Université Lille 1 - Sciences et Technologies

Préparation au CAPES 2010

Algèbre et Géométrie

Chapitres arithmétique, polynômes et fractions rationnelles

Exercices

§1. Structure des ensembles de nombres

§1.1. Division euclidienne et algorithme d'Euclide

1. Quiz

On fixe un entier $q > 1$.

1.1) Donner un algorithme pour calculer le développement d'un entier x en base q. *Indication :* Si le développement de x en base q s'écrit $x = x_0 + x_1 q + \cdots + x_i q^i + \cdots + x_r q^r$ pour des chiffres $0 \leq x_i \leq q-1$, $i = 0, \ldots, r$, alors comment s'identifient le reste et le quotient de la division euclidienne de x par q?

1.2) Comment s'écrit le développement de $x = q^n - 1$ en base q?

2. Exercice

Calculer le pgcd des couples $(93, 133)$, $(161, 451)$, $(408, 595)$. On déterminera aussi des relations de Bézout en remontant l'algorithme d'Euclide.

3. Exercice

3.1) Soient $p, q \in \mathbb{Z}$ tels que $pgcd(p, q) = 1$. On suppose que l'on a une relation de la forme $xp + yq = 0$. Prouver que p divise nécessairement y et que q divise nécessairement x.

Indication : On utilisera une relation de Bezout $up + vq = 1$ pour écrire y comme un multiple de p.

3.2) Quelles sont les solutions $(x, y) \in \mathbb{Z}^2$ des équations

$$93x + 133y = 1 \qquad \text{et} \qquad 161x + 451y = 1?$$

Indications : On a déterminé une solution particulière de ces équations dans l'exercice précédent. On a par exemple $93x_0 + 133y_0 = 1$ pour un certain couple $(x_0, y_0) \in \mathbb{Z}^2$. On fait la différence des équations $93x + 133y = 1$ et $93x_0 + 133y_0 = 1$. On utilise ensuite les observations de la question précédente.

3.3) Quelles sont les solutions $x, y \in \mathbb{Z}$ des équations

$$408x + 595y = 34 \qquad \text{et} \qquad 408x + 595y = 8?$$

4. Exercice

4.1) On considère la suite des nombres de Fibonacci $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$. Comment s'écrit la division euclidienne de F_n par F_{n-1}? Quel est le reste de cette division? Quel est le pgcd de F_n et F_{n-1}?

BF, Courriel: `Benoit.Fresse@math.univ-lille1.fr`

4.2) !! Soit $c(a,b)$ le nombre de divisions que fait intervenir l'algorithme d'Euclide pour calculer $pgcd(a,b)$. Que vaut $c(a,b)$ dans le cas $a = F_{n-1}$ et $b = F_n$? Prouver que l'on a en général

$$c(a,b) \leq \frac{\log(\max(|a|,|b|)}{\log(\theta)}$$

où $\theta = (1+\sqrt{5})/2$. Conclusion?

5. Exercice

Soit $E_n = 2^{2^n}+1$, $n \in \mathbb{N}$. Expliciter une relation de récurrence entre $E_{n+1}-1 = 2^{2^{n+1}}$ et $E_n - 1 = 2^{2^n}$. En déduire une relation de récurrence entre E_{n+1} et E_n. Quel est le reste de la division euclidienne de E_{n+1} par E_n? Quel est le plus grand diviseur commun de E_{n+1} et E_n?

§1.2. Idéaux et nombres premiers de $\mathbb{Z}$

6. Exercice

Soit A un anneau. Un élément $p \in A$ est *irréductible* si $p = xy$ entraine que x est inversible ou que y est inversible. Un idéal $P \subseteq A$ est *premier* si $xy \in P$ entraine $x \in P$ ou $y \in P$.

On travaille avec l'anneau $A = \mathbb{Z}$. Le but de l'exercice est de caractériser les idéaux premiers de $\mathbb{Z}$, tout en retrouvant des résultats du cours d'arithmétique. On voudrait établir l'assertion suivante :

THÉORÈME : *Un élément $p \in \mathbb{Z}$ est irréductible si et seulement si l'idéal associé $P = (p)$ est premier.*

Un élément irréductible de $\mathbb{Z}$ est aussi appelé un nombre premier.

6.1) LEMME : Si $P = (p)$ est un idéal premier de $\mathbb{Z}$, alors p est un élément irréductible de $\mathbb{Z}$. Prouver cette implication.

On suppose maintenant que p est irréductible. On va prouver l'implication inverse : si p est un élément irréductible de $\mathbb{Z}$, alors $P = (p)$ est un idéal premier de $\mathbb{Z}$. Cette preuve se décompose en une série d'observations qui sont utiles par ailleurs.

6.2) OBSERVATION : Observer que, si $x \in \mathbb{Z}$, alors des deux choses l'une : ou p est premier à x, ou p divise x.
6.3) LEMME : Soit $n \in \mathbb{Z}$. Prouver que $pgcd(n,x) = pgcd(n,y) = 1$ entraine $pgcd(n,xy) = 1$. (*Indication :* On pourra faire le produit des relations de Bézout pour les couples (n,x) et (n,y).)
6.4) LEMME : Si p divise xy, alors p divise x ou p divise y. Constater que cette assertion est une conséquence du lemme et de l'observation ci-dessus.
6.5) Conclure quant au théorème.

7. Exercice

On voudrait montrer que $\mathbb{Z}$ contient un nombre infini de nombres premiers. On raisonne par l'absurde. On suppose que la suite $p_1, p_2, \ldots, p_n$ représente l'ensemble des nombres premiers. Que peut-on dire du nombre $q = p_1 p_2 \cdots p_n + 1$?

Commentaire : Cet argument se trouve dans le livre IX des éléments d'Euclide.

8. Quiz

Soit a_n, $n \geq 1$, la suite de nombres entiers telle que

$$a_1 = 2 \qquad \text{et} \qquad a_{n+1} = 1 + a_1 a_2 a_3 \cdots a_n \qquad \text{pour } n \geq 1.$$

8.1) Si $n \neq m$, alors $pgcd(a_n, a_m) = 1$. *Vrai ou Faux?*
8.2) Les nombres a_n, $n \geq 1$, sont tous irréductibles (premiers). *Vrai ou Faux?*
(Toute réponse non justifiée est nulle et non avenue.)

§1.3. Les anneaux $\mathbb{Z}/n\mathbb{Z}$ et leurs éléments inversibles

9. Quiz

La classe de x modulo d est une unité de $\mathbb{Z}/d\mathbb{Z}$ si et seulement si $pgcd(x,d)=1$. Prouver cette assertion.

10. Quiz

Montrer que les assertions suivantes sont équivalentes :
(1) L'anneau $\mathbb{Z}/d\mathbb{Z}$ est un corps.
(2) L'anneau $\mathbb{Z}/d\mathbb{Z}$ est intègre.
(3) L'idéal (d) est un idéal premier de $\mathbb{Z}$.
(4) L'entier d est un nombre premier.

11. Quiz

Soit p un nombre premier. Prouver les relations suivantes en utilisant la structure du groupe des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$:

$$a^p \equiv a \,(\mathrm{mod}\, p), \quad \forall a \in \mathbb{Z}, \tag{1}$$

$$(p-1)! \equiv -1 \,(\mathrm{mod}\, p). \tag{2}$$

12. Problème

On note $\phi(d)$ l'ordre du groupe $(\mathbb{Z}/d\mathbb{Z})^*$ des éléments inversibles de $\mathbb{Z}/d\mathbb{Z}$.

I. Applications de méthodes de dénombrement.

12.1) Que vaut $\phi(p)$ quand p est un nombre premier?

12.2) On suppose que p et q sont des nombres premiers. Combien y a-t-il d'éléments $0 \leq x < pq$ divisibles par p? Combien y a-t-il d'éléments $0 \leq x < pq$ divisibles par q? Combien y a-t-il d'éléments $0 \leq x < pq$ divisibles par p et par q? Conclure : que vaut $\phi(pq)$?

12.3) On suppose que p est un nombre premier. Combien y a-t-il d'éléments $0 \leq x < p^r$ divisibles par p? Conclure : que vaut $\phi(p^r)$?

Remarque : Dans l'exercice 8 de la section 4.1, on démontre que l'on a en fait $\phi(mn) = \phi(m)\phi(n)$ pour tout couple d'entiers (m,n) tels que $pgcd(m,n)=1$.

II. Une méthode de cryptographie.

12.4) Si $x \in \mathbb{Z}$ est premier à d, alors que vaut $\bar{x}^{\phi(d)}$ dans $\mathbb{Z}/d\mathbb{Z}$?

12.5) On fixe $n = 17 \cdot 13 = 221$. On pose $d = 35$. Déterminer un nombre e tel que $x^{de} \equiv x \,(\mathrm{mod}\, n)$, quelque soit x tel que $(x,n)=1$.

Commentaires : On peut construire un tel e pour tout couple $(n=pq, d)$ telle que $pgcd(d,(p-1)(q-1))=1$, où (p,q) sont des nombres premiers. Cette construction est utilisée dans une méthode de cryptographie avec une clé de chiffrement publique. Les nombres n et d constitue la clé publique de chiffrement. Les nombres n et e en constitue la clé (privée) permettant le déchiffrement. Un nombre $x = 0, 1, \ldots, 15$ qui représente une information est chiffré en $x \mapsto x^d$. On déchiffre le message en effectuant l'opération $y \mapsto y^e$.

La sécurité du code est assurée par la difficulté de retrouver les facteurs d'une décomposition $n = p \cdot q$ lorsque'on choisit des nombres premiers (p,q) assez grand et de remonter à la clé privée à partir de la clé publique. On sait en fait produire de grand nombres premiers (de l'ordre de 1200 chiffres décimaux), cependant il est difficile de décomposer un grand nombre entier (comportant plus de 120 chiffres) en facteurs premiers.

13. Quiz

On peut montrer que le groupe des éléments inversibles d'un corps fini $\mathbb{K}$ est cyclique. Le but de ce quiz est d'étudier les applications de ce théorème de structure pour des anneaux de la forme $\mathbb{Z}/d\mathbb{Z}$.

13.1) Expliciter un générateur de $\mathbb{K}^*$ pour les corps $K = \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/11\mathbb{Z}, \mathbb{Z}/13\mathbb{Z}$.
13.2) Le groupe des éléments inversibles de $\mathbb{Z}/d\mathbb{Z}$ est-il toujours cyclique, quand d n'est pas premier?

14. Problème

0. On travaille dans $\mathbb{Z}/23\mathbb{Z}$. On utilisera la méthode suivante pour calculer efficacement les puissances d'un élément donné $\xi \in \mathbb{Z}/23\mathbb{Z}$. On calcule d'abord les puissances

$$\xi^2, \xi^4, \xi^8, \ldots, \xi^{2^i}, \ldots$$

en utilisant la relation de récurrence $\xi^{2^{i+1}} = \xi^{2^i \cdot 2} = (\xi^{2^i})^2$. Ensuite, si on veut calculer une puissance ξ^n quelconque, alors on décompose l'exposant n en somme de puissances de 2. On a par exemple, $26 = 16 + 8 + 2$, d'où $\xi^{26} = \xi^{16} \cdot \xi^8 \cdot \xi^2$.
14.1) Calculer $\bar{5}^{17}$ en appliquant cette méthode.

I. On rappelle que $(\mathbb{Z}/23\mathbb{Z})^*$ désigne le groupe des éléments inversibles de $\mathbb{Z}/23\mathbb{Z}$.
14.2) Quel est l'ordre du groupe $(\mathbb{Z}/23\mathbb{Z})^*$? Quel sont les ordres possibles des éléments $\xi \in (\mathbb{Z}/23\mathbb{Z})^*$? Corollaire : quel est l'ordre maximal que puisse atteindre un élément $\xi \in (\mathbb{Z}/23\mathbb{Z})^*$?
14.3) Prouver que l'élément $\xi = \bar{5}$ est d'ordre maximal dans $(\mathbb{Z}/23\mathbb{Z})^*$. Que peut-on en conclure quant au groupe $< \bar{5} >= \{ \bar{5}^n, n \in \mathbb{Z} \}$ engendré par cet élément?

II. On se demande si, quand on se donne $d \in \mathbb{Z}$, l'équation $\bar{5}^d = (\bar{5}^4)^x$ dans $\mathbb{Z}/23\mathbb{Z}$ possède une solution $x \in \mathbb{Z}$.
14.4) Montrer que $x \in \mathbb{Z}$ est une solution de l'équation $\bar{5}^d = (\bar{5}^4)^x$ si et seulement si on a $d = 4x + 22q$ pour un certain $q \in \mathbb{Z}$. *Indication :* On réécrira l'équation sous la forme $\bar{5}^{truc} = \bar{1}$ et on donnera un argument précis.
14.5) En déduire une condition nécessaire sur l'entier d pour que l'équation $\bar{5}^d = (\bar{5}^4)^x$ possède au moins une solution.
14.6) On suppose que $d = 6$. Soit $y = \bar{5}^6$. On explicitera une solution particulière $x = x_0$ de l'équation $\bar{5}^6 = (\bar{5}^4)^x$. Comment s'écrit la solution générale?

15. Exercice
15.1) Résoudre l'équation $\bar{x}^2 = 2$ dans $\mathbb{Z}/7\mathbb{Z}$.
15.2) Montrer que l'équation $\bar{x}^2 = 2$ a une solution dans $\mathbb{Z}/7^r\mathbb{Z}$, pour tout $r \geq 1$.

Indications : On procédera par récurrence. Si on a x_r tel que $x_r^2 \equiv 2 \pmod{7^r}$, alors on cherchera une solution de l'équation $x_{r+1}^2 \equiv 2 \pmod{7^{r+1}}$, de la forme $x_{r+1} = x_r + 7^r t$.

16. Exercice
16.1) Le nombre -3 est-il un carré dans $\mathbb{Z}/11\mathbb{Z}$?
16.2) Quels sont les couples $(\bar{x}, \bar{y})$ qui sont solutions de l'équation $\bar{y}^2 + \bar{3}\bar{x}^2 = \bar{0}$ dans $\mathbb{Z}/11\mathbb{Z}$? *Indication :* Cette équation a-t-elle une solution telle que $\bar{x}$ ou $\bar{y}$ soit inversible dans $\mathbb{Z}/11\mathbb{Z}$?

17. Exercice

L'équation $15x^2 - 7y^2 = 9$ a-t-elle une solution dans $\mathbb{Z}$?

Indication : Si c'était le cas, alors cette équation aurait une solution dans $\mathbb{Z}/d\mathbb{Z}$ (pour $d = 2, 3, 5, 7, \ldots$).

§1.4. Décomposition en facteurs premiers et valuations p-adiques

18. Quiz
18.1) L'équation $x^2 = 2$ a-t-elle une solution $x \in \mathbb{Z}$? (Quelle relation vérifierait $v_2(x)$?)
18.2) L'équation $x^2 = 2$ a-t-elle une solution $x = p/q \in \mathbb{Q}$? (Quelle relation vérifieraient $v_2(p)$ et $v_2(q)$?)

19. Quiz

Soit p un nombre premier. Prouver que les coefficients du binôme

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

vérifient la relation

$$\binom{p}{i} \equiv 0 \,(\mathrm{mod}\, p)$$

pour $i = 1, \ldots, p-1$.

20. Exercice

La valuation p-adique d'un entier x, définie comme l'exposant de p dans la décomposition de p en produit de nombres premiers, sera notée $v_p(x)$.

20.1) Soit $x \in \mathbb{Z}$. Soit

$$x = x_0 + x_1 p + x_2 p^2 + \cdots + x_r p^r, \quad 0 \leq x_i \leq p-1$$

la décomposition de x en base p. Quels sont les quotients euclidiens des divisions de x par p, par p^2, ..., par p^r?

20.2) Combien y a-t-il d'éléments y tels que $1 \leq y \leq x$ qui sont divisibles par p, par p^2, ..., par p^r?

20.3) Utiliser les observations ci-dessus pour prouver l'identité :

$$v_p(x!) = (x - \alpha_p(x))/(p-1),$$

où $\alpha_p(x) = x_0 + x_1 + x_2 + \cdots + x_r$ représente la somme des chiffres du développement de x en base p.

Puis déterminer la valuation p-adique d'un coefficient binomial :

$$\binom{n}{a} = \frac{n!}{a!\,(n-a)!}.$$

20.4) Soit x tel que $0 < x < p^r$. Quelle est la valuation p-adique du coefficient binomial

$$\binom{p^r + x}{x} = \frac{(p^r + x)!}{p^r!\,x!}?$$

Conclusion : ce coefficient binomial est-il divisible par p?

20.5) Soit y tel que $0 < y < p^r$. On suppose que le développement de y en base p s'écrit $y = y_v p^v + \cdots + y_{r-1} p^{r-1}$ avec $y_v \neq 0$. Comment s'écrit le développement en base p de $y' = p^r - y$? Quelle est la valuation p-adique du coefficient binomial

$$\binom{p^r}{y} = \frac{p^r!}{y!\,(p^r - y)!}?$$

Conclusion : ce coefficient binomial est-il divisible par p?

§2. Polynômes à une indéterminée

§2.1. Arithmétique des polynômes

1. Quiz

Comment se développe le polynôme $(X+1)^p$ dans $\mathbb{Z}/p\mathbb{Z}[X]$?

2. Exercice

2.1) Calculer le pgcd des couples de polynômes suivants

$$(X^5+1, X^4+X^2+1) \qquad \text{et} \qquad (X^5+X^4+1, X^5+X+1),$$

avec $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$ comme corps de coefficients. On déterminera aussi des relations de Bézout en remontant l'algorithme d'Euclide.

2.2) Calculer le pgcd du couple (X^2+1, X^2+X) par l'algorithme d'Euclide en prenant $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{K} = \mathbb{Q}$ comme corps de coefficients. Commentaires?

3. Exercice

Soient (P, Q) des polynômes premiers entre eux.

3.1) Donner la forme générale des solutions de l'équation $UP + VQ = A$, pour un polynôme A donné.

3.2) On suppose maintenant $\deg(A) < \deg(P) + \deg(Q)$. Montrer qu'il existe un couple solution (U, V) tel que $\deg(V) < \deg(P)$ (*indication :* utiliser une division euclidienne), puis montrer que l'on a alors $\deg(U) < \deg(Q)$. Prouver qu'il n'existe qu'une seule solution vérifiant ces relations.

3.3) *Application numérique :* calculer la valeur de cette solution pour le couple $(P, Q) = (X^5 + 1, X^4 + X^2 + 1)$.

4. Exercice

On travaille sur un corps $\mathbb{K}$ quelconque. Si $n \in \mathbb{N}$, alors la notation $\mathbb{K}_{<n}[X]$ désigne le sous espace vectoriel de $\mathbb{K}[X]$ formé des polynômes de degré strictement inférieur à n.

Soient $F, G \in \mathbb{K}[X]$ des polynômes On note $d = \deg F$ et $e = \deg G$. On a ainsi $F(X) = a_0 + a_1X + \cdots + a_dX^d$ et $G(X) = b_0 + b_1X + \cdots + b_eX^e$. Soit

$$L : \mathbb{K}_{<e}[X] \times \mathbb{K}_{<d}[X] \to \mathbb{K}_{<d+e}[X]$$

l'application linéaire telle que

$$L(U(X), V(X)) = U(X) \cdot F(X) + V(X) \cdot G(X).$$

4.1) Comment s'écrit la matrice de L quand $d = 2$, $e = 1$, puis quand $d = 2$, $e = 2$? (On munit tout les espaces vectoriels de leur base naturelle.)

4.2) Montrer que F et G n'ont pas de diviseurs en commun si et seulement si L est injective.

4.3) En utilisant le résultat précédent, montrer que F et G n'ont pas de diviseurs en commun si et seulement si L est surjective.

4.4) Que peut-on conclure de cet exercice quant aux polynômes qui apparaissent dans une relation de Bezout :

$$U(X) \cdot F(X) + V(X) \cdot G(X) = 1?$$

Commentaire : Le déterminant de L s'appelle le résultant des polynômes (F, G). D'après les résultats obtenus, on a $pgcd(F, G) = 1$ si et seulement si le résultant de (F, G) est un élément non nul de $\mathbb{K}$.

5. Exercice

Reprendre les exercices 6 et 10 du §1 dans le cadre des polynômes.

§2.2. Racines des polynômes

6. Exercice

6.1) Soit $F(X) = a_0 + a_1X + \cdots + a_dX^d$ un polynôme tel que $a_i \in \mathbb{Z}$, $i = 0, \ldots, d$. Soit $\alpha = p/q$ une racine rationnelle de $F(X)$. On suppose $pgcd(p, q) = 1$. Observer que le numérateur p de α divise a_0 et que le dénominateur q de α divise a_d.

6.2) Quelles sont les racines du polynôme $F(X) = 3X^3 + 2X^2 - 6X - 4$?

7. Exercice

On fixe des points $a_1, \ldots, a_r \in \mathbb{C}$ deux à deux distincts. On se donne également des valeurs $b_1, \ldots, b_r \in \mathbb{C}$.

7.1) Construire un polynôme $F(X)$ de degré strictement inférieur à r et tel que $F(a_i) = b_i$, $i = 1, \ldots, r$. *Indications :* On pourra introduire les polynômes $L_i(X) = \prod_{j \neq i}(X - a_j)$.

7.2) On suppose que $G(X)$ est également un polynôme de degré strictement inférieur à r tel que $G(a_i) = b_i$, $i = 1, \ldots, r$. Que peut-on dire des racines du polynôme $F(X) - G(X)$? Conclusion?

8. Quiz

Quelles sont les facteurs irréductibles du polynôme $X^4 + 1$ dans $\mathbb{C}[X]$? dans $\mathbb{R}[X]$? dans $\mathbb{Q}[X]$?

9. Exercice

On note $\alpha = \sqrt{2} + i\sqrt{3}$.

9.1) Expliciter un polynôme $F(X) = X^4 + pX^2 + q$ à coefficients entiers $p, q \in \mathbb{Z}$ tel que $F(\alpha) = 0$.

9.2) Quelles sont les autres racines de $F(X)$? *Indication :* Comment les déduire de α?

9.3) Comment s'écrit la décomposition de $F(X)$ en facteurs irréductibles dans $\mathbb{R}[X]$?

9.4) Quels sont les diviseurs de $F(X)$ dans $\mathbb{R}[X]$? Quels sont les diviseurs de $F(X)$ dans $\mathbb{Q}[X]$? Conclusion?

9.5) Soit $P(X) \in \mathbb{Q}[X]$ un polynôme à coefficients rationnels. Si $P(\alpha) = 0$, alors que peut-on dire du pgcd de $P(X)$ et de $F(X)$? Que peut-on conclure quant aux polynômes à coefficients rationnels $P(X) \in \mathbb{Q}[X]$ tels que $P(\alpha) = 0$?

10. Exercice (règle de Newton)

Soit $F(x)$ un polynôme non-nul à coefficients réels. Soit $c \in \mathbb{R}$ un nombre tel que $F(c) > 0$ et $F^{(i)}(c) \geq 0$ pour $i \geq 1$. Prouver que les racines réelles de $F(x)$ vérifient $\alpha \leq c$.

Indication : On utilisera le développement de Taylor de $F(x)$ en $x = c$.

11. Exercice

Soit $F(x)$ un polynôme à coefficients réels qui possède m racines (comptées avec leur multiplicités) dans un intervalle fermé $[a, b] \subset \mathbb{R}$. Prouver que $F'(x)$ possède au moins $m - 1$ racines dans $[a, b]$.

12. Exercice

Soit $F(x)$ un polynôme unitaire à coefficients complexes. On note $(\alpha_1, \ldots, \alpha_r)$ les racines de $F(x)$ et $(m_1, \ldots, m_r)$ leurs multiplicités respectives, de sorte que $F(x)$ s'écrit :

$$F(x) = \prod_{i=1}^{r}(x - a_i)^{m_i}.$$

Soit β une racine (complexe) de $F'(x)$. On suppose $\beta \neq \alpha_i$, $\forall i$.

12.1) Établir la relation

$$\sum_{i=1}^{r} \frac{m_i}{\beta - \alpha_i} = 0$$

en utilisant la décomposition en éléments simples de la fraction $F'(x)/F(x)$.
12.2) Utiliser le conjugé de cette identité (et la formule d'inversion des complexes $1/\zeta = \bar{\zeta}/|\zeta|$) pour montrer que β est dans l'enveloppe convexe des racines de $F(x)$ dans $\mathbb{C}$, l'ensemble des points $z \in \mathbb{C}$ tels que $z = t_1\alpha_1 + \ldots + t_r\alpha_r$ pour des coefficients réels t_i tels que $t_1 + \cdots + t_r = 1$ et $t_i \geq 0$, $\forall i$ (autrement dit, l'enveloppe convexe est l'ensemble des barycentres à coefficients $t_i \geq 0$ des points $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$).

13. Exercice

Soient $(x_1, \ldots, x_n)$ des indéterminées. On considère les polynômes symétriques élémentaires

$$s_r(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \cdots < i_r \leq n} x_{i_1} \cdots x_{i_r}, \quad r = 0, 1, \ldots, n,$$

et les fonctions puissances

$$p_r(x_1, \ldots, x_n) = \sum_{1 \leq i \leq n} x_i^r, \quad r = 0, 1, \ldots, n.$$

Prouver les formules de Newton :

$$p_r = \sum_{i=1}^{r} (-1)^{i-1} s_i p_{r-i} + (-1)^{r-1} s_r.$$

§3. Fractions rationnelles à une indéterminée

1. Problème

Le but de cet exercice est de reprendre la méthode de décomposition en éléments simples des fractions rationnelles. La méthode purement algébrique est valable pour tout corps de coefficients.

1.1) On se donne une fraction $R = F/G$. Prouver que l'on peut décomposer cette fraction en

$$R = E + \frac{N}{G}$$

avec $E, N \in \mathbb{K}[X]$ et $\deg(N) < \deg(G)$.

1.2) On se donne une fraction $R = F/G$. On suppose $G = PQ$ avec $pgcd(P, Q) = 1$. Prouver que l'on peut décomposer R en

$$R = \frac{A}{P} + \frac{B}{Q}.$$

Prouver que l'on peut choisir (A, B) tels que $\deg(A) < \deg(P)$ et $\deg(B) < \deg(Q)$ si on a au départ $\deg(F) < \deg(G)$.

Indication : application des exercices 3 ou 4 de §2.1.

1.3) On se donne une fraction de la forme $R = F/P^\nu$. Adapter l'algorithme de décomposition en base p des entiers (exercice 1 de §1.1) pour montrer que le polynôme F possède une décomposition de la forme

$$F = F_0 + F_1 P + \cdots + F_n P^n$$

où F_i est un polynôme de degré $\deg(F_i) < \deg(P)$. En déduire la décomposition en éléments simples de R.

1.4) On se donne une fraction

$$R = \frac{F}{G} \quad \text{telle que} \quad G = P_1^{\nu_1} \cdots P_r^{\nu_r} \quad \text{avec} \quad i \neq j \Rightarrow pgcd(P_i, P_j) = 1.$$

Récapituler les constructions des questions (1-3) pour donner la forme de la décomposition en éléments simples de R et l'algorithme permettant de l'obtenir.

Remarque : la décomposition en éléments simples est unique, mais on ne demande pas d'établir ce résultat.

1.5) Application : Déterminer la décomposition en élément simples de la fraction

$$R(X) = \frac{1}{(1+X)^2(1+X+X^2)^2} \in \mathbb{K}(X).$$

Pour limiter les calculs, on pourra travailler avec le corps de coefficients $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$.

2. Quiz

Soit

$$\frac{F(x)}{G(x)} = \frac{F(x)}{\prod_{i=1}^{r}(x - \alpha_i)}$$

une fraction avec des pôles simples $(\alpha_1, \ldots, \alpha_r)$ et telle que $\deg(F) < r$. Relier les coefficients de la décomposition en éléments simples de F/G aux valeurs de la dérivée de G.

3. Quiz

Relier les coefficients de la décomposition en éléments simples d'une fraction de la forme $F(x)/(X - \alpha)^\nu$ au développement de Taylor de $F(x)$.

4. Exercice (division selon les puissances croissantes)
4.1) On se donne des polynômes $A(x)$ et $B(x)$ tels que $B(0) \neq 0$. Prouver par récurrence que pour tout $n \in \mathbb{N}$, il existe un unique couple de polynômes $Q_n(x)$ et $R_n(x)$ tels que $\deg(Q_n) \leq n$ et

$$A(x) = B(x)Q_n(x) + x^{n+1}R_n(x).$$

Le polynôme $Q_n(x)$ est le n-ième quotient et $R_n(x)$ est le n-ième reste de la division selon les puissances croissantes de $A(x)$ par $B(x)$.

Application : faire la division selon les puissances croissantes à l'ordre 3 de $A(y) = (y+1)^2$ par $B(y) = (y+1)^3 + 1$.
4.2) On considère une fraction de la forme

$$R(x) = \frac{F(x)}{(x-\alpha)^m \cdot G(x)}.$$

Observer que la division selon les puissances croissantes de $A(y) = F(y+\alpha)$ par $B(y) = G(y+\alpha)$ permet de détermminer les coefficients des termes $1/(x-\alpha)^\nu$ dans la décomposition en éléments simples de $R(x)$.
4.3) Application : déterminer la décomposition en éléments simples de la fraction

$$R(x) = \frac{x^2}{(x-1)^3 \cdot (x^3+1)}.$$

5. Exercice !! (la fraction qui rend la monnaie)

Pour un entier $n \in \mathbb{N}$, on note a_n le nombre de solutions entières $(p,q,r) \in \mathbb{N}^3$ de l'équation $p + 2q + 4r = n$.

Remarque : une calculatrice est nécessaire pour traiter cet exercice. Pour simplifier, on pourra traiter l'exercice en retirant le terme en r.
5.1) Prouver les relations

$$\frac{1}{(1-x)(1-x^2)(1-x^4)} = \Big\{\sum_{p=0}^{\infty} x^p\Big\} \cdot \Big\{\sum_{q=0}^{\infty} x^{2q}\Big\} \cdot \Big\{\sum_{r=0}^{\infty} x^{4r}\Big\} = \sum_{n=0}^{\infty} a_n x^n.$$

5.2) Décomposer la fraction

$$F(x) = \frac{1}{(1-x)(1-x^2)(1-x^4)}$$

en éléments simples pour obtenir une autre expression du développement en série formelle de $F(x)$. Déduire du résultat obtenu une formule explicite de a_n en fonction de n.
5.3) Combien y a-t-il de façons de rendre 8€50 de monnaie avec des pièces de 0€50, 1€ et 2€?

§4. Anneaux et corps

§4.1. Anneaux et idéaux

1. Quiz

1.1) Prouver ou infirmer les assertions suivantes :

(a) "On peut construire un morphisme d'anneaux de $\mathbb{Z}/15\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$."

(b) "On peut construire un morphisme d'anneaux de $\mathbb{Z}/15\mathbb{Z}$ dans $\mathbb{Z}/5\mathbb{Z}$."

(c) "On peut construire un morphisme d'anneaux de $\mathbb{Z}/15\mathbb{Z}$ dans $\mathbb{Z}/30\mathbb{Z}$."

1.2) En général, sous quelle condition existe-t-il un morphisme d'anneaux de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?

2. Exercice (anneaux de fractions)

2.1) On dit que $S \subset \mathbb{N} - \{0\}$ est une partie multiplicative de l'anneau $\mathbb{Z}$ si $1 \in S$ et si $s, t \in S$ entraine $s\,t \in S$. On note $S^{-1}\mathbb{Z}$ le sous ensemble de $\mathbb{Q}$ constitué des fractions x/s telles que $s \in S$.

Montrer que $S^{-1}\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$. Quels sont les éléments inversibles de $S^{-1}\mathbb{Z}$?

2.2) On se donne une famille d'entiers $u_1, \ldots, u_r \in \mathbb{N} - \{0\}$. Expliciter une partie multiplicative S telle que $S^{-1}\mathbb{Z}$ est le plus petit sous-anneau de $\mathbb{Q}$ contenant les inverses des éléments $u_1, \ldots, u_r \in \mathbb{Z}$. L'anneau de fractions $S^{-1}\mathbb{Z}$ associé à cette partie multiplicative est habituellement noté $\mathbb{Z}[u_1^{-1}, \ldots, u_r^{-1}]$ ou $\mathbb{Z}[1/u_1, \ldots, 1/u_r]$.

Comparer les anneaux de fractions $\mathbb{Z}[u_1^{-1}, \ldots, u_r^{-1}]$ et $\mathbb{Z}[(u_1 \ldots u_r)^{-1}]$.

On suppose que la décomposition en facteurs premiers d'un entier $u \in \mathbb{N} - \{0\}$ s'écrit $u = p_1^{\alpha_1} \cdot \cdots \cdot p_r^{\alpha_r}$. Comparer les anneaux de fractions $\mathbb{Z}[u^{-1}]$ et $\mathbb{Z}[p_1^{-1}, \ldots, p_r^{-1}]$? Quels sont les nombres premiers q qui sont inversibles dans $\mathbb{Z}[u^{-1}]$?

2.3) On se donne un nombre premier p. On considère le sous ensemble $S \subset \mathbb{N} - \{0\}$ constitué des nombres $s \in \mathbb{N} - \{0\}$ tels que $pgcd(s, p) = 1$. Montrer que S est une partie multiplicative. L'anneau de fractions $S^{-1}\mathbb{Z}$ associé à cette partie multiplicative est habituellement noté $\mathbb{Z}_{(p)}$. Quels sont les nombres premiers q qui sont inversibles dans $\mathbb{Z}_{(p)}$?

Remarque : L'anneau $\mathbb{Z}[10^{-1}]$ est l'anneau bien connu des nombres décimaux (relatifs).

3. Exercice

3.1) Soit S une partie multiplicative de $\mathbb{Z}$. Si I est un idéal de $\mathbb{Z}$, alors à quelle condition l'ensemble $S^{-1}I$ constitué des fractions $x/s \in \mathbb{Q}$ telles que $x \in I$ et $s \in S$ forme un idéal propre de $S^{-1}\mathbb{Z}$?

3.2) Les idéaux de $S^{-1}\mathbb{Z}$ sont-ils tous de la forme $S^{-1}I$, avec I un idéal de $\mathbb{Z}$? *Indication :* Si I' est un idéal de $S^{-1}\mathbb{Z}$, alors que peut-on dire de $I = I' \cap \mathbb{Z}$?

3.3) ! Comment caractériser les idéaux de $\mathbb{Z}_{(p)}$? Quels sont les idéaux maximaux de $\mathbb{Z}_{(p)}$?

4. Exercice

4.1) Soit $\phi : R \to S$ un morphisme d'anneaux. On suppose que $r \in R$ est un élément inversible de R. Que peut-on dire de $\phi(r) \in S$?

4.2) Peut-on construire un morphisme d'anneaux de $\mathbb{Z}[3^{-1}]$ dans $\mathbb{Z}/15$? De $\mathbb{Z}[3^{-1}]$ dans $\mathbb{Z}/5$? Ce morphisme, s'il existe, est-il unique?

En général, sous quelle condition peut-on construire un morphisme d'anneaux de l'anneau de fractions $\mathbb{Z}[u_1^{-1}, \ldots, u_r^{-1}]$ dans A? Ce morphisme, s'il existe est-il unique?

5. Exercice

Soit $\phi : A \to B$ un morphisme d'anneaux. On suppose que J est un idéal de B. On note

$$\phi^{-1}(J) = \{\, a \in A \text{ tel que } \phi(a) \in J \,\}$$

l'image réciproque de J par l'application $\phi : A \to B$.

5.1) Montrer que $\phi^{-1}(J)$ est un idéal de A.

5.2) Si J est un idéal premier, alors $\phi^{-1}(J)$ est aussi un idéal premier. Cette assertion est-elle vraie (donner une preuve) ou fausse (donner un contre-exemple)?

6. Exercice

Soit A un anneau. On fixe un idéal $I \subset A$. On voudrait déterminer l'ensemble des idéaux de l'anneau quotient A/I. On notera $[a \bmod I]$ la classe d'un élément $a \in A$ dans A/I.

6.1) On se donne un idéal J tel que $I \subset J$. On note $K = \pi_*(J)$ le sous-ensemble de A/I constitué des classes $[a \bmod I]$ telles que $a \in J$. Prouver que K est un idéal de A/I.

6.2) On se donne un idéal de A/I, soit $K \subset A/I$. On note $J = \pi^*(K)$ le sous-ensemble de A constitué des éléments $a \in A$ tels que $[a \bmod I] \in K$. Prouver que J est un idéal de A et observer que $I \subset J$.

6.3) On considère l'ensemble des idéaux de A contenant I d'une part, l'ensemble des idéaux de A/I d'autre part. Vérifier que les applications $J \mapsto \pi_*(J)$ et $K \mapsto \pi^*(K)$ définissent des bijections réciproques entre ces ensembles.

7. Exercice

7.1) Soient R et S des anneaux (commutatifs). On considère le produit cartésien $A = R \times S$ qui est muni d'une structure d'anneau caractérisée par les formules

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \qquad \text{et} \qquad (r_1, s_1) \cdot (r_2, s_2) = (r_1\, r_2, s_1\, s_2).$$

Quel est l'élément unité $1_A \in R \times S$? Trouver des éléments $e \in A$ et $f \in A$ tels que $1_A = e + f$ et tels que $e^2 = e$, $f^2 = f$ et $e\, f = f\, e = 0_A$. On dit que $1_A = e + f$ est une décomposition de l'élément $1_A \in A$ en idempotents orthogonaux.

L'application $p : A \to R$, respectivement $i : R \to A$, telle que $p(r, s) = r$, respectivement $i(r) = (r, 0)$, forme-t-elle un morphisme d'anneaux?

7.2) Inversement, soit A un anneau (commutatif). On suppose que l'unité de A possède une décomposition en idempotents orthogonaux $1_A = e+f$. Soit $R = \{e\, a,\ a \in A\}$ et $S = \{f\, a,\ a \in A\}$. Montrer que R et S sont munis d'une structure d'anneau, l'application $A \to R \times S$ qui à un élément $a \in A$ associe le couple $(e\, a, f\, a) \in R \times S$ formant un isomorphisme.

7.3) On note $[x \bmod n]$ la classe d'un entier $x \in \mathbb{Z}$ dans Z/n. On sait (théorème des restes Chinois) que l'application

$$\epsilon([x \bmod p\, q]) = ([x \bmod p], [x \bmod q]),$$

définit un isomorphisme d'anneaux de $\mathbb{Z}/p\, q\mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ dès lors que $pgcd(p, q) = 1$. Comment utiliser ce résultat pour construire une décomposition en idempotents orthogonaux de l'unité de $\mathbb{Z}/p\, q\mathbb{Z}$?

Application numérique: Construire une décomposition en idempotents orthogonaux de l'unité de $\mathbb{Z}/83 \cdot 127\mathbb{Z}$.

8. Exercice

8.1) Soient $A_1, \ldots, A_r$ des anneaux. Quels sont les éléments inversibles de l'anneau produit $(a_1, \ldots, a_r) \in A_1 \times \cdots \times A_r$? Comment déterminer l'ordre de ce groupe?

8.2) Soit $\pi : A \to B$ un isomorphisme d'anneaux. Que peut-on dire des groupes des éléments inversibles de A et B?

8.3) On rappelle que $\phi(n)$ désigne l'ordre du groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Prouver que $pgcd(m, n) = 1$ entraine $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

9. Quiz !!

Déterminer les anneaux quotients $\mathbb{R}[X]/(X^2 + 1)$ et $\mathbb{C}[X]/(X^2 + 1)$.

10. Exercice !!

I. Un idéal I dans un anneau A est *premier* si $xy \in I$ entraine $x \in I$ ou $y \in I$. On dit qu'un idéal (propre) I est *maximal* (pour l'inclusion) si et seulement si il n'existe pas d'idéal (propre) J de A tel que

$$I \underset{\neq}{\subset} J \underset{\neq}{\subset} A.$$

10.1) Prouver qu'un idéal I est premier si et seulement si l'anneau quotient A/I est intègre.
10.2) Prouver qu'un idéal I est maximal si et seulement si l'anneau quotient A/I est un corps. *Indications :* Soit $x \notin I$. Que peut-on dire de l'idéal $Ax + I$? Inversement, si on a un idéal J contenant strictement I, alors que peut-on dire de la classe d'un élément $x \in J \setminus I$ dans A/I?
10.3) Déduire de la question précédente que tout idéal maximal dans un anneau est automatiquement premier.
10.4) Quiz : Quels sont les idéaux premiers (respectivements, maximaux) de $A = \mathbb{Z}$? De $A = \mathbb{K}[X]$?

II. On étudie des idéaux de l'anneau $A = \mathbb{C}[X, Y]$ des polynômes à deux variables (X, Y) et à coefficients dans $\mathbb{C}$.
10.5) Soit $I = (X, Y)$. Peut-on trouver un polynôme $P \in \mathbb{C}[X, Y]$ tel que $I = (P)$? *Indication :* Que pourrait-on déduire des relations $X \in (P)$ et $Y \in (P)$?
10.6) Construire un isomorphisme d'anneaux $\mathbb{C}[X, Y]/(X, Y) \to \mathbb{C}$ et en déduire que $I = (X, Y)$ est un idéal maximal de $\mathbb{C}$.
10.7) On fixe $\alpha \in \mathbb{C}$ et $\beta \in \mathbb{C}$. Généraliser l'argument de la question précédente pour prouver que $(X - \alpha, Y - \beta)$ est un idéal maximal de $\mathbb{C}$.
10.8) Soit $J = (Y)$. Construire un isomorphisme d'anneaux $\mathbb{C}[X, Y]/(Y) \to \mathbb{C}[X]$. Que peut-on conclure de cette construction : l'idéal J est-il maximal ou premier?

Commentaire : Les idéaux $(X - \alpha, Y - \beta)$ associés aux points $(\alpha, \beta) \in \mathbb{C}^2$ forment en fait l'ensemble des idéaux maximaux de $\mathbb{C}[X, Y]$. Ce résultat est une forme du *Nullstellensatz* de Hilbert.

§4.2. Corps

11. Quiz

Prouver les assertions générales suivantes.
11.1) Si $\mathbb{K}$ est un corps, alors l'idéal nul $I = (0)$ est le seul idéal propre de $\mathbb{K}$.
11.2) Réciproquement, si un anneau R n'a pas d'idéal propre non trivial, alors cet anneau est un corps. *Indication :* On se donne un élément $x \in R$. Si $x \neq 0$, alors que peut-on dire de l'idéal $(x) \subset R$ engendré par x?
11.3) Un morphisme d'anneaux $\phi : \mathbb{K} \to R$ dont le domaine $\mathbb{K}$ est un corps est toujours injectif.

12. Quiz

Un anneau intègre et fini est automatiquement un corps. *Vrai ou Faux?*

13. Exercice

13.1) Dans cet exercice, on suppose que $\mathbb{K}$ est un corps, et on considère le morphisme d'anneaux canonique $\eta : \mathbb{Z} \to \mathbb{K}$ qui est caractérisé par la formule $\eta(x) = x \cdot 1_{\mathbb{K}}$, $\forall x \in \mathbb{K}$. Montrer que le noyau de ce morphisme est un idéal premier de $\mathbb{Z}$. On a donc soit $\mathrm{Ker}(\eta) = 0$, soit $\mathrm{Ker}(\eta) = (p)$, pour un certain nombre premier $p \in \mathbb{Z}$ (non nul).
13.2) On veut montrer qu'il existe un morphisme d'anneaux $\tilde{\eta} : \mathbb{Q} \to \mathbb{K}$ si et seulement si $\eta : \mathbb{Z} \to \mathbb{K}$ est injectif (ce qui équivaut à $\mathrm{Ker}(\eta) = 0$). On dit alors que $\mathbb{K}$ est un *corps de caractéristique nulle*. *Indications :* Si un tel morphisme existe, alors quelle est l'image d'un entier $x \in \mathbb{Z}$; d'un inverse d'entier $1/s \in \mathbb{Q}$, $s \in \mathbb{Z} - \{0\}$; et, finalement, d'une fraction $x/s \in \mathbb{Q}$ par $\tilde{\eta} : \mathbb{Q} \to \mathbb{K}$? Comment déduire de ces observations que $\eta(x) = x \cdot 1_{\mathbb{K}}$ est non-nul pour tout $x \in \mathbb{Z} - \{0\}$? Conclure.

13.3) On veut montrer qu'il existe un morphisme d'anneaux $\tilde{\eta} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{K}$ si et seulement si $\ker(\eta) = (p)$. On dit alors que $\mathbb{K}$ est un *corps de caractéristique positive p*. *Indications :* Si un tel morphisme existe, alors quel est l'image de la classe d'un entier $x \in \mathbb{Z}$ par $\tilde{\eta} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{K}$? Comment prouver que $\tilde{\eta} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{K}$ est injectif? Comment conclure que $\ker(\eta) = (p)$?
13.4) On suppose que $\mathbb{K}$ est un corps fini. On note q le nombre d'éléments de $\mathbb{K}$. On veut montrer que $\mathbb{K}$ est nécessairement de caractéristique $p > 0$ et que $q = p^d$ pour un certain exposant $d \in \mathbb{N}$. Comment prouver la première assertion? Comment utiliser le morphisme $\tilde{\eta} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{K}$ pour donner à $\mathbb{K}$ une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel? En général, si V est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie d, alors quel est le nombre d'éléments de V? Comment justifier que $\mathbb{K}$ forme un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie?

14. Exercice !!

Quand p est un nombre premier, l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est un corps à p éléments et est aussi noté $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Quels sont les polynômes irréductibles de degré 2 de l'anneau $\mathbb{F}_2[X]$? Si $P(X)$ est un tel polynôme, alors quelle est la dimension de $\mathbb{F}_2[X]/(P(X))$ comme espace vectoriel sur $\mathbb{F}_2$? Quel est le nombre d'éléments de $\mathbb{F}_2[X]/(P(X))$? Comment construire un corps $\mathbb{F}_4$ comportant 4 éléments?