Colles semaine 23

En bref

— Polynôme. Brèves construction formelle. Somme, produit, composition et dérivation formelle. Compatibilité avec les relations fonctionnelles équivalentes sur les fonctions polynomiales.
— Arithmétique des polynômes. Diviseurs et multiples. Théorème de division euclidienne.
— Zéros et racines : équivalence entre les deux notions. Multiplicité des racines, liens avec les dérivées itérées.
— Théorème fondamental de l'algèbre dans $\mathbb{C}$.
— Notion de polynômes irréductibles. Recensement de tous les polynômes irréductibles dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.
— Écriture factorisée des polynômes comme produit d'irréductibles (dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.)
— Fractions rationnelles : on s'intéresse seulement aux fonctions correspondantes. Décomposition en éléments simples des fractions rationnelles.
— Arithmétique des entiers : diviseurs multiples, division euclidienne, PGCD et PPCM

Exemples non exhaustifs de questions de cours

Les étudiantes et étudiants se présentent à la colle en sachant répondre rapidement et précisément à TOUTES les questions suivantes. Ils seront interrogés sur l'une d'entre elles.

— Citer le théorème de division euclidienne dans $\mathbb{K}[X]$. montrer l'unicité [1] afférente.
— Montrer que $X-\alpha$ divise P si et seulement si $P(\alpha)=0$.
— Pour α une racine de P de multiplicité d, α est-elle racine de P' ? Si oui de quelle multiplicité ?
— Montrer qu'un polynôme de degré n admet au plus n racines distinctes. Citer sans preuve le résultat analogue en comptant les racines avec multiplicité.
— Déterminer la factorisation de $1+3X+9X^2+27X^3$ en produits de polynômes irréductibles (dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$)
— Avec une décomposition en éléments simples, déterminer une expression sans symbole intégral de $I_x := \int_0^x \frac{1}{t^3-2t^2-t+2}\mathrm{d}x$ pour tout réels x pour lequel l'intégrale a un sens (et quels sont ces fameux réels x ?)

Note aux colleurs

— Jusqu'à la fin de l'année, on commencera ou terminera la colle en demandant à chaque étudiant de citer un développement limité au programme. On sanctionnera sévèrement en cas d'échec.
— On évitera toute théorie formelle sur les fractions rationnelles. Cette partie ne sert qu'à établir des formules de calculs (par exemple pour déterminer des intégarles ou des formules de sommation).
— Pour décomposer une fraction rationnelle dont le dénominateur n'est pas scindé à racines simples, il faut donner aux étudiants la forme cherchée. *Recommandation du programme officiel de PT.* Si le dénominateur est scindé à racines simples, les étudiants doivent pouvoir être autonome.
— La partie sur l'arithmétique des entiers est là pour servir d'analogie avec l'arithmétique des polynômes et parce que c'est utile pour le cours d'informatique. On pourra poser de brèves questions dessus pour meubler quelques minutes de fin de colle mais cela ne constitue pas un objectif majeur du programme.

1. Les étudiants s'assureront qu'ils savent aussi montrer l'existence. Mais pour des raisons purement temporelles, les colleurs s'abstiendront de le vérifier explicitement.

En détail

Polynômes

Reprise du programme précédent

1 Nouveauté de la semaine : polynômes irréductibles

Le théorème fondamental de l'algèbre permet donc d'écrire une forme factorisé des polynômes. Bien sûr, une telle forme factorisé sera plus simple pour les polynômes complexes.

Définition 1. Un polynôme P de $\mathbb{K}[X]$ est dit *irréductible* s'il n'est pas constant et si tous ses diviseurs sont constants ou de degré égal à $\deg(P)$.

Thèmes de réflexions 2. Quel est l'analogue de cette notion sur l'arithmétique des entiers naturels ?

Remarque 3. Pour la première fois du chapitre, cette notion dépend fondamentalement du corps $\mathbb{K}$. Ainsi, le polynôme X^2+1 est irréductible dans $\mathbb{R}$ (prouvez le) mais pas dans $\mathbb{C}$ car il admet, par exemple $X-\mathrm{i}$ pour diviseur.

Théorème 4 (Reformulation du théorème de D'Alembert-Gauss)**.** *Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont exactement les polynômes de degré* 1.

Ceci permet d'écrire une forme factorisée simple des polynômes complexes.

Proposition 5 (factorisation des polynômes, cas simple)**.** *Soit P un polynôme complexe non constant. On note $(\alpha_1, \alpha_2, \alpha_r)$ ses racines et $(m_1, m_2, \dots, m_r)$ leur multiplicité respective.*
Alors on dispose d'un scalaire a tel que :

$$P = a\prod_{i=1}^{r}(X-\alpha_i)^{m_i}\,.$$

Le lecteur, fin limier, comprendra bien sûr que le scalaire a n'est autre que le coefficient dominant du polynôme P et que le degré du polynôme s'exprime alors comme $\deg(P) = \sum_{i=1}^{r} m_i$.

Pour la culture, mentionnons que ceci peut se retraduire à l'aide de la notion de polynôme scindé.

Définition 6. Un polynôme de $\mathbb{K}[X]$ est dit *scindé* s'il peut s'écrire comme un produit de polynômes de degré 1.

Théorème 7 (Troisième formulation du théorème de D'alembert-Gauss)**.** *Tout polynôme non constant de* $\mathbb{C}[X]$ *est scindé.*

Passons maintenant au cas des polynômes réels. C'est évidemment un peu plus compliqué car le lecteur sait qu'il existe des polynômes irréductibles qui ne sont pas de degré 1. Par exemple, tous les polynômes de degré 2 à discriminant strictement négatif. Cela dit, en utilisant le lemme suivant, on montrera que ce sont les seuls autres polynômes irréductibles.

Lemme 8. *Soit P un polynôme à coefficient réel. Si $\alpha \in \mathbb{C}$ est une racine de P, alors $\overline{\alpha}$ est également une racine de P.*

Corollaire 9. *Les polynômes irréductibles de* $\mathbb{R}[X]$ *sont exactement les polynômes de degré* 1 *et les polynômes de degré* 2 *à discriminant strictement négatif.*

On en déduit les factorisations suivantes :

Théorème 10 (Factorisation des polynôme, cas général, Admis)**.** *Soit P un polynôme réel non constant. Alors on dispose d'un scalaire a, de deux entiers naturels et s et r ; de trois familles de scalaires $(\alpha_1, \dots, \alpha_r)$, $(\beta_{r+1}, \beta_{r+2}, \dots, \beta_{r+s})$ et $(\gamma_{r+1}, \gamma_{r+2}, \dots, \gamma_{r+s})$ ainsi que d'une famille $(m_1, \dots, m_r, m_{r+1}, \dots, m_{r+s}))$ d'entiers naturels non nuls de sorte que*

$$P = a \prod_{k=1}^{r} (X - \alpha_k)^{m_k} \prod_{k=r+1}^{r+s} (X^2 + \beta_k X + \gamma_k)^{m_k}.$$

et de sorte que : $\forall k \in [\![r+1\,;\, r+s]\!]$, $\beta_k^2 - 4\gamma_k < 0$. Le lecteur, fin limier, comprendra bien sûr que le scalaire a n'est autre que le coefficient dominant du polynôme P et que le degré du polynôme ne s'exprime pas aussi simplement que précédemment.

2 Complément sur les fractions rationnelles

2.1 Construction formelle (peu utile en PTSI)

De la même manière qu'à partir de l'ensemble des entiers $\mathbb{Z}$, on a défini un ensemble de fractions $\mathbb{Q}$, on va définir des fractions rationnelles comme l'ensemble des quotient de polynômes.

Définition 11. On admet que l'on peut construire un ensemble noté $\mathbb{K}(X)$, appelé *corps des fractions rationnelles*, constitué d'éléments de la forme

$$F = \frac{P}{Q}$$

avec P et Q dans $\mathbb{K}[X]$, $Q \neq 0$.
Le couple $(P, Q) \in \mathbb{K}[X] \times (\mathbb{K}[X] - \{0\})$ est appelé *un représentant* de la fraction rationnelle F, avec P le *numérateur* et Q le *dénominateur* de la fraction.
Deux couples (P_1, Q_1), (P_2, Q_2) représentent la même fraction si, et seulement si, $P_1 Q_2 - P_2 Q_1 = 0$.
Si P et Q n'ont aucun diviseur commun (autre que les polynômes constants), on dit que F est écrite sous *forme irréductible*.

2.2 En pratique

Définition 12. Soit $F = \frac{P}{Q}$ dans $\mathbb{K}(X)$ sous forme irréductible. On appelle **fonction rationnelle** $\widetilde{F}$ associée à F l'application

$$x \mapsto \widetilde{F}(x) = \frac{\widetilde{P}(x)}{\widetilde{Q}(x)}$$

définie sur $\mathbb{K}$ privé de l'ensemble des racines de Q, où $\widetilde{P}$ et $\widetilde{Q}$ sont les fonctions polynomiales respectives associées à P et à Q.

Remarque 13. Comme pour les polynômes, l'application qui à une fraction rationnelle associe sa fonction rationnelle est une application injective.

2.3 Décomposition en éléments simples

On commence par étudier le cas des fractions rationnelles de degré inférieur ou égal à 1. On peut décomposer les fractions rationnelles en somme de différents terme. La forme de cette décomposition dépend des polynômes irréductibles et est donc assez différente selon que l'on étudie cela dans $\mathbb{R}$ ou $\mathbb{C}$.

Commençons par un peu de terminologie

Définition 14 (Pôle d'une fraction rationnelle)**.** Soient $F = \frac{P}{Q}$ dans $\mathbb{K}(X)$ écrite sous forme irréductible, $\alpha \in \mathbb{K}$ et $\mu \in \mathbb{N}^*$.
On dit que α est un *pôle* de F, avec la multiplicité μ, lorsque α est une racine du polynôme Q de multiplicité μ, soit lorsque

$$F = \frac{P}{(X-\alpha)^\mu Q_1} \quad \text{avec } P(\alpha) \neq 0 \text{ et } Q_1(\alpha) \neq 0.$$

Remarque 15. Il est primordial que F soit écrite sous forme irréductible dans la définition précédente. En particulier, cela implique que α n'est pas racine du numérateur P.

2.3.1 Cas complexe

Théorème 16 (Décomposition en éléments simples sur $\mathbb{C}$, hors-programme en général.). *Soit $F = \frac{P}{Q}$ dans $\mathbb{C}(X)$ écrite sous forme irréductible avec P non nul et Q non constant. On suppose que* $\deg(F) < 0$. *On note $Q = \prod_{k=1}^{n} (X-\alpha_k)^{\mu_k}$. Alors, il existe une unique famille $(\lambda_{k,j})_{1\leqslant k\leqslant n, 1\leqslant j\leqslant \mu_k}$ d'éléments de $\mathbb{C}$ telle que*

$$F = \sum_{k=1}^{n} \left(\sum_{j=1}^{\mu_k} \frac{\lambda_{k,j}}{(X-\alpha_k)^j} \right)$$

Cette décomposition est appelée décomposition en éléments simples de $F \in \mathbb{C}(X)$ sur $\mathbb{C}$.

Remarque 17. Le problème pratique est alors de déterminer la valeur des coefficients $\lambda_{k,j}$. La méthode générale consiste à réduire au même dénominateur l'égalité du théorème précédent et à résoudre un système d'équation. Néanmoins un certain nombre de techniques différentes peuvent parfois être plus simple. Par exemple lorsque la fraction rationnelle n'a que des pôles simples, il est souvent intéressant de s'intéresser aux limites au voisinage de ces pôles.

La décomposition précédente est particulièrement simple dans le cas où le dénominateur Q est scindé à racines simples.

Corollaire 18 (Cas particulier, le seul à connaître selon le programme officiel). *Soit $(\alpha_1, \dots, \alpha_n) \in \mathbb{C}^n$ une famille de scalaires. Soit également P un autre polynôme qui n'admet aucun des α_i pour racine. Alors, il existe une (et une unique) famille de scalaire $(\lambda_1, \dots, \lambda_n) \in \mathbb{C}^n$ et un (et un unique) polynôme E tel que :*

$$\frac{P}{\prod_{k=1}^{n}(X-\alpha_k)} = E + \sum_{k=1}^{n} \frac{\lambda_k}{X-\alpha_k}. \tag{1}$$

Remarque 19. Le polynôme E se calcule comme le quotient dans la division euclidienne de P par $Q := \prod_{k=1}^{n}(X-\alpha_k)$.

Pour calculer les coefficients λ_k, le plus simple est de déterminer un équivalent de $\frac{P(x)}{Q(x)}$ au voisinage de $x = \alpha_k$.

Précisons donc que si le dénominateur de la fraction rationnelle n'est pas scindé à racine simple, alors le programme stipule que l'on doit vous rappeler la forme de la décomposition en éléments simples.

2.3.2 Cas réel

Théorème 20 (Décomposition en éléments simples sur $\mathbb{R}$. Hors-programme en cas général). *Soit $F = \frac{P}{Q}$ dans $\mathbb{C}(X)$ écrite sous forme irréductible avec P non nul et Q non constant. On suppose que* $\deg(F) < 0$.
On note

$$Q = \lambda \prod_{i=1}^{p} (X-a_i)^{\mu_i} \prod_{j=1}^{r} \left(\underbrace{X^2 + p_j X + q_j}_{\Delta_j < 0} \right)^{\nu_j} ;$$

la décomposition de Q en produit de polynômes irréductibles. Alors, il existe trois uniques familles $(\lambda_{k,j})_{1\leqslant k\leqslant n, 1\leqslant j\leqslant \mu_k}$; $(\gamma_{k,j})_{1\leqslant k\leqslant n, 1\leqslant j\leqslant \mu_k}$ et $(\delta_{k,j})_{1\leqslant k\leqslant n, 1\leqslant j\leqslant \mu_k}$ d'éléments de $\mathbb{R}$ telle que

$$F = \sum_{k=1}^{p} \left(\sum_{j=1}^{\mu_k} \frac{\lambda_{k,j}}{(X-a_k)^j} \right) + \sum_{k=1}^{r} \left(\sum_{j=1}^{\nu_k} \frac{\gamma_{k,j}X + \delta_{k,j}}{(X^2+p_kX+q_k)^j} \right).$$

2.3.3 Et si la fraction rationnelle est de degré positif ?

Qu'on soit dans $\mathbb{R}$ ou $\mathbb{C}$, on utilise le résultat suivant.

Proposition-Définition 21. *Soit $F = \frac{P}{Q}$ dans $\mathbb{K}(X)$. Il existe un unique couple (E, R) de $\mathbb{K}[X]^2$ tel que*

$$F = E + \frac{R}{Q} \quad \text{avec } \deg(R) < \deg(Q)$$

Le polynôme E s'appelle alors partie entière *de la fraction rationnelle F.*

Remarque 22. Les polynômes E et R de la définition précédente se calculent aisément comme le quotient et le reste dans la division euclidienne de P par Q

3 Arithmétique des entiers

3.1 Multiples et diviseurs

Le lecteur connaît normalement parfaitement les notions de multiples et diviseurs et cette partie ne devrait apporter aucune surprise.

Définition 23. Soit a et b deux entiers relatifs. On dit que a *divise* b ou que a *est un diviseur de* b ou encore que b *est un multiple de* a si $\exists c \in \mathbb{Z},\ b = ac$.

On trouve parfois dans la littérature, la notation $a \mid b$ pour signifier que a divise b.

Proposition 24 (Propositions élémentaires sur la divisibilité)**.** *Soit $(a, b, c) \in \mathbb{Z}^3$*

i) 0 *est multiple de tous les entiers.*

ii) 0 *n'est le diviseur d'aucun entier autre que lui-même.*

iii) 1 *et* -1 *divisent tous les entiers. Ce sont les seuls entiers dans ce cas.*

iv) a divise a.

v) Si a divise b et si b divise a, alors $a = \pm b$.

vi) Si a divise b et si b divise c, alors a divise c.

vii) Si a divise b et a divise c, alors a divise $\lambda b + \mu c$ pour tout couple $(\lambda, \mu) \in \mathbb{Z}^2$.

viii) Si a divise b et si $b \neq 0$, alors $|a| \leqslant |b|$.

3.2 Nombre premiers

Définition 25 (Nombre premier)**.** Un entier naturel p est dit *premier* s'il admet exactement deux diviseurs positifs.

Remarque 26. Si p est un nombre premier, alors ses deux diviseurs positifs sont donc 1 et p. Par ailleurs, il admet aussi exactement deux diviseurs négatifs qui sont -1 et $-p$.

On notera que 1 n'est pas un nombre premier au vu de cette définition.

Définition 27 (Nombres premiers entre eux)**.** Soit a et b deux entiers relatifs. Ces entiers sont dits *premiers entre eux* si leurs seuls diviseurs communs sont 1 et -1.

3.3 Quelques théorèmes à connaître

Théorème 28 (théorème d'Euclide)**.** *Il existe une infinité de nombres premiers.*

Proposition-Définition 29 (division euclidienne)**.** *Soit a un entier relatif et d un entier naturel non nul. Alors il existe un unique couple d'entier (q, r) vérifiant les deux conditions suivantes :*

$$\begin{cases} a = qd + r \\ 0 \leqslant r < d \end{cases} \tag{2}$$

Théorème 30 (Théorème fondamental de l'arithmétique)**.** *Tout entier se décompose comme produit de facteurs premier. En outre, cette décomposition est unique à l'ordre des facteurs près.*

3.4 PGCD et PPCM

3.4.1 Définition

Notons que si l'on considère deux entiers (non nuls pour simplifier), alors l'ensemble de leurs diviseurs communs est non vide (il contient au moins 1) et majoré. Cet ensemble admet donc un maximum. Ceci conduit à la notion de PGCD

Proposition-Définition 31. *Soit a et b deux entiers naturels dont au moins l'un est non nul. Alors il existe un plus grand diviseur commun à a et b. On le note* $\mathrm{PGCD}(a,b)$ *(ou parfois $a \wedge b$).*

Si a et b sont chacun non nul, alors il existe un plus petit multiple commun à a et à b strictement positif, on le note $\mathrm{PPCM}(a,b)$ *(ou parfois $a \vee b$).*

Remarque 32. Si a est non nul, alors $\mathrm{PGCD}(a,0) = a$ et $\mathrm{PPCM}(a,0)$ n'est pas défini.

3.4.2 Détermination algorithmique

Le théorème de division euclidienne permet de produire un algorithme pour le calcul du PGCD.

Méthode 33 (Algorithme d'Euclide)**.** Soit a et b deux entiers naturels non nuls. Supposons que l'on souhaite calculer leur PGCD. On utilise alors l'algorithme suivant.

On définit une suite finie par récurrence en initialisant avec $r_0 = \max(a,b)$ et $r_1 = \min(a,b)$.

Ensuite, on construit par récurrence de la manière suivante. Pour tout entier n, si les termes $(r_0, r_1, r_2, \ldots, r_n, r_{n+1})$ ont été construits, alors ... on effectue la division euclidienne de r_n par r_{n+1} (tant que r_{n+1} est non nul) et on note r_{n+2} ce reste dans la division euclidienne.

Ce procédé assure que la suite construite est ainsi à valeurs dans $\mathbb{N}$ et strictement décroissante. Par conséquent, elle finit par atteindre 0 (et ensuite, on ne peut plus définir les termes suivants). Autrement dit il existe un entier n tel que $r_n > 0 = r_{n+1}$. La valeur de $PGCD(a,b)$ est alors égal à ce terme r_n ; autrement dit au dernier terme non nul de la suite.

3.4.3 Propriétés théoriques

Lemme 34. *Soit a et b deux entiers chacun non nul. Alors, on a l'équivalence suivante :*

$$\mathrm{PGCD}(a,b) = a \iff \mathrm{PPCM}(a,b) = b \iff (a \text{ divise } b)\,.$$

On continue avec un théorème de calcul crucial.

Théorème 35. *Soit a et b deux entiers chacun non nul. Alors* $\mathrm{PGCD}(a,b) \times ppcm(a,b) = |ab|$. *A*

Corollaire 36. *Soit a et b deux entiers non nuls. Alors les trois assertions suivantes sont équivalentes :*

i) a *et* b *sont premiers entre eux.*

ii) $\mathrm{PGCD}(a,b) = 1$.

iii) $\mathrm{PPCM}(a,b) = |ab|$.

Proposition 37. *Soit a et b deux entiers dont au moins un est non nul. Alors*

$$\forall c \in \mathbb{N}^*,\ \begin{cases} \mathrm{PGCD}(ac,bc) = c\,\mathrm{PGCD}(a,b) \\ \text{si de plus, } a \text{ et } b \text{ sont chacun non nul, } \mathrm{PPCM}(ac,bc) = c\,\mathrm{PPCM}(a,b) \end{cases}.$$