Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
http://www.math.jussieu.fr/∼miw/

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

`Les calculatrices ne sont pas autorisées, les documents non plus,`
`les téléphones portables encore moins`

Examen du lundi 18 Juin 2007

Barême approximatif : sur 30

(2) **Exercice 1.** Un corps fini peut-il être algébriquement clos ?

(7) **Exercice 2.** Quand m est un entier positif, on désigne par $k_m = \mathbf{Q}(\zeta_m)$ le corps cyclotomique d'indice m, où ζ_m est une racine primitive m-ième de l'unité. Soient m et n deux entiers positifs.

a) On suppose que n divise m. Montrer que k_n est un sous-corps de k_m.

b) On suppose encore que n divise m. Montrer que k_m/k_n est une extension galoisienne et décrire le groupe de Galois.

Expliciter l'exemple $n = 3$, $m = 15$.

c) Quel est le degré de l'extension k_{2n}/k_n ?

d) On suppose que k_n est un sous-corps de k_m et que n ne divise pas m. Montrer que m est impair, n est pair et n divise $2m$.

`Indication.` *on pourra admettre le fait que les nombres premiers impairs qui se ramifient dans l'extension* $k_n/\mathbf{Q}$ *(c'est-à-dire ceux divisent le discriminant absolu de* k_n*) sont ceux qui divisent* n.

(10) **Exercice 3.**

Quand K est un corps de nombres, on note $r_1(K)$ le nombre de plongements réels de K et $2r_2(K)$ le nombre de plongements complexes non réels, de sorte que $[K : \mathbf{Q}] = r_1(K) + 2r_2(K)$. Le corps K est *totalement réel* si $r_2(K) = 0$, il est *totalement imaginaire* si $r_1(K) = 0$.

On note aussi $r(K)$ le rang du groupe des unités de K.

a) Rappeler la formule qui relie $r(K)$ à $r_1(K)$ et $r_2(K)$.

b) Soit L un sous-corps de $\mathbf{C}$ qui est une extension finie de $\mathbf{Q}$ et soit K un sous-corps de L avec $K \neq L$. Montrer que les conditions suivantes sont équivalentes.

(i) Le groupe des unités de K est un sous-groupe d'indice fini du groupe des unités de L.

(ii) $r(K) = r(L)$.

(iii) Le corps K est totalement réel, L est totalement imaginaire et $[L : K] = 2$.

c) Montrer que, si les conditions (i), (ii) et (iii) sont vérifiées, alors $L \cap \mathbf{R} = K$.

d) Soit L une extension galoisienne de $\mathbf{Q}$ de degré n. Montrer que le corps L est soit totalement réel, soit totalement imaginaire.

e) On suppose encore que L est une extension galoisienne de $\mathbf{Q}$ de degré n. Soit K le sous-corps de L fixé par la conjugaison complexe. On note G le groupe de Galois de L sur $\mathbf{Q}$ et H le sous-groupe engendré par la conjugaison complexe.

À quelle condition peut-on affirmer que l'extension $K/\mathbf{Q}$ est galoisienne ?

Donner un exemple où l'extension $K/\mathbf{Q}$ n'est pas galoisienne.

On suppose que l'extension $K/\mathbf{Q}$ est galoisienne. Montrer que le groupe des unités de K est un sous-groupe d'indice fini du groupe des unités de L.
Quel est le rang du groupe des unités du corps cyclotomique $L = \mathbf{Q}(\zeta_8)$ des racines 8èmes de l'unité ? Quel est son sous-corps réel maximal K ? Quel est le rang du groupe des unités de K ?

(5) **Exercice 4.** Soient p un nombre premier, $s \geq 0$ et $f \geq 1$ deux entiers, m un entier positif non divisible par p. On pose $q = p^f$ et $n = p^s m$. On désigne par $\mathbf{F}_q$ un corps fini à q éléments. On désigne par Φ_n et Φ_m les polynômes cyclotomiques d'indice n et m et par $\varphi(n)$ et $\varphi(m)$ leurs degrés (φ est la fonction d'Euler).
a) Montrer que dans $\mathbf{F}_q[X]$ on a

$$\Phi_n(X) = \Phi_m(X)^{\varphi(p^s)}.$$

b) On désigne par r l'ordre de q modulo m. Montrer que Φ_m est produit de $\varphi(m)/r$ polynômes unitaires irréductibles distincts dans $\mathbf{F}_q[X]$, chacun d'eux étant de degré r.

(6) **Exercice 5.** Soit k un entier ≥ 0 et s un nombre réel $> k$. Pour n entier ≥ 1 on pose

$$\sigma_k(n) = \sum_{d|n} d^k.$$

a) Vérifier

$$\zeta(s)\zeta(s-k) = \sum_{n\geq 1} \frac{\sigma_k(n)}{n^s}\cdot$$

b) Montrer que si m et n sont deux entiers positifs premiers entre eux on a

$$\sigma_k(mn) = \sigma_k(m)\sigma_k(n).$$

c) Calculer $\sigma_k(p^a)$ quand p est un nombre premier et a un entier ≥ 0.
d) Vérifier

$$\sum_{n\geq 1} \frac{\sigma_k(n)}{n^s} = \prod_p \bigl(1 - (p^k+1)p^{-s} + p^{k-2s}\bigr)^{-1}.$$

Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
http://www.math.jussieu.fr/∼miw/

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Examen du Lundi 18 Juin 2007
Corrigé

Exercice 1. Il y a de nombreuses raisons pour qu'un corps fini ne soit pas algébriquement clos. On a vu en cours que pour tout nombre premier p et toute puissance $q = p^r$ de p, il existe un corps fini ayant p^r éléments et qu'un tel corps est unique à isomorphisme près. De plus un corps à p^r éléments contient un sous-corps à p^s éléments si et seulement si s divise r. Donc pour tout corps fini k à p^s éléments et pour tout entier $d > 0$ il existe au moins une extension de k de degré d, par conséquent il existe un polynôme irréductible à coefficients dans k de degré d.

Un autre argument consiste à dire qu'un corps fini F ayant q éléments contient les racines m-ièmes de l'unité (avec m entier premier avec q) si et seulement si m divise $q - 1$, c'est-à-dire si q est congru à 1 modulo m. Si un entier m premier avec q ne satisfait pas cette condition (par exemple $m = q + 1$) alors le polynôme $X^m - 1$ n'est pas totalement décomposé dans F.

On peut encore adapter l'argument d'Euclide pour montrer qu'il y a une infinité de polynômes irréductibles sur un corps donné K. En effet si $f_1, \ldots, f_r$ sont des polynômes irréductibles de $K[X]$ alors $1 + f_1 \cdots f_r$ est divisible par un polynôme irréductible qui n'est pas dans l'ensemble $\{f_1, \ldots, f_r\}$. Par exemple si F est un corps fini le polynôme

$$1 + \prod_{\alpha \in F} (X - \alpha) \in F[X]$$

admet un facteur irréductible de degré > 1 dans $F[X]$.

Exercice 2.

a) Quand n divise m, comme le sous-groupe de $k_m^\times$ formé par les racines de $X^m - 1$ est cyclique d'ordre m, il contient un unique sous-groupe d'ordre n, qui est cyclique formé par les racines n-ièmes de l'unité. Donc $k_n \subset k_m$.

b) Si n divise m on peut écrire $m = dn$. On prend $\zeta_n = \zeta_m^d$ (c'est bien une racine primitive n-ième de l'unité). À chaque entier h de l'intervalle $1 \le h \le m$ qui est premier avec m on associe l'automorphisme σ_h de k_m qui est déterminé par la condition $\sigma_h(\zeta_m) = \zeta_m^h$. L'application $h \mapsto \sigma_h$ définit un isomorphisme du groupe multiplicatif $(\mathbf{Z}/m\mathbf{Z})^\times$ sur le groupe de Galois $G = \mathrm{Gal}(k_m/\mathbf{Q})$ de l'extension $k_m/\mathbf{Q}$. Soit H le sous-groupe de G formé des éléments qui fixent ζ_n : c'est le groupe de Galois de k_m/k_n. Le quotient de G par H est isomorphe au groupe de Galois de k_n sur $\mathbf{Q}$, donc à $(\mathbf{Z}/n\mathbf{Z})^\times$.

On peut aussi décrire la situation de la manière suivante : comme l'idéal $m\mathbf{Z}$ est contenu dans $n\mathbf{Z}$, les surjections canoniques de $\mathbf{Z}$ sur les quotients $\mathbf{Z}/m\mathbf{Z}$ et $\mathbf{Z}/n\mathbf{Z}$ induisent un homomorphisme d'anneaux ψ de $\mathbf{Z}/m\mathbf{Z}$ sur $\mathbf{Z}/n\mathbf{Z}$ qui envoie une classe h modulo m sur la classe de h modulo n. La restriction de ψ au groupe multiplicatif $(\mathbf{Z}/m\mathbf{Z})^\times$ est un homomorphisme surjectif de groupes

$(\mathbf{Z}/m\mathbf{Z})^\times \to (\mathbf{Z}/n\mathbf{Z})^\times$ dont le noyau, qui n'est autre que H, est formé des classes h modulo m avec $h \equiv 1 \pmod n$: on vérifie d'ailleurs que pour $h \equiv 1 \pmod n$, on a $dh \equiv d \pmod m$, donc

$$\sigma_h(\zeta_n) = \zeta_n^h = \zeta_m^{dh} = \zeta_m^d = \zeta_n.$$

Pour obtenir les éléments du groupe de Galois de $k_n/\mathbf{Q}$, on choisit dans chacune des classes de G modulo H un représentant et on prend sa restriction à k_n.
Dans l'exemple $n = 3$, $m = 15$, on peut prendre $\zeta_3 = \zeta_{15}^5$. Le groupe $G = \mathrm{Gal}(k_{15}/\mathbf{Q})$ est d'ordre $\varphi(15) = 8$, ses éléments σ_h peuvent être indexés par les entiers $h = 1, 2, 4, 7, 8, 11, 13, 14$ qui sont les entiers de l'intervalle $1 \le h \le 15$ premiers avec 15, avec $\sigma_h(\zeta) = \zeta^h$. Les éléments de G qui fixent k_3 sont ceux dont l'indice est congru à 1 modulo 3, c'est-à-dire σ_1, σ_4, σ_7 et σ_{13}. La restriction à k_3 de l'un quelconque des quatre autres automorphismes σ_2, σ_8, σ_{11}, σ_{14} est l'automorphisme non trivial de k_3.
c) Si n est impair on a $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$, donc $k_{2n} = k_n$ et $[k_{2n} : k_n] = 1$.
Si n est pair on a $\varphi(2n) = 2\varphi(n)$, donc k_{2n} est une extension quadratique de k_n et $[k_{2n} : k_n] = 2$.
d) Pour commencer on considère le cas m et h sont deux entiers tels que $k_h = k_m$ et $m < h$. On remarque d'abord que la condition $k_m = k_h$ implique que h et m ont les même diviseurs premiers impairs, car ce sont les diviseurs premiers impairs du discriminant absolu de k_m. Si

$$m = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{et} \quad h = 2^{\beta_0} p_1^{\beta_1} \cdots p_r^{\beta_r},$$

avec $p_1, \dots, p_r$ nombres premiers impairs deux à deux distincts, $\alpha_0 \ge 0$ $\beta_0 \ge 0$, $\alpha_i \ge 1$ et $\beta_i \ge 1$ pour $1 \le i \le r$, on a

$$\varphi(m) = 2^{\alpha_0'} p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1) \quad \text{et} \quad \varphi(h) = 2^{\beta_0'} p_1^{\beta_1 - 1}(p_1 - 1) \cdots p_r^{\beta_r - 1}(p_r - 1),$$

avec $\alpha_0' = \max\{0, \alpha_0 - 1\}$, $\beta_0' = \max\{0, \beta_0 - 1\}$. On déduit alors facilement de l'égalité $\varphi(h) = \varphi(m)$ que $\alpha_i = \beta_i$ pour $1 \le i \le r$ et $\alpha_0' = \beta_0'$. L'hypothèse $m < h$ entraîne alors $h = 2m$, $\alpha_0 = 0$ (donc m est impair) et $\beta_0 = 1$.
Il en résulte que si n et m sont deux entiers positifs pour lesquels $k_n \subset k_m$ et n ne divise pas m, alors $k_m = k_h$ avec $h = \mathrm{ppcm}(m, n) > m$, donc $h = 2m$, n divise $2m$, de plus m est impair et n est pair.

Exercice 3.

a) Le rang du groupe des unités de $r(K)$ est donné par la formule de Dirichlet

$$r(K) = r_1(K) + r_2(K) - 1.$$

b) L'équivalence entre (i) et (ii) est banale : le groupe des unités $\mathbf{Z}_K^\times$ de K est un sous-groupe du groupe des unités $\mathbf{Z}_K^\times$ de L, et $\mathbf{Z}_K^\times$ est d'indice fini dans $\mathbf{Z}_L^\times$ si et seulement si les deux groupes ont le même rang.

Si K est totalement réel on a $r_1(K) = [K : \mathbf{Q}]$ et $r_2(K) = 0$, donc $r(K) = [K : \mathbf{Q}] - 1$. Si L est totalement imaginaire on a $r_1(L) = 0$ et $r_2(L) = [L : \mathbf{Q}]$, d'où $r(L) = [L : \mathbf{Q}]/2 - 1$. Si de plus $[L : K] = 2$ alors $[L : \mathbf{Q}] = 2[K : \mathbf{Q}]$ et $r(K) = r(L)$. Ceci montre que (iii) implique (ii).

Pour démontrer la réciproque écrivons

$$r_1 = r_1(K),\ r_2 = r_2(K),\ n = [K : \mathbf{Q}] = r_1 + 2r_2,$$

$$r_1' = r_1(L),\ r_2' = r_2(L),\ n' = [L:\mathbf{Q}] = r_1' + 2r_2'.$$

L'hypothèse $r(K) = r(L)$ s'écrit

$$r_1 + r_2 = r_1' + r_2'.$$

Comme L est une extension de K de degré ≥ 2 on a aussi $n' \geq 2n$, c'est-à-dire

$$2r_1 + 4r_2 \leq r_1' + 2r_2'.$$

Alors $2r_1 + 4r_2 \leq 2(r_1 + r_2) - r_1'$, ce qui donne $r_1' + 2r_2 \leq 0$. Donc

$$r_1' = r_2 = 0, \quad r_1 = n, \quad r_2' = n'/2, \quad r(K) = n-1, \quad r(L) = (n'/2) - 1$$

et finalement $n' = 2n$. Ainsi (ii) implique (iii).
c) Comme L est une extension totalement imaginaire de $\mathbf{Q}$, ce n'est pas un sous-corps de $\mathbf{R}$. Alors $L \cap \mathbf{R}$ est un sous corps de L distinct de L et qui contient K ; comme $[L:K] = 2$ on en déduit $K = L \cap \mathbf{R}$.
d) Quand L est un corps de nombres d'après le théorème de l'élément primitif on peut écrire $L = \mathbf{Q}(\alpha)$. Supposons que L admette un plongement réel : soit $\alpha' \in \mathbf{R}$ l'image de α par ce plongement. Alors $L' = \mathbf{Q}(\alpha')$ est un sous-corps de $\mathbf{R}$, il est isomorphe à L et donc galoisien sur $\mathbf{Q}$, donc tous les conjugués de α' sont dans L', et par conséquent sont réels. Il en résulte qu'une extension galoisienne de $\mathbf{Q}$ est soit totalement réelle, soit totalement imaginaire.
e) Quand l'extension $L/\mathbf{Q}$ est galoisienne de groupe de Galois G et que K est un sous-corps de L, le sous-groupe H de G associé à K par la correspondance de Galois est formé des éléments de G qui fixent K. L'extension $K/\mathbf{Q}$ est galoisienne si et seulement si H est un sous-groupe normal de G, dans ce cas le groupe de Galois de $K/\mathbf{Q}$ est isomorphe au groupe quotient de G par H. La conjugaison complexe est un élément de $\mathrm{Gal}(L/\mathbf{Q})$ dont le carré est 1 (c'est une involution), donc cet élément est d'ordre 1 ou 2 (selon que L est totalement réel ou totalement imaginaire).

Dans l'exemple habituel $L = \mathbf{Q}(j, \sqrt[3]{2})$, le sous-corps fixé par la conjugaison complexe est $K = \mathbf{Q}(\sqrt[3]{2})$ qui n'est pas galoisien sur $\mathbf{Q}$. Le rang du groupe des unités de L est 2 car $r_1(L) = 0$ et $r_2(L) = 3$, celui de K est 1 car $r_1(K) = r_2(K) = 1$.

On suppose maintenant l'extension $K/\mathbf{Q}$ galoisienne. Alors K est un corps totalement réel d'après la question d).
Si L est un sous-corps de $\mathbf{R}$ (la conjugaison complexe est d'ordre 1, elle agit comme l'identité sur L) on a $K = L$ et $\mathbf{Z}_K^\times = \mathbf{Z}_L^\times$.
Si L n'est pas un sous-corps de $\mathbf{R}$ alors la conjugaison complexe est d'ordre 2 dans $\mathrm{Gal}(L/\mathbf{Q})$, donc l'extension L/K est de degré 2, L est totalement imaginaire, K est totalement réel et par ce qui précède $\mathbf{Z}_K^\times$ est un sous-groupe d'indice fini de $\mathbf{Z}_L^\times$.

Le corps $\mathbf{Q}(\zeta_8)$ est une extension de degré $\varphi(8) = 4$ (quartique) de $\mathbf{Q}$, engendrée par i et $\sqrt{2}$, galoisienne sur $\mathbf{Q}$ et totalement imaginaire, son groupe des unités est de rang 1 (car $r_1 = 0$ et $r_2 = 2$), le sous-corps réel maximal (fixé par la conjugaison complexe) est $K = \mathbf{Q}(\sqrt{2})$, c'est un corps quadratique réel dont le groupe des unités est aussi de rang 1 (car $r_1 = 1$ et $r_2 = 0$).

Exercice 4 On a d'une part

$$X^n - 1 = \prod_{e|n} \Phi_e(X).$$

Quand $n = p^s m$ un diviseur e de n s'écrit de manière unique $e = p^j d$ avec $0 \leq j \leq s$ et d divise m. Dans cette écriture le diviseur $e = n$ correspond à $j = s$, $d = m$. Ceci permet d'écrire

$$\prod_{e|n} \Phi_e(X) = \prod_{j=0}^{s} \prod_{d|m} \Phi_{p^j d}(X). \tag{1}$$

D'autre part en caractéristique p on a

$$X^n - 1 = X^{p^s m} - 1 = (X^m - 1)^{p^s} = \prod_{d|m} \Phi_d(X)^{p^s}.$$

On va démontrer la relation demandée

$$\Phi_n(X) = \Phi_m(X)^{\varphi(p^s)}$$

dans $\mathbf{F}_q[X]$ par récurrence sur n. Elle est triviale pour $s = 0$ avec $\varphi(1) = 1$, $n = m$. Si elle est satisfaite pour tous les diviseurs stricts de n, alors dans le membre de droite de (1) le facteur correspondant à $d \mid m$, $d \neq m$ est

$$\prod_{j=0}^{s} \Phi_{p^j d}(X) = \prod_{j=0}^{s} \Phi_d(X)^{\varphi(p^j)} = \Phi_d(X)^{1+(p-1)+(p-1)p+\cdots+(p-1)p^{s-1}} = \Phi_d(X)^{p^s},$$

tandis que celui correspondant à $d = m$ est

$$\begin{aligned}\prod_{j=0}^{s} \Phi_{p^j m}(X) &= \Phi_n(X) \prod_{j=0}^{s-1} \Phi_m(X)^{\varphi(p^j)} \\ &= \Phi_n(X)\Phi_m(X)^{1+(p-1)+(p-1)p+\cdots+(p-1)p^{s-2}} \\ &= \Phi_n(X)\Phi_m(X)^{p^{s-1}}.\end{aligned}$$

En identifiant les facteurs on trouve

$$\Phi_n(X)\Phi_m(X)^{p^{s-1}} = \Phi_m(X)^{p^s}.$$

La relation demandée en résulte puisque $\varphi(p^s) = p^s - p^{s-1}$.
b) Comme p ne divise pas m le polynôme $X^m - 1$ a une dérivée non nulle, donc il n'a pas de facteurs multiples. Il en est de même à plus forte raison pour $\Phi_m(X)$.

Soient P un facteur irréductible de Φ_m dans $\mathbf{F}_q[X]$, t son degré et F un corps de rupture de P sur $\mathbf{F}_q$. Le corps F a donc q^t éléments. Soit $\zeta \in F$ une racine de P. On a $P(\zeta) = 0$, donc $\Phi_m(\zeta) = 0$, ce qui signifie que ζ est une racine primitive m-ième de l'unité : ζ est d'ordre m dans le groupe multiplicatif $F^\times$ qui est d'ordre $q^t - 1$. Alors (Lagrange) m divise $q^t - 1$, c'est à dire $q^t \equiv 1 \pmod{m}$. Cela signifie que t est multiple de l'ordre r de q modulo m.

D'autre part on a $q^r \equiv 1 \pmod{m}$ et $\zeta^m = 1$, donc $\zeta^{q^r} = \zeta$, ce qui signifie que ζ appartient à un corps E ayant q^r éléments. Comme $F = \mathbf{F}_q(\zeta)$ a q^t éléments l'inclusion $F \subset E$ implique que t divise r. Finalement $t = r$ et tous les facteurs irréductibles de Φ_m ont le même degré r. Leur nombre est alors $\varphi(m)/r$.

Exercice 5. Comme $\sigma_k(n) \leq n^k$, la série de Dirichlet

$$\sum_{n\geq 1} \frac{\sigma_k(n)}{n^s}$$

converge (absolument et uniformément sur tout compact) dans le demi plan $\Re s > k$ (donc à plus forte raison pour s réel $> k$).
a) Dans ce demi plan on a

$$\zeta(s)\zeta(s-k) = \sum_{h\geq 1}\sum_{d\geq 1} \frac{1}{h^s}\frac{1}{d^{s-k}} = \sum_{n\geq 1}\frac{1}{n^s}\sum_{d|n} d^k = \sum_{n\geq 1}\frac{\sigma_k(n)}{n^s}\cdot$$

b) Si pgcd$(m, n) = 1$ l'application $(h, \ell) \mapsto h\ell$ définit une bijection entre les couples (h, ℓ) où h est un diviseur de m et ℓ un diviseur de n d'une part, et les diviseurs de mn d'autre part. Donc

$$\sigma_k(mn) = \sum_{d|mn} d^k = \sum_{h|m}\sum_{\ell|n}(h\ell)^k = \sum_{h|m} h^k \sum_{\ell|n}\ell^k = \sigma_k(m)\sigma_k(n).$$

c) Soient p est un nombre premier et a un entier ≥ 0. Les diviseurs de p^a sont les entiers $1, p, p^2, \ldots, p^a$, donc

$$\sigma_k(p^a) = 1 + p^k + \cdots + p^{ak} = \frac{p^{k(a+1)} - 1}{p^k - 1}\cdot$$

d) Comme

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}, \quad \zeta(s-k) = \prod_p \frac{1}{1-p^{k-s}}$$

et que

$$(1-p^{-s})(1-p^{k-s}) = 1 - p^{-s}(p^k+1) + p^{k-2s}$$

on a

$$\sum_{n\geq 1}\frac{\sigma_k(n)}{n^s} = \zeta(s)\zeta(s-k) = \prod_p \bigl(1 - (p^k+1)p^{-s} + p^{k-2s}\bigr)^{-1}.$$

On peut aussi bien sûr redémontrer cette formule à partir de la multiplicativité de la fonction σ_k : quand f est une fonction multiplicative et que la série $\sum_{n\geq 1}|f(n)|n^{-s}$ converge on a (cf. feuille 4 de TD)

$$\sum_{n\geq 1} f(n)n^{-s} = \prod_p \sum_{a\geq 0} f(p^a)p^{-as}.$$

Pour $f(n) = \sigma_k(n)$ on a

$$\sigma_k(p^a)p^{-as} = \frac{p^{(a+1)k}-1}{p^k-1}p^{-as} = \frac{p^k}{p^k-1}p^{a(k-s)} - \frac{1}{p^k-1}p^{-as}$$

et

$$\sum_{a\geq 0}\sigma_k(p^a)p^{-as} = \frac{1}{p^k-1}\left(\frac{p^k}{1-p^{k-s}} - \frac{1}{1-p^{-s}}\right) = \frac{1}{(1-p^{k-s})(1-p^{-s})} = \frac{1}{1-(p^k+1)p^{-s}+p^{k-2s}}\cdot$$