Séance du 26/11/08 avec M. LAFFONT

A. Calcul approché de $\int_0^1 f(t)dt$: Méthode des rectangles, des trapèzes , de Simpson.

f désigne une application de [0 ;1] dans $\mathbb{R}$, de classe C^1 et pour tout $n\in\mathbb{N}^*$ on note :

$R_n(f) = \frac{1}{n}\sum_{k=0}^{n-1} f(\frac{k}{n})$, $T_n(f) = \frac{1}{2n}\sum_{k=0}^{n-1} f(\frac{k}{n})+f(\frac{k+1}{n})$ et $S_n(f) = \frac{1}{6n}\sum_{k=0}^{n-1} f(\frac{k}{n})+4f(\frac{2k+1}{2n})+f(\frac{k+1}{n})$

On rappelle que $R_n(f) = \int_0^1 f(t)dt + o(1)$ (somme de Riemann d'une fonction continue) .

1. Vérifier que $R_n(f) + \frac{f(1)-f(0)}{2n} = T_n(f)$ et que $3\,S_n(f) = 4\,T_{2n}(f) - T_n(f)$.

2. Démontrer que : pour tout $n\in\mathbb{N}^*$, il existe $(c_0 ;c_1\ldots\ldots ;c_{n-1}) \in \prod_{k=0}^{n-1}\left[\frac{k}{n} ; \frac{k+1}{n}\right]$ tel que

$$\int_0^1 f(t)dt = R_n(f) + \frac{1}{2n^2}\sum_{k=0}^{n-1} f'(c_k)$$

3. Démontrer que : $R_n(f) = \int_0^1 f(t)dt - \frac{f(1)-f(0)}{2n} + o(\frac{1}{n})$. En déduire que : $T_n(f) = \int_0^1 f(t)dt + o(\frac{1}{n})$.

4. On suppose désormais que f est de classe C^2, démontrer que : pour tout $n\in\mathbb{N}^*$,
il existe $(c_0 ;c_1\ldots\ldots;c_{n-1}) \in \prod_{k=0}^{n-1}\left[\frac{k}{n} ; \frac{k+1}{n}\right]$ tel que $\int_0^1 f(t)dt = R_n(f) + \frac{1}{2n^2}\sum_{k=0}^{n-1} f'(\frac{k}{n}) + \frac{1}{6n^3}\sum_{k=0}^{n-1} f''(c_k)$.

5. Démontrer que: $R_n(f) = \int_0^1 f(t)dt - \frac{f(1)-f(0)}{2n} + \frac{f'(1)-f'(0)}{12n^2} + o(\frac{1}{n^2})$.

6. En déduire que : $T_n(f) = \int_0^1 f(t)dt + \frac{f'(1)-f'(0)}{12n^2} + o(\frac{1}{n^2})$ et $S_n(f) = \int_0^1 f(t)dt + o(\frac{1}{n^2})$.

(Pour $f \in C^\infty$, on montre que $T_n(f) = \int_0^1 f(t)dt + \frac{f'(1)-f'(0)}{12n^2} + \frac{f'''(1)-f'''(0)}{720n^4} + \frac{\alpha_3}{n^6}+\ldots..+\frac{\alpha_p}{n^{2p}} + o(\frac{1}{n^{2p}})$)

B. Méthode des trapèzes : majoration de l'erreur.

Soit $f \in C^2([a ;b] ; \mathbb{R})$ et p la fonction affine telle que : $p(a) = f(a)$, $p(b) = f(b)$

1. Pour t appartenant à]a ;b[, soit g_t la fonction définie sur [a ;b] par :
$g_t(x) = f(x) - p(x) - \frac{f(t)-p(t)}{(t-a)(t-b)}(x-a)(x-b)$. Démontrer qu'il existe $c \in [a ;b]$ tel que $g_t''(c) = 0$.

2. En déduire que : pour tout $t \in [a ;b]$, $|f(t)-p(t)| \leq \frac{M}{2}(t-a)(b-t)$ où $M = \sup_{t\in[a;b]}|f''(t)|$

3. Démontrer que : $\left|\int_a^b f(t)dt - \frac{b-a}{2}(f(a)+f(b))\right| \leq \frac{M(b-a)^3}{12}$

C. Méthode de Simpson : majoration de l'erreur.

On suppose que $f \in C^4([a ;b] ; \mathbb{R})$ et soit Φ l'application de $\mathbb{R}_3[X]$ dans $\mathbb{R}^4$, définie par :

$$\Phi(p) = (p(a) ; p(\frac{a+b}{2}) ; p'(\frac{a+b}{2}) ; p(b))$$

1. Démontrer que Φ est une bijection ; en déduire l'existence d'une fonction polynôme p de degré inférieur ou égal à 3 telle que : $p(a) = f(a)$, $p(\frac{a+b}{2}) = f(\frac{a+b}{2})$, $p'(\frac{a+b}{2}) = f'(\frac{a+b}{2})$, $p(b) = f(b)$.

2. Pour t appartenant à]a ;b[et différent de $\frac{a+b}{2}$, soit g_t la fonction définie sur [a ;b] par :

$$g_t(x) = f(x) - p(x) - \frac{f(t)-p(t)}{(t-a)\left(t-\frac{a+b}{2}\right)^2(t-b)}(x-a)(x-\frac{a+b}{2})^2(x-b) .$$

Démontrer qu'il existe $c\in [a ;b]$ tel que $g_t^{(4)}(c) = 0$.

3. En déduire que : pour tout $t \in [a ;b]$, $|f(t)-p(t)| \leq \frac{M}{4!}(t-a)\left(t-\frac{a+b}{2}\right)^2(b-t)$ où $M = \sup_{t\in[a;b]}|f^{(4)}(t)|$

4. Démontrer que : $\left|\int_a^b f(t)dt - \frac{b-a}{6}(f(a)+4f(\frac{a+b}{2})+f(b))\right| \leq \frac{M(b-a)^5}{2880}$.

Séance du 17/09/08 : fin de correction et compléments

IV) L'anneau A[X]

(A ,+, $\times$) est un anneau commutatif (unitaire) intègre qui n'est pas un corps et A[X] est l'anneau des polynômes de A; soit a un élément de A non nul et non inversible et soit I l'idéal engendré par a et X .

1. On suppose que I = (P).
   a. **Démontrons que deg (P) = 0** : a appartient à I donc a appartient à (P) ; on en déduit qu'il existe un polynôme Q tel que a = PQ ; mais deg(a) = 0 et, A étant intègre, deg(P+Q) = deg(P) + deg(Q) d'où deg(P) = deg(Q) = 0.

   b. **Démontrons que P est inversible dans A :** X appartient à I donc X appartient à (P) ; on en déduit qu'il existe un polynôme Q tel que X = PQ ; mais deg(P) = 0 et deg(X) = 1 donc deg(Q) = 1 donc Q = bX +c et donc X = P(bX+c) = Pb X + Pc ; on en déduit que Pb = 1 (et Pc = 0) donc que P est inversible dans A.
2. **Conclusion** : P étant inversible dans A, (P) = A donc I = A et donc 1 appartient à I ; on en déduit qu'il existe deux polynômes R et S tels que 1 = aR + XS ; soit r_0 le terme constant de R alors on a $1 = ar_0$ et donc a est inversible dans A ; contradiction donc I n'est pas principal. **A[X] n'est donc pas principal.**

COMPLEMENTS : Z[x] est un anneau factoriel

D'après ce qui précède, Z[X] n'est pas un anneau principal, montrons que c'est un anneau factoriel.

Définition : Soit $P = a_nX^n + \ldots a_1X + a_0$ un polynôme non nul de Z[X]. On dit que P est primitif lorsque ses coefficients $a_n,\ldots,a_0$ sont premiers entre-eux dans leur ensemble et que $a_n > 0$.

Lemme. Tout polynôme non nul P appartenant à Q[X] s'écrit P = cPo où $c \in Q^*$ et Po est un polynôme primitif dans Z[X]. Par ailleurs cette écriture est unique. Le polynôme P est à coefficients entiers si et seulement si $c \in$ Z. Si $c \in$ Z alors $|c|$ est le plus grand commun diviseur des coefficients de P et le signe de c est le signe du coefficient dominant de P.

Le nombre rationnel c du lemme est appelé le contenu de P. Si P est à coefficients entiers, son contenu divise P dans Z[X] et par le lemme, le polynôme P est primitif si et seulement si son contenu vaut 1.

Démonstration du lemme : Pour trouver Po on multiplie P par le plus petit commun multiple des dénominateurs de ses coefficients pour obtenir un polynôme P_1 à coefficients entiers. Ensuite on factorise au signe près, par le plus grand commun diviseur des coefficients de P_1 de sorte que le coefficient dominant soit positif. Ce qui en résulte est un polynôme primitif Po, et on a P = c Po où $c \in$ Q. Ceci démontre l'existence de c et Po. L'unicité est immédiate .

Proposition : Le produit de deux polynômes primitifs de Z[X] est encore primitif.

Démonstration : Soient P et Q deux polynômes primitifs de Z[X] et soit R = PQ. Puisque les coefficients dominants de P et de Q sont positifs, alors le coefficient dominant de R l'est aussi. Pour démontrer que R est primitif, il suffit de démontrer qu'aucun nombre premier p ne divise R.
Fixons un nombre premier p. On montre que l'application $\rho : Z[X] \to (Z/pZ)[X]$ qui transforme le polynôme $a_nX^n + \ldots a_1X + a_0$ en $\overline{a_n}X^n + \ldots \overline{a_1}X + \overline{a_0}$ est un homomorphisme d'anneaux.
Ainsi $\rho(R) = \rho(P)\rho(Q)$ et comme P et Q sont primitifs, $\rho(P)$ et $\rho(Q)$ ne sont pas nuls ; mais (Z/pZ)[X] est intègre donc $\rho(R)$ n'est pas nul , donc le polynôme R n'est pas divisible par p, donc il est primitif.

Proposition : Soient P et Q deux polynômes de Z[X] ; supposons que P soit primitif et que P divise Q dans Q[X]. Alors P divise Q dans Z[X].

Démonstration : Supposons que Q = PR avec R de Q[X] ; on a R = cRo où Ro est primitif dans Z[x] et $c \in$Q et par la proposition précédente, le produit PR_0 est primitif, donc l'égalité Q = cPRo démontre que PRo est l'unique polynôme primitif associé à Q, et que c est le contenu de Q. Mais Q est à coefficients entiers, donc son contenu est dans Z et donc R est dans Z[X] .

Corollaire : Si un polynôme non constant est irréductible dans Z[X], alors il est irréductible dans Q[X].

Démonstration : Les unités de Q[X] sont les rationnels non nuls et les unités de Z[X] sont 1 et –1; Soit P un polynôme non constant irréductible dans Z[X] ; Supposons que P = QR où Q et R sont dans Q[X], on doit donc prouver que si Q n'est pas constant alors R l'est. On écrit Q = cQo où Qo est primitif dans Z[X] et c dans Q^*. Alors P = cRQo avec cR dans Q[X] et Qo dans Z[X] et la proposition précédente implique que cR appartient à Z[X]. Puisque P est irréductible dans Z[X] on en déduit que cR$\in$ {-1 ;1} et donc R $\in$ Q .

Proposition : Soit P appartenant à Z[X] un polynôme non nul. Alors P est irréductible dans Z[X] si et seulement si

ï) P ou -P est un nombre premier de N, ou

ii) P ou -P est un polynôme primitif qui est irréductible dans Q[X],

Démonstration : Il est clair que si P est l'un des deux types de polynômes ci-dessus, alors P est irréductible dans Z[X] . Pour la réciproque, soit P irréductible dans Z[X] , avec les notation habituelles, P = cPo et , puisque P est irréductible, P $\notin$ {-1 ;1} et cette factorisation doit être triviale : c $\in$ {-1 ;1} ou Po = 1.
Si Po = 1 alors P est constant, et pour être irréductible un polynôme constant doit être au signe près, un nombre premier de N .
Si c $\in$ {-1 ;1}, alors P n'est pas constant, -P ou P est primitif, et avec le corollaire, P étant irréductible dans Z[X], on en déduit que P est irréductible dans Q [X] .

Proposition : tout élément irréductible de Z[X] est un élément premier de Z[X].

Démonstration : Supposons que P soit irréductible et que P divise QR où Q et R appartiennent à Z[x].

i) Si au signe près, P est un nombre premier de N alors, avec les notations habituelles, soit Q = cQ_0 , R = dRo , QoRo étant primitif, il existe un coefficient a de QoR_0 qui n'est pas divisible par P. Mais puisque P divise QR, donc P divise cda. Ainsi P divise c ou d donc P divise Q ou R.

ii) Supposons que –P ou P soit un polynôme primitif qui est irréductible dans Q[X]. Puisque Q[X] est principal, les éléments irréductibles sont premiers, donc P est un élément premier de Q[X]. Ainsi P divise Q ou R dans Q[X] et donc, on en déduit que P divise Q ou R dans Z[X].

Conclusion : Z[x] est un anneau factoriel

En effet : Soit P appartenant à Z[X] alors P peut être vu comme un polynôme de Q[X] qui est euclidien, donc P admet une factorisation en polynômes irréductibles de Q[X] ; en écrivant chaque polynôme de cette factorisation sous forme « cQ_0 » on obtient $P = cQ_0Q_1\ldots Q_n$ où les Q_i sont des polynômes primitifs de Z[X] irréductibles dans Q[X], donc irréductibles dans Z[X] et comme P et les Q_i sont dans Z[X], c est dans Z donc se décompose en produit de nombres premiers qui sont irréductibles dans Z[X].

L'unicité provient de ce que tout élément irréductible de Z[X] est premier.