DM 5 : Corrigé.
Ordinaux et suites de Goodstein.

1 Suites de Goodstein

1°) $144 = 81 + 63 = 3^4 + 2 \times 27 + 9 = 3^4 + 2.3^3 + 3^2$.

2°) La décomposition héréditaire de 144 en base 3 est égale à $3^{(3^1+1)} + 2.3^3 + 3^2$ donc celle de $3^{144} + 144$ est

$$3^{[3^{(3^1+1)}+2.3^3+3^2]} + 3^{(3^1+1)} + 2.3^3 + 3^2.$$

3°) Démontrons par récurrence sur h l'assertion $S(h)$ suivante : $2^h > h$.
Initialisation : pour $h = 0$, $2^0 = 1 > 0$.
Hérédité : pour $h \geq 0$, supposons que $2^h > h$.
Ainsi, $2^h \geq h + 1$, donc $2^{h+1} \geq 2(h + 1) \geq h + 2 = (h + 1) + 1$. Ainsi, $2^{h+1} > h + 1$, ce qui prouve $S(h + 1)$.
D'après le principe de récurrence, pour tout $h \in \mathbb{N}$, $2^h > h$.

4°) Fixons $b \in \mathbb{N}$ avec $b \geq 2$.
Montrons par récurrence forte sur n que $R(n) : \mathrm{dh}_b(n)$ est correctement défini.
Initialisation : Supposons que $n < b^{b+1}$. Alors la décomposition en base b de n s'écrit $n = \sum_{i=0}^{h} a_i b^i$ avec $h \leq b$ (sinon, sachant que $a_h \neq 0$, $n \geq b^h \geq b^{b+1}$), donc cette écriture de n ne fait intervenir que des entiers compris entre 0 et b. Il est donc correct de convenir que c'est aussi la décomposition héréditaire de n en base b.
Hérédité : Pour $n \geq b^{b+1}$, on suppose que, pour tout $k \in \{0, \ldots, n-1\}$, $R(k)$ est vraie et l'on montre $R(n)$.

Décomposons n en base b : $\mathrm{d}_b(n) = \sum_{i=0}^{h} a_i b^i$, avec $h \in \mathbb{N}$ et $a_h \neq 0$.

Alors $n \geq b^h \geq 2^h > h$. Ainsi, pour tout $i \in \{0, \ldots, h\}$, $i < n$ et on peut appliquer $R(i)$: $\mathrm{dh}_b(i)$ est correctement défini, donc l'écriture $\sum_{i=0}^{h} a_i b^{dh_b(i)}$ est correctement définie. Ceci prouve $R(n)$.

5°) On montre par récurrence forte que, avec la définition proposée en question 5, pour tout $n \in \mathbb{N}$, on a $T(n)$: $f_{q,r}(n)$ est bien défini et il correspond à la définition initiale.
Initialisation : Si $n \in \{0, \dots, q-1\}$, alors la décomposition héréditaire de n en base q correspond seulement à l'écriture $n = n : q$ n'apparaît pas dans cette écriture, donc si l'on remplace q par r, on ne change rien : il est correct de poser $f_{q,r}(n) = n$ dans ce cas.
Toujours dans ce cas, la seconde définition est compatible avec la première, car dans l'expression $\sum_{i=0}^{k} a_i\ q^i$, on a $k = 0$.
Hérédité : Supposons maintenant que $n \geq q$ et que $T(k)$ est vraie
pour tout $k \in \{0, \dots, n-1\}$.
On a encore $n = \sum_{i=0}^{h} a_i\ q^i$, avec $h \in \mathbb{N}$, $a_h \neq 0$ et pour tout $i \in \{0, \dots, h\}$,
$a_i \in \{0, \dots, q-1\}$. Ainsi, $n \geq q^h \geq 2^h > h$, donc, de même que lors de la question précédente, d'après l'hypothèse de récurrence, pour tout $i \in \{0, \dots, k\}$, $f_{q,r}(i)$ est bien défini et il correspond à la définition initiale de $f_{q,r}$. Alors, selon la définition initiale, on a bien $f_{q,r}(n) = \sum_{i=0}^{h} a_i\ r^{f_{q,r}(i)}$, ce qui prouve $T(n)$.

6°) $g_0 = 3 = 2^1 + 1$, donc $f_{2,3}(g_0) = 3^1 + 1$ puis $g_1 = 3$.
$f_{3,4}(g_1) = 4$, donc $g_2 = 3$. $f_{4,5}(g_2) = 3$, donc $g_3 = 2$, puis $g_4 = 1$, $g_5 = 0$ et la suite (g_n) stationne à 0 pour $n \geq 5$.

7°) $$\sum_{i=0}^{h}(b-1)b^i = \sum_{i=0}^{h} b^{i+1} - \sum_{i=0}^{h} b^i = \sum_{i=1}^{h+1} b^i - \sum_{i=0}^{h} b^i = b^{h+1} - 1.$$

8°) Calculons les premières valeurs de la suite (g_n).
$g_0 = 4 = 2^2$, donc $g_1 = 3^3 - 1 = 2.3^2 + 2.3^1 + 2$ (d'après la question précédente).
Alors $f_{3,4}(g_1) = 2.4^2 + 2.4^1 + 2$, donc $g_2 = 2.4^2 + 2.4 + 1$, puis $g_3 = 2.5^2 + 2.5$.
Ensuite, $g_4 = 2.6^2 + 2.6 - 1 = 2.6^2 + 6 + 5$.
Par récurence, on obtient $g_{4+k} = 2.(6+k)^2 + (6+k) + 5 - k$, pour $k \in \{0, \dots, 5\}$, donc $g_9 = 2.(11)^2 + 11$. Ainsi, $h = 9$.
Ensuite $g_{10} = 2.(12)^2 + 11$. Par récurrence, on obtient $g_{10+k} = 2.(12+k)^2 + 11 - k$, pour tout $k \in \{0, \dots, 11\}$, donc $g_{21} = 2.(23)^2$.
Ainsi, 21 est le plus petit k tel que $g_k = 2.(23)^2$.

9°) On a ensuite $g_{22} = 2.(24)^2 - 1 = (24)^2 + 23 \times 24 + 23$,
puis $g_{23} = f_{24,25}((24)^2 + 23 \times 24 + 23) - 1 = (25)^2 + 23 \times 25 + 22$,
donc $g_{21+24} = (23+24)^2 + 23 \times (23+24)$,
c'est-à-dire $g_{3.2^4-3} = (3.2^4 - 1)^2 + 23 \times (3.2^4 - 1)$.
Ensuite, $g_{3.2^4-2} = (3.2^4)^2 + 23 \times (3.2^4) - 1 = (3.2^4)^2 + 22 \times (3.2^4) + (3.2^4 - 1)$, donc $g_{3.2^4-3+3.2^4} = g_{3.2^5-3} = (3.2^5 - 1)^2 + 22 \times (3.2^5 - 1)$.

Par récurrence sur h, on montrerait que $g_{3.2^h-3} = (3.2^h-1)^2 + (27-h)\times(3.2^h-1)$, pour tout $h \in \{4,\dots,27\}$. En particulier, lorsque $h = 27$,
on obtient que $g_{3.2^{27}-3} = (3.2^{27}-1)^2$.

10°) Posons $b = 3.2^{27}-1$. Ainsi $g_{b-2} = b^2$,
donc $g_{b-1} = f_{b,b+1}(b^2) - 1 = (b+1)^2 - 1 = b(b+1)+b$, puis $g_b = b(b+2)+b-1$ donc $g_{b-1+b} = g_{2(b+1)-3} = b(2b+1)$, puis $g_{2(b+1)-2} = (b-1)(2b+2)+2b+1$,
donc $g_{2^2(b+1)-3} = (b-1)(2^2(b+1)-1)$. Par récurrence, on montre que
$g_{2^k(b+1)-3} = (b-k+1)(2^k(b+1)-1)$ pour tout $k \in \{1,\dots,b\}$.
En particulier, lorsque $k = b$, $g_{2^b(b+1)-3} = 2^b(b+1)-1$, donc si l'on pose $B = 2^b(b+1)$, $g_{B-3} = B-1$, puis $g_{B-2} = f_{B-1,B}(B-1)-1 = B-1$,
puis $g_{B-1} = f_{B,B+1}(B-1)-1 = B-2$ et finalement $g_{2B-3} = 0$.
Ainsi, le plus petit k tel que $g_k = 0$ est

$$k = 2B-3 = 2^{b+1}(b+1)-3 = 2^{3.2^{27}} \times 3.2^{27} - 3.$$

2 Ensembles bien ordonnés

11°) Supposons que R est un ordre strict.
- Par définition, r est réflexive.
- Soit $x, y \in E$ tels que $x\ r\ y$ et $y\ r\ x$.
  Si $x \neq y$, alors $x\ R\ y$ et $y\ R\ x$, donc par transitivité $x\ R\ x$, ce qui est impossible.
  Ainsi, $x = y$, ce qui prouve que r est antisymétrique.
- Soit $x, y, z \in E$ tels que $x\ r\ y$ et $y\ r\ z$.
  Si $x = y$, alors $x = y\ r\ z$. Si $y = z$, alors $x\ r\ y = z$.
  Si maintenant $x \neq y$ et $y \neq z$, alors $x\ R\ y$ et $y\ R\ z$, donc par transitivité de R, $x\ R\ z$, donc $x\ r\ z$. Ainsi, dans tous les cas, $x\ r\ z$, ce qui prouve que r est transitive.

r est réflexive, antisymétrique et transitive, donc c'est une relation d'ordre.

12°) Réciproquement, supposons que r est une relation d'ordre.
Analyse : Supposons qu'il existe un ordre strict R tel que r est la relation d'ordre associée à R. Ainsi, pour tout $x, y \in E$, $x\ r\ y \iff (x\ R\ y) \vee (x = y)$.
Soit $x, y \in E$. Si $x\ R\ y$, alors $x\ r\ y$ et $x \neq y$ car R est antiréflexive.
Réciproquement, si $x\ r\ y$ et $x \neq y$, alors $x\ R\ y$,
donc $\forall x, y \in E,\ [x\ R\ y \iff (x\ r\ y) \wedge (x \neq y)]$.
Ceci montre que, sous condition d'existence, l'ordre strict R est unique.
Synthèse : Considérons sur E la relation binaire R définie par :
$\forall x, y \in E,\ [x\ R\ y \iff (x\ r\ y) \wedge (x \neq y)]$.
- Par définition de R, pour tout $x \in E$, $\neg(x\ R\ x)$, donc R est antiréflexive.
- Soit $x, y, z \in E$ tels que $x\ R\ y$ et $y\ R\ z$.
  Ainsi, $x \neq y$, $y \neq z$, $x\ r\ y$ et $y\ r\ z$. Par transitivité de r, $x\ r\ z$.
  Supposons que $x = z$. Alors $z = x\ r\ y$ et $y\ r\ z = x$, donc par antisymétrie de r, $x = y$, ce qui est faux. Ainsi, $x \neq z$ et $x\ r\ z$, donc $x\ R\ z$.

Ceci prouve que R est transitive.
Ainsi R est un ordre strict.
Il reste à montrer que r est la relation d'ordre associée à R : pour tout $x, y \in E$, $x\ r\ y \iff [(x\ r\ y) \wedge (x \neq y)] \vee (x = y)$, le sens indirect provenant de la réflexivité de r, donc $x\ r\ y \iff (x\ R\ y) \vee (x = y)$, ce qu'il fallait démontrer.

13°) $\diamond$ Soit $x, y \in E$.
$\{x, y\}$ est une partie non vide de E, donc elle possède un minimum, noté m.
Si $m = x$, alors $x \leq y$ et si $m = y$, alors $y \leq x$. Ainsi, dans tous les cas, x et y sont comparables, donc l'ordre est total.
$\diamond$ Supposons qu'il existe une suite $(x_n)_{n\in\mathbb{N}}$ strictement décroissante.
Posons $X = \{x_n \ / \ n \in \mathbb{N}\}$. X est non vide, donc il possède un minimum, noté x_m où $m \in \mathbb{N}$. $x_{m+1} \in X$, donc $x_{m+1} \geq \min(X) = x_m$, mais (x_n) décroît strictement, donc $x_{m+1} < x_m$. C'est impossible.

14°) On notera $\leq$ la relation d'ordre associée à l'ordre strict "$<$".
$\diamond$ Soit $(c, i) \in A + B$ tel que $(c, i) < (c, i)$. Ainsi, $(i < i) \vee ((i = i) \wedge (c < c))$: c'est faux, donc $<$ est antiréflexive sur $A + B$.
$\diamond$ Soit $(c, i), (d, j), (e, k) \in A + B$ tels que $(c, i) < (d, j)$ et $(d, j) < (e, k)$.
Nécessairement $i \leq j$ et $j \leq k$.
Si $i < j$ ou bien si $j < k$, alors $i < k$, donc $(c, i) < (e, k)$.
Sinon, $i = j = k$, donc $c < d$ et $d < e$, or $<$ est transitive, donc $c < e$ puis $(c, i) < (e, k)$.
Ainsi, dans tous les cas, $(c, i) < (e, k)$ et $<$ est transitive et antiréflexive sur $A + B$: c'est un ordre strict.
$\diamond$ Soit M une partie non vide de $A + B$.
Premier cas : Supposons que $M \subset B \times \{1\}$.
Notons $B' = \{b \in B \ / \ (b, 1) \in M\}$. M est non vide, donc B' est une partie non vide de B qui est bien ordonné par $<$, donc B' possède un minimum, noté m.
Alors $(m, 1) \in M$ et si $x \in M$, il existe $b \in B$ tel que $x = (b, 1)$. Alors $b \in B'$, donc $m \leq b$ puis $(m, 1) \leq (b, 1) = x$. Ainsi, $(m, 1)$ est le minimum de M.
Deuxième cas : Lorsque $M \not\subset B \times \{1\}$, l'ensemble $A' = \{a \in A \ / \ (a, 0) \in M\}$ est une partie non vide de A, donc elle possède un minimum noté m. Alors $(m, 0) \in M$.
Soit $x \in M$. Si $x \in B \times \{1\}$, alors $(m, 0) < x$.
Sinon, $x \in A \times \{0\}$, donc il existe $a \in A'$ tel que $x = (a, 0)$. Alors $m \leq a$, donc $(m, 0) \leq x$. Ainsi $(m, 0)$ est le minimum de M.
Ceci prouve que $(A + B, <)$ est bien ordonné.

15°) $\diamond$ Soit $(a, b) \in A \times B$ tel que $(a, b) < (a, b)$.
Alors $(a < a) \vee ((a = a) \wedge (b < b))$. C'est faux car $<$ sur A et sur B sont antiréflexifs.
Ainsi, $<$ est antiréflexive sur $A \times B$.
Soit $(a, b), (a', b'), (a'', b'') \in A \times B$ tels que $(a, b) < (a', b')$ et $(a', b') < (a'', b'')$.
Nécessairement, $b \leq b'$ et $b' \leq b''$.
Si $b < b'$ ou si $b' < b''$, alors $b < b''$ et $(a, b) < (a'', b'')$.
Sinon, $b = b'$ et $b' = b''$, donc $a < a'$ et $a' < a''$, puis $(a, b) < (a'', b) = (a'', b'')$.
Ceci prouve que $<$ sur $A \times B$ est antiréflexive et transitive, donc c'est un ordre strict.

$\diamond$ Soit M une partie non vide de $A \times B$. Notons $B' = \{b \in B \ / \ \exists a \in A, \ (a,b) \in M\}$.
M étant non vide, $B' \neq \emptyset$, or $(B, <)$ est bien ordonné, donc B' possède un minimum noté b_0.
$b_0 \in B'$ donc il existe $a \in A$ tel que $(a, b_0) \in M$. Ainsi, $A' = \{a \in A \ / \ (a, b_0) \in M\}$ est une partie non vide de A : elle possède un minimum noté a_0.
Posons $m = (a_0, b_0) : m \in M$.
Soit $x = (a, b) \in M$. $b \in B'$, donc $b \geq b_0$.
Si $b_0 < b$, alors $m = (a_0, b_0) < (a, b) = x$.
Sinon, $x = (a, b_0)$ et $a \in A'$. Ainsi $a \geq a_0$ et $m = (a_0, b_0) \geq (a, b_0) = x$.
Ainsi, m est le minimum de M, ce qui prouve que $(A \times B, <)$ est bien ordonné.

16°) $\diamond$ Si $(a_b) < (a'_b)$, il existe $b_0 \in B$ tel que $a_{b_0} < a'_{b_0}$ or $<$ est antiréflexive sur B, donc $a_{b_0} \neq a'_{b_0}$ puis $(a_b) \neq (a'_b)$. Ainsi, $<$ est antiréflexive sur $A^{(B)}$.
Soit $(a_b), (a'_b), (a''_b) \in A^{(B)}$ tels que $(a_b) < (a'_b)$ et $(a'_b) < (a''_b)$.
Il existe $b_0, b_1 \in B$ tels que $a_{b_0} < a'_{b_0}$, $a'_{b_1} < a''_{b_1}$, pour tout $b > b_0$, $a_b = a'_b$, pour tout $b > b_1$, $a'_b = a''_b$.
Supposons que $b_0 < b_1$. Alors $a_{b_1} = a'_{b_1} < a''_{b_1}$ et pour tout $b > b_1$, $a_b = a'_b = a''_b$, donc $(a_b) < (a''_b)$.
Supposons que $b_0 > b_1$. Alors $a_{b_0} < a'_{b_0} = a''_{b_0}$ et pour tout $b > b_0$, $a_b = a'_b = a''_b$, donc $(a_b) < (a''_b)$.
Supposons que $b_0 = b_1$. Alors par transitivité de $<$ dans A, $a_{b_0} < a''_{b_0}$ et pour tout $b > b_0$, $a_b = a'_b = a''_b$, donc $(a_b) < (a''_b)$.
D'après la question 13, b_0 et b_1 sont comparables, donc on a envisagé tous les cas.
Ceci prouve que $<$ sur $A^{(B)}$ est antiréflexive et transitive, donc c'est un ordre strict.

17°) Il s'agit d'une généralisation du principe de récurrence forte à un ensemble bien ordonné quelconque.
Raisonnons par l'absurde en supposant qu'il existe $x \in E$ tel que $\neg(P(x))$. Alors $A = \{x \in E \ / \ \neg(P(x))\}$ est non vide, or E est bien ordonné, donc A possède un minimum, que l'on notera m.
Soit $y \in E$ tel que $y < m$. Par construction de m, $y \notin A$, donc $P(y)$ est vrai. Ainsi, on a montré que $[\forall y \in E, \ y < m \Longrightarrow P(y)]$, donc $P(m)$ est vrai et $m \notin A$, ce qui est faux. On en déduit que pour tout $x \in E$, $P(x)$ est vraie.
On peut remarquer qu'on a bien une forme d'initialisation car $P(\min(E))$ est vrai. En effet, pour tout $y \in E$, l'assertion "$y < \min(E)$" est fausse,
donc $[\forall y \in E, \ y < \min(E) \Longrightarrow P(y)]$.

18°) $\diamond$ Soit $x_0 \in E$. Soit $x \in S_{x_0}$ et $y \in E$ tel que $y < x$. Alors par transitivité, $y < x_0$, donc $y \in S_{x_0}$. Ainsi, pour tout $x_0 \in E$, S_{x_0} est un segment initial et il est clair que E est un segment initial de E.
$\diamond$ Réciproquement, soit S un segment initial de E. Supposons que $S \neq E$.
Alors $E \setminus S$ est une partie non vide de E, donc on peut poser $x_0 = \min(E \setminus S)$.
Soit $x \in S_{x_0}$. Alors $x < x_0$, donc $x \notin (E \setminus S)$ (par définition de x_0), donc $x \in S$.

Réciproquement, supposons que $x \in S$. Alors $x \neq x_0$, car $x_0 \in E \setminus S$, donc $x < x_0$ ou $x > x_0$, mais si $x > x_0$, S étant un segment initial, on en déduirait que $x_0 \in S$, ce qui est faux. Ainsi $x < x_0$, donc $x \in S_{x_0}$. Ceci montre que $S = S_{x_0}$.
Remarque : plus précisément, on a montré que lorsque S est un segment initial différent de E, alors $S = S_{x_0}$, où $x_0 = \min(E \setminus S)$.

19°) Soit f et g deux bijections strictement croissantes de E dans F.
$\diamond$ Soit $x, y \in E$. Montrons que $x < y \iff f(x) < f(y)$:
le sens direct provient de la définition de la croissance stricte de f. De plus, si $x \geq y$, alors $f(x) \geq f(y)$, donc par contraposée, $f(x) < f(y) \Longrightarrow x < y$ (les ordres sont totaux d'après la question 13).
Ainsi, pour tout $x, y \in E$, $x < y \iff f(x) < f(y) \iff g(x) < g(y)$.
$\diamond$ Supposons que $f \neq g$. Alors l'ensemble $A = \{x \in E \ / \ f(x) \neq g(x)\}$ est non vide, donc il possède un minimum que l'on notera x_0. Sans perte de généralité, on peut supposer que $f(x_0) > g(x_0)$.
f étant surjective, il existe $x_1 \in E$ tel que $g(x_0) = f(x_1)$. Alors $f(x_0) > f(x_1)$, donc d'après le point précédent, $x_1 < x_0$, donc $g(x_1) < g(x_0) = f(x_1)$. Ainsi, $f(x_1) \neq g(x_1)$, donc $x_1 \in A$, mais $x_1 < x_0 = \min(A)$. C'est impossible, donc $f = g$.

3 Les ordinaux

20°) Pour tout prédicat $P(x)$, l'assertion "$\forall x \in \emptyset,\ \ P(x)$" est toujours vraie, donc "$\in$" est un ordre strict sur E et comme $\emptyset$ n'admet aucune partie non vide, $(\emptyset, \in)$ est bien ordonné. Il est de plus clairement transitif, donc $\emptyset$ est bien un ordinal.

21°) Posons $a = \emptyset$, $b = \{\emptyset\}$ et $A = \{a, b\}$. Il s'agit de montrer que A est un ordinal.
Notons également R la relation d'appartenance : $b \ R \ b \iff b \in b \iff b = \emptyset$, ce qui est faux, donc, tout $x, y \in A$, $x \ R \ y \iff (x = a) \wedge (y = b)$.
La relation R est clairement antiréflexive.
Soit $x, y, z \in A$ tels que $x \ R \ y$ et $y \ R \ z$. Alors $y = b$ et $y = a$, ce qui n'est pas possible.
Ainsi, la propriété $(x \ R \ y) \wedge (y \ R \ z)$ est fausse, donc on a bien
$(x \ R \ y) \wedge (y \ R \ z) \Longrightarrow (x \ R \ z)$: R est transitive, donc c'est un ordre strict.
Les parties non vides de A sont $\{a\}$, $\{b\}$ et A. Elles possèdent toutes un minimum, respectivement égal à a, b et a. Ainsi, (A, R) est bien ordonné.
Soit $x \in A$ et $y \in x$. Alors x est non vide, donc $x = b$ et $y = a$. On a bien $y \in A$, donc A est transitif.
Ceci démontre que A est un ordinal.

22°) $(\alpha, \in)$ est bien ordonné et α est une partie non vide de α, donc on peut poser $m = \min(\alpha)$. Si m est non vide, il existe $x \in m$. Alors $x \in m \in \alpha$, donc par transitivité de α, $x \in \alpha$ et $x < m$. Ceci contredit la définition de m. Ainsi $m = \emptyset$, donc $\emptyset \in \alpha$ et on a même montré que $\emptyset$ est le minimum de α.

23°) Supposons que $\alpha \in \alpha$.
α étant un ordinal, "$\in$" est un ordre strict sur α, donc "$\in$" est en particulier antiréflexive. Ainsi, pour tout $\beta \in \alpha$, $\beta \notin \beta$, donc en particulier, avec $\beta = \alpha$, $\alpha \notin \alpha$.
Ainsi, $\alpha \in \alpha \Longrightarrow \alpha \notin \alpha$, donc $\alpha \notin \alpha$.

24°) Pour tout $x \in \beta$, par transitivité de α, $x \in \alpha$, donc $\beta \subset \alpha$. Or il est clair que si $(E, <)$ est bien ordonné, toute partie de E est également bien ordonnée par $<$, donc $(\beta, \in)$ est bien ordonné.
Supposons de plus que $x \in y \in \beta$. On a $y \in \beta \in \alpha$, donc par transitivité de α, $y \in \alpha$, donc on a $x \in y \in \alpha$, donc à nouveau par transitivité de α, $x \in \alpha$. Ainsi, x, y, β sont trois éléments de α, or "$\in$" est transititive dans α et $x \in y \in \beta$, donc $x \in \beta$.
Ceci démontre que β est transitif, donc β est un ordinal.

25°) Soit $\beta \in \alpha$.
D'après la transitivité de α, $\beta \subset \alpha$, donc $\beta = \{x \in \alpha \,/\, x \in \beta\} = \{x \in \alpha \,/\, x < \beta\} = S_\beta$.

26°) $\diamond$ Supposons que $\beta \subset \alpha$ et que $\beta \neq \alpha$.
β est un segment initial de α car, si $x \in \beta$ et $y \in \alpha$ avec $y < x$, alors $y \in x \in \beta$, or β est transitif (car c'est un ordinal), donc $y \in \beta$.
Alors, d'après la remarque faite en fin de question 18, $\beta = S_\gamma$, où $\gamma = \min(\alpha \setminus \beta)$. D'après la question précédente, $\beta = \gamma$, or $\gamma \in \alpha$, donc $\beta \in \alpha$.
$\diamond$ Réciproquement, si $\beta = \alpha$ alors $\beta \subset \alpha$ et si $\beta \in \alpha$, pour tout $x \in \beta$, α étant transitif, on a bien $x \in \alpha$, donc on a aussi $\beta \subset \alpha$.

27°)

- Soit $x \in \alpha^+$. Si $x \in \alpha$ alors $x \notin x$ car α est un ordinal donc "$\in$" est antiréflexive sur α. Sinon, alors $x = \alpha$ et d'après la question 23, $x \notin x$. Ainsi, "$\in$" est antiréflexive sur α^+.
- Soit $x, y, z \in \alpha^+$ tels que $x \in y \in z$. Si $x, y, z \in \alpha$, alors $x \in z$ par transitivité de $\in$ sur α. Sinon, parmi x, y, z, l'un au moins est égal à α. Mais si $z \neq \alpha$, alors $x \in y \in z \in \alpha$, donc par transitivité de α, $x, y \in \alpha$ et d'après la question 23, $x \neq \alpha$ et $y \neq \alpha$. Ainsi $z = \alpha$ et $x \in y \in \alpha$. Toujours par transitivité de α, $x \in \alpha = z$. Ainsi, dans tous les cas, $x \in z$.
  Ceci prouve que $(\alpha^+, \in)$ est ordonné (strictement).
- Soit A une partie non vide de α^+. Si $A \subset \alpha$, elle possède un minimum car α est bien ordonné. Si $A = \{\alpha\}$, alors $\min(A) = \alpha$. Il reste le cas où $\alpha \in A$ et $A \cap \alpha \neq \emptyset$. Alors, α étant bien ordonné, on peut poser $m = \min(A \cap \alpha)$. $m \in \alpha$ c'est-à-dire $m < \alpha$, donc $m = \min(A)$.
  Ceci prouve que $(\alpha^+, \in)$ est bien ordonné.
- Supposons que $x \in \alpha^+$ et que $y \in x$.
  Si $x \in \alpha$, alors $y \in \alpha$ car α est transitif, donc $y \in \alpha^+$.
  Sinon, $x = \alpha$, donc $y \in \alpha$ puis $y \in \alpha^+$.
  Ceci prouve que α^+ est transitif.
- Soit β un ordinal tel que $\alpha \in \beta$.
  D'après la question précédente, $\alpha \subset \beta$ et $\{\alpha\} \subset \beta$, donc $\alpha^+ \subset \beta$.

28°) Posons $\gamma = \alpha \cap \beta$. Montrons que γ est un ordinal.
$(\alpha, \in)$ est bien ordonné, donc c'est le cas de toute partie de α. Ainsi, $(\gamma, \in)$ est bien ordonné.
Soit $x \in \gamma$ et $y \in x$. On a $y \in x \in \alpha$ et α est transitif, donc $y \in \alpha$. De même on montre que $y \in \beta$, donc $y \in \alpha \cap \beta = \gamma$. Ceci prouve que γ est transitif, donc c'est un ordinal.
Si $\gamma = \alpha$, alors $\alpha \subset \beta$, donc d'après la question 26, $\alpha \in \beta$ ou $\alpha = \beta$.
De même, si $\gamma = \beta$, on montre que $\beta \in \alpha$ ou $\alpha = \beta$.
Il reste à étudier le cas où $\gamma \neq \alpha$ et $\gamma \neq \beta$. γ est un ordinal inclus dans α et dans β, donc toujours d'après la question 26, $\gamma \in \alpha$ et $\gamma \in \beta$. On en déduit que $\gamma \in (\alpha \cap \beta) = \gamma$, ce qui est impossible d'après la question 23. Ainsi le cas où $\gamma \neq \alpha$ et $\gamma \neq \beta$ ne se produit jamais et la question est démontrée.

29°)

- Pour tout $\alpha \in A$, d'après la question 23, $\alpha \notin \alpha$, donc $\in$ est antiréflexive sur A.
- Soit $\alpha, \beta, \gamma \in A$ tels que $\alpha \in \beta \in \gamma$. γ est transitif, donc $\alpha \in \gamma$.
  Ainsi, $\in$ est un ordre strict sur A.
- Soit B une partie non vide de A. Il reste à montrer que B possède un minimum.
  Posons $m = \bigcap_{\beta \in B} \beta$.
  En adaptant la preuve de la question précédente, on montre que m est un ordinal.
  Pour tout $\beta \in B$. $m \subset \beta$, donc d'après la question 26, $m = \beta$ ou $m \in \beta$. Mais si pour tout $\beta \in B$, $m \in \beta$, alors $m \in \bigcap_{\beta \in B} \beta = m$ ce qui est impossible d'après la question 23. Ainsi il existe $\beta \in B$ tel que $m = \beta$, donc $m \in B$.
  On vient de voir que pour tout $\beta \in B$ avec $\beta \neq m$, $m \in \beta$, donc m est bien le minimum de B pour la relation d'appartenance.

30°) Posons $\beta = \bigcup_{\alpha \in A} \alpha$.
Si $x \in \beta$, il existe $\alpha \in A$ tel que $x \in \alpha$, donc x est un élément d'un ordinal. D'après la question 24, x est aussi un ordinal. Ainsi, β est un ensemble d'ordinaux, donc d'après la question précédente, $(\beta, \in)$ est bien ordonné. Il reste à montrer que β est transitif.
Soit $x \in \beta$ et $y \in x$. Il existe $\alpha \in A$ tel que $x \in \alpha$, or α est transitif, donc $y \in \alpha$, donc $y \in \beta$.

4 Le théorème de Goodstein

31°) $g_n \neq 0$, donc $g_{n+1} + 1 = f_{q+n,q+n+1}(g_n)$. Ainsi,
$f_{q+n+1,\omega}(g_{n+1} + 1) = f_{q+n+1,\omega}(f_{q+n,q+n+1}(g_n))$, donc on conclut si l'on démontre que $f_{q+n+1,\omega}(f_{q+n,q+n+1}(g_n)) = f_{q+n,\omega}(g_n) = \alpha_n$.
Pour cela, on fixe $q \in \mathbb{N}$ avec $q \geq 2$ et on montre par récurrence forte sur n que, pour tout $n \in \mathbb{N}$, $f_{q+1,\omega}(f_{q,q+1}(n)) = f_{q,\omega}(n)$. Notons $T(n)$ cette assertion.
Initialisation : Si $n \in \{0, \ldots, q-1\}$, alors $f_{q+1,\omega}(f_{q,q+1}(n)) = f_{q+1,\omega}(n) = \overline{n} = f_{q,\omega}(n)$.
Hérédité : Supposons maintenant que $n \geq q$ et que $T(k)$ est vraie

pour tout $k \in \{0, \dots, n-1\}$.

On peut écrire $n = \sum_{i=0}^{k} a_i \, q^i$, avec $k \in \mathbb{N}$, $a_k \neq 0$ et pour tout $i \in \{0, \dots, k\}$, $a_i \in \{0, \dots, q-1\}$. Ainsi, $n \geq q^k \geq 2^k > k$, donc on peut utiliser $T(i)$ pour tout $i \in \{0, \dots, k\}$. Ainsi,

$$f_{q+1,\omega}(f_{q,q+1}(n)) = f_{q+1,\omega}\Big(\sum_{i=0}^{k} a_i \, (q+1)^{f_{q,q+1}(i)}\Big) = \sum_{i=0}^{k} \omega^{f_{q+1,\omega}(f_{q,q+1}(i))}\overline{a_i},$$

donc $f_{q+1,\omega}(f_{q,q+1}(n)) = \sum_{i=0}^{k} \omega^{f_{q,\omega}(i)}\overline{a_i} = f_{q,\omega}(n)$.

Remarque : Nous avons utilisé la convention suivante : si $(\alpha_h)_{0 \leq h \leq k}$ est une famille de $k+1$ ordinaux, alors $\sum_{h=0}^{k} \alpha_h = \alpha_k + \alpha_{k-1} + \cdots + \alpha_0$. Nous poursuivons le corrigé en conservant cette même convention.

32°) Il suffit de montrer que, pour tout $x \in \mathbb{N}$, $f_{n,\omega}(x+1) > f_{n,\omega}(x)$ (car un ensemble d'ordinaux est ordonné par $\in$ d'après la question 29). Démontrons-le par récurrence.

Initialisation : Lorsque $x = 0$, $f_{n,\omega}(0) = \overline{0} < \overline{1} = f_{n,\omega}(1)$, car $\overline{1} = \overline{0}^{+} = \emptyset \cup \{\emptyset\} = \{\emptyset\}$, donc $\overline{0} = \emptyset \in \overline{1}$.

Hérédité : On suppose que $x \geq 1$ et que,
pour tout $y \in \{0, \dots, x-1\}$, $f_{n,\omega}(y+1) > f_{n,\omega}(y)$.
Montrons que $f_{n,\omega}(x+1) > f_{n,\omega}(x)$. On note f à la place de $f_{n,\omega}$.

$\{h \in \mathbb{N} \ / \ n^h \leq x+1\}$ est non vide et il est majoré par $\dfrac{\ln(x+1)}{\ln n}$, donc il possède un maximum, que l'on notera k. Ainsi, $n^k \leq x+1 < n^{k+1}$.

$\{b \in \mathbb{N} \ / \ bn^k \leq x+1\}$ est non vide et majoré, donc il possède également un maximum, que l'on note a. Ainsi, $an^k \leq x+1 < (a+1)n^k$.

Si l'on pose $j = x+1-an^k$, on a donc $0 \leq j < n^k$.

Par construction, $an^k < n^{k+1}$, donc $a \in \{0, \dots, n-1\}$, or $x+1 = an^k + j$, donc si l'écriture de j en base n est $j = \sum_{i=0}^{h} a_i n^i$, celle de $x+1$ est $x+1 = an^k + \sum_{i=0}^{h} a_i n^i$.

Ceci démontre que $f(x+1) = \omega^{f(k)}\overline{a} + f(j)$.

Premier cas : Supposons que $j \neq 0$.

Alors on a également $x = an^k + (j-1)$ avec $j - 1 \in \{0, \dots, n^k - 1\}$, donc pour les mêmes raisons, $f(x) = \omega^{f(k)}\overline{a} + f(j-1)$.

$a \geq 1$, car $1 \times n^k \leq x+1$ et $n^k \geq 1$, donc $j = x+1-an^k \leq x$. Ainsi, d'après l'hypothèse de récurrence, $f(j-1) < f(j)$. Alors, d'après la propriété admise numéro 2, $f(x+1) > f(x)$.

Second cas : On suppose maintenant que $j = 0$.

Alors $f(x+1) = \omega^{f(k)}\overline{a}$. D'autre part $x = an^k - 1 = (a-1)n^k + \sum_{i=0}^{k-1}(n-1)n^i$, d'après

la question 7, donc $f(x) = \omega^{f(k)}\overline{(a-1)} + \sum_{i=0}^{k-1} \omega^{f(i)}\overline{(n-1)}$.

D'après la propriété 1 puis la définition de la suite $(\overline{n})$, $\overline{(a-1)}+\overline{1} = \overline{(a-1)^+} = \overline{a}$, donc d'après les propriétés 5 et 8, $f(x+1) = \omega^{f(k)}\overline{(a-1)} + \omega^{f(k)}\overline{1} = \omega^{f(k)}\overline{(a-1)} + \omega^{f(k)}$.

D'après la propriété 2, il suffit donc de montrer que $\omega^{f(k)} > \sum_{i=0}^{k-1} \omega^{f(i)}\overline{(n-1)}$.

Si $k = 0$, $f(x+1) = \overline{a}$ et $f(x) = \overline{(a-1)}$, or pour tout ordinal α, $\alpha \in \alpha^+$, donc $\overline{(a-1)} \in \overline{a}$, c'est-à-dire $\overline{(a-1)} < \overline{a}$. Dans ce cas, on a bien $f(x+1) > f(x)$.

Si $k = 1$, $\omega^{f(k)} = \omega^{\overline{1}} = \omega$ (prop 6) et $\sum_{i=0}^{k-1} \omega^{f(i)}\overline{(n-1)} = \overline{(n-1)}$ (prop 6 et 8).

Mais on a vu que $\overline{(n-1)} \in \overline{n}$. De plus $\omega = \bigcup_{n\in\mathbb{N}} \overline{n}$,

donc $\overline{(n-1)} \in \omega$, c'est-à-dire $\overline{(n-1)} < \omega$. Ainsi, lorsque $k = 1$, on a montré que $f(x+1) > f(x)$.

On peut maintenant supposer que $k \geq 2$.

D'après la question 3, $2^x \geq x+1$, donc $n^x \geq x+1$. Ainsi, par définition de k, $k \leq x$. Alors, d'après l'hypothèse de récurrence, $f(k) > f(k-1)$. On a donc $f(k-1) \in f(k)$, donc d'après la question 27, $f(k-1)^+ \subset f(k)$, puis d'après la question 26,
$f(k-1) + \overline{1} = f(k-1)^+ \leq f(k)$.

D'après la prop 4, sachant que $\omega > \overline{1}$ (on a vu que, pour tout $n \in \mathbb{N}$, $\omega > \overline{n}$), $\omega^{f(k)} \geq \omega^{f(k-1)+\overline{1}} = \omega^{f(k-1)}\omega$ (prop 7), donc (prop 3) $\omega^{f(k)} \geq \omega^{f(k-1)}\overline{n}$. Ainsi, pour conclure, il suffit de montrer que $\omega^{f(k-1)}\overline{n} > \sum_{i=0}^{k-1} \omega^{f(i)}\overline{(n-1)}$.

Or d'après la prop 5, $\omega^{f(k-1)}\overline{n} = \omega^{f(k-1)}\overline{(n-1)} + \omega^{f(k-1)}$, donc (prop 2) il suffit de montrer que $\omega^{f(k-1)} > \sum_{i=0}^{k-2} \omega^{f(i)}\overline{(n-1)}$, c'est-à-dire que

$$f(n^{k-1}) > f\Big(\sum_{i=0}^{k-2} (n-1)n^i\Big) = f(n^{k-1}-1).$$

Mais $n^{k-1} < n^k \leq x+1$, donc $n^{k-1} \leq x$. Alors, d'après l'hypothèse de récurrence, on a bien $f(n^{k-1}) > f(n^{k-1}-1)$.

On a ainsi démontré dans tous les cas que $f(x+1) > f(x)$.

33°) Si $g_n \neq 0$, alors $\alpha_n = f_{q+n+1,\omega}(g_{n+1}+1)$, donc d'après la question précédente, $\alpha_n > f_{q+n+1,\omega}(g_{n+1}) = \alpha_{n+1}$.

L'ensemble $A = \{\alpha_n \ / \ n \in \mathbb{N}\}$ est un ensemble non vide d'ordinaux, donc d'après la question 29, il possède un minimum, de la forme α_{n_0} où $n_0 \in \mathbb{N}$. Alors $\alpha_{n_0+1} \geq \alpha_{n_0}$, donc $g_{n_0} = 0$, ce qui démontre le théorème de Goodstein.