Agrégation de mathématiques : exercices d'algèbre 2007-2008 Arithmétique, anneaux, corps, polynômes

P. HUBERT

1 Exercices classiques, à faire en priorité

Exercice 1: [Indicateur d'Euler]
Soit n un nombre entier naturel non nul, on pose :

$$\phi(n) = \text{ card } \{k, 1 \leq k \leq n, \text{ tels que } k \text{ et } n \text{ sont premiers entre eux}\}.$$

Le but de l'exercice est de montrer la formule $(\star)$:

$$\sum_{d/n} \phi(d) = n.$$

[[Soit d un diviseur de n, on montre qu'il y a $\phi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.]]

1. Soit m un élément d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$, montrer que m appartient au sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\frac{n}{d}$.
2. Montrer que les éléments d'ordre d dans H sont ceux de la forme : $\frac{kn}{d}$ où k et d sont premiers entre eux.
3. Conclure qu'il y a exactement $\phi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.
4. Prouver la formule $(\star)$.

Exercice 2:
Soit $(A, +, .)$ un anneau commutatif et unitaire. On dit qu'un élément de A est *nilpotent* s'il existe un entier n non nul tel que $x^n = 0$.

1. Montrer que l'ensemble des éléments nilpotents, muni de l'addition, est un sous-groupe de $(A, +)$.
2. Montrer que, si x est nilpotent, $1 - x$ est inversible.

3. Montrer que l'ensemble des diviseurs de 0 dans A (c'est-à-dire, l'ensemble des éléments $a \in A$ tels qu'il existe $b \in A$, $b \neq 0$ et $a.b = 0$) contient le sous-groupe des éléments nilpotents. L'ensemble des diviseurs de 0 est-il un groupe?

4. Dans $\mathbb{Z}/24\mathbb{Z}$, déterminer les éléments nilpotents, les diviseurs de 0 et les éléments inversibles, et vérifier les propriétés précédentes. Quel est l'ordre du groupe des éléments nilpotents? A quel groupe connu est-il isomorphe?

Exercice 3:

1. On considère l'ensemble $\mathbb{Z}[\sqrt{2}] = \{n + p\sqrt{2} \mid n, p \in \mathbb{Z}\}$. Montrer que cet ensemble, muni de l'addition et de la multiplication usuelle, est un anneau.

2. Montrer que l'application σ, de $(\mathbb{Z}[\sqrt{2}], +, \times)$ dans lui-même, qui, à $n + p\sqrt{2}$ associe $\sigma(n + p\sqrt{2}) = n - p\sqrt{2}$ est un automorphisme d'anneau ; quel est son inverse ?

3. On définit la fonction N sur $\mathbb{Z}[\sqrt{2}]$ par $N(x) = x\sigma(x)$. Calculer $N(p + q\sqrt{2})$; montrer que $N(x)$ appartient à $\mathbb{Z}$, et que $N(xy) = N(x)N(y)$.

4. Montrer que x est inversible dans A si et seulement si $N(x) = \pm 1$.

5. On considère les solutions entières de l'équation $a^2 = 2b^2 + 1$; donner une solution différente de $(\pm 1, 0)$ pour cette équation. Montrer que cette équation admet une infinité de solutions entières distinctes.

6. On considère l'ensemble $A = \{n + p\pi \mid n, p \in \mathbb{Z}\}$; cet ensemble, muni de l'addition, est-il un groupe ? Muni de l'addition et de la multiplication, est-il un anneau ?

Exercice 4: [Entiers de Gauss]

1. On considère l'ensemble $\mathbb{Z}[i] = \{n + ip \mid n, p \in \mathbb{Z}\}$. Montrer que cet ensemble, muni de l'addition et de la multiplication usuelles, est un anneau.

2. On définit l'application N (restriction à $\mathbb{Z}[i]$ du carré du module) par :

$$N : \begin{array}{ccc} Z[i] & \rightarrow & \mathbb{N} \\ a + ib & \mapsto & a^2 + b^2. \end{array}$$

   Montrer que, pour tous x, y dans $\mathbb{Z}[i]$, on a :

$$N(xy) = N(x)N(y).$$

3. Déduire, de la question précédente, quels sont les éléments inversibles de $\mathbb{Z}[i]$.

   [[Montrer que les éléments inversibles de $\mathbb{Z}[i]$ sont les éléments de norme 1.]]

4. Soit x élément de $\mathbb{Z}[i]$ tel que $N(x)$ est un nombre premier, montrer que x est irréductible dans $\mathbb{Z}[i]$. La réciproque est-elle vraie ?

   [[On pourra montrer que 2 n'est pas irréductible dans $\mathbb{Z}[i]$.]]

5. Soient x et y éléments de $\mathbb{Z}[i]$ ($y \neq 0$), remarquer qu'il existe u et v éléments de $\mathbb{Q}$ tels que $\frac{x}{y} = u + iv$. Montrer qu'il existe deux entiers u_0 et v_0 tels que $|u - u_0| \leq \frac{1}{2}$ et $|v - v_0| \leq \frac{1}{2}$.

6. Montrer qu'il existe r appartenant à $\mathbb{Z}[i]$ vérifiant $N(r) < N(b)$ tel que $x = y(u_0 + iv_0) + r$.

   (On dit qu'on a construit une division euclidienne sur $\mathbb{Z}[i]$.)

7. Déduire, de la question précédente, que tout idéal de $\mathbb{Z}[i]$ est principal.

   [[Utiliser un argument similaire à celui employé pour montrer que $\mathbb{Z}$ est principal.]]

Exercice 5: [idéaux maximaux]

Soit A un anneau intègre et I un idéal, on dit que I est *maximal* si I est différent de A et si tout idéal J contenant strictement I est égal à A.

1. Déterminer les idéaux maximaux de $\mathbb{Z}$, ceux de $K[X]$ où K est un corps.

2. Montrer que I est un idéal maximal si et seulement si A/I est un corps.

3. Soit P un polynôme à coefficients dans K. Déduire des questions précédentes que $K[X]/(P)$ est un corps si et seulement si P est irréductible.

Exercice 6:

1. Montrer que $\mathbb{Z}[X]$ n'est pas un anneau principal.

   [[Introduire l'idéal engendré par 2 et X.]]

2. Soit A un anneau intègre. Adapter la preuve précédente pounr montrer que : $A[X]$ est principal si et seulement si A est un corps.

Exercice 7: Soit P un polynôme à coefficients dans $\mathbb{Z}$, $P(x) = \displaystyle\sum_{i=0}^{n} a_i X^i$, tel que $a_0 = a_n = 1$, montrer que P ne peut pas avoir d'autres racines rationnelles que -1 et 1.

Application : Montrer que le polynôme $X^5 - X^2 + 1$ n'a pas de racines rationnelles.

Exercice 8: [Polynômes cyclotomiques]

Soit n un entier naturel non nul, on appelle racine primitive $n^{ième}$ de 1, une racine $n^{ième}$ de 1 qui engendre le groupe des racines $n^{ième}$ de 1. Notons $A(n)$ l'ensemble des racines primitives $n^{ième}$ de 1. Le $n^{ième}$ polynôme cyclotomique est :

$$\Phi_n(X) = \prod_{\xi \,\in\, A(n)} (X - \xi).$$

1. Montrer que $e^{\frac{2ik\pi}{n}}$ est une racine primitive de 1 si et seulement si k et n sont premiers entre eux.

2. Déduire de la question précédente que $\Phi_n(X)$ est de degré $\phi(n)$.

3. Calculer $\Phi_1(X)$, $\Phi_2(X)$, $\Phi_3(X)$, $\Phi_4(X)$, $\Phi_p(X)$ pour p premier.

4. Montrer la formule :
$$X^n - 1 = \prod_{d\ /\ n} \Phi_d(X).$$

5. En déduire, par récurrence sur n, que Φ_n est un polynôme à coefficients dans $\mathbb{Q}$, puis à coefficients dans $\mathbb{Z}$.

6. Montrer que $\Phi_n(0) = 1$ pour $n > 1$.

7. Calculer $\Phi_{12}(X)$, $\Phi_{24}(X)$.

Remarque : On montrera plus tard que Φ_n est un polynôme irréductible sur $\mathbb{Q}$.

Exercice 9: [carrés dans $\mathbb{Z}/p\mathbb{Z}$.]
Soit p un nombre premier différent de 2.

1. On note $C(p) = \{x \in \mathbb{Z}/p\mathbb{Z}\ |\exists y \in \mathbb{Z}/p\mathbb{Z}$ tel que $x = y^2\}$ ($C(p)$ est l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$) et on note $C(p)^* = C(p) \setminus \{0\}$. Montrer que $C(p)^*$ est un sous-groupe multiplicatif de $\mathbb{Z}/p\mathbb{Z}^*$.

2. Soit ϕ l'application définie par :
$$\phi : \begin{array}{ccc} \mathbb{Z}/p\mathbb{Z}^* & \rightarrow & C(p)^* \\ x & \mapsto & x^2. \end{array}$$
Montrer que ϕ est un morphisme de groupes.

3. En appliquant le théorème de factorisation des morphismes, montrer que le cardinal de $C(p)^*$ est égal à $\frac{p-1}{2}$.

4. Montrer que :
$$x \in C(p)^* \Leftrightarrow x^{\frac{p-1}{2}} = 1.$$
[[Utiliser le fait qu'un polynôme, à coefficients dans un corps K, de degré $\frac{p-1}{2}$ a, au plus, $\frac{p-1}{2}$ racines dans K.]]

5. Déduire, de la question précédente, que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si : $p \equiv 1[4]$.

6. Application arithmétique :

   Montrer qu'il y a une infinité de nombres premiers congrus à 1 modulo 4.

   [[Pour n donné, considérer le nombre $N = (n!)^2 + 1$ et montrer que N a un diviseur p premier plus grand que n, congru à 1 modulo 4.]]

7. Soit a appartenant à $\mathbb{Z}/5Z$. Résoudre dans $\mathbb{Z}/5Z$ l'équation $X^2 - 3X + a = 0$. On envisagera plusieurs cas suivant la valeur de a.

2 Arithmétique élémentaire

Exercice 10: [fonctions arithmétiques]

On notera $\mathcal{P}$ l'ensemble des nombres premiers. Soit μ la fonction de Möbius de $\mathbb{N}^*$ dans $\mathbb{N}$ définie par

$\mu(1) = 1$
$\mu(p_1 \cdots p_k) = (-1)^k$où $p_1, \cdots, p_k$ sont des nombres premiers distincts
$\mu(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = 0$ s'il existe i tel que $\alpha_i > 2$

1. Montrer que μ est une fonction multiplicative c'est-à-dire que $\mu(mn) = \mu(m)\mu(n)$ si n et m sont premiers entre eux.

2. Montrer la formule :
$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ sinon.} \end{cases}$$

3. Montrer la formule d'inversion de Möbius

   Soit f et g deux fonctions de $\mathbb{N}$ à valeurs dans $\mathbb{C}$, telles que
$$f(n) = \sum_{d|n} g(d).$$
   Montrer que
$$g(n) = \sum_{d|n} \mu(n/d)g(d).$$

4. Deuxième formule d'inversion de Möbius

   Soit f et g deux fonctions de $\mathbb{N}$ à valeurs dans $\mathbb{C}$, telles que
$$g(n) = \sum_{d|n} \mu(n/d)f(d).$$
   Montrer que
$$f(n) = \sum_{d|n} g(d).$$

5. Soit ϕ la fonction d'Euler. On rappelle la formule :
$$\phi(n) = n \prod_{p\in\mathcal{P},\ p|n} (1 - \frac{1}{p}).$$
   Montrer la formule
$$\phi(n) = n - \sum_{p|n,\ p\ \in\mathcal{P}} \frac{n}{p} + \sum_{p,p'\in\mathcal{P},\ p\neq p',\ p|n,\ p'|n} \frac{n}{pp'} + \cdots$$
   En déduire la formule $(*)$:

$$\phi(n) = \sum_{d|n} d\mu(n/d).$$

En utilisant la deuxième formule d'inversion, retrouver la formule :

$$\sum_{d|n} \phi(d) = n.$$

6. soient (a_n) et (b_n) deux suites bornées, montrer que

$$(\sum_{k=1}^{+\infty} \frac{a_k}{k^2})(\sum_{m=1}^{+\infty} \frac{b_m}{m^2}) = \sum_{n=1}^{+\infty} \sum_{km=n} \frac{a_k b_m}{n^2}.$$

En déduire que :

$$(\sum_{k=1}^{+\infty} \frac{1}{k^2})(\sum_{m=1}^{+\infty} \frac{\mu(m)}{m^2}) = 1,$$

et

$$\sum_{m=1}^{+\infty} \frac{\mu(m)}{m^2} = \frac{6}{\pi^2}.$$

[[utiliser la relation classique

$$\sum_{m=1}^{+\infty} \frac{1}{m^2} = \frac{\pi^2}{6}.]]$$

7. Soit $\Phi(n) = \phi(1)+\cdots\phi(n)$. En utilisant la relation $(*)$ et la question précédente, montrer que

$$\Phi(n) = \frac{3n^2}{\pi^2} + O(nln(n)).$$

Exercice 11: [Théorème de Lucas]

Le but de cet exercice est de démontrer le théorème de Lucas : $PGCD(F_n, F_m) = F_{PGCD(n,m)}$ où (F_n) est la suite de Fibonnacci.

La suite de Fibonnacci est définie par la relation de récurrence $F_{n+2} = F_{n+1} + F_n$ et les conditions initiales $F_0 = 0$ et $F_1 = 1$.

1. Montrer la relation $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$, pour tout $n \geq 1$. En déduire que F_n et F_{n+1} sont premiers entre eux.

2. Montrer, par récurrence, la relation $F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$ pour $m \geq 1$ et $n \geq 0$.

3. Soit d un nombre entier montrer que :

   $(*)$ d divise F_m et F_n si et seulement si d divise F_n et F_{n+m}.

4. On va montrer qu'une suite d'entiers (F_n), possédant la propriété $(*)$ et $F_0 = 0$, vérifie la conclusion du théorème de Lucas.

   (a) Montrer, que, pour tout $k \geq 1$, on a
   [[d divise F_m et F_n si et seulement si d divise F_n et F_{n+km}, où $d \in \mathbb{N}$.]]

   (b) On suppose $m > n$. Soit r le reste de la division euclidienne de m par n. Montrer que $PGCD(F_m, F_n) = PGCD(F_n, F_r)$.

   (c) En utilisant l'algorithme d'Euclide, montrer que $PGCD(F_m, F_n) = F_{PGCD(n,m)}$.

Exercice 12: [Fractions continues]

Soit x un nombre irrationnel. On définit une suite d'entiers (a_n) appelés quotients partiels de x et une suite de nombres réels (x_n) par le procédé suivant :

$a_0 = E(x)$ et $x_0 = \{x\}$ la partie fractionnaire de x, $a_1 = E(\frac{1}{x_0})$, $x_1 = \{\frac{1}{x_0}\}$ et par itération $a_n = E(\frac{1}{x_{n-1}})$, $x_n = \{\frac{1}{x_{n-1}}\}$.

1. Montrer que ce procédé est bien défini et que $a_n \leq 1$ si $n > 0$.

2. Montrer que

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_n + x_n}}}}$$

   On écrira $x = [a_0;\ a_1, a_2, \ldots, a_n + x_n]$. On note la fraction continue finie

$$[a_0;\ a_1, a_2, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_n}}}}$$

   On veut montrer que $[a_0;\ a_1, a_2, \ldots, a_n]$ converge vers x quand n tend vers l'infini et obtenir une majoration de la vitesse de convergence.

3. On définit les deux suites d'entiers (p_n) et (q_n) par les relations de récurrence

$$p_n = a_n p_{n-1} + p_{n-2}$$

$$q_n = a_n q_{n-1} + q_{n-2}$$

   avec les conditions initiales $p_0 = a_0$, $q_0 = 1$, $p_1 = a_0 a_1 + 1$, $q_1 = a_1$. Montrer que $\frac{p_n}{q_n} = [a_0;\ a_1, a_2, \ldots, a_n]$.

   [[raisonner, par récurrence, sur la longueur de la fraction continue.]]

La suite $(\frac{p_n}{q_n})$ est appelée suite des convergents de x. Montrer que

$$p_{n-1}q_n - p_nq_{n-1} = (-1)^n$$

pour tout $n \leq 1$. En déduire que la fraction $\frac{p_n}{q_n}$ est réduite (p_n et q_n premiers entre eux).

4. Montrer, comme à la question précédente que, pour tout n, $x = \dfrac{\tilde{p}_n}{\tilde{q}_n}$ où $(\tilde{p}_n)$ et $(\tilde{q}_n)$ vérifie les relations de récurrence

$$\tilde{p}_n = (a_n + x_n)p_{n-1} + p_{n-2} = p_n + x_np_{n-1}$$

$$\tilde{q}_n = (a_n + x_n)q_{n-1} + q_{n-2} = q_n + x_nq_{n-1}.$$

5. En déduire que

$$|x - \frac{p_n}{q_n}| < \frac{1}{q_n^2}.$$

Comparer cette approximation avec l'approximation décimale. On pourra voir que l'erreur entre un nombre et ses n premières décimales est, en général, de l'ordre du dénominateur 10^{-n} alors qu'ici, on a une erreur en $1/q^2$ ce qui est bien meilleur. Avec un peu plus de travail, on peut montrer que l'approximation par les fractions continues est la meilleure possible.

(Le résultat précis est le suivant :

soit (p, q) premiers entre eux vérifiant $|qx - p| < |q_nx - p_n|$ alors $q \geq q_n$).

Par exemple la fraction $\frac{22}{7}$ qui est connue pour être une bonne approximation de π est obtenue par les fractions continues.

3 Anneaux

Exercice 13: Soit A un anneau intègre qui n'est pas un corps. Soit $\mathcal{I}(A)$ l'ensemble des idéaux principaux de A.

Soit p élement de A. Montrer que p est irréductible dans A si et seulement si (p) est maximal dans $\mathcal{I}(A) \setminus \{A\}$

Exercice 14: [Radical d'un idéal]

Soit A un anneau et I un idéal de A. On définit le radical (ou racine) de I noté $\sqrt{I}$ comme :

$$\sqrt{I} = \{x \in A, \text{ tel que } \exists n \in \mathbb{N}, \text{ tel que } x^n \in I\}.$$

1. Montrer que $\sqrt{I}$ est un idéal de A contenant I.

2. Soient $A = \mathbb{Z}$, p et q deux nombres premiers trouver $\sqrt{p^2q^3\mathbb{Z}}$.

3. Montrer $\sqrt{0}$ est égal à $\mathcal{N}(A)$ l'ensemble des éléments nilpotents de A

4. Montrer que $\mathcal{N}(A)$ est l'intersection des idéaux premiers de A.

   [[Soit x nilpotent et P idéal premier, pour montrer que x est élément de P, on montrera que la classe de x est nulle dans A/P.

   Réciproquement, soit x non nilpotent, définir $S = \{x^n, n \in \mathbb{N}\}$. Considérer $\mathcal{E} = \{I \text{ idéal tel que } S \cap I = \emptyset\}$. Montrer que $\mathcal{E}$ muni de l'inclusion est un ensemble inductif et donc (d'après le lemme de Zorn) admet un élément maximal P. Montrer que P est un idéal premier qui ne contient pas x.]]

5. Soit Π la projection canonique de A sur A/I. Montrer que Π induit une bijection entre les idéaux de A contenant I et les idéaux de A/I.

6. En utilisant les deux questions précédentes, montrer que $\sqrt{I}$ est l'intersection des idéaux de A contenant I.

   [[On remarquera que $x \in \sqrt{I}$ si et seulement si $\Pi(x) \in \mathcal{N}(A/I)$.]]

Exercice 15: [Anneau principal et non euclidien]

1. Soit A un anneau euclidien, $\mathcal{U}(A)$ les inversibles de A. Pour x dans A on note Π_x la projection canonique de A vers $A/(x)$. Montrer qu'il existe x dans A tel que
$$\Pi_x(\mathcal{U}(A) \cup \{0\}) = A/(x).$$
   [[Prendre ϕ un stathme adapté et x tel que $\phi(x)$ est minimal parmi les éléments inversibles non nuls de A.]]

2. On veut montrer que $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ n'est pas un anneau euclidien. On va montrer que les seuls éléments inversibles sont 1 et -1 et appliquer la question 1. On pose $\alpha = \frac{1+i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$.

   (a) Montrer que tout élément z de A s'écrit, de manière unique, $z = a + b\,\alpha$ où a et b sont dans $\mathbb{Z}$.

   (b) Soit z dans A, on note $N(z) = z\overline{z}$ le carré du module de z. Montrer que z est inversible dans A si et seulement si $N(z) = 1$.

   (c) Soit $z = a + b\alpha$ où a et b sont éléments de $\mathbb{Z}$. Montrer que
$$N(z) = a^2 + ab + 5b^2.$$
   En déduire que $N(z) \geq 4b^2$. Conclure que si z est inversible alors $z = \pm 1$.

   (d) On raisonne par l'absurde. En utilisant la question 1, montrer que, si A est euclidien, il existe x_0 dans A tel que le cardinal de $F = A/(x_0) \leq 3$. En déduire que F est isomorphe soit à $\mathbb{Z}/2\mathbb{Z}$ soit à $\mathbb{Z}/3\mathbb{Z}$.

   (e) Montrer que α vérifie l'équation $\alpha^2 - \alpha + 5 = 0$. Soit $\beta = \Pi_{x_0}(\alpha)$. Etablir une équation vérifiée par β et montrer que cette équation n'a pas de solution dans F. Conclure.

Remarque : On peut montrer que A est un anneau principal. C'est donc un exemple d'anneau principal non euclidien.

Exercice 16: [Décimaux relatifs]

1. Soit D l'ensemble des décimaux relatifs, montrer que
$$D = \{x \in \mathbb{Q}, \text{ tels que } \exists n \in \mathbb{N} \text{ tel que } 10^n x \in \mathbb{Z}\}.$$
2. Soit I un idéal de D, montrer que $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$.
3. Soit q un générateur de $I \cap \mathbb{Z}$, montrer que $I = qD$. En déduire que D est un anneau principal.
4. Montrer que tout élément de D s'écrit de façon unique $x = 2^a 5^b y$ où $a, b, y \in \mathbb{Z}$ et y est premier avec 2 et 5.
5. Montrer que les éléments inversibles de D sont de la forme $2^a 5^b$ où $a, b \in \mathbb{Z}$.
6. Montrer que D est un anneau euclidien.

   [[Définir un stathme ϕ sur D comme suit : si $x = \frac{a}{10^n}$ avec a non divisible par 10, poser $\phi(x) = |a|$.]]

Exercice 17: [Entiers des corps quadratiques]

Un corps quadratique est une extension de degré 2 de $\mathbb{Q}$.

1. Montrer que K est un corps quadratique si et seulement si il existe $d \in \mathbb{Z}$ sans facteurs carrés tels que $K = \mathbb{Q}[\sqrt{d}]$.
2. Soit $K = \mathbb{Q}[\sqrt{d}]$ est un entier sans facteurs carrés. Montrer que
$$\sigma \ : \ \begin{array}{ccc} K & \to & K \\ a + b\sqrt{d} & \mapsto & a - b\sqrt{d} \end{array}$$
   est un morphisme de corps.
3. On dit que $x \in K$ est un entier de K si x est racine d'un polynôme **unitaire** à coefficient dans $\mathbb{Z}$. On note A l'ensemble des entiers de K. Montrer que si $x \in A$, alors $\sigma(x) \in A$.
4. Soit $x = a + b\sqrt{d}$ avec a et b rationnels. Montrer que x appartient à A si et seulement si :
$$\begin{cases} x + \sigma(x) = 2a \in \mathbb{Z} \\ x\sigma(x) = a^2 - db^2 \in \mathbb{Z} \end{cases}$$
5. Supposons $x \in A$, montrer que $2b$ appartient à $\mathbb{Z}$.

   [[Montrer tout d'abord que $d(2b)^2 \in \mathbb{Z}$ et supposer, par l'absurde, que $2b$ n'appartient pas à $\mathbb{Z}$.]]

6. On pose $u = a/2$, $v = b/2$. Montrer que $x \in A$ si et seulement si

$$\begin{cases} u, v \in \mathbb{Z} \\ u^2 - dv^2 \in 4\mathbb{Z} \end{cases}$$

7. Montrer que

   - si $d \equiv 2$ ou 3 mod 4 alors $A = \mathbb{Z}[\sqrt{d}]$
   - si $d \equiv 1$ mod 4 alors

$$A = \{\frac{1}{2}(u + \sqrt{d}v),\ u, v \in \mathbb{Z} \text{ de même parité}\}.$$

Exercice 18: [Entiers de Gauss et théorème des deux carrés]

On rappelle que $\mathbb{Z}[i]$ est un anneau euclidien et donc principal.

On note $\mathcal{P}$, l'ensemble des nombres premiers et on appelle Σ l'ensemble des entiers naturels qui sont somme de deux carrés. Autrement dit :

$$\Sigma = \{n \in \mathbb{N} \text{ tel que } \exists (a, b) \in \mathbb{N}, \text{ tels que } n = a^2 + b^2\}.$$

On veut montrer les théorèmes suivants :

Théorème 1 *Soit p un nombre premier alors :*
p appartient à Σ si et seulement si $p = 2$ ou $p \equiv 1$ $mod 4$.

Théorème 2 *Soit $n \in \mathbb{N}^*$ décomposé en facteurs premiers :*

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

où $v_p(n)$ est la valuation p-adique de n. On a :
n appartient à Σ si et seulement si $v_p(n)$ est pair pour tout $p \equiv 3$ $mod 4$.

1. Soit n congru à 3 $mod 4$. Montrer que n n'appartient pas à Σ.

2. Soit p un nombre premier, montrer que :

   p appartient à Σ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

   [[Si p est non irréductible, écrire $p = z_1 z_2$ et montrer que $N(z_1) = N(z_2) = p$.]]

3. Montrer que si p divise $1 + a^2$ avec $a \in \mathbb{Z}$, alors $p \in \Sigma$.

   [[Raisonner par l'absurde.]]

4. Montrer que si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ alors $p \in \Sigma$.

5. En utilisant le fait que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1$ $mod 4$, démontrer le théorème 1.

6. Montrer que Σ est stable par multiplication, c'est-à-dire, si n et m sont dans Σ alors nm appartient à Σ.

7. Déduire de la question précédente et du théorème 1 que, si $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ avec $v_p(n)$ pair pour tout $p \equiv 3\ mod 4$, alors $n \in \Sigma$.

8. Soit p premier $p \equiv 3\ mod 4$, montrer, par récurrence sur $v_p(n)$, que, si n appartient à Σ, alors $v_p(n)$ est pair.

   [[Utiliser le fait que p est irréductible dans $\mathbb{Z}[i]$.]]

9. Montrer le théorème 2.

4 Polynômes

Exercice 19: Soit P un polynôme à coefficients dans $\mathbb{Z}$, unitaire, qui a une unique racine complexe de module supérieur ou égal à 1 et tel que $P(0) \neq 0$. Montrer que P est irréductible sur $\mathbb{Q}$.

Exercice 20: Soit P un polynôme à coefficients dans $\mathbb{Q}$.

1. Montrer que, si P est irréductible sur $\mathbb{Q}$ alors P n'a que des racines simples dans $\mathbb{C}$.

   Peut-on étendre ce résultat à une situation plus générale ?

2. Soit $\lambda \in \mathbb{C}$, racine de P de multiplicité strictement plus grande que $\frac{d(P)}{2}$, montrer que $\lambda \in \mathbb{Q}$.

   [[On pourra faire deux preuves de ce résultat, soit directement, soit en utilisant la première question.]]

Exercice 21: [Critère d'Eisenstein]
Soit P un polynôme à coefficients dans $\mathbb{Z}$, $P(X) = \sum_{i=0}^{n} a_i X^i$ et p un nombre premier. On suppose :

- p ne divise pas a_n
- p divise $a_0, \ldots, a_{n-1}$
- p^2 ne divise pas a_0.

Montrer que P est irréductible sur $\mathbb{Z}$.

Application : Montrer que si p est un nombre premier, le polynôme $X^{p-1} + X^{p-2} \ldots X + 1$ est irréductible sur $\mathbb{Z}$.
[[On pourra introduire $Q(X) = P(X+1)$.]]

Exercice 22: [Critère d'irréductibilité]
Soit P un polynôme à coefficients dans $\mathbb{Z}$. Soit p un nombre premier. Notons $P[p]$ l'image de P par la surjection canonique de $\mathbb{Z}$ vers $\mathbb{Z}/p\mathbb{Z}$ (les coefficients de $P[p]$ sont les coefficients de P réduits modulo p). On suppose que P et $P[p]$ ont même degré.

Montrer que si $P[p]$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$ alors P est irréductible sur $\mathbb{Q}$. La réciproque est-elle vraie ?

Exercice 23: [polynômes binomiaux]
Pour tout $n \in N$, on définit le polynôme (polynôme binomial) P_n par, $P_0 = 1$, et

$$P_n(X) = \frac{X(X-1)\dots(X-n+1)}{n!}, \text{ pour } n \geq 1.$$

1. Montrer que la famille $(P_n)_{n\in\mathbb{N}}$ est une base que $\mathbb{Q}[X]$.
2. Soit P appartenant à $\mathbb{Q}[X]$, on écrit P dans la base $(P_n)_{n\in\mathbb{N}}$,

$$P(X) = \sum_{k=0}^{M} d_k P_k(X)$$

   où $d_k \in \mathbb{Q}$. Exprimer les d_k en fonction des valeurs $P(0), P(1), \dots, P(M)$.
3. Déduire des questions précédentes que P est une combinaison linéaire à coefficients dans $\mathbb{Z}$ des polynômes binomiaux si et seulement si $P(\mathbb{Z}) \subset \mathbb{Z}$.

Exercice 24: Soit P un polynôme à coefficients dans $\mathbb{R}$, montrer l'équivalence suivante :
(i) Pour tout t appartenant $\mathbb{R}$, $P(t) \geq 0$.

(ii) Il existe Q, R polynômes à coefficients dans $\mathbb{R}$ tels que $P = Q^2 + R^2$.

[[On pourra montrer que l'ensemble des polynômes vérifiants (ii) est stable par multiplication.]]

Exercice 25: [Localisation des racines]
Soit P un polynôme à coefficients complexes et P' son polynôme dérivée, montrer que les racines de P' sont dans l'enveloppe convexe des racines de P.

5 Polynômes à plusieurs variables

Exercice 26:

1. Montrer que l'idéal (X, Y) n'est pas principal dans $\mathbb{Q}[X, Y]$.
2. Montrer que (X) est un idéal premier de $\mathbb{Q}[X, Y]$ mais pas maximal.

Exercice 27: Montrer que, dans $\mathbb{R}^n$ (ou $\mathbb{C}^n$), le complémentaire des zéros d'un polynôme non nul est dense.
[[Raisonner par l'absurde.]]

Applications :

1. Soit P un polynôme appartenant à $\mathbb{R}^n[X]$.

   Soit $\Omega = \{Q \in \mathbb{R}^n[X],\ \text{tels que } \mathrm{PGCD}(P,Q) = 1\}$. Montrer que Ω est dense dans $\mathbb{R}^n[X]$.

   [[Faire intervenir les racines de P.]]

2. Montrer que l'ensemble des polynômes de degré n à racines simples est dense dans $\mathbb{R}^n[X]$.

   [[Introduire le discriminant.]]

Exercice 28: Calculer le discriminant des polynômes aX^2+bX+c et X^3+pX+q.

Exercice 29: Soit $P(X) = (X-x_1)\dots(X-x_n)$ et $D(P)$ son discriminant. Pour tout entier k, on note $S_k = x_1^k + \dots + x_n^k$ avec la convention $S_0 = n$. Montrer que

$$D(P) = (-1)^{n(n-1)/2}P'(x_1)\dots P'(x_n) = \prod_{1\le k<l\le n}(x_l - x_k)^2 = \begin{pmatrix} S_0 & S_1 & \cdots & S_{n-1} \\ S_1 & S_2 & \cdots & S_n \\ \vdots & \vdots & \vdots & \vdots \\ S_{n-1} & S_n & \cdots & S_{2n-2} \end{pmatrix}$$

[[Pour obtenir la deuxième égalité, écrire explicitement $P'(x_i)$ pour $1 \le i \le n$. Pour la troisième, introduire un déterminant de Vandermonde.]]

Exercice 30: [Application des formules de Newton]
Soit K un corps de caractéristique nulle et A appartenant à $M_n(K)$ telle que $tr(A) = tr(A^2) = \dots = tr(A^n) = 0$. Montrer que A est une matrice nilpotente.
[[Trigonaliser A sur $\mathbb{C}$ et appliquer les formules de Newton.]]

6 Corps finis

Exercice 31: [Groupe multiplicatif de $\mathbb{Z}/p\mathbb{Z}$]
Le but de l'exercice est de montrer que le groupe multiplicatif du corps $\mathbb{Z}/p\mathbb{Z}$ (p premier) est cyclique.

1. Soit d un diviseur de $p-1$ et x un élément d'ordre d, montrer que les éléments d'ordre d du groupe $\mathbb{Z}/p\mathbb{Z}^*$ appartiennent au sous-groupe engendré par x.

   [[Utiliser le fait que le polynôme $X^d - 1$ a, au plus, d racines dans $\mathbb{Z}/p\mathbb{Z}$]].

2. Déduire, de la question précédente, qu'il y a 0 ou $\phi(d)$ éléments d'ordre d dans $\mathbb{Z}/p\mathbb{Z}^*$.

3. En utilisant le fait que :
$$\sum_{d/p-1} \phi(d) = p-1,$$
montrer qu'il y a $\phi(p-1)$ éléments d'ordre $p-1$ dans $\mathbb{Z}/p\mathbb{Z}^*$ et, en déduire, que $\mathbb{Z}/p\mathbb{Z}^*$ est un groupe cyclique.

Exercice 32: [Clôture algébrique des corps finis]

1. Soit p un nombre premier. Soit
$$K = \bigcup_{n\in\mathbb{N}} F_{p^{n!}}$$
Montrer que K est la clôture algébrique de F_p.
2. Soit q une puissance de p. Soit F l'union des extensions finies de F_q. Montrer que $K = F$.

Exercice 33: Soit $P(X) = X^p - X - 1$ vu comme polynôme sur F_p.

1. Montrer que P n'a pas de racine dans F_p.
2. Soit α une racine de P dans la clôture algébrique de F_p. Montrer que les autres racines de P sont $\alpha + i$ pour $i \in F_p$.
3. Montrer que le polynôme $P(X) = X^p - X - 1$ est irréductible sur F_p.
[[Raisonner par l'absurde et montrer que α appartient à F_p.]]

Exercice 34: Soit Q un polynôme à coefficients dans F_p.

1. A quelle condition $F_p[X]/(Q)$ est-il un corps ?
2. On suppose que Q n'a que des racines simples. Trouver un isomorphisme entre $F_p[X]/(Q)$ et un anneau connu. [[faire intervenir la décomposition de Q en facteurs irréductibles.]]
3. Quel est le cardinal de $F_p[X]/(Q)$?

Exercice 35: [Les corps finis sont parfaits]
On dit qu'un corps est parfait si tout polynôme irréductible est à racines simples.

1. Soit K un corps fini de caractéristique p et $P(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme irréductible sur K. Montrer que si P n'a pas toutes ses racines distinctes alors $P' = 0$.

2. On suppose, dans la suite de l'exercice, que $P' = 0$. Montrer que $P = \sum_{k=O}^{E(n/p)} a_{kp} X^{kp}$.

3. On rappelle que le morphisme de Frobenius :
$$f : \begin{array}{ccc} K & \to & K \\ x & \mapsto & x^p \end{array}$$
est un isomorphisme de K (car K est fini). En déduire qu'il existe un polynôme Q à coefficients dans K tel que $P = Q^p$.

4. En déduire que P n'est pas irréductible.

7 Extension de corps

Exercice 36: [Corps de décomposition] Soit $P = X^3 - 2$ et $\alpha = \sqrt[3]{2}$.

1. Montrer que $\mathbb{Q}[\alpha]$ n'est pas le corps de décomposition de P.

2. Soit D_P le corps de décomposition de P. Montrer que $D_P = \mathbb{Q}[\alpha, j]$ où j est une racine primitive $3^{ème}$ de 1.

3. On définit le polynôme R par l'équation :
$$P(X) = R(X)(X - \alpha).$$
Montrer que R à coefficients dans $\mathbb{Q}[\alpha]$ et que R est irréductible sur $\mathbb{Q}[\alpha]$. En déduire que K le corps de rupture de R sur $\mathbb{Q}[\alpha]$ est une extension de degré deux de $\mathbb{Q}[\alpha]$.

4. Montrer que $K = D_P$ et donner le degré de l'extension de D_P sur $\mathbb{Q}$.

5. Généralisation : soient α et β deux nombres algébriques dont les degrés d et δ sont premiers entre eux. Soit $K = \mathbb{Q}(\alpha, \beta)$, montrer que $[K : \mathbb{Q}] = d\,\delta$.

Exercice 37: [Equation $P(X) = X^4 - 10X^2 + 1$]

1. Montrer que $x = \sqrt{2} + \sqrt{3}$ est racine de P.

2. Montrer que $X^2 - 3$ est irréductible sur $\mathbb{Q}[\sqrt{2}]$. En déduire une base de $\mathbb{Q}[\sqrt{2},\ \sqrt{3}]$ sur $\mathbb{Q}$ et déterminer $[\mathbb{Q}[\sqrt{2},\ \sqrt{3}]\ :\ \mathbb{Q}]$.

3. Montrer que $\mathbb{Q}[\sqrt{2},\ \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Donner une autre base de $\mathbb{Q}[\sqrt{2},\ \sqrt{3}]$ sur $\mathbb{Q}$.

4. Montrer que les racines de P sont $\pm(\sqrt{2} + \sqrt{3})$ et $\pm(\sqrt{2} - \sqrt{3})$. Trouver D_P le corps de décomposition de P.

Exercice 38: [Equation binôme de degré 4]
Soit $P(X) = X^4 - x$ où x est un rationnel strictement positif.

1. Trouver les racines de P.
2. Montrer que P est irréductible sur $\mathbb{Q}$ si et seulement si $\sqrt{x} \notin \mathbb{Q}$.
3. Lorsque $u = \sqrt[4]{x} \in \mathbb{Q}$, donner la décomposition de P en facteurs irréductibles.
4. Lorsque $\sqrt[4]{x}$ n'appartient pas à $\mathbb{Q}$ et $\sqrt{x} \in \mathbb{Q}$, donner la décomposition de P en facteurs irréductibles. Montrer que $D_P = \mathbb{Q}(u, i)$ et que $[D_P : \mathbb{Q}] = 4$.
5. On suppose que $\sqrt{x}$ n'appartient pas à $\mathbb{Q}$. Montrer que $\mathbb{Q}(u, i) = D_P$ et que $[D_P : \mathbb{Q}] = 8$.

Exercice 39: [Utilisation du théorème de l'élément primitif]
Soit $L = Q[j, \sqrt[3]{2}]$. Trouver un élément primitif de L sur $\mathbb{Q}$.
[[On pourra vérifier, par exemple, que $\lambda = 1$ convient dans la preuve du théorème de l'élément primitif.]]

Exercice 40: Soit L une extension d'un corps K tel que $[L : K]$ est un nombre premier p. Soit α élément de L tel que α n'appartient pas K. Montrer que $L = K[\alpha]$.

Exercice 41: Soit K un corps de caractéristique nulle et P un polynôme irréductible sur K de degré n. On note D_P son corps de décomposition. Montrer que

$$[D_P : K] \leq n!$$

[[Raisonner par récurrence sur n.]]

Exercice 42: Soit K un corps de caractéristique nulle et L une extension de K.

1. Montrer que
   i) $[L : K] \leq n$
   $\Leftrightarrow$
   ii) pour tout x dans L, $[K[x] : K] \leq n$.
2. Existe-t-il L une extension de degré infini de K telle que, pour tout x dans L, $[K[x] : K]$ est fini ?

Exercice 43: Soit L une extension de degré m d'un corps K et P un polynôme unitaire de $K[X]$ irréductible de degré n. On suppose que n et m sont premiers entre eux. Montrer que P est irréductible sur L.
[[Raisonner par l'absurde. Considérer x une racine de P et $M = L[x]$.]]

APPLICATIONS

1. (a) Soit $P = X^3 - 2$, montrer que P est irréductible sur $\mathbb{Q}[i]$.

(b) Soit $\alpha = \sqrt[3]{2}$. Montrer que $\mathbb{Q}[i, \alpha] = \mathbb{Q}[i\alpha]$. Quel est le degré de cette extension ?

(c) En dduire que $X^6 + 4$ est irrductible sur $\mathbb{Q}$.

2. (a) Montrer que $P = X^5 - 7$ est irréductible sur $\mathbb{Q}$.

   (b) Soit $\beta = e^{2i\pi/5}$, trouver le polynôme minimal de β sur $\mathbb{Q}$. En déduire la valeur de $[\mathbb{Q}[\beta] : \mathbb{Q}]$ et montrer que $X^5 - 7$ est irréductible sur $\mathbb{Q}[\beta]$.

   (c) Montrer que le corps de décomposition de P sur $\mathbb{Q}$ est $\mathbb{Q}[\alpha, \beta]$ où $\alpha = \sqrt[5]{7}$. Quel est le degré de cette extension ?