pour tout $j \in \mathbb{N}$ $(U^{(k+1)} - U^k)$ converge vers 0_F.

6. Soit $j \in \mathbb{N}$. Par définition de S_n, $(\sum_n S_n)_j$ est constante à partir de la $j+1^{\text{ème}}$ somme partielle (ensuite ne sont rajoutés que de $(X_F)^n$, avec $n > j$, dont le terme d'indice j est nul), et vaut u_j. D'après la question 1.5.b, $(\sum_n S_n)$ converge donc vers $\sum u_n X^n$.

7. Je pense que vous devriez y arriver...

Partie 2 : Équations de séries formelles

1. • Supposons l'existence de T telle que $S = (X_F)^k.T$. Soit $j < k$. On a $s_j = \sum_{i=0}^{j}((X_F)^k)_i t_{j-i}$. Pour tout $i \in [\![0, j]\!]$, $((X_F)^k)_i = 0$, car $i < k$. On a donc $s_j = 0$, d'où $\nu(S) \geq k$.
• Réciproquement, si $\nu(S) \geq k$, on définit T par $\forall j \in \mathbb{N}$, $t_j = s_{j+k}$. On vérifie alors (à faire !) que $S = (X_F)^k.T$.

2. (a) On doit avoir $s_0 t_0 = 1$, et pour tout $k \in \mathbb{N}^*$, $\displaystyle\sum_{i=0}^{k} s_i t_{k-i} = 0$.

(b) Supposons $s_0 \neq 0$. On montre par récurrence forte sur $k \in \mathbb{N}$ l'existence de t_k satisfaisant les équations ci-dessus.
Pour l'initialisation, on pose $t_0 = \dfrac{1}{s_0}$. Si le résultat est vrai jusqu'à $k \in \mathbb{N}$, on pose $t_{k+1} = -\dfrac{1}{s_0}\displaystyle\sum_{i=1}^{k+1} s_i t_{k+1-i}$, et l'égalité ci-dessus est vérifiée.
L'existence de l'inverse est prouvée (l'unicité également au passage).
Si $s_0 = 0$, l'équation $s_0 t_0$ ne peut pas être satisfaite, et donc S n'admet pas d'inverse.

(c) $t_0 = \frac{1}{0!} = 1$.
$t_1 = -s_1 t_0 = -1$.
$t_2 = -s_1 t_1 - s_2 t_0 = 1 - 2 = -1$.
$t_3 = -s_1 t_2 - s_2 t_1 - s_3 t_0 = 1 + 2 - 6 = -3$.

3. (a) Soient S_1 et S_2 solutions de l'équation. On a $P - Q.S_1 = P - Q.S_2$, d'où $Q.(S_1 - S_2) = 0$, puis $S_1 = S_2$ d'après la question 1.4.

   (b) Supposons $Q(0) \neq 0$. Notons Q^{-1} l'inverse de Q, qui existe d'après la question 2.2.b. On a alors (par associativité du produit...) $P - Q.(Q^{-1}.P) = 0$: $Q^{-1}.P$ est donc solution.

   (c) Si $Q(0) \neq 0$, l'équation admet une solution d'après la question précédente.
   Supposons donc $Q(0) = 0$. D'après des calculs déjà menés ci-dessus, $\nu(Q.S) \geq \nu(Q)$ pour tout série formelle S. Si l'équation admet une solution, on a donc $\nu(P) \geq \nu(Q)$.
   Réciproquement, supposons $\nu(P) \geq \nu(Q)$. Notons $k = \nu(Q)$. D'après la question 2.1, il existe deux séries formelles $\hat{P}$ et $\hat{Q}$ telles que $P = (X_F)^k.\hat{P}$ et $Q = (X_F)^k.\hat{Q}$.
   On a depuis $\hat{Q}_0 \neq 0$, et $\hat{Q}$ est donc inversible. Notons alors $S = \hat{Q}^{-1}.\hat{P}$.
   On a alors $P - Q.S = P - (X_F)^k.\hat{Q}\hat{Q}^{-1}.\hat{P} = P - (X_F)^k.\hat{P} = P - P = 0$. S est donc solution de l'équation, et le résultat est prouvé.

4. $S = \sum_{n=0}^{+\infty} s_n X^n = s_0 + s_n X + \sum_{n=2}^{+\infty}(s_{n-1} + s_{n-2})X^n = s_0 + s_1 X_F + \sum_{n=2}^{+\infty}(s_{n-1} + s_{n-2})X^n =$
$s_0 + s_1 X_F + X_F \sum_{n=2}^{+\infty} s_{n-1}X^{n-1} + (X_F)^2 \sum_{n=0}^{+\infty} s_{n-2})X^{n-2} = s_0 + s_1 X_F + X_F(S - s_0) + (X_F)^2 S =$
$s_0 + (s_1 - s_0)X_F + (X_F + (X_F)^2)S$.
S est donc solution de $P - Q.S = 0_F$, avec $P = s_0 + (s_1 - s_0)X_F$ et $Q = 1 - X_F - (X_F)^2 (\neq 0)$.

5. Soit S rationnelle, non-nulle. Par définition, il existe deux polynômes P et $Q \neq 0$ tels que S soit solution de $P - Q.S = 0_F$ (avec P unitaire quitte à tout diviser par son coefficient dominant). On pose alors $P^* = \frac{P}{pgcd(P,Q)}$ et $Q^* = \frac{Q}{pgcd(P,Q)}$.
On a alors $pgcd(P,Q)(P^* - Q^*.S) = P - Q.S = 0_F$. On en déduit soit que $pgcd(P,Q) = 0$ (exclu, car $Q \neq 0$), soit que $(P^* - Q^*.S)$. On a donc bien l'existence.
Pour l'unicité : soit (P_1, Q_1) répondant aux hypothèses avec P_1 de degré minimal et (P_2, Q_2) répondant aux hypothèses.
Notons $d_1 = \deg(P_1)$.
Effectuons la division euclidienne de P_2 par P_1 : il existe Q et R, avec $\deg(R) < d_1$ tels que $P_2 = P_1.Q + R$.
De plus, $P_1 - S.Q_1 = 0$ et $P_2 - S.Q_2 = 0$, d'où $(Q.P_1 - P_2) - S.(Q.Q_1 - Q_2) = 0$, i.e. $R - S.(Q.Q_1 - Q_2) = 0$.
Par hypothèse de minimalité de d_1, on en déduit que $R = 0$ (sinon, quitte à tout diviser par le coefficient dominant de ce polynôme, on a construit un nouveau couple solution dont le premier polynôme a un degré strictement inférieur à d_1).
On a donc $P_2 = Q.P_1$. On en déduit $S.(Q.Q_1 - Q_2) = 0$, puis $Q_2 = Q.Q_1$ car $S \neq 0$.
P_2 et Q_2 étant premiers entre eux par hypothèse, Q, qui les divise tous deux, est un polynôme constant. P_1 et P_2 étant unitaires, on a de plus $Q = 1$.
Finalement, $P_1 = P_2$ et $Q_1 = Q_2$, d'où l'unicité.

6. Soit S rationnelle. Si $S = 0_F$, le résultat est évident avec $k = 1$, $n_0 = 0$ et $a_1 = 0$.
Sinon, d'après la question précédente, on a $P - Q.S = 0_F$, où $P = Num(S)$ et $Q = Den(S)$. On note que l'on a nécessairement $q_0 \neq 0$, sans quoi $p_0 = 0$, et P et Q sont tous deux divisibles par X, ce qui est exclut. Notons $n_0 = \deg(P) + 1$.

Pour tout $n \geq n_0$, $(Q.S)_n = \sum_{i=0}^{n} q_i s_{n-i} = 0$, i.e. $s_n q_0 = \sum_{i=1}^{n}(-q_i)s_{n-i}$, ou encore $s_n = \sum_{i=1}^{n}(-\frac{q_i}{q_0})s_{n-i}$.

Si l'on note $k = \deg(Q)$, on a donc $\forall n \geq n_0 s_n = \sum_{i=1}^{k}(-\frac{q_i}{q_0})s_{n-i}$.

Le résultat est donc prouvé, en posant $a_i = -\frac{q_i}{q_0}$.

7. Je laisse les détails au lecteur : la démarche est l'inverse de celle de la question précédente : on pose $Q = 1 - \sum_{i=1}^{k} a_i X^i$, de telle façon que $\forall n \geq n_0$, $(Q.S)_n = 0$ (on reprend les calculs précédents). On note alors $P = -Q.S$, qui est bien un polynôme, et l'on a bien le résultat voulu.
8. C'est immédiat d'après les questions 2.6 et 2.7. On calcule les coefficients a_i à partir de Q (en temps constant), et les premiers coefficients de S sont ceux de P. Ensuite, chaque calcul de s_n s'effectue en temps constant à partir des valeurs précédentes à l'aide de (1) (la somme contient un nombre constant de termes).

   s_n peut donc être calculé en temps $O(n)$.
9. (a) Soit Φ contractante. Soient S_1 et S_2 deux solutions de l'équation. On a $S_1 = \Phi(S_1)$ et $S_2 = \Phi(S_2)$.

   Comme Φ est contractante, si $S_1 \neq S_2$, on a $d(S_1, S_2) = d(\Phi(S_1), \Phi(S_2)) < d(S_1, S_2)$, ce qui est absurde.

   (b) Si $S^{(n+1)} \neq S^{(n)}$, alors $S^{(n-1)} \neq S^{(n)}$.

   On en déduit que $d(S^{(n+1)}, S^{(n)}) < d(S^{(n-1)}, S^{(n)})$, d'où $\nu(S^{(n+1)} - S^{(n)}) > \nu(S^{(n-1)} - S^{(n)})$. ν étant à valeurs entières, on en déduit le résultat demandé.

   (c) L'unicité découle de la question a.

   On définit $(S^{(n)})_{n\geq 0}$ comme à la question précédente.

   Si cette suite est constante à partir d'un certain rang n, alors $\Phi(S^{(n)}) = S^{(n+1)} = S^{(n)}$, et $S^{(n)}$ est solution de l'équation.

   Sinon, une récurrence immédiate et la question précédente montrent que $\nu(S^{(n+1)} - S^{(n)}) \geq n$. On en déduit que pour $j \in \mathbb{N}$, $\forall n \geq j$, $(S^{(n+1)} - S^{(n)})_j = 0$. D'après la question 1.5.c, $(S^{(n)})$ converge donc au sens des séries formelles.

   Notons S sa limite. Montrons que $\Phi(S) = S$, ce qui conclura la démonstration.

   Par inégalité triangulaire, $d(\Phi(S), S) \leq d(\Phi(S), S^{(n+1)}) + d(S, S^{(n+1)}) \leq d(S, S^{(n+1)}) + d(S, S^{(n+1)})$.

   Par convergence de $S^{(n)}$ vers S, le membre de droite est de limite nulle, d'où $d(\Phi(S), S) = 0$, i.e. $S = \Phi(S)$.
10. Construisons les coefficients d'une solution de proche en proche. Si S est solution, par hypothèse, on a $0 = p_{0,0} + p_{1,0}s_0$: comme $p_{1,0} \neq 0$, il n'y a qu'une seule valeur possible pour s_0.

    On a de plus $0 = p_{0,1} + p_{1,0}s_1 + p_{1,1}s_0 + p_{2,1}s_0^2 + \ldots p_{k,1}s_0^k$, et comme précédemment, il n'y a qu'une solution pour s_1.

    Supposons $s_0 \ldots s_n$ construits. On a $0 = p_{0,n+1} + p_{1,0}s_{n+1} + A$, où A est une somme de termes où interviennent seulement $s_0 \ldots s_n$. Il n'y a qu'une solution pour s_{n+1}.

    En poursuivant de cette façon, on construit donc S solution de $\Phi(S) = 0$, et elle est de plus unique.
11. (a) On a pour tout $n \in \mathbb{N}$ $S_n^2 = \sum_{k=0}^{n} s_k s_{n-k}$.

    Si S est solution de l'équation, on doit avoir en particulier $s_0^2 = p_0$, i.e. $s_0 \in \{\sqrt{p_0}, -\sqrt{p_0}\}$.

    (b) On choisit l'une des 2 valeurs possibles pour s_0. On montre alors que l'on peut construire une unique solution de l'équation.

    On a $p_1 = s_0 s_1 + s_1 s_0 = 2s_1 s_0$, et l'on doit donc poser $s_1 = \frac{p_1}{2s_0}$ ($s_0 \neq 0$).

Si l'on a construit $s_0 \dots s_n$, on remarque que $p_{n+1} = s_0 s_{n+1} + s_1 s_n + \dots + s_n s_1 + s_{n+1} s_0 = 2 s_0 s_{n+1} + \dots$, où les points de suspension ne fait intervenir que $s_0 \dots s_n$. Comme $s_0 \neq 0$, il existe donc une unique valeur de s_{n+1} qui convienne.

On construit ainsi une unique solution de l'équation.

Il y a deux valeurs de s_0 possibles, et donc exactement 2 solutions de l'équation dans $\mathbb{R}[[X]]$.

Partie 3 : Séries génératrices de langages

1. Supposons $L \subset L'$. Alors $\forall n \in \mathbb{N},\ L \cap A^n \subset L' \cap A^n$, d'où $L_n \subset L'_n$, puis $l_n \leq l'_n$ avec les notations évidentes. On en déduit $S_L \leq_F S_{L'}$ par définition de l'ordre sur $S[[X]]$.
   S'il y a égalité dans la dernière égalité, il y a en remontant égalité dans chacune des précédentes, et on a bien $L = L'$.
2. Soit $n \in \mathbb{N}$. On a $(L \cup L') \cap A^n = (L \cap A^n) \cup (L' \cap A^n)$.
   On en déduit $\forall n \in \mathbb{N} \#((L \cup L') \cap A^n) \leq \#(L \cap A^n) + \#(L' \cap A^n)$, avec égalité partout Ssi $\forall n \in \mathbb{N}$, $(L \cap A^n)$ et $(L' \cap A^n)$ sont disjoints Ssi L et L' sont disjoints.
   Le résultat s'en déduit immédiatement.
3. Soit $v_1.v'_1 = w_1.w'_1 \in L.L'$, avec $v_1, w_1 \in L$ et $v'_1, w'_1 \in L'$.
   Supposons $|v_1| < |w_1|$. Alors v_1 est un préfixe strict de w_1 ce qui est exclu car L est préfixe. De la même façon, $|v_1| > |w_1|$ est exclu. Finalement, $|v_1| = |w_1|$, d'où $v_1 = w_1$, puis $v'_1 = w'_1$: $L.L'$ est non ambigu.
4. (a) Raisonnons par double inclusion.
   - Soit $w \in F$. Si $w \in \{\epsilon, a, b\}$, alors $w \in \{\epsilon, b\} \cup (\{a, ba\}.F)$.
     Sinon, w est de longueur au moins 2. Il commence nécessairement par a ou ba. On peut donc écrire $w = a.w'$ ou $w = ba.w'$. Dans les 2 cas, $w' \in F$, car il ne peut pas y avoir 2 b consécutifs dans w'.
     L'inclusion directe est donc prouvée.
   - Pour l'inclusion réciproque, on remarque que $\{\epsilon, b\} \subset F$.
     De plus, si $w' \in F$, $aw' \in F$ et $baw' \in F$ (on ne fait pas apparaitre de b consécutif en concaténant a ou ba au début du mot).
     L'inclusion réciproque est donc prouvée.

   (b) Dans l'inégalité précédente, l'union est disjointe.
   Le produit est de plus non-ambigu, $\{a, ba\}$ étant préfixe. La série génératrice de $\{\epsilon, b\}$ est $1 + X$, et celle de $\{a, ba\}$ est $X + X^2$. D'après les questions précédentes, on a donc
   $S_F = 1_F + X_F + (X_F + X_F^2)S_F$, i.e. $1_F + X_F - (1_F - X_F - X_F^2)S_F$, ce qui prouve que S_F est rationnelle, avec de plus $Num(S) = 1 + X$ et $Den(S) = 1 - X - X^2$ (qui sont bien premiers entre eux).

   (c) En reprenant l'égalité de la question a, et en intersectant avec A_n pour tout $n \in \mathbb{N}$, on obtient $f_0 = 1$, $f_1 = 2$ et pour tout $n \geq 2$, $f_n = f_{n-1} + f_{n-2}$ (il s'agit donc d'une suite de Fibonacci).
5. (a) Soit w_1 et w_2 dans D. Notons $w = a.w_1.b.w_2$.
   On a $|w|_a = 1 + |w_1|_a + |w_2|_a = 1 + |w_1|_b + |w_2|_b = |w_b|$.
   Si v est un préfixe de w :
   - soit c'est a, et il contient plus de a que de b ;
   - soit c'est $a.v_1$, où v_1 est un préfixe de w_1. On a donc $|v_1|_a \leq |v_1|_b$, d'où $|v|_a = 1 + |v_1|_a \leq 1 + |v_1|_b = 1 + |v|_b < |v|_b$;
   - soit c'est $a.w_1.b$, et il contient autant de a que de b ;
   - soit c'est $a.w_1.b.v_2$, où v_2 est un préfixe de w_2, qui contient plus de a que de b. Comme $a.w_1.b$ contient aucun de a que de b, on a donc bien $|v|_a \geq |v_b|$ dans ce cas aussi.

(b) Soit $w \in D$, $w \neq \epsilon$. w commence nécessairement par a. On note w' le plus court préfixe de w tel que $|w'|_a = |w'|_b$ – un tel préfixe existe car w satisfait $|w|_a = |w|_b$. w' termine par b (sans quoi le préfixe de longueur w de longueur $|w|' - 1$ contient strictement plus de b que de a).

On peut donc écrire $w' = a.w_1.b$, d'où l'on déduit une décomposition $w = a.w_1.b.w_2$ (avec éventuellement $w_1 = \epsilon$ ou $w_2 = \epsilon$).

- Par définition, de w', $|w_1|_a = |w'|_a - 1 = |w'|_b - 1 = |w_1|_b$.
Soit v_1 un préfixe de w_1. $a.v_1$ est un préfixe de w, et donc $|a.v_1|_a \geq |a.v_1|_b$, d'où $|v_1|_a \geq |v_1|_b - 1$. Supposons $|v_1|_a = |v_1|_b - 1$. Alors $|a.v_1|_a = |a.v_1|_b$, ce qui contredit la minimalité de la longueur w'. On a donc bien $|v_1|_a \geq |v_1|_b$, et donc $w_1 \in D$.
- On a $|w_2|_a = |w|_a - 1 - |w_1|_a = |w|_b - 1 - |w_1|_b = |w_2|_b$. Par ailleurs, si v_2 est un préfixe de w_2, $a.w_1.b.v_2$ est un préfixe de w', et contient donc plus de a que de b. Comme $a.w_1.b$ contient autant de a que de b, v_2 contient donc plus de a que de b. On a donc $w_2 \in D$.

L'existence de la décomposition est prouvée.

Pour l'unicité, soit $a.w'_1.b.w'_2$ une autre décomposition convenant. Supposons $|w'_1| < |w_1|$. Alors w'_1 est un préfixe de w_1, qui contient autant de a que de b. $w'_1.b$ est donc un préfixe de w_1 qui contient strictement plus de b que de a : exclu. Symétriquement, on ne peut avoir $|w_1| < |w'_1|$. Finalement, $|w_1| = |w'_1|$, d'où $w_1 = w'_1$ puis l'unicité de la décomposition.

(c) C'est immédiat par double inclusion, et en utilisant les deux questions précédentes.

(d) En utilisant l'équation précédente, et en remarquant que l'union est disjointe et le produit non ambigu, on obtient $S_D = 1_F + X_F.S_D.X_F.S_D = 1_F + (X_F)^2 S_D^2$ (S_D est en particulier algébrique).

6. Pour montrer la convergence, il s'agit de montrer d'après la question 1.5 que pour tout $n \in \mathbb{N}$, $(l_{n,k})_k$ soit ultimement constante et égale à l_n, où $l_{n,k} = \#(L_k \cap A^n)$ et $l_n = \#(L \cap A^n)$.
On a $L = \cup_k L_k$, d'où pour tout $n \in \mathbb{N}$, $L \cap A^n = \cup_k (L_k \cap A^n)$.
$L \cap A^n$ étant fini, et la suite (L_k) étant croissante, il existe k_0 tel que $\forall k \geq k_0$, $L_k \cap A^n = L \cap A^n$, d'où $l_{n,k} = l_n$.
Le résultat est donc démontré.

7. (a) On procède par récurrence sur $n \in \mathbb{N}$.

Initialisation $K_0 = \varnothing \subset K_1$. $M_1 \subset A^* = M_0$. De plus, comme $K_0 \subset M_0$ et que Ψ est croissante, $K_1 = \Psi(K_0) \subset \Psi(M_0) = M_1$.

Hérédité Supposons le résultat montré au rang n. En composant les inclusions par Ψ, qui est croissante, on obtient $K_{n+1} \subset K_{n+2} \subset M_{n+2} \subset M_{n+1}$.

(b) Démontrons les inclusions les unes après les autres.

- Soit $w \in K$. Il existe $n \in \mathbb{N}$ tel que $w \in K_n$. $n \neq 0$, donc $w \in \Psi(K_{n-1}) \subset \Psi(K)$ par croissance de Φ.
- Soit $w \in \Psi(K)$. $w = \Psi(w')$, où $w' \in K_n$ pour un certain $n \in \mathbb{N}$. On a donc $\Psi(w') \in K_{n+1}$, d'où $w \in K$.
- Soit $w \in \Psi(K)$. $w = \Psi(w')$, où $w' \in K_{n_0}$ pour un certain $n_0 \in \mathbb{N}$. (K_n) étant une suite croissante, $w' \in K_n$ pour tout $n \geq n_0$. On en déduit que $\forall n \geq n_0$, $w' \in M_n$, et $(M_n)_n$ étant une suite décroissante, $w' \in M$. Finalement, $w \in \Psi(M)$.
- Soit $w \in \Psi(M)$. $w = \Psi(w')$, où $\forall n \in \mathbb{N}$, $w' \in M_n$. On en déduit que $\forall n \in \mathbb{N}$, $w \in \Psi(M_n) = M_{n+1}$. Comme trivialement $w \in M_0 = A^*$, w appartient à tous les M_n, d'où $w \in M$.

(c) (Erreur d'énoncé, il faut évidemment lire Ψ au lieu de Φ)

- On a $K_0 \subset L$. En utilisant une récurrence immédiate, et la croissance de Ψ, on obtient $\forall n \in \mathbb{N}$ $K_n \subset L$, d'où $K \subset L$.
- Par ailleurs, soit $w \in L = \Psi(L)$. $w = \Psi(w')$, avec $w' \in L$.
Une récurrence immédiate montre que $\forall n \in \mathbb{N}$, $L \subset M_n$. On en déduit que $w' \in M$, puis $w \in \Psi(M)$, ce qui prouve la seconde inclusion.

8. On prend $k = 2$, $\psi_0 = L_1$, $\psi_1 : w_1 \mapsto L_2.w_1$ et $\psi_2 : (w_1.w_2) \mapsto L_3.w_1.w_2$.
9. Soient L et L' deux langages tels que $L \subset L'$.
   Soit $w \in \Psi(L)$.
   - Soit $w \in \psi_0$, auquel cas $w \in \Psi(L')$.
   - Soit $w \in \psi_l(w_1, \dots w_l)$, pour un certain $l \in [\![1, k]\!]$, et $(w_1 \dots w_l) \in L^l$. Comme $L \subset L'$, $(w_1 \dots w_l) \in L'^l$, d'où $\psi_l(w_1, \dots w_l) \subset \Psi(L')$. Finalement, on a donc bien $w \in \Psi(L')$.

   On a donc bien montré $\Psi(L) \subset \Psi(L')$: Ψ est croissante.
10. K satisfait l'équation $\Psi(K) = K$ d'après 3.8.b. Reste à montrer l'unicité. Soit L tel que $\Psi(L) = L$. D'après 3.8.c, on a déjà $K \subset L$. Reste donc à montrer que $L \subset K$.
    On commence par remarquer que $K_1 = \Psi(K_0) = \psi_0$. Si $w \in \psi_0$, on a donc $w \in K_1 \subset K$.
    Par récurrence forte sur $|w|$, on montre que $w \in L \Rightarrow w \in K$.

    Initialisation Si $|w| = 0$, $w = \epsilon$. Si $\epsilon \in L = \varphi(L)$, alors $\epsilon \in \psi_0$ ($\psi_l(w_1 \dots w_l)$ étant toujours de longueur non-nulle par hypothèse). On a donc $w \in \Psi(K) = K$.

    Hérédité On suppose le résultat vrai pour tous les mots de longueur inférieure à n. Soit $w \in L$, tel que $|w| = n + 1$. Si $w \in \psi_0$, on conclut comme précédemment.
    Sinon, $w \in \psi_l(w_1, \dots w_l)$, pour un certain $l \in [\![1, k]\!]$, et $(w_1 \dots w_l) \in L^l$. $|w_1| < |w|$, ... $|w_l| < |w|$ par hypothèse. Par hypothèse de récurrence, on a donc $(w_1 \dots w_l) \in K^l$, d'où $\psi_l(w_1, \dots w_l) \subset \Psi(K) = K$. Finalement, $w \in K$, ce qui achève la récurrence.
11. (a) On note $\Psi(L) = L_1 \cup L_2.L$ – qui est bien de la forme ci-dessus avec $\psi_0 = L_1$ et $\psi_1 : w \mapsto L_2.w$.
    L_2 est préfixe, donc $\epsilon \notin L_2$, d'où $\forall w' \in L_2.w$, $|w'| > |w|$.
    Il existe donc d'après la question précédente un unique langage L solution de $L = L_1 \cup L_2.L$.
    $L_2.L$ n'est pas ambigu, L_2 étant préfixe.
    Aucun mot de L_1 n'a de préfixe dans L_2, donc l'union est disjointe (supposons le contraire : soit $w \in L_1 \cap L_2.L$. On écrit alors $w = w_2.w'$, avec $w_2 \in L_2$ et $w' \in L$. w_2 est un préfixe d'un mot de L_1 (w) qui est dans L_2 : c'est exclu).
    On en déduit que l'on a donc $S_L = S_{L_1} + S_{L_2}.S_L$.

    (b) Supposons S_{L_1} et S_{L_2} rationnelles. Notons $P_1 = num(S_{L_1})$, $P_2 = num(S_{L_2})$, $Q_1 = den(S_{L_1})$, $Q_2 = den(S_{L_2})$.
    On a alors très envie d'écrire les choses suivantes : $S_{L_1} = \frac{P_1}{Q_1}$, $S_{L_2} = \frac{P_2}{Q_2}$, d'où $S_L = \frac{P_1}{Q_1} + \frac{P_2}{Q_2}.S_L$, d'où $S_L(1 - \frac{P_2}{Q_2}) = \frac{P_1}{Q_1}$, puis $S_L = \frac{P_1 Q_2}{Q_1(Q_2 - P_2)}$, ou encore $P_1 Q_2 - Q_1(Q_2 - P_2).S_L = 0$.
    Pour respecter les notations de l'énoncé – refractaire aux fractions, on écrit plutôt :
    $S_{L_1} Q_1 = P_1$ et $S_{L_2} Q_2 = P_2$, d'où
    $Q_1 Q_2 S_L = Q_1 Q_2 S_{L_1} + Q_1 Q_2 S_{L_2}.S_L = Q_2 P_1 + Q_1 S_L P_2$
    puis
    $Q_1 Q_2 S_L = P_1 Q_2 + Q_1 P_2 S_L$
    d'où finalement
    $P_1 Q_2 - Q_1(Q_2 - P_2).S_L = 0$
    S_L est donc rationnel.

Partie 4 : Séries formelles et séries entières

1. On a pour tout $n \in \mathbb{N}$, $L_n \subset A^n$, d'où $l_n \leq (\#A)^n$. On en déduit que le rayon de convergence de S_L est supérieur à $\dfrac{1}{\#A}$, et est donc strictement positif.
2. Ce sont des résultats du cours. En voici des preuves. Notons ρ_T et ρ_U les rayons de convergence respectifs de T et U.

- Soit $\rho = \min\{\rho_T, \rho_U\}$. Pour tout t tel que $|t| < \rho$, U et T convergent en t. Pour tout $N \in \mathbb{N}$, $\sum_{k=0}^{n} v_k t^k = \sum_{k=0}^{n} u_k t^k + \sum_{k=0}^{n} t_k t^k$. V converge donc également en t, et de plus en passant à la limite dans l'égalité précédente, $\tilde{V}(t) = \tilde{T}(t) + \tilde{U}(t)$.
- On prend le même ρ que précédemment. Soit t tel que $|t| < \rho$. U et T convergent en t.

  Soit $n \in \mathbb{N}$. On a $\displaystyle\sum_{k=0}^{n} |w_k||t|^k = \sum_{k=0}^{n} |\sum_{i=0}^{k} u_i t_{k-i}||t|^k \leq \sum_{k=0}^{n}\sum_{i=0}^{k} |u_i t_{k-i}||t|^k = \sum_{k=0}^{n}\sum_{i=0}^{k} |u_i||t|^i |t_{k-i}||t|^{k-i} =$
  $\displaystyle\sum_{i=0}^{n}(|u_i||t|^i)\sum_{k=i}^{n}(|t_{k-i}||t|^{k-i}) = \sum_{i=0}^{n}|u_i||t|^i \sum_{k=0}^{n-i}|t_k||t|^k \leq \sum_{i=0}^{n}|u_i||t|^i\sum_{k=0}^{n}|t_k||t|^k$.

  Les deux séries entières du dernier membre convergent, et donc $\displaystyle\sum_{k=0}^{n} w_k t^k$ converge absolument, et donc converge.

  De plus, $\displaystyle\left|\sum_{k=0}^{2n} w_k t^k - \sum_{k=0}^{n} u_k t^k \sum_{j=0}^{n} t_j t^j\right|$
  $$\leq \sum_{p=0}^{2n}\sum_{q=n+1}^{2n}|u_p t_q t^{p+q}| + \sum_{p=n+1}^{2n}\sum_{q=0}^{2n}|u_p t_q t^{p+q}|$$
  $$\leq \left(\sum_{p=0}^{+\infty}|u_p t^p|\right)\left(\sum_{q=n+1}^{+\infty}|t_q t^q|\right) + \left(\sum_{p=n+1}^{+\infty}|u_p t^p|\right)\left(\sum_{q=0}^{+\infty}|t_q t^q|\right).$$

  Les restes tendent vers 0, et on en déduit donc que $\displaystyle\sum_{k=0}^{+\infty} w_k = \sum_{k=0}^{+\infty} u_k t^k \sum_{j=0}^{+\infty} u_j t^j$, i.e. $\tilde{W}(t) = \tilde{T}(t).\tilde{U}(t)$.

3. (a) On repart de l'équation $S_D = 1_F + (X_F)^2 S_D^2$. D'après la question 4.1, $\tilde{S}_D$ converge sur un voisinage de 0. Sur ce même voisinage, la série entière correspondant à $1_F + (X_F)^2 S_D^2$ converge d'après la question précédente, et de plus si t appartient au voisinage de zéro considéré, elle converge vers $1 + t^2\tilde{S}_D(t)$, toujours d'après la question précédente. On en déduit que $\tilde{S}_D$ est bien solution de l'équation fonctionnelle $F(t) = 1 + t^2 F(t)^2$.

   (b) Notons ρ le rayon de convergence de la série $\tilde{S}_D$. Pour tout $t \in]-\rho, \rho[$, on a $\tilde{S}_D(t) = 1 + t^2\tilde{S}_D^2$, d'où $t^2\tilde{S}_D^2 - \tilde{S}_D(t) + 1 = 0$.

   On en déduit $\tilde{S}_D(0) = 1$. Sinon, en notant $X = \tilde{S}_D(t)$, on obtient $t^2X^2 - X + 1$, équation du second degré, de discriminant $1 - 4t^2$ qui a le bon goût d'être strictement positif au voisinage de 0, et de racines $\dfrac{1 + \sqrt{1-4t^2}}{2t^2}$ et $\dfrac{1 - \sqrt{1-4t^2}}{2t^2}$.

   Si ça n'est pas trop lui demander, $\tilde{S}_D$ doit être continue sur $]-\rho, \rho[$, et on en déduit donc que $\forall t \in]-\rho, \rho[,\ \tilde{S}_D(t) = \dfrac{1 - \sqrt{1-4t^2}}{2t^2}$ (l'autre expression produisant une discontinuité en 0 – il est par ailleurs clair que l'on ne peut pas passer continument d'une expression à l'autre.)

4. Finissons en beauté avec un développement en série entières.

   Sur les voisinages de 0 adaptés, on a $\displaystyle\sqrt{1+t} = 1 + \sum_{n=1}^{+\infty}\frac{1/2(-1/2)(-3/2)\dots((3-2n)/2)}{n!}t^n =$
   $$1 + \sum_{n=1}^{+\infty}(-1)^{n-1}\frac{1.3\dots(2n-3)}{2^n n!}t^n = 1 + \sum_{n=1}^{+\infty}(-1)^{n-1}\frac{(2n-2)!}{2^{n-1}(n-1)!2^n n!}t^n.$$

   On en déduit $\displaystyle\sqrt{1-4t^2} = 1 + \sum_{n=1}^{+\infty}(-1)^{n-1}\frac{(2n-2)!}{2^{n-1}(n-1)!2^n n!}(-4t^2)^n = 1 - 2\sum_{n=1}^{+\infty}\frac{(2n-2)!}{(n-1)!n!}t^{2n}$,

   puis $\displaystyle\frac{1 - \sqrt{1+4t^2}}{2t^2} = \sum_{n=1}^{+\infty}\frac{(2n-2)!}{(n-1)!n!}t^{2n-2} = \sum_{n=0}^{+\infty}\frac{(2n)!}{n!(n+1)!}t^{2n} = \sum_{n=0}^{+\infty} d_n t^n$.

On en déduit donc que $d_n = 0$ si n est impair, et que $d_n = \dfrac{n!}{(n/2)!(n/2+1)!}$ si n est pair.