Première partie

Algèbre générale

1 Arithmétique dans $\mathbb{Z}$

1.1 Division dans $\mathbb{Z}$

1.1 Définition. Soient $a, b \in \mathbb{Z}$. On dit que a divise b et on écrit $a|b$ s'il existe $c \in \mathbb{Z}$ tel que $b = ac$.

On dit aussi que b est un multiple de a, que b est divisible par a, que a est un diviseur de b...

1.2 Propriétés élémentaires. a) Pour tout $a \in \mathbb{Z}$, on a : $1|a$, $a|a$ et $a|0$.

b) Pour tout $a, b \in \mathbb{Z}$, on a : ($a|b$ et $b|a$) $\iff$ $|a| = |b|$.

c) Pour tout $a, b, c \in \mathbb{Z}$, on a : ($a|b$ et $b|c$) $\Rightarrow$ $a|c$.

d) Pour tout $a, b, c \in \mathbb{Z}$, on a : ($a|b$ et $a|c$) $\Rightarrow$ $a|b + c$.

1.3 Exercice. a) Soient $a, b, c, d \in \mathbb{Z}$. Démontrer que si $a|b$ et $c|d$ alors $ac|bd$.

b) Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$. Démontrer que si $a|b$, alors $a^n|b^n$.

1.4 Théorème : Division euclidienne. *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}$ non nul. Alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tels que $a = bq + r$ et $0 \leqslant r < b$.*

1.5 Définition. Un nombre $p \in \mathbb{Z}$ est dit *premier* s'il a exactement 4 diviseurs : $1, p, -1$ et $-p$.

En particulier, 1 (et -1) n'est pas (ne sont) pas premier(s).

1.6 Proposition. *Soit $n \in \mathbb{Z}$ un nombre distinct de 1 et de -1. Alors n admet un diviseur premier.*

Le plus petit diviseur strictement supérieur à 1 de n est un nombre premier.

1.7 Théorème. *Il y a une infinité de nombres premiers.*

Il suffit en effet de remarquer que tout diviseur premier de $n! + 1$ est $\geqslant n + 1$.

1.2 Sous-groupes additifs de $\mathbb{Z}$

1.8 Notation. Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a, c'est à dire l'ensemble $\{ab;\ b \in \mathbb{Z}\}$ est noté $a\mathbb{Z}$.

1.9 Remarque. Pour $a, b \in \mathbb{Z}$ on a l'équivalence entre :

$$\text{(i) } a|b; \qquad \text{(ii) } b \in a\mathbb{Z} \qquad \text{et} \quad \text{(iii) } b\mathbb{Z} \subset a\mathbb{Z}.$$

D'après 1.2.a), on a $a\mathbb{Z} = b\mathbb{Z}$ si et seulement si $|a| = |b|$ (*i.e.* $b = \pm a$).

1.10 Proposition. *Pour tout $a \in \mathbb{Z}$, l'ensemble $a\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$. C'est le plus petit sous-groupe de $\mathbb{Z}$ contenant a.*

1.11 Théorème. *Tout sous-groupe de $\mathbb{Z}$ est de cette forme : si $G \subset \mathbb{Z}$ est un sous-groupe additif, il existe (un unique) $a \in \mathbb{N}$ tel que $G = a\mathbb{Z}$.*

1.3 PGCD, PPCM algorithme d'Euclide

1.12 Corollaire. *Soient $a, b \in \mathbb{Z}$.*

a) *Il existe un unique $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Le nombre m est un multiple commun de a et de b. Les multiples communs de a et b sont les multiples de m.*

b) *Il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Le nombre d est un diviseur commun de a et de b. Les diviseurs communs de a et b sont les diviseurs de d.*

1.13 Définition. Le nombre d de ce corollaire s'appelle le plus grand commun diviseur (PGCD) de a et b ; on le note $pgcd(a, b)$. Le nombre m de ce corollaire s'appelle le plus petit commun multiple (PPCM) de a et b ; on le note $ppcm(a, b)$.

1.14 Remarque. Soient $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n \in \mathbb{Z}$. On définit de même le plus grand commun diviseur d et le plus petit commun multiple m de $x_1, \ldots, x_n$:

- Le nombre $m \in \mathbb{N}$ est un multiple commun des x_i ; les multiples communs des x_i sont les multiples de m. Autrement dit
$$m\mathbb{Z} = x_1\mathbb{Z} \cap x_2\mathbb{Z} \cap \ldots \cap x_n\mathbb{Z} = \bigcap_{i=1}^{n} x_i\mathbb{Z}.$$
- Le nombre $d \in \mathbb{N}$ est un diviseur commun des x_i ; les diviseurs communs des x_i sont les diviseurs de d. On a
$$d\mathbb{Z} = x_1\mathbb{Z} + x_2\mathbb{Z} + \ldots + x_n\mathbb{Z} = \sum_{i=1}^{n} x_i\mathbb{Z}.$$

1.15 Lemme. *Soient $a, b \in \mathbb{Z}$. On suppose que $b \neq 0$. On note r le reste de la division euclidienne de a par $|b|$. On a $pgcd(a, b) = pgcd(b, r)$.*

1.16 Algorithme d'Euclide. Soient $a, b \in \mathbb{N}$. On suppose que $b \neq 0$.

- On pose $r_0 = a$, $r_1 = b$ et on note r_2 le reste de la division euclidienne de a par b.
- Soit $n \in \mathbb{N}$ non nul et supposons r_j construits pour $1 \leqslant j \leqslant n$. Si r_n n'est pas nul, alors on définit r_{n+1} comme le reste de la division euclidienne de r_{n-1} par r_n : $r_{n-1} = q_n r_n + r_{n+1}$. Si r_n est nul, on arrête la construction.

a) La construction s'arrête en un nombre fini d'étapes.

b) Le PGCD de a et b est le dernier reste non nul.

1.17 Remarques. a) On peut majorer le nombre N d'étapes qu'il faut pour trouver le PGCD. Sachant que la suite r_k est strictement décroissante, on trouve évidemment $N \leqslant b$. Mais on peut faire bien mieux !

Remarquons que $r_{N-1} = q_N r_N \geqslant 2r_N$ (puisque et $0 \leqslant r_N < r_{N-1}$), et pour $1 \leqslant k \leqslant N-1$, on a $r_{k-1} = q_k r_k + r_{k+1} \geqslant r_k + r_{k+1}$, de sorte que, par récurrence, $r_{N-k} \geqslant r_N F_{k+2}$, où F_k est le k-ième nombre de Fibonacci (donné par récurrence par les formules $F_0 = 0$, $F_1 = 1$ et $F_{k+1} = F_k + F_{k-1}$ pour $k \geqslant 1$ - on initialise la récurrence avec $k = 0$ et 1 sachant que $F_2 = 1$ et $F_3 = 2$). Rappelons que F_k croît géométriquement : $F_k = \dfrac{\phi^k - (-1)^k \phi^{-k}}{\sqrt{5}}$ où $\phi = \dfrac{1+\sqrt{5}}{2}$ est le nombre d'or. On a donc $b = r_1 \geqslant F_{N+1} > \dfrac{\phi^{N+1} - 1}{\sqrt{5}}$ une estimation pour N logarithmique en b : $N < \dfrac{\ln(1 + b\sqrt{5})}{\ln \phi} - 1$.

b) Pour écrire une relation de Bézout $d = r_N = au + bv$, on peut remonter les opérations : $r_N = r_{N-2} - r_{N-1}q_{N-1} = r_{N-2} - q_{N-1}(r_{N-3} - r_{N-2}q_{N-2}) = (1 + q_{N-1}q_{N-2})r_{N-2} - q_{N-1}r_{N-3}$, puis en écrivant $r_{N-2} = r_{N-4} - r_{N-3}q_{N-3}$ on exprime r_N en fonction de r_{N-3} et r_{N-4}, et on continue... Cela demande de garder en mémoire la suite des quotients q_k.

On peut faire un peu mieux, en écrivant à chaque étape de l'algorithme $r_k = u_k a + v_k b$. On aura $r_{k+1} = r_{k-1} - q_k r_k = (u_{k-1} - q_k u_k)a + (v_{k-1} - q_k v_k)b$. En même temps qu'on trouvera le PGCD, on aura une relation de Bézout !

1.18 Quelques explications sur la suite de Fibonacci. Soient $a, b \in \mathbb{C}$. On considère les suites u_n qui satisfont une propriété de récurrence $u_{n+2} = au_{n+1} + bu_n$. Elles forment un sous-espace vectoriel E de l'espace $\mathbb{C}^{\mathbb{N}}$ des suites complexes. Comme une telle suite est entièrement déterminée par u_0 et u_1, cet espace vectoriel est de dimension 2 (l'application linéaire $(u) \mapsto (u_0, u_1)$ est un isomorphisme de E sur $\mathbb{C}^2$). On cherche une base de E de la forme $u_n = x^n$ (avec $x \in \mathbb{C}$). La suite (x^n) est dans E si et seulement si $x^2 = ax + b$. Si les racines r_1 et r_2 du polynôme $X^2 - aX - b$ sont distinctes, on obtient deux suites indépendantes r_1^n et r_2^n, donc toutes les solutions s'écrivent $u_n = \alpha r_1^n + \beta r_2^n$ (avec $\alpha, \beta \in \mathbb{C}$). Si $r_1 = r_2 = r$, on vérifie que $u_n = nr^n$ est aussi solution ; les solutions s'écrivent donc (si $r \neq 0$) $u_n = (\alpha + n\beta)r^n$ (avec $\alpha, \beta \in \mathbb{C}$).

Dans le cas de la suite de Fibonacci, $a = b = 1$ et les racines du polynôme $X^2 - X - 1$ sont ϕ et $-\phi^{-1}$ où ϕ est le nombre d'or. Donc $F_k = \alpha\phi^k + \beta(-1)^k\phi^{-k}$. On détermine α et β à l'aide des premiers termes.

1.4 Nombres premiers entre eux

1.19 Définition. On dit que a et b sont premiers entre eux si leur plus grand commun diviseur est 1.

Si $a, b \in \mathbb{Z}$, on peut écrire $a = a'd$ et $b = b'd$ où a' et b' sont premiers entre eux et d est le plus grand commun diviseur de a et b.

Soient $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n$ des nombres entiers. On dit que les x_i sont *premiers entre eux dans leur ensemble* si le plus grand commun diviseur de $x_1, \ldots, x_n$ est 1 ; on dit que les x_i sont *premiers entre eux deux à deux*, si pour tout couple d'entiers i, j avec $1 \leqslant i < j \leqslant n$, les nombres x_i et x_j sont premiers entre eux.

1.20 Théorème de Bézout. *Soient $a, b \in \mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

1.21 Théorème de Gauss. *Soient $a, b, c \in \mathbb{Z}$. Si a divise bc et est premier à b, alors a divise c.*

1.22 Corollaire. *Soient $a, b \in \mathbb{Z}$ et p un nombre premier. Si p divise ab alors p divise a ou b.*

1.23 Lemme. *Soient $p_1, \ldots, p_k \in \mathbb{N}$ des nombres premiers distincts deux à deux et $\beta_1, \ldots \beta_k \in \mathbb{N}^*$. Posons $n = \prod_{j=1}^{k} p_j^{\beta_j}$. L'ensemble des diviseurs premiers de n est $\{p_1, \ldots, p_k\}$ et pour tout j, $p_j^{\beta_j}$ divise n et $p_j^{\beta_j+1}$ ne divise pas n.*

1.24 Théorème. *Tout nombre entier admet une décomposition en produit de nombres premiers unique à permutation des termes près.*

On démontre l'existence à l'aide d'une « récurrence forte » sur n. L'unicité résulte du lemme.

1.5 Congruences, l'anneau $\mathbb{Z}/n\mathbb{Z}$

1.25 Définition. Soient $a, b, n \in \mathbb{Z}$. On dit que a est congru à b modulo n et on écrit $a \equiv b\ [n]$ si n divise $b - a$.

1.26 Proposition. *Soit $n \in \mathbb{Z}$. La relation de congruence modulo n est une relation d'équivalence.*

1.27 Lemme. *Soit p un nombre premier. Pour tout entier k tel que $1 \leqslant k \leqslant p - 1$ le coefficient binomial $\binom{p}{k}$ est divisible par p.*

On a $(p - k)\binom{p}{k} = p\binom{p-1}{k}$.

1.28 Petit théorème de Fermat. *Soit p un nombre premier. Pour tout entier k on a $k^p \equiv k\ [p]$. Si k n'est pas divisible par p, alors $k^{p-1} \equiv 1\ [p]$.*

1.29 Théorème de Wilson. *Pour tout nombre premier p, on a $(p-1)! \equiv -1\ [p]$.*

1.30 Définition. Soit $n \in \mathbb{Z}$. On note $\mathbb{Z}/n\mathbb{Z}$ le *quotient d'équivalence* pour la relation de congruence modulo n.

Pour $n \in \mathbb{N}^*$, on a $a \equiv b\ [n]$ si et seulement si a et b ont même reste dans la division euclidienne par n ; on en déduit que $\mathbb{Z}/n\mathbb{Z}$ a n éléments (autant que des restes possibles).

1.31 Proposition. *Soit $n \in \mathbb{Z}$. L'addition et la multiplication de $\mathbb{Z}$ passent au quotient et définissent une structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$.*

En d'autres termes, si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors $a + a' \equiv b + b'\ [n]$ et $aa' \equiv bb'\ [n]$.

1.32 Proposition. *Soit $n \in \mathbb{N}^*$. Les propriétés suivantes sont équivalentes.*

(i) *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.*

(ii) *Le nombre n est premier.*

1.33 Proposition. *Soient $n \in \mathbb{Z}$. La classe d'un élément $a \in \mathbb{Z}$ est un élément inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a et n sont premiers entre eux.*

Pour $n \in \mathbb{N}^*$, le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est donc égal au nombre d'entiers $a \in [0, n-1]$ premiers à n. Ce nombre se note $\varphi(n)$. L'application φ ainsi construite s'appelle *l'indicatrice d'Euler.*

Soit p un nombre premier. Tout nombre non divisible par p est premier à p ; on a donc $\varphi(p) = p - 1$. Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$; alors a est premier avec p^n si et seulement si a est premier avec p, *i.e.* s'il n'est pas divisible par p. Les nombres $a \in [0, p^n - 1]$ divisibles par p sont les kp avec $0 \leqslant k < p^{n-1}$. Ils sont au nombre de p^{n-1}. Donc $\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$.

1.34 Remarque. Soient $m, n \in \mathbb{Z}$ deux nombres entiers. On suppose que $m|n$. Pour $a, b \in \mathbb{Z}$, si $a \equiv b\ [n]$, alors *a fortiori* $a \equiv b\ [m]$. On définit une application naturelle $\pi_{m,n} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ qui à la classe de a modulo n associe sa classe modulo m. C'est clairement un homomorphisme d'anneaux.

1.35 Théorème « Chinois ». *Soient m, n deux nombres premiers entre eux. L'application*

$$\begin{array}{rcl} \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ a & \mapsto & (\pi_{m,mn}(a), \pi_{n,mn}(a)) \end{array}$$

est bijective ; c'est un isomorphisme d'anneaux.

En particulier, si m, n sont premiers entre eux on a $\varphi(mn) = \varphi(m)\varphi(n)$.

1.36 Proposition. *Soit $n \in \mathbb{N}$, $n \geqslant 2$. Notons $p_1, \ldots, p_k$ les nombres premiers (positifs et) distincts qui divisent n. On a $\varphi(n) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right)$.*

1.37 Résolution générale de deux équations type. On va donner une méthode générale pour deux équations : un système de congruences et une équation diophantienne. Chacune de ces équations demande d'abord un calcul de plus grand commun diviseur et une « relation de Bézout ».

a) Résoudre l'équation de congruences : $x \equiv a\ [m]$ et $x \equiv b\ [n]$.

- **On suppose que m et n sont premiers entre eux.** Écrivons une relation de Bézout $mu + nv = 1$. Posons $x_0 = mub + nva$. Alors $x_0 - a = mub + (nv - 1)a = mub - mua$ est un multiple de m et $x_0 - b = (mu - 1)b + nva = nv(a - b)$ est un multiple de n. Notre équation devient
$$x \equiv x_0 \ [m] \ \text{ et } \ x \equiv x_0 \ [n],$$
qui est équivalente à $x \equiv x_0 \ [mn]$. L'ensemble de ses solutions est $\{x_0 + mnk;\ k \in \mathbb{Z}\}$.
- **Cas général.** Notons d le plus grand commun diviseur de m et n. Si x est solution de notre équation, comme d divise $x - a$ et $x - b$, alors $d|b - a$. Si a n'est pas congru à b modulo d, alors notre équation n'a pas de solution. Sinon, écrivons $b - a = \ell d$ et écrivons une relation de Bézout $mu + nv = d$. Posons $x_0 = a + \ell mu = a + \ell(d - nv) = b - n\ell v$. C'est une solution de notre équation. Notre équation devient
$$x \equiv x_0 \ [m] \ \text{ et } \ x \equiv x_0 \ [n],$$
qui est équivalente à $x \equiv x_0 \ [M]$ où $M = \dfrac{|mn|}{d}$ est le plus petit commun multiple de m et n. L'ensemble de ses solutions est $\{x_0 + Mk;\ k \in \mathbb{Z}\}$.

b) Résoudre l'équation diophantienne : $ax + by = c$.

On va supposer que a n'est pas nul. Notons d le plus grand commun diviseur de a et b. Écrivons $a = da'$ et $b = db'$ où a' et b' sont deux nombres premiers entre eux, et donnons une relation de Bézout $a'u + b'v = 1$. L'équation devient $d(a'x + b'y) = c$. Si c n'est pas multiple de d, il n'y a pas de solution. Sinon, écrivons $c = dc'$. L'équation devient $a'x + b'y = c' = c'(a'u + b'v)$, soit $a'(x - c'u) = b'(c'v - y)$. Si (x, y) est solution, alors a' divise $b'(c'v - y)$ et est premier avec b', donc il divise $c'v - y$. Écrivons $c'v - y = ka'$. On doit alors avoir : $a'(x - c'u) = a'b'k$, donc $x - c'u = b'k$. L'ensemble des solutions est contenu dans $\{(c'u + b'k, c'v - ka');\ k \in \mathbb{Z}\}$. On vérifie immédiatement que, inversement, pour tout $k \in \mathbb{Z}$, on a $a(c'u + b'k) + b(c'v - ka') = c$.

Remarquons que dans ces deux équations on a trouvé une *solution particulière* et résolu l'*équation homogène associée.* ***Pourquoi ?***

1.6 Exercices

1.6.1 Divisibilité et congruences

1.1 Exercice. 1. Soient $a, b, \delta \in \mathbb{Z}$. On suppose que δ est un diviseur commun de a et b et qu'il existe $u, v \in \mathbb{Z}$ tels que $\delta = au + bv$. Démontrer que le plus grand commun diviseur de a et b est $|\delta|$.

2. Soient $a, b, c \in \mathbb{N}$. Notons d et m le plus grand commun diviseur et le plus petit commun multiple de a et b. Démontrer que le plus grand commun diviseur de ac et bc est dc et que le plus petit commun multiple de ac et bc est mc.

3. Soient $a, b \in \mathbb{N}$. Démontrer que $dm = ab$ où l'on a noté d et m le plus grand commun diviseur et le plus petit commun multiple de a et b respectivement.

1.2 Exercice. 1. Soient $a, b, c \in \mathbb{Z}$. On suppose que a et b sont premiers entre eux, que $a|c$ et $b|c$. Démontrer que $ab|c$.

2. Soient $a, b, c \in \mathbb{Z}$. On suppose que a est premier à b et à c. Démontrer que a est premier à bc.

3. Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.

   a) On suppose que a et b sont premiers entre eux. Démontrer que a et b^n sont premiers entre eux. En déduire que a^n et b^n sont premiers entre eux.

b) Démontrer que le plus grand commun diviseur de a^n et b^n est d^n où d est le plus grand commun diviseur de a et b.

4. Soient $a, b, c \in \mathbb{Z}$ tels que $a|bc$. Démontrer qu'il existe $d, e \in \mathbb{Z}$ tels que $a = de$ et $d|b$ et $e|c$.

1.3 Exercice. *Propriétés arithmétiques à la base de RSA.*
Soient p, q deux nombres premiers distincts, on note N un multiple commun de $p-1$ et $q-1$. Soit $e \in \{1, \dots, N\}$ un entier premier avec N.

1. Démontrer qu'il existe un entier $d \in \{1, \dots, N\}$ tel que $ed \equiv 1[N]$.
2. En utilisant le théorème de Fermat, démontrer que pour tout entier n, $n^{ed} \equiv n[p]$ et $n^{ed} \equiv n[q]$.
3. En déduire que l'application $C : \{0, \dots, pq-1\} \to \{0, \dots, pq-1\}$ qui à a associe le reste dans la division de a^e par pq est une bijection de $\{0, \dots, pq-1\}$ sur lui-même.

Sur le système de cryptage à clé appelé RSA (Ron Rivest, Adi Shamir, and Leonard Adleman, 1977) :
Je veux pouvoir recevoir des messages chiffrés de telle sorte que je serai seul à pouvoir les déchiffrer. Pour cela

- Je choisis deux nombres premiers p et q grands (environ 100 chiffres chacun), je calcule leur produit n que je rends public, ainsi que la clé de chiffrement e - un nombre premier à $(p-1)(q-1)$.
- Je calcule aussi un nombre d qui est inverse de e modulo $p-1$ et modulo $q-1$; ce nombre je suis le seul à le connaître, ainsi que les nombres p et q qui m'ont permis de le trouver.

Supposons maintenant que vous vouliez m'envoyer de façon secrète un message qui est un nombre a ayant à peu près 200 chiffres, c'est à dire grand mais inférieur à $n = pq$ (ou une suite a_i de tels nombres si votre message est long). Vous m'envoyez juste le nombre b qui est le reste de a^e dans la division par n (ou la suite des $b_i \equiv a_i^e$ modulo n). Pour retrouver le message d'origine, je n'aurai qu'à calculer le reste de b^d (ou b_i^d) modulo n. Ce système repose sur les faits suivants :

1. Il est « relativement rapide » de vérifier qu'un nombre est premier, et il y a beaucoup de nombres premiers : si je donne un nombre m de 100 chiffres au hasard, d'après le théorème des nombres premiers, le plus petit nombre premier $p > m$ a beaucoup de chances d'être tel que $p - m$ soit du même ordre que $\ln m \sim 100 \ln 10$. Donc je peux trouver des nombres premiers p et q « rapidement ».
2. Le nombre e est en général choisi petit ($e = 3, 5$ ou 7 sont des choix courants). Le nombre d est par contre grand (200 chiffres...). Élever à la puissance d modulo n un nombre x est cependant une opération « rapide » : cela implique d'élever des éléments de $\mathbb{Z}/n\mathbb{Z}$ au carré $\log_2 d$ ($\simeq 700$) fois et de multiplier des nombres par x au plus $\log_2 d$ fois.
3. Par contre, on ne sait pas trouver le nombre d connaissant n et e sans trouver p et q, et on ne sait pas trouver la décomposition $n = pq$ rapidement.

1.4 Exercice. *Équations Diophantiennes*
Soient $a, b \in \mathbb{N}^*$ des nombres entiers.

1. Soit $c \in \mathbb{Z}$. Quelles sont toutes les solutions de l'équation $ax + by = c$ avec $(x, y) \in \mathbb{Z}$?
   On suppose dorénavant que a et b sont premiers entre eux.
2. Quel est le plus petit entier qui s'écrit de deux façons sous la forme $ax + by$ avec $x, y \in \mathbb{N}$?
3. On suppose que a et b sont tous deux distincts de 1. Notons A l'ensemble des entiers naturels qui ne peuvent s'écrire sous la forme $ax + by$ avec $x, y \in \mathbb{N}$.
   a) Quel est le plus grand élément de A ?
   b) Démontrer que $A = \{|ua - vb|; (u, v) \in \mathbb{N}^2;\ 1 \leqslant u \leqslant b-1;\ 1 \leqslant v \leqslant a-1\}$.
   c) Combien d'éléments a A ?
4. Rappelons qu'au rugby un essai transformé vaut 7 points, un essai non transformé en vaut 5, un drop ou une pénalité 3.
   a) Quel est le plus grand score pour lequel on est sûr qu'il n'a pas été obtenu que par des essais - transformés ou non ?
   b) Quels sont les scores impossibles ?

1.5 Exercice. *Théorème Chinois.* Soient $a, b \in \mathbb{N}^*$. Posons $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$.

1. Ecrire la décomposition de d et m en facteurs premiers en fonction de celle de a et de b. Comparer cette méthode de calcul de pgcd avec l'algorithme d'Euclide.

2. Démontrer qu'il existe a_1, a_2, b_1, b_2 tels que
   - $a = a_1 a_2$, $b = b_1 b_2$;
   - $a_1 | b_1$, $b_2 | a_2$;
   - a_2 et b_1 sont premiers entre eux.
3. Démontrer que $a_1 b_2 = d$ et $a_2 b_1 = m$.
4. En déduire que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est isomorphe à $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

1.6 Exercice. *Jouons avec la suite de Fibonacci.*

1. Écrire les premiers nombres de Fibonacci. Lesquels sont pairs ? multiples de 3 ? multiples de 5 ?
2. a) Démontrer que, si m divise n alors F_m divise F_n.
   b) Démontrer que pour tout n, l'ensemble des $k \in \mathbb{N}$ tel que n divise F_k est de la forme $a\mathbb{N}$ où $a \in \mathbb{N}^*$. *(Utiliser l'exercice 1.7.3).*
3. Soit $p \geqslant 7$ un nombre premier. Notons J la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ à coefficients dans $\mathbb{F}_p$.
   a) On suppose que 5 est un carré modulo p. Démontrer que la matrice J est diagonalisable (dans $\mathbb{F}_p$). En déduire que F_{p-1} est multiple de p.
   b) (**) On suppose que 5 n'est pas un carré modulo p. Notons $K = \{aI_2 + bJ;\ a, b \in \mathbb{F}_p\}$. Démontrer que
      (i) K est un sous-anneau commutatif de $M_2(\mathbb{F}_p)$;
      (ii) l'anneau K est un corps ;
      (iii) l'application $x \mapsto x^p$ est un automorphisme de K ;
      (iv) pour $x \in K$ on a $x^p = x \iff x \in \{aI_2;\ a \in \mathbb{F}_p\}$;
      (v) posant $J' = J^p$, on a $J' \neq J$ et $J'^2 = J' + 1$;
      (vi) on a $J^p = -J^{-1}$;
      (vii) p divise F_{p+1} ; de plus $F_p \equiv F_{p+2} \equiv -1 \ \ [p]$.

1.7 Exercice. *Algorithme d'Euclide et matrices* 2×2.
Soient $a, b \in \mathbb{N}$, avec $0 < a < b$. On effectue l'algorithme d'Euclide : on pose $r_0 = b$, $r_1 = a$, et, supposant r_{j-1} et r_j construits, si $r_j \neq 0$ on note $r_{j-1} = r_j q_j + r_{j+1}$ la division euclidienne de r_{j-1} par r_j. On note n l'entier pour lequel l'algorithme s'arrête de sorte que $r_{n+1} = 0$ et r_n est le $PGCD$ de a, b.

1. Démontrer que $q_n \geqslant 2$.
2. a) Démontrer que, pour tout $k \in \{1, \ldots, n\}$, on a
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} r_1 \\ r_0 \end{pmatrix}.$$
   b) Démontrer qu'il existe des suites $(a_k)_{1 \leqslant k \leqslant n+1}$ et $(b_k)_{1 \leqslant k \leqslant n+1}$ de nombres entiers telles que pour $k \in \{1, \ldots, n\}$ on ait
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} = \begin{pmatrix} a_k & a_{k+1} \\ b_k & b_{k+1} \end{pmatrix}.$$
   c) Démontrer que $a_1 = 0,\ a_2 = 1,\ b_1 = 1,\ b_2 = q_1$ et, pour $2 \leqslant j \leqslant n$, on a $a_{j+1} = a_j q_j + a_{j-1}$ et $b_{j+1} = b_j q_j + b_{j-1}$. En déduire que les suites a_k et b_k sont croissantes et que l'on a $a_{n+1} \geqslant 2a_n$ et $b_{n+1} \geqslant 2b_n$. Dans quel cas a-t-on égalité dans l'une de ces inégalités ?
   d) Démontrer que l'on a $a_k b_{k+1} - a_{k+1} b_k = (-1)^k$ pour $1 \leqslant k \leqslant n$.
   e) Démontrer que l'on a une relation de Bézout $r_n = (-1)^n a_n b + (-1)^{n+1} b_n a$.

3. a) Démontrer que $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^k = \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix}$ où F_k est le k-ème nombre de Fibonacci.

   b) Démontrer que $b_k \geqslant F_k$ et $a_k \geqslant F_{k-1}$.

4. Expliquer en quoi cette méthode permet de trouver « rapidement » le $PGCD$ de a et b et une identité de Bézout $d = au + bv$.

5. On suppose que a et b sont premiers entre eux. Démontrer qu'il existe $n \in \mathbb{N}^*$ une suite $q_1, \ldots, q_n$ de nombres entiers strictement positifs et $u, v \in \mathbb{N}$ tels que $q_n \geqslant 2$ et

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$

6. On suppose qu'il existe une suite $q_1, \ldots, q_n$ de nombres entiers strictement positifs et $u, v \in \mathbb{N}$ tels que $q_n \geqslant 2$ et

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$

   Démontrer que a et b sont premiers entre eux et que la suite des quotients successifs de la division euclidienne de b par a est $q_1, q_2, \ldots, q_n$.

1.8 Exercice. *Algorithme de Cornacchia* (**)

1. Soient $a, b \in \mathbb{N}$ tels que $a < b$ et $a^2 + b^2$ soit un nombre premier p.

   a) Démontrer que a et b sont premiers entre eux.

   b) Démontrer qu'il existe $n \in \mathbb{N}^*$, des nombres entiers strictement positifs $q_1, \ldots, q_n$ avec $q_n \geqslant 2$ et des nombres $u, v \in \mathbb{N}$ tels que

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$

   c) Démontrer que $2u \leqslant a$ et $2v \leqslant b$.

   d) Démontrer que $\begin{pmatrix} u & v \\ a & b \end{pmatrix} \begin{pmatrix} u & a \\ v & b \end{pmatrix}$ s'écrit $\begin{pmatrix} x & \ell \\ \ell & p \end{pmatrix}$ où ℓ est l'unique entier tel que $\ell^2 \equiv -1\ [p]$ et $0 \leqslant \ell < p/2$.

2. Soit $p > 2$ un nombre premier tel que -1 est un carré modulo p (*i.e.* congru à 1 modulo 4 - voir exercice 1.11). Supposons qu'on ait trouvé ℓ tel que $0 \leqslant \ell < p/2$ et $\ell^2 = xp - 1$ avec $x \in \mathbb{N}$. Expliquer comment, grâce à l'algorithme d'Euclide, on trouve alors a et b tels que $a^2 + b^2 = p$.

1.6.2 Nombres premiers

1.9 Exercice. *Nombres de Fermat, nombres de Mersenne.*
Pour tout entier $n \geqslant 1$, on note $f_n = 2^n + 1$ et $M_n = 2^n - 1$.

1. Soit $n \geqslant 1$ un entier.
   Démontrer que si M_n est premier, alors n aussi, et que si f_n est premier alors n est une puissance de 2.

   Indication : Remarquer que, pour $a \in \mathbb{Z}$ et $k, m \in \mathbb{N}$, $a^k - 1$ divise $a^{km} - 1$ et, si m est impair $a^k + 1$ divise $a^{mk} + 1$.

   On pose $F_k = f_{2^k}$.

2. Soient k, ℓ deux nombres entiers avec $k < \ell$. Démontrer que $2^{2^\ell} \equiv 1[F_k]$. En déduire que F_k et F_ℓ sont premiers entre eux.

3. Soit $p > 2$ un nombre premier et soit q un diviseur premier de M_p. Quel est l'ordre de 2 dans le groupe $(\mathbb{F}_q^*, \cdot)$? En déduire que q est de la forme $2kp + 1$.

4. Démontrer que M_{13} est premier.
5. De même soit $\ell \in \mathbb{N}$ et q un diviseur premier de F_ℓ.
   a) Quel est l'ordre de 2 dans le groupe $(\mathbb{F}_q^*, \cdot)$?
   b) En déduire que q est de la forme $2^{\ell+1}k + 1$.
   c) On suppose que $\ell \geqslant 2$. Notons ω le classe de $2^{2^{\ell-2}}$ dans $\mathbb{F}_q$. Remarquant que $\omega^4 = -1$, démontrer que $2 = (\omega + \omega^{-1})^2$ est un carré modulo q. En déduire que $2^{\ell+2}$ divise $q - 1$.
   d) Démontrer que le plus petit diviseur de F_5 distinct de 1 est $\geqslant 641$.
   e) En remarquant que $641 = 5^4 + 2^4$, démontrer que $F_5 \equiv 1 - 5^4 2^{28}$ [641].
   f) Démontrer que $641 | F_5$.

1.10 Exercice. *Cas du théorème de Dirichlet.* (*cf.* Combes. *Algèbre et géométrie* 12.6).

Théorème de Dirichlet. *Soient $a, b \in \mathbb{N}^*$ premiers entre eux. Il y a une infinité de nombres premiers congrus à a modulo b.*

Nous étudions ici le cas où $a = 1$.

Le cas $b = 4$: Soit $a \in \mathbb{N}$ et p un diviseur premier de $a^2 + 1$ distinct de 2.

1. Démontrer que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^4 = 1$.
3. Démontrer que $x^2 \neq 1$.
4. En déduire que p est congru à 1 modulo 4.
5. En prenant a sous-la forme $n!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.
6. Démontrer que, pour $n \geqslant 4$, $n! - 1$ a au moins un diviseur premier congru à 3 modulo 4. En déduire qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Le cas $b = 6$ Soit $a \in \mathbb{N}$ et p un diviseur premier de $a^2 + a + 1$ distinct de 3.

1. Démontrer que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^3 = 1$.
3. Démontrer que $x \neq 1$.
4. En déduire que p est congru à 1 modulo 3.
5. En prenant a sous-la forme $n!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 6.
6. Démontrer que, pour $n \geqslant 3$, $n! - 1$ a au moins un diviseur premier congru à 5 modulo 6. En déduire qu'il existe une infinité de nombres premiers congrus à 5 modulo 6.

Le cas $b = 12$: Soit $a \in \mathbb{N}$ et p un diviseur premier de $a^4 - a^2 + 1$.

1. Démontrer que $p \neq 2$ et $p \neq 3$. Démontrer que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^{12} = 1$.
3. Démontrer que $x^4 \neq 1$ et $x^6 \neq 1$.
4. En déduire que p est congru à 1 modulo 12.
5. En prenant a sous-la forme $n!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 12.

Le cas général [**] Pour $n \in \mathbb{N}^*$, on note Φ_n le n-ième polynôme cyclotomique : $\Phi_n = \prod_{0 \leqslant k < n;\ k \wedge n = 1} X - e^{\frac{2ik\pi}{n}}$. Rappelons que $\Phi_n \in \mathbb{Z}[X]$ et que l'on a l'égalité $X^n - 1 = \prod_{d|n} \Phi_d$.

Soient $n \in \mathbb{N}$, $n \geqslant 2$, $a \in \mathbb{N}$ un multiple de n et p un diviseur premier de $\Phi_n(a)$.

1. Démontrer que $\Phi_n(0) = 1$. En déduire que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^n = 1$.
3. Démontrer que le polynôme $X^n - 1$ n'a pas de facteur carré dans $\mathbb{F}_p[X]$.

   Indication : Utiliser la dérivée
4. Soit $d \in \mathbb{N}$ un diviseur de n distinct de n. Démontrer que les polynômes $X^d - 1$ et Φ_n sont premiers entre eux dans $\mathbb{F}_p[X]$. En déduire que $x^d \neq 1$.
5. En déduire que p est congru à 1 modulo n.
6. En prenant a sous-la forme $N!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo n.

1.11 Exercice. *Carrés dans $\mathbb{F}_p$.* (*cf.* COMBES p. 267)
Soit p un nombre premier distinct de 2. Notons $C \subset \mathbb{F}_p^*$ l'ensemble des carrés, *i.e.* l'ensemble des $x \in \mathbb{F}_p^*$ tels qu'il existe $y \in \mathbb{F}_p^*$ avec $x = y^2$.

1. Le cas de -1.
   a) Démontrer que pour tout $x \in C$ il existe un et un seul $c \in \left\{1, \ldots, \dfrac{p-1}{2}\right\}$ tel que x soit la classe de c^2. Combien y a-t-il de carrés dans F_p^* ?
   b) Démontrer que tout $x \in C$, on a $x^{\frac{p-1}{2}} = 1$.
   c) En déduire que, pour $x \in \mathbb{F}_p^*$, on a $x \in C \iff x^{\frac{p-1}{2}} = 1$.
   d) Démontrer que -1 est un carré modulo p si et seulement si p est congru à 1 modulo 4.
2. Le cas de 3.
   a) Soit $P = X^2 + aX + b$ un polynôme à coefficients dans $\mathbb{F}_p$. Démontrer que P a une racine dans $\mathbb{F}_p$ si et seulement si $a^2 - 4b$ est un carré (*i.e.* $a^2 - 4b \in \{0\} \cup C$).
   b) On suppose que $p \notin \{2, 3\}$. Démontrer l'équivalence entre
      (i) $-3 \in C$.
      (ii) Il existe $x \in \mathbb{F}_p^*$, $x^2 + x + 1 = 0$.
      (iii) Il existe x d'ordre 3 dans le groupe $\mathbb{F}_p^*$.
      (iv) $p \equiv 1$ [3] (ce qui signifie encore $p \equiv 1$ [6]).
3. Le polynôme $X^4 + 1$.
   a) Démontrer que si $a, b \in \mathbb{F}_p^* \setminus C$, alors $ab \in C$.
   b) En déduire qu'un au moins des éléments $-1, 2, -2$ est un carré dans $\mathbb{F}_p$.
   c) En écrivant $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - 1)^2 + 2X^2$ en déduire que pour tout p le polynôme $X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$.
   d) Quelle est la décomposition dans $\mathbb{R}[X]$ du polynôme $X^4 + 1$ en polynômes irréductibles ?
   e) En déduire que $X^4 + 1$ est irréductible sur $\mathbb{Q}$ (et sur $\mathbb{Z}$).

1.12 Exercice. *Réciprocité quadratique pour 2, pour 5.*
Soit p un nombre premier.

1. Soit L un corps commutatif de caractéristique p, autrement dit une extension de $\mathbb{F}_p$.
   a) Démontrer que $x \mapsto x^p$ est un endomorphisme de corps de L.
   b) Quelles sont les racines du polynôme $X^p - X$ dans L ?
2. On suppose que p est distinct de 2. Soit L une extension de $\mathbb{F}_p$ et $\omega \in L$ tel que $\omega^4 = -1$. Une telle extension existe d'après le corollaire 3.18. Posons $x = \omega + \omega^{-1}$.
   a) Démontrer que $\omega^2 + \omega^{-2} = 0$ et $x^2 = 2$.
   b) Démontrer que les assertions suivantes sont équivalentes :

(i) Il existe $y \in \mathbb{F}_p$ tel que $y^2 = 2$.
(ii) $x \in \mathbb{F}_p$;
(iii) $x^p = x$;
(iv) $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$;
(v) $p \equiv \pm 1$ [8] ;

3. On suppose que p est distinct de 2 et de 5. Soit L une extension de $\mathbb{F}_p$ et $\omega \in L$ tel que $\omega^5 = 1$ et $\omega \neq 1$ (*i.e.* une racine du polynôme $1 + X + X^2 + X^3 + X^4$ - une telle extension L existe d'après le corollaire 3.18). Posons $x = \omega + \omega^{-1}$.
   a) Démontrer que $\omega^2 + \omega^{-2} = -1 - x$ et $x^2 + x - 1 = 0$.
   b) Démontrer que les assertions suivantes sont équivalentes :
      (i) Il existe $y \in \mathbb{F}_p$ tel que $y^2 = 5$.
      (ii) $x \in \mathbb{F}_p$;
      (iii) $x^p = x$;
      (iv) $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$;
      (v) $p \equiv \pm 1$ [5] ;
      (vi) La classe de p est un carré modulo 5.

1.13 Exercice. *Racine carrée de -1 dans $\mathbb{F}_p$.*

Soit p un (grand !) nombre premier. Soit $x \in \mathbb{F}_p^*$.

1. Démontrer que x est un carré dans $\mathbb{F}_p$ si et seulement si $x^{(p-1)/2} = 1$. *(Voir exercice 1.11).*
   On suppose que x est un carré et on veut trouver une racine carrée de x.
2. On suppose que $p \equiv 3$ [4]. Démontrer que, si x est un carré, alors $x^{\frac{p+1}{4}}$ est une racine carrée de x.
3. On suppose que $p \equiv 1$ [4] et on cherche une racine carrée de -1. On écrit $p - 1 = 2^\ell u$ avec u entier impair.
   a) Soit $a \in \mathbb{F}_p^*$; posons $b = a^u$. Démontrer que b est d'ordre 2^k avec $0 \leqslant k \leqslant \ell$.
   b) En choisissant a au hasard, quelle est la probabilité que $b = \pm 1$?
   c) Expliquer comment trouver une racine carrée de -1 si $b \neq \pm 1$.

1.14 Exercice. 1. *Les nombres premiers sont espacés.* Démontrer que pour tout $n \in \mathbb{N}$, il existe une suite de n nombres consécutifs non premiers (*i.e.* il existe $a \in \mathbb{N}$ tel que les nombres entiers k avec $a \leqslant k \leqslant a + n - 1$ ne soient pas premiers).

2. *Il y a beaucoup de nombres premiers.* On désigne par $(p_n)_{n \geqslant 1}$ la suite ordonnée des nombres premiers. On veut démontrer que la série $\displaystyle\sum_{n=1}^{+\infty} 1/p_n$ diverge.

   On suit Combes (p. 269).
   Soit $k \in \mathbb{N}$. Notons $p_1, \ldots, p_k$ les k plus petits nombres premiers et $A_k \subset \mathbb{N}^*$ l'ensemble des nombres entiers dont tous les diviseurs premiers sont $\leqslant p_k$.
   a) Démontrer que tout $a \in A_k$ s'écrit sous la forme $a = b^2 p_1^{\varepsilon_1} \ldots p_k^{\varepsilon_k}$ avec $b \in \mathbb{N}$ et $\varepsilon_j \in \{0, 1\}$. En déduire que, pour tout $x \in \mathbb{N}^*$, le nombre d'éléments de A_k inférieurs à x est $\leqslant \sqrt{x} 2^k$.
   b) Démontrer que, pour $x \in \mathbb{N}^*$, la proportion d'éléments $\mathbb{N} \setminus A_k$ dans $[1, x]$ est plus petite que $\displaystyle\sum_{p \in \mathcal{P},\ p_k < p \leqslant x} 1/p$.
   c) Démontrer que pour $x = 4^{k+1}$ on a $\displaystyle\sum_{p \in \mathcal{P},\ p_k < p \leqslant x} 1/p \geqslant 1/2$. En déduire que la série $\displaystyle\sum_{n=1}^{+\infty} 1/p_n$ diverge.

3. Démontrer que pour tout entier $k \geqslant 1$, $\displaystyle\prod_{i=1}^{k} \frac{p_i}{p_i - 1} \geqslant \sum_{i=1}^{k} \frac{1}{i}$.

4. Démontrer qu'il existe une infinité de nombres premiers comportant au moins un 9 dans leur développement décimal.

D'après le théorème des nombres premiers, $\pi(x)$ est équivalent à $\dfrac{x}{\ln x}$. Les inégalités de Tchebychef, ci-dessous s'approchent de cet équivalent.

1.15 Exercice. *Inégalités de Tchebychef*

1. Pour $N \in \mathbb{Z}^*$ et un nombre premier p, on appelle *valuation* p-adique de N et on note $v_p(N)$ le plus grand entier k tel que $p^k | N$ - de sorte que l'on a $|N| = \displaystyle\prod_p p^{v_p(N)}$.

   Soient $n \in \mathbb{N}$, $n \geqslant 3$ et p un nombre premier.

   a) Démontrer que l'on a $v_p(n!) = \displaystyle\sum_{k=1}^{+\infty} E\big(np^{-k}\big)$ (où E désigne la partie entière).

   b) En déduire que $v_p\binom{2n}{n}$ est le nombre de $k \in \mathbb{N}$ tel que $E\big(2np^{-k}\big)$ soit impair.

   c) Démontrer que
   - $v_p\binom{2n}{n} \leqslant \dfrac{\ln 2n}{\ln p}$.
   - Si $n < p \leqslant 2n$ alors $v_p\binom{2n}{n} = 1$.
   - Si $p \leqslant n < \dfrac{3p}{2}$ alors $v_p\binom{2n}{n} = 0$.

   d) Démontrer que l'on a :

   (i) $\ln\binom{2n}{n} \geqslant \displaystyle\sum_{n \leqslant p \leqslant 2n;\ p \text{ premier}} \ln p$.

   (ii) $\ln\binom{2n}{n} \leqslant (\ln 2n)\Big(\pi(2n/3) + \pi(2n) - \pi(n)\Big) \leqslant (\ln 2n)\pi(2n)$.

2. Soit $n \in \mathbb{N}^*$. Démontrer que $\displaystyle\sum_{k=0}^{n-1} \binom{2n-1}{k} = 2^{2n-2}$. En déduire que $\dfrac{2^{2n-2}}{n} \leqslant \binom{2n-1}{n-1} \leqslant 2^{2n-2}$, puis que $\dfrac{2^{2n-1}}{n} \leqslant \binom{2n}{n} \leqslant 2^{2n-1}$.

3. Démontrer que, pour tout $n \in \mathbb{N}$, $n > 2$, on a

   a) $\displaystyle\sum_{n \leqslant p \leqslant 2n;\ p \text{ premier}} \ln p \leqslant (2n-1)\ln 2$ et en déduire que $\displaystyle\sum_{p \leqslant n;\ p \text{ premier}} \ln p \leqslant n \ln 4$

   b) $\pi(n) \geqslant \dfrac{n(\ln 2)}{\ln n} - 1$.

2 Anneaux

2.1 Généralités

2.1 Définition. Un anneau est un ensemble A muni de deux lois : la première s'appelle en général l'addition et est notée $+$; la deuxième s'appelle en général la multiplication et est notée $(x, y) \mapsto xy$. On suppose que :

- Muni de l'addition A est un groupe abélien ; son élément neutre est noté en général 0 ou 0_A en cas d'ambiguïté ; le symétrique d'un élément $x \in A$ pour $+$ s'appelle l'opposé de x et se note $-x$.
- La multiplication est associative et possède un élément neutre, en général noté 1 ou 1_A en cas d'ambiguïté.
- La multiplication est distributive par rapport à l'addition : pour tout $a, b, c \in A$, on a $a(b+c) = ab+ac$ et $(a + b)c = ac + bc$.
  Lorsque la multiplication est aussi commutative, on dit que l'anneau A est abélien ou commutatif.

2.2 Exemples. a) Munis des opérations (addition et multiplication) usuelles, les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs, ainsi que l'anneau $K[X]$ des polynômes sur un corps (ou un anneau) commutatif K.

b) L'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{R}$, muni de l'addition et de la multiplication des matrices est un anneau non commutatif pour $n \geqslant 2$.

Si A et B sont deux anneaux, une application $f : A \to B$ est appelée un *homomorphisme (ou morphisme) d'anneaux* si pour tout $x, y \in A$ on a $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ et si $f(1_A) = 1_B$. (Remarquons qu'on a automatiquement $f(0_A) = 0_B$).

Soient A un anneau et $x \in A$. On définit nx pour $n \in \mathbb{Z}$ en posant $0x = 0$, $1x = x$, puis, pour tout $n \in \mathbb{N}$, $(n + 1)x = (nx) + x$; enfin pour n négatif $nx = -\big((-n)x\big)$. L'application $n \mapsto nx$ est un homomorphisme d'anneaux de $\mathbb{Z}$ dans A.

L'élément $n1_A$ se note parfois n même lorsque cet homomorphisme n'est pas injectif.

On définit de même x^n pour $x \in A$ et $n \in \mathbb{N}$: on pose $x^0 = 1_A$, $x^1 = x$ puis $x^{n+1} = x^n x (= xx^n)$.

2.3 Formule du binôme. Soient A un anneau et $a, b \in A$ deux éléments *permutables* - *i.e.* tels que $ab = ba$. Alors, pour tout $n \in \mathbb{N}$, on a

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

C'est faux si $ab \neq ba$. Par exemple $(a + b)^2 = a^2 + ab + ba + b^2 \neq a^2 + 2ab + b^2$.

2.4 Définition. Soit A un anneau. Un élément $a \in A$ est dit *inversible* (on dit parfois une unité de A) s'il existe a' dans A (nécessairement unique) tel que $a'a = aa' = 1_A$. Si a est inversible, l'élément a' tel que $a'a = aa' = 1_A$ s'appelle l'inverse de a et se note a^{-1}.

2.5 Proposition. *L'ensemble (noté parfois A^{-1}) des éléments inversibles de A est un groupe pour la multiplication.*

2.6 Définition. Un corps est un anneau K tel que $K^{-1} = K - \{0_K\}$.

2.7 Exercice. Soient A un anneau et $a \in A$. Démontrer que a est inversible si et seulement si l'application $b \mapsto ab$ est bijective de A dans A.

2.2 Anneaux intègres ; anneaux principaux

Dans la suite, tous les anneaux seront supposés commutatifs.

2.8 Définition. On dit qu'un anneau commutatif A est *intègre* si le produit de deux éléments non nuls de A est non nul.

2.9 Division ; éléments associés. Dans un anneau commutatif intègre, on peut définir la divisibilité comme dans $\mathbb{Z}$. On dit que a divise b et on écrit $a|b$ s'il existe c (*nécessairement unique* si a n'est pas nul) tel que $b = ac$. Autrement dit $a|b$ si $b \in aA$.

On dira que deux éléments a et b de A sont *associés* si $a|b$ et $b|a$, c'est à dire s'il existe $u \in A$ inversible tel que $a = ub$.

Le sous-ensemble aA de A est un sous-groupe de A. Mais contrairement au cas de $\mathbb{Z}$, les sous-groupes de A sont loin d'être en général tous de cette forme.

2.10 Définition. Soit A un anneau commutatif. On appelle *idéal* de A une partie I de A qui est un sous-groupe de $(A, +)$ et telle que, pour tout $a \in A$ et tout $x \in I$ on ait $ax \in I$.

A un idéal on peut encore associer une relation d'équivalence et définir un anneau quotient :

2.11 Proposition. *Soient A un anneau commutatif et I un idéal dans A. La relation R définie sur A par $a\,R\,b$ si $b - a \in I$ est une relation d'équivalence.*

2.12 Définition. Soient A un anneau commutatif et I un idéal dans A. On note A/I le *quotient d'équivalence* pour la relation R.

2.13 Proposition. *Soient A un anneau commutatif et I un idéal dans A. L'addition et la multiplication de A passent au quotient et définissent une structure d'anneau sur A/I.*

En effet, si $a, b \in A$ et $x, y \in I$, alors $(a+x)+(b+y)\,R\,a+b$ et $(a+x)(b+y) = ab+(ay+x(b+y))\,R\,ab$.

2.14 A retenir. a) Si I est un idéal d'un anneau (commutatif) A, on peut construire un anneau A/I et un homomorphisme surjectif d'anneaux $\pi : A \to A/I$ de noyau I.

b) Inversement, le noyau d'un homomorphisme d'anneaux $\pi : A \to B$ est un idéal.

Pour $a \in A$, l'ensemble aA est un idéal de A. On l'appelle l'idéal principal associé à a.

2.15 Définition. On dit qu'un anneau commutatif est *principal* s'il est intègre et tous ses idéaux sont principaux.

Un idéal étant en particulier un sous-groupe, l'anneau $\mathbb{Z}$ est principal. Nous verrons que si K est un corps commutatif, l'anneau $K[X]$ des polynômes à coefficients dans K est aussi un anneau principal. D'autres exemples d'anneaux principaux et d'anneaux intègres non principaux seront donnés plus bas.

Dans un anneau principal, la division se comporte essentiellement comme dans $\mathbb{Z}$.

2.16 Théorème. *Soient A un anneau principal et $a, b \in A$.*

a) *Il existe un élément $m \in A$ tel que $aA \cap bA = mA$. L'élément m est un multiple commun de a et de b. Les multiples communs de a et b sont les multiples de m.*

b) *Il existe un élément $d \in A$ tel que $aA + bA = dA$. L'élément d est un diviseur commun de a et de b. Les diviseurs communs de a et b sont les diviseurs de d.*

2.17 Définition. L'élément d de ce théorème s'appelle un plus grand commun diviseur (PGCD) de a et b. L'élément m s'appelle un plus petit commun multiple (PPCM) de a et b.

Un *PGCD* de a et de b n'est en général pas unique : il est unique à multiplication par un élément inversible de A près. On a fait un choix dans $\mathbb{Z}$ en les prenant dans $\mathbb{N}$ ce qui les a rendus uniques. On fait un tel choix aussi dans $K[X]$, mais il n'y a pas en général un choix « meilleur que les autres ».

Comme dans le cas de $\mathbb{Z}$, on peut définir la notion d'éléments premiers entre eux : leurs seuls diviseurs communs sont les éléments inversibles. Alors 1_A est un PGCD, *i.e.* $aA+bA = A$. On a donc le théorème de Bézout dans ce cadre, dont découle le théorème de Gauss :

2.18 Théorème de Bézout. *Soit A un anneau principal. Soient $a, b \in A$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in A$ tels que $au + bv = 1$.*

2.19 Théorème de Gauss. *Soit A un anneau principal. Soient $a, b, c \in A$. Si a divise bc et est premier à b, alors a divise c.*

Le rôle des nombres premiers est ici joué par les éléments irréductibles.

2.20 Définition. Soit A un anneau intègre. Un élément $a \in A$ est dit *irréductible* s'il n'est pas inversible et dans toute décomposition $a = bc$ un des deux facteurs b ou c est inversible.

2.21 Proposition. *Soient A un anneau principal et $a \in A$ non nul. Alors a est irréductible si et seulement si l'anneau quotient A/aA est un corps.*

Pour établir la décomposition en produit d'éléments irréductibles dans un anneau principal, la difficulté est de démontrer que tout élément non nul et non inversible possède un diviseur irréductible, et qu'il n'en possède qu'un nombre fini. Nous esquissons une preuve ci-dessous :

2.22 Lemme. a) *Soit A un anneau principal. Toute suite croissante d'idéaux de A stationne.*

b) *Toute suite décroissante d'idéaux d'intersection non nulle stationne.*

Démonstration. Soit I_n une suite d'idéaux de A.

a) On suppose que la suite I_n est croissante, c'est à dire que, pour $k, \ell \in \mathbb{N}$ avec $k \leqslant \ell$, on a $I_k \subset I_\ell$. On veut démontrer qu'il existe n tel que, pour $k \geqslant \ell$ on a $I_k = I_n$.
Comme la suite I_n est croissante, on vérifie que la réunion des I_n est un idéal J de A.
Puisque A est principal, il existe $a \in A$ tel que $J = aA$. Alors $a \in J$ et il existe $n \in \mathbb{N}$ tel que $a \in I_n$ (par définition d'une réunion). On a alors $J = aA \subset I_n$ donc $J = I_n$ (puisque J est la réunion de I_k). Pour $k \geqslant n$, on a $I_n \subset I_k \subset J = I_n$.

b) On suppose que la suite I_n est décroissante, c'est à dire que, pour $k, \ell \in \mathbb{N}$ avec $k \leqslant \ell$, on a $I_k \supset I_\ell$. Soit a un élément non nul de l'intersection $\bigcap_{k\in\mathbb{N}} I_k$. Pour $k \in \mathbb{N}$, il existe b_k tel que $I_k = b_k A$ (A étant principal). Comme $a \in I_k$, il existe $c_k \in A$ tel que $b_k c_k = a$. Pour $k \leqslant \ell$, on a $I_k \supset I_\ell$, de sorte que $b_k \in I_\ell$: il existe $x \in A$ tel que $b_k = x b_\ell$. Comme $b_k c_k = a = b_\ell c_\ell$, il vient $x c_k = c_\ell$, soit $c_k | c_\ell$. Posons $J_k = c_k A$. La suite J_k est croissante, donc stationne d'après a). Il existe donc n tel que, pour $k \geqslant n$ on ait $J_k = J_n$. Pour $k \geqslant n$, on a $c_k \in J_n$, donc il existe $y \in A$ tel que $c_k = y c_n$; comme $b_k c_k = a = b_n c_n$ il vient $b_n = y b_k$, donc $I_n \subset I_k$, et l'on a l'égalité.

□

2.23 Théorème. *Soient A un anneau principal et $a \in A$ un élément non nul et non inversible.*

a) *Il existe un élément irréductible $p \in A$ tel que $p|a$.*

b) *Il existe un ensemble fini F d'éléments irréductibles de A tels que tout élément irréductible de A qui divise a est associé à un élément de F ; pour tout irréductible p, il existe $n \in \mathbb{N}$ tel que $p^n \not| a$.*

Une fois ce théorème établi, on en déduit immédiatement l'existence de la décomposition en facteurs irréductibles. L'unicité est plus difficile à énoncer mais se démontre comme dans le cas de $\mathbb{Z}$:

2.24 Théorème. *Soient A un anneau principal et $a \in A$ un élément non nul et non inversible. Il existe un entier $n \geqslant 1$ et des éléments irréductibles $p_1, \ldots, p_n \in A$ tels que $a = \prod_{j=1}^{n} p_j$. Cette décomposition est unique à l'ordre des facteurs près : si $a = \prod_{j=1}^{n} p_j = \prod_{j=1}^{m} q_j$, alors $n = m$ et il existe $\sigma \in \mathfrak{S}_n$, i.e. une bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ telle que p_j soit associé à $q_{\sigma(j)}$ (pour tout j).*

2.3 Anneaux euclidiens

Les anneaux euclidiens sont ceux pour lesquels on dispose d'une division euclidienne. La même preuve que pour $\mathbb{Z}$ démontre qu'ils sont principaux. De plus, dans un anneau euclidien, comme dans $\mathbb{Z}$, on peut calculer le PGCD, écrire une relation de Bézout, résoudre des équations diophantiennes ou de congruence, *etc.* de façon algorithmique.

2.25 Définition. Soit A un anneau commutatif et intègre. On dit que A est *euclidien* s'il existe une application $v : A - \{0\} \to \mathbb{N}$, - appelée *stathme euclidien* telle que pour tous $a, b \in A - \{0\}$ il existe $q, r \in A$ tels que $a = bq + r$ et $r = 0$ ou $v(r) < v(b)$.

2.26 Remarque. En général, on demande de plus que, pour tous $a, b \in A - \{0\}$ tels que $a|b$ on ait $v(a) \leqslant v(b)$. Cette condition est en pratique toujours vérifiée, mais n'est pas utile dans ce qui suit. On peut démontrer que si A possède un stathme qui ne vérifie pas cette propriété, il en possède un qui la vérifie.

L'anneau $\mathbb{Z}$ est euclidien de stathme $a \mapsto |a|$. Nous verrons plus bas que l'anneau $K[X]$ est aussi euclidien : l'application qui à un polynôme associe son degré est un stathme euclidien sur $K[X]$.

2.27 Théorème. *Tout anneau euclidien est principal.*

Soit A un anneau euclidien ; notons v son stathme. Soit I un idéal non nul de A et $a \in I - \{0\}$ tel que $v(a) = \inf\{v(x);\ x \in I - \{0\}\}$. Puisque $a \in I$, on a $aA \subset I$. Soit x un élément de I ; écrivons $x = aq + r$, avec $q, r \in A$ et $r = 0$ ou $r \neq 0$ et $v(r) < v(a)$. Or $r = x - aq \in I$, et on ne peut avoir $r \neq 0$ et $v(r) < v(a)$ par définition de a. Il vient $r = 0$, donc $x \in aA$. Cela prouve que $I = aA$.

2.28 Remarque. Dans un anneau euclidien, comme pour le cas de $\mathbb{Z}$, on dispose de l'*algorithme d'Euclide* qui permet de calculer en pratique le plus grand commun diviseur de deux éléments.

2.29 Exemples d'anneaux euclidiens. Soit $\tau \in \mathbb{C} - \mathbb{R}$ un entier quadratique, *i.e.* tel qu'il existe $a, b \in \mathbb{Z}$ avec $\tau^2 + a\tau + b = 0$. Il est alors immédiat que l'ensemble $\mathbb{Z} + \tau\mathbb{Z} = \{m + n\tau;\ (m, n) \in \mathbb{Z}^2\}$ est un sous anneau - noté $\mathbb{Z}[\tau]$ de $\mathbb{C}$. Inversement, si $\mathbb{Z} + \tau\mathbb{Z}$ est un anneau, alors $\tau^2 \in \mathbb{Z} + \tau\mathbb{Z}$, donc τ est racine d'un polynôme $X^2 + aX + b$ avec $a, b \in \mathbb{Z}$.

Les racines du polynôme $X^2 + aX + b$ sont τ et $\overline{\tau}$, de sorte que $\tau + \overline{\tau} = -a$ et $\tau\overline{\tau} = b$. En particulier $\overline{\tau} = -a - \tau \in \mathbb{Z}[\tau]$.

Pour $x \in \mathbb{Z}[\tau]$, on a $\overline{x} \in \mathbb{Z}[\tau]$, donc $|x|^2 = \overline{x}x \in \mathbb{Z}[\tau] \cap \mathbb{R}_+ = \mathbb{N}$ (et, de même, $\overline{x} + x \in \mathbb{Z}[\tau] \cap \mathbb{R} = \mathbb{Z}$). Posons $v(x) = |x|^2$. Nous allons voir que *pour des valeurs très particulières* de τ, l'anneau $\mathbb{Z}[\tau]$ est euclidien de stathme v, et que dans d'autres cas, il n'est pas principal.

2.30 Proposition. *Un élément x de $\mathbb{Z}[\tau]$ est inversible si et seulement si $v(x) = 1$.*

Si $xy = 1$, on a $v(x)v(y) = |x|^2|y|^2 = 1$ donc $v(x)$ est inversible dans $\mathbb{N}$: $v(x) = 1$.

Si $v(x) = 1$ alors $x\overline{x} = 1$, donc x est inversible dans $\mathbb{Z}[\tau]$.

2.31 Lemme. *On suppose que $|\mathrm{Im}(\tau)| < \sqrt{3}$. Alors pour tout $z \in \mathbb{C}$, il existe $q \in \mathbb{Z}[\tau]$ tel que $|z - q| < 1$.*

Démonstration. Soit $n \in \mathbb{Z}$ l'entier le plus proche de $\dfrac{\mathrm{Im}(z)}{\mathrm{Im}(\tau)}$, de sorte que $|\mathrm{Im}(z-n\tau)| \leqslant \dfrac{|\mathrm{Im}(\tau)|}{2}$. Soit aussi m le nombre entier le plus proche de la partie réelle de $z-n\tau$, de sorte que $|\mathrm{Re}(z-n\tau-m)| \leqslant \dfrac{1}{2}$. Posons $q = m+n\tau$. On a $|\mathrm{Re}(z-q)| \leqslant \dfrac{1}{2}$ et $|\mathrm{Im}(z-q)| \leqslant \dfrac{|\mathrm{Im}(\tau)|}{2}$, donc $|z-q|^2 \leqslant \dfrac{1+\mathrm{Im}(\tau)^2}{4} < 1$. □

2.32 Théorème. *Si $|\mathrm{Im}(\tau)| < \sqrt{3}$, l'anneau $\mathbb{Z}[\tau]$ est euclidien de stathme $v : x \mapsto |x|^2$.*

Démonstration. Soient $a, b \in \mathbb{Z}[\tau] - \{0\}$; posons $z = \dfrac{a}{b}$ et soit $q \in \mathbb{Z}[\tau]$ tel que $|z-q| < 1$. Posons $r = a - bq$. On a $a = bq + r$ et $|r| = |b||z-q| < |b|$ donc $v(r) < v(b)$. □

2.33 Remarque. Sans changer l'anneau $\mathbb{Z}[\tau]$, on peut remplacer τ par $\overline{\tau}$, de sorte que l'on peut supposer que $\mathrm{Im}(\tau) > 0$; on peut aussi remplacer τ par $\tau + n$ (avec n dans $\mathbb{Z}$). On peut donc supposer que la partie réelle de τ est dans $[0, 1[$; comme $\tau + \overline{\tau} \in \mathbb{Z}$, on a $\tau + \overline{\tau} = 0$ ou 1. Cela nous ramène à étudier seulement le cas où τ est racine d'un polynôme $X^2 + b$, ou $X^2 - X + b$ (avec $b \in \mathbb{N}^*$). Dans le premier cas, $\tau = i\sqrt{b}$; dans le deuxième $\tau = \dfrac{1 + i\sqrt{4b-1}}{2}$.
Le théorème s'applique donc uniquement dans les cinq cas suivants :

$$\tau \in \left\{ i, i\sqrt{2}, \frac{1+i\sqrt{3}}{2}, \frac{1+i\sqrt{7}}{2}, \frac{1+i\sqrt{11}}{2} \right\}.$$

Commentaire. On peut démontrer relativement facilement (*cf.* exerc. 2.4) que dans tous les autres cas, l'anneau $\mathbb{Z}[\tau]$ n'est pas euclidien. Cependant, il y a quelques cas où $\mathbb{Z}[\tau]$ est quand même principal. Cela se produit pour $\tau = \dfrac{1+i\sqrt{19}}{2}$· (*cf.* exerc. 2.6). Cependant, pour $b \geqslant 3$, l'anneau $\mathbb{Z}[i\sqrt{b}]$ n'est pas factoriel, donc il n'est pas principal (*cf.* exerc. 2.7).

2.34 L'équation diophantienne $x^2 + y^2 = z^2$. On cherche à trouver tous les triples $(x, y, z) \in \mathbb{Z}^3$ tels que $x^2 + y^2 = z^2$. Si (x, y, z) est une solution et $k \in \mathbb{Z}$, alors (kx, ky, kz) est aussi une solution. On peut donc supposer que (x, y, z) sont premiers entre eux. Si d divise x et y, alors d^2 divise z^2, donc d divise z. On peut donc supposer que x et y sont premiers entre eux. Remarquons que x et y ne peuvent être tous deux impairs car alors $x^2 \equiv y^2 \equiv 1$ [4], donc $z^2 \equiv 2$ [4] ce qui est impossible. Donc l'un des deux est pair et l'autre impair.

Dans ce cas, l'idéal $(x+iy)\mathbb{Z}[i] + (x-iy)\mathbb{Z}[i]$ de $\mathbb{Z}[i]$ contient $(x+iy) + (x-iy) = 2x$, ainsi que $i\big((x-iy) - (x+iy)\big) = 2y$ donc il contient 2. Or il existe $q \in \mathbb{Z}[i]$ tel que $(x+iy) - 2q$ soit égal à 1 ou à i. Cela prouve que $(x+iy)$ et $(x-iy)$ sont premiers entre eux. Décomposons $z^2 = (x+iy)(x-iy)$ en éléments irréductibles dans $\mathbb{Z}[i]$; puisque c'est un carré, chacun figure un nombre pair de fois. Cela prouve que $x+iy$ est associé à un carré : il existe $(a, b) \in \mathbb{Z}$, tels que $x+iy$ soit associé à $(a+ib)^2$ c'est à dire $x + iy = \pm(a+ib)^2$ (si y est pair) ou $x + iy = \pm i(a+ib)^2$ (si x est pair). On en déduit que les solutions sont nécessairement de la forme $(k(a^2-b^2), 2kab, k(a^2+b^2))$ ou $(2kab, k(a^2-b^2), k(a^2+b^2))$ (avec $a, b, k \in \mathbb{Z}$).

2.35 Proposition. *On suppose que $\mathbb{Z}[\tau]$ est principal. Soit q un élément irréductible de $\mathbb{Z}[\tau]$. Alors deux cas sont possibles :*
- *il existe un nombre premier $p \in \mathbb{N}$ tel que $v(q) = p$;*
- *il existe un nombre premier $p \in \mathbb{N}$ tel que q soit associé à p (et l'on a $v(q) = p^2$).*

Décomposons $v(q) = q\overline{q}$ en facteurs premiers dans $\mathbb{Z}$. C'est une décomposition dans $\mathbb{Z}[\tau]$ qui ne peut donc avoir que un ou deux éléments : dans le premier cas $v(q)$ est premier ; dans le deuxième un des facteurs p est associé à q, donc $v(q) = v(p) = p^2$.

Pour finir, signalons sans démonstration quels nombres premiers de $\mathbb{N}$ ne sont plus irréductibles dans $\mathbb{Z}[i]$.

2.36 Proposition. *Soit $p \in \mathbb{N}$ un nombre premier. Les assertions suivantes sont équivalentes :*

(i) *il existe $x, y \in \mathbb{Z}$ tels que $x^2 + y^2 = p$;*

(ii) *l'élément $p \in \mathbb{Z}[i]$ n'est pas irréductible dans $\mathbb{Z}[i]$;*

(iii) *-1 est un carré modulo p ;*

(iv) *$p \not\equiv 3$ [4].*

2.4 Sous-corps

2.4.1 Caractéristique d'un corps ; sous-corps premier

Soit K un corps. Tout morphisme f d'anneaux de K dans un anneau non nul est injectif : si $x \in K^*$, alors $f(x^{-1})f(x) = 1$, donc $f(x) \neq 0$.

Soit K un corps et $f : \mathbb{Z} \to K$ l'unique homomorphisme d'anneaux (défini par $f(n) = n1_K$). Le noyau de f est un idéal $n\mathbb{Z}$ de $\mathbb{Z}$. L'image $f(\mathbb{Z})$ est un sous-anneau commutatif de $\mathbb{K}$ isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Puisque K est un corps, $f(\mathbb{Z})$ est un anneau intègre, donc ou bien n est premier, ou bien f est injective. Ce nombre n s'appelle la *caractéristique* de K.

- Lorsque la caractéristique p n'est pas nulle, l'image $f(\mathbb{Z})$ est un sous-corps de K isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
- Lorsque f est injective, on peut étendre f en un homomorphisme $\tilde{f} : \mathbb{Q} \to K$ en posant $\tilde{f}\left(\frac{p}{q}\right) = f(p)f(q)^{-1}$ pour $p, q \in \mathbb{Z}$ avec $q \neq 0$. L'image $\tilde{f}(\mathbb{Q})$ est un sous-corps de K isomorphe à $\mathbb{Q}$.
- Le corps ainsi obtenu, isomorphe selon les cas à $\mathbb{Z}/p\mathbb{Z}$ ou à $\mathbb{Q}$ est le plus petit sous-corps de K. On l'appelle le *sous-corps premier* de K.

2.4.2 Corps des fractions d'un anneau intègre

Soit A un anneau commutatif intègre non nul. On définit un corps K contenant A. Sa construction est la généralisation de la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$. Les éléments de K sont des fractions $\frac{a}{b}$ où $a \in A$ et $b \in A - \{0\}$. On peut alors dire quand deux fractions sont égales, définir l'addition et la multiplication des fractions, et vérifier que l'on obtient ainsi un corps qui contient l'anneau A.

Pour formaliser cela, considérons la relation R sur $A \times (A - \{0\})$ définie par $(a, b)\, R\, (c, d)$ si $ad = bc$. On vérifie sans peine que R est une relation d'équivalence. Notons K l'ensemble quotient. La classe dans K d'un élément $(a, b) \in A \times (A - \{0\})$ se note $\frac{a}{b}$.

On définit la somme et le produit d'éléments de K en posant pour des éléments a, b, c, d de A avec b, d non nuls

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{et} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Ces opérations sont bien définies : si $(a, b)\, R\, (a', b')$ et $(c, d)\, R\, (c', d')$, alors $(ad + bc, bd)\, R\, (a'd' + b'c', b'd')$ et $(ac, bd)\, R\, (a'c', b'd')$. De plus, on a

$$\frac{a}{d} + \frac{c}{d} = \frac{a + c}{d}$$

ce qui permet de démontrer facilement les règles des opérations : K est bien un anneau commutatif. De plus K est un corps : l'inverse de $\frac{a}{b}$ est $\frac{b}{a}$ (pour $a, b \in A - \{0\}$).

Le corps K s'appelle le *corps de fractions* de A.

Enfin, on plonge A dans K au moyen de l'application $a \mapsto \frac{a}{1}$: cette application est un morphisme injectif qui plonge l'anneau A dans K.

2.37 Proposition. *Soit A un anneau commutatif intègre. Notons $K(A)$ son corps des fractions. Pour tout corps L et tout homomorphisme injectif $f : A \to L$, il existe un unique homomorphisme $\tilde{f} : K(A) \to L$ dont la restriction à $A \subset K(A)$ soit f*

2.4.3 Éléments algébriques, éléments transcendants

Soient L un corps commutatif et $K \subset L$ un sous-corps.

Soit $x \in L$. Considérons L comme espace vectoriel sur K et introduisons le sous-espace $K[x] \subset L$ engendré par les éléments x^n pour $n \in \mathbb{N}$. Cet espace est l'image de l'application $f : P \mapsto P(x)$ de $K[X]$ dans L. Cette application étant un homomorphisme d'anneaux, son noyau est un idéal de l'anneau principal $K[X]$. Il existe donc un polynôme $\varpi \in K[X]$ tel que $\ker f = \varpi K[X]$. Deux cas sont possibles :

a) Si $\varpi = 0$, l'application $f : P \mapsto P(x)$ est injective de $K[X]$ dans L. On dit alors que x est *transcendant* sur K.

b) Si $\varpi \neq 0$. Remarquons que f n'est pas l'application nulle, donc ϖ n'est pas inversible ; si $\varpi = PQ$, on trouve $P(x)Q(x) = 0$, ce qui implique que $P(x) = 0$ ou $Q(x) = 0$, *i.e.* l'un des deux est dans $\ker f$ donc multiple de ϖ. Il s'ensuit que ϖ est irréductible. On dit alors que x est *algébrique* sur K et le polynôme ϖ s'appelle le *polynôme minimal* de x.

Citons sans démonstration le résultat suivant (*cf.* exercice 2.8) :

2.38 Proposition. *Soient L un corps commutatif et $K \subset L$ un sous corps. Les éléments de L algébriques sur K forment un sous-corps de L.*

Cela signifie que la somme, le produit, l'inverse d'éléments algébriques est algébrique.

2.39 Proposition. *Le corps des nombres complexes algébriques sur $\mathbb{Q}$ est dénombrable.*

En effet, les éléments algébriques sont les racines de polynômes à coefficients rationnels (non nuls). Or $\mathbb{Q}$ étant dénombrable, l'ensemble des polynômes à coefficients rationnels est dénombrable, et chacun a un nombre fini de racines

On déduit de ce résultat qu'il y a « bien plus » de nombres transcendants que de nombres algébriques. On peut démontrer que les nombres e et π sont transcendants, mais ce n'est pas si facile.

2.5 Exercices

2.1 Exercice. *Le groupe $\mathbb{F}_p^*$ est cyclique. (1)*

1. Soit G un groupe commutatif fini.
   a) Soient $a, b \in G$. On note k_a et k_b leurs ordres respectifs. On suppose que k_a et k_b sont premiers entre eux. Démontrer que l'ordre de ab est $k_a k_b$.
   b) Démontrer qu'il existe $n \in \mathbb{N}^*$ tel que $\{k \in \mathbb{Z};\ \forall x \in G;\ x^k = 1\} = n\mathbb{Z}$. Démontrer que n divise le cardinal de G.
   Le nombre n s'appelle l'*exposant* de G.
   c) Ecrivons $n = \prod p_j^{m_j}$ la décomposition de n en nombres premiers distincts. Démontrer que pour tout j, il existe $x_j \in G$ d'ordre $p_j^{m_j}$.
   d) En déduire qu'il existe $x \in G$ d'ordre n.
2. Soit K un corps commutatif et G un sous-groupe fini à N éléments de K^*. Soit n son exposant.
   a) Démontrer que l'équation $x^n = 1$ a au plus n solutions dans K. En déduire que $N \leqslant n$.

b) Démontrer que G est cyclique.

2.2 Exercice. *Le groupe $\mathbb{F}_p^*$ est cyclique. (2)*

1. Soit $n \in \mathbb{N}^*$. On considère l'ensemble $A_n = \left\{ \frac{k}{n};\ k \in \mathbb{N},\ \ 0 \leqslant k < n \right\}$.
   a) Soit d un diviseur de n. Combien d'éléments de A_n ont leur écriture irréductible de la forme $\frac{a}{d}$?
   b) En déduire l'égalité $\sum_{d|n} \varphi(d) = n$.
2. Soit K un corps commutatif et G un sous-groupe fini à n éléments de K^*. Pour $d \in \mathbb{N}^*$, on note s_d le nombre d'éléments d'ordre d de G.
   a) Démontrer que $\sum_{d|n} s_d = n$.
   b) Soit $x \in G$; notons d son ordre et H le sous-groupe (cyclique) de G engendré par x. Démontrer que
   - H a d éléments et $\varphi(d)$ éléments d'ordre d.
   - Tout élément $y \in H$ vérifie $y^d = 1$.
   - L'équation $y^d = 1$ a au plus d solutions dans K.
   - Tout élément d'ordre d de G est dans H.

   c) En déduire que si $s_d \neq 0$, alors $s_d = \varphi(d)$.
   d) En déduire que pour tout diviseur d de n on a $s_d = \varphi(d)$, puis que G est cyclique.

2.3 Exercice. *Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est-il cyclique ?* Perrin, *Cours d'algèbre* p.24.

Cet exercice complète les précédents.

1. a) Soient G et H deux groupes commutatifs finis. Démontrer que $G \times H$ est cyclique si et seulement si G et H sont cycliques et que leurs ordres sont premiers entre eux.
   b) Quels sont les nombres n tels que $\varphi(n)$ soit impair ?
   c) Soient m et n deux nombres entiers premiers entre eux distincts de 1 et de 2. Démontrer que $(\mathbb{Z}/nm\mathbb{Z})^*$ n'est pas cyclique.
   d) $\mathbb{Z}/8\mathbb{Z}^*$ est-il cyclique ?
2. Soient p un nombre premier distinct de 2 et $n \in \mathbb{N}$, $n \geqslant 2$.
   a) Démontrer (par récurrence) que, pour tout $k \in \mathbb{N}$, $(1+p)^{p^k} \equiv 1 + p^{k+1} \ \ [p^{k+2}]$.
   b) Quel est l'ordre de $1+p$ dans le groupe $\mathbb{Z}/p^n\mathbb{Z}^*$?
   c) Soit $a \in \mathbb{Z}$ dont la classe dans $\mathbb{Z}/p\mathbb{Z}$ engendre $\mathbb{Z}/p\mathbb{Z}^*$, et soit $x \in \mathbb{Z}/p^n\mathbb{Z}^*$ la classe de a. Démontrer que l'ordre de x dans $\mathbb{Z}/p^n\mathbb{Z}^*$ est un multiple de $p-1$. En déduire qu'il existe dans $\mathbb{Z}/p\mathbb{Z}$ un élément d'ordre $p-1$.
   d) Démontrer que $\mathbb{Z}/p^n\mathbb{Z}^*$ est cyclique. Démontrer que $\mathbb{Z}/2p^n\mathbb{Z}^*$ est aussi cyclique.
3. Quels sont les entiers n tels que $\mathbb{Z}/n\mathbb{Z}^*$ soit cyclique ?

2.4 Exercice. Soit $a \in \mathbb{N}^*$ et $\tau \in \mathbb{C}$ une racine du polynôme $X^2 + X + a$. On note $\mathbb{Z}[\tau]$ l'anneau $\mathbb{Z} + \tau\mathbb{Z}$.

1. a) Soit $x \in \mathbb{Z}[\tau]$ non nul. Démontrer que $\mathbb{Z}[\tau]/x\mathbb{Z}[\tau]$ est fini. Notons $v(x)$ le nombre de ses éléments.
   b) Soient $x, y \in \mathbb{Z}[\tau]$ non nuls. Donnons nous des représentants $r_1, \ldots, r_n$ des classes d'éléments de $\mathbb{Z}[\tau]$ modulo x et des représentants $s_1, \ldots, s_m$ des classes d'éléments de $\mathbb{Z}[\tau]$ modulo y. Démontrer que tout élément de $\mathbb{Z}[\tau]$ est congru modulo xy à un un et un seul élément de la forme $r_i + xs_j$. En déduire que $v(xy) = v(x)v(y)$.

c) En calculant $v(k)$ pour $k \in \mathbb{Z}$, démontrer que, pour tout $x \in \mathbb{Z}[\tau]$ non nul, on a $v(x) = |x|^2$.

2. On suppose que $\mathbb{Z}[\tau]$ possède un stathme euclidien V.
   a) On suppose aussi que les seuls éléments inversibles de $\mathbb{Z}[\tau]$ sont ± 1. Soit $x \in \mathbb{Z}[\tau]$ non nul et non inversible de stathme minimal. Démontrer que tout élément de $\mathbb{Z}[\tau]$ est congru modulo x à $0, 1$ ou -1 ; en déduire que $v(x) \leqslant 3$.
   b) Démontrer que $\operatorname{Im} \tau \leqslant \sqrt{3}$.

2.5 Exercice. *Sous-groupes de* $\mathbb{Z}[\tau]$. Soit $\tau \in \mathbb{C}$ racine d'un polynôme $X^2 + X + a$ ou $X^2 + a$ avec $a \in \mathbb{N}^*$. Soit G un sous-groupe non nul de $\mathbb{Z}[\tau]$. Soit $\alpha \in G$ un élément non nul tel que $|\alpha|^2$ soit minimal dans $\{|x|^2;\ x \in G \setminus \{0\}\}$. (Un tel élément existe d'après le « principe de récurrence »- puisque $|x|^2 \in \mathbb{N}$ pour tout $x \in \mathbb{Z}[\tau]$).

1. Démontrer que $G \cap \mathbb{R}\alpha = \mathbb{Z}\alpha$.
   On suppose désormais que $G \not\subset \mathbb{R}\alpha$. Soit $\beta \in G \setminus \mathbb{Z}\alpha$ tel que $|\beta|^2$ soit minimal dans $\{|x|^2;\ x \in G \setminus \mathbb{Z}\alpha\}$. Quitte à remplacer β par $-\beta$, on peut supposer que $\operatorname{Im} \dfrac{\beta}{\alpha} > 0$.
2. Démontrer que $\left|\dfrac{\beta}{\alpha}\right| \geqslant 1$ et $\left|\operatorname{Re} \dfrac{\beta}{\alpha}\right| \leqslant \dfrac{1}{2}$.
3. Soit $x \in G$. Démontrer qu'il existe $m, n \in \mathbb{Z}$ tels que
$$\left|\operatorname{Im} \frac{x - n\beta}{\alpha}\right| \leqslant \frac{1}{2} \operatorname{Im} \frac{\beta}{\alpha} \quad \text{et} \quad \left|\operatorname{Re} \frac{x - (m\alpha + n\beta)}{\alpha}\right| \leqslant \frac{1}{2}.$$
   En déduire que $|x - (m\alpha + n\beta)| < |\beta|$, puis que $x = m\alpha + n\beta$.
   Il s'ensuit que $G = \alpha\mathbb{Z} + \beta\mathbb{Z}$.

2.6 Exercice. *Un anneau principal non euclidien*

Le but de cet exercice est de démontrer que pour $\tau = \dfrac{1 + i\sqrt{19}}{2}$, l'anneau $\mathbb{Z}[\tau]$ est principal mais n'est pas euclidien. Soit J un idéal non nul de $\mathbb{Z}[\tau]$. Puisque J est un sous-groupe de $\mathbb{Z}[\tau]$, non contenu dans un $a\mathbb{R}$ (il contient un élément non nul a et $a\tau$) il existe d'après l'exercice 2.5 $\alpha, \beta \in \mathbb{Z}[\tau]$ tels que
$$\operatorname{Im} \frac{\beta}{\alpha} > 0, \quad \left|\frac{\beta}{\alpha}\right| \geqslant 1, \quad \left|\operatorname{Re} \frac{\beta}{\alpha}\right| \leqslant \frac{1}{2} \quad \text{et} \quad G = \alpha\mathbb{Z} + \beta\mathbb{Z}$$
(remarquons que $\tau\alpha \in J$, donc $J \not\subset \mathbb{R}\alpha$).

1. Démontrer qu'il existe $a, b, c, d \in \mathbb{Z}$ tels que $\tau\alpha = a\alpha + b\beta$ et $\tau\beta = c\alpha + d\beta$.
2. En regardant les signes des parties imaginaires de τ et $\dfrac{\beta}{\alpha}$, démontrer que $b > 0$.
3. Quelles sont les valeurs propres et espaces propres de la matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$? Démontrer que $a + d = 1$ et $ad - bc = 5$. En déduire que $ad \leqslant 0$, que ad est pair, que $bc < 0$, que b et c sont impairs et que $4bc + (a - d)^2 = -19$.
4. Posons $x = \dfrac{\beta}{\alpha}$. Démontrer que $\begin{vmatrix} a + bx & 1 \\ c + dx & x \end{vmatrix} = 0$. En déduire que
   a) x et $\overline{x}$ sont racines du polynôme $bX^2 + (a - d)X - c$,
   b) $|x|^2 = -\dfrac{c}{b}$ et $\operatorname{Re} x = \dfrac{d - a}{2b}$.
5. Démontrer que $|a - d| \leqslant b$ et $b \leqslant -c$. En déduire que $3b^2 \leqslant 19$, puis que $b = 1$.
6. En déduire que $(\alpha, \tau\alpha)$ est une $\mathbb{Z}$-base de J et conclure.

On démontre de même que pour $D \in \{19, 43, 67, 163\}$, l'anneau $\mathbb{Z}\left[\dfrac{1 + i\sqrt{D}}{2}\right]$ est principal.

2.7 Exercice. 1. Dans $\mathbb{Z}[X]$, démontrer que l'idéal engendré par 2 et X n'est pas principal.

2. Démontrons que pour $\tau = i\sqrt{b}$ avec $b \geqslant 3$ et pour $\tau = \dfrac{1+i\sqrt{15}}{2}$, l'anneau $\mathbb{Z}[\tau]$ n'est pas factoriel (donc n'est pas principal). En utilisant les égalités :
   - pour $\tau = i\sqrt{3}$, on a $(1+\tau)(1+\overline{\tau}) = 4 = 2 \times 2$;
   - pour $\tau = 2i$ ou $\tau = \dfrac{1+i\sqrt{15}}{2}$, on a $\tau\overline{\tau} = 4 = 2 \times 2$;
   - pour $\tau = i\sqrt{5}$, on a $(1+\tau)(1+\overline{\tau}) = 6 = 2 \times 3$;

   démontrer que l'on n'a pas l'unicité dans la décomposition en éléments irréductibles. Pour $b \geqslant 5$, et $\tau = i\sqrt{b}$, écrire une égalité de ce style en discutant la parité de p. En déduire que $\mathbb{Z}[\tau]$ n'est pas principal.

2.8 Exercice. Soient L un corps commutatif et $K \subset L$ un sous-corps. Remarquons que L est un espace vectoriel sur K et que tout sous-anneau de L contenant K est un sous-K-espace vectoriel de L.

1. Soit K_1 un sous-corps de L contenant K. Démontrer que tout élément algébrique sur K est algébrique sur K_1.
2. Démontrer que pour $x \in L$ les conditions suivantes sont équivalentes :
   (i) x est algébrique sur K ;
   (ii) il existe un sous-anneau K_1 de L contenant K et x et qui soit un espace vectoriel de dimension finie sur K ;
   (iii) il existe un sous-corps K_1 de L contenant K et x et qui soit un espace vectoriel de dimension finie sur K.
3. Soient K_1, K_2 des sous-corps de L tels que $K \subset K_1 \subset K_2$. Démontrer que K_2 est un K-espace vectoriel de dimension finie si et seulement si K_2 est un K_1-espace vectoriel de dimension finie et K_1 est un K-espace vectoriel de dimension finie, et que dans ce cas, on a $\dim_K(K_2) = \dim_{K_1}(K_2)\dim_K(K_1)$.
4. Soient $\alpha, \beta \in L$ des éléments algébriques sur K. Soit K_1 un sous-corps de L contenant K et α et de dimension finie sur K.
   a) On suppose que $\alpha \neq 0$. Démontrer que α^{-1} est algébrique sur K.
   b) Démontrer que $\alpha + \beta$ et $\alpha\beta$ sont algébriques sur K.
5. Démontrer que les éléments de L algébriques sur K forment un sous-corps K' de L. Démontrer que si $x \in L$ est algébrique sur K' alors $x \in K'$.

3 Polynômes et fractions rationnelles

3.1 Polynômes à une indéterminée sur un corps commutatif K

Soit K un corps commutatif. On sait très bien ce qu'est un polynôme à coefficients dans K : c'est une expression abstraite $P = \sum_{k=0}^{n} a_k X^k$ où les a_i sont des éléments de K appelés les coefficients de P. On sait ajouter et multiplier les polynômes, les multiplier par un scalaire : les polynômes forment une K-algèbre.

3.1 Quelques mots sur la définition de l'algèbre $K[X]$. Se donner un polynôme revient à se donner ses coefficients c'est à dire une suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de K qui sont nuls pour k assez grand : il existe $n \in \mathbb{N}$ satisfaisant $a_k = 0$ pour $k > n$. On peut formaliser cela en définissant un polynôme comme la suite abstraite de ses coefficients : l'ensemble des polynômes est alors l'ensemble $K^{(\mathbb{N})}$ des suites $(a_k)_{k\in\mathbb{N}}$ telles qu'il existe $n \in \mathbb{N}$ satisfaisant $a_k = 0$ pour $k > n$. Dans cette vision, le $k^{\text{ème}}$ coefficient du polynôme X^k est égal à 1, et tous les autres sont nuls. L'ensemble $K^{(\mathbb{N})}$ est naturellement un K-espace vectoriel de dimension infinie et $(X^k)_{k\in\mathbb{N}}$ en est une base.

L'algèbre $K[X]$ est donc l'espace vectoriel $K^{(\mathbb{N})}$ muni de l'unique produit tel que $X^k X^\ell = X^{k+\ell}$ (pour tous $k, \ell \in \mathbb{N}$). Enfin, on identifie K avec l'ensemble des polynômes constants (au moyen de $a \mapsto aX^{(0)}$).

Soit $P \in K[X]$ un polynôme non nul. On appelle *degré* de P l'entier $\partial P = n \in \mathbb{N}$ tel que $a_n \neq 0$ et, $a_k = 0$ pour $k > n$ (où les a_k sont les coefficients de P). Le coefficient non nul de plus haut degré (a_n si $\partial P = n$) s'appelle le *coefficient directeur* de P. On dit que P est *unitaire* (ou *monique*) si son coefficient directeur est 1.

3.2 Proposition. *Pour $P, Q \in K[X]$ deux polynômes non nuls, on a $PQ \neq 0$, $\partial(PQ) = \partial P + \partial Q$, et le coefficient directeur de PQ est le produit des coefficients directeurs de P et de Q. En particulier, l'anneau $K[X]$ est intègre.*

L'anneau $K[X]$ est euclidien de stathme ∂. Plus précisément on a (où l'on a convenu $\partial 0 < 0$) :

3.3 Proposition : Division euclidienne dans $K[X]$. *Soient $A, B \in K[X]$ avec $B \neq 0$. Il existe un unique couple $Q, R \in K[X]$ tels que $A = BQ + R$ et $\partial R < \partial B$.*

On en déduit que $K[X]$ est principal, c'est-à-dire que tous les idéaux de $K[X]$ sont de la forme $AK[X]$. On peut alors définir le plus grand commun diviseur (PGCD) et plus petit commun multiple (PPCM) de deux polynômes, établir un théorème de Bézout, un algorithme d'Euclide qui permet de trouver le PGCD et une relation de Bézout ainsi que la décomposition unique d'un polynôme en facteurs irréductibles.

3.4 Exercices. a) Soient L un corps commutatif et K un sous-corps de L. Soient $A, B \in K[X]$; Démontrer que leur PGCD est le même qu'on les considère comme éléments de $K[X]$ ou de $L[X]$.

b) Calculer $PGCD(X^m - 1, X^n - 1)$.

De l'égalité $\partial(PQ) = \partial P + \partial Q$ on déduit :

3.5 Proposition. *a) Les éléments inversibles de $K[X]$ sont les polynômes non nuls de degré nul, i.e. les éléments de K.*

b) Tout polynôme de degré 1 est irréductible.

3.2 Fonctions polynômes

3.2.1 Racines

Soit K un corps. Si $x \in K$ et $P = \sum_{k=0}^{n} a_k X^k \in K[X]$, on pose $P(x) = \sum_{k=0}^{n} a_k x^k$. L'application $x \mapsto P(x)$ s'appelle la fonction polynôme associée à P. L'application $P \mapsto P(x)$ est un homomorphisme d'anneaux de $K[X]$ dans K. On dit que x est une *racine* de P si $P(x) = 0$.

3.6 Proposition. *Le reste de la division euclidienne de P par $X - a$ est $P(a)$. En particulier, $X - a$ divise P si et seulement si $P(a) = 0$.*

En effet, écrivons $P = (X - a)Q + R$ avec $\partial R < 0$, donc $R \in K$. Comme $(X - a)(a) = 0$, on trouve $P(a) = R$.

Cette proposition nous conduit à dire que a est une racine d'ordre k (au moins) si $(X - a)^k$ divise P et d'ordre exactement k si de plus $(X - a)^{k+1}$ ne divise pas P. Si $k = 2, 3$, on dira que a est racine double, triple... de P. Si $k \geqslant 2$ on dira que a est *racine multiple* de P

3.7 Proposition. *Soient $a_1, \ldots, a_k \in K$ des éléments deux à deux distincts et $m_1, \ldots, m_k \in \mathbb{N}$. Si un polynôme non nul P admet les racines a_j avec multiplicité m_j, il est divisible par $\prod_{j=1}^{k}(X - a_j)^{m_j}$. En particulier $\partial P \geqslant \sum m_j$ et si $\partial P = \sum m_j$, alors $P = a\prod_{j=1}^{k}(X - a_j)^{m_j}$ où $a \in K$ est le coefficient directeur de P.*

Les polynômes $X - a_j$ sont premiers entre eux deux à deux, donc il en va de même pour $(X - a_j)^{m_j}$. Si P admet les racines a_j avec multiplicité m_j, il est divisible par $(X - a_j)^{m_j}$, donc par leur produit.

3.8 Exemple. Soit p un nombre premier. D'après le (petit) théorème de Fermat, pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, on a $x^p = x$. En d'autres termes, tout élément de $\mathbb{Z}/p\mathbb{Z}$ est racine du polynôme $X^p - X \in \mathbb{Z}/p\mathbb{Z}[X]$. On en déduit que $\prod_{x \in \mathbb{Z}/p\mathbb{Z}} (X - x) = X^p - X$.

3.9 Corollaire. *Si K est infini, l'homomorphisme qui à un polynôme P associe la fonction polynôme $x \mapsto P(x)$ de K dans K est injectif.*

En effet, un polynôme non nul ne peut avoir qu'un nombre fini de racines. Il ne peut s'annuler sur tout K.

A cause de ce corollaire, on confond souvent les polynômes avec les fonctions polynômes.

3.10 Remarque. Pour $K = \mathbb{Z}/p\mathbb{Z}$, le noyau de l'homomorphisme qui à un polynôme P associe la fonction polynôme $x \mapsto P(x)$ de K dans K est l'idéal engendré par $X^p - X$.

3.11 Exemple. Polynôme d'interpolation de Lagrange. Soient $x_1, x_2 \ldots, x_n$ des éléments distincts de K et $\lambda_1, \lambda_2, \ldots, \lambda_n$ des éléments de K. Il existe un unique polynôme P de degré au plus $n - 1$ tel que $P(x_i) = \lambda_i$ pour tout i.

Existence. Pour $i = 1, \ldots, n$, posons $Q_i = \prod_{1 \leqslant j \leqslant n;\ j \neq i} (X - x_j)$. On prend $P = \sum_{i=1}^{n} \frac{\lambda_i}{Q_i(x_i)} Q_i$.

Unicité. Si P et Q satisfont ces conditions alors $P - Q$ s'annule en les x_i ; comme $\partial(P - Q) < n$, il vient $P - Q = 0$.

3.2.2 Polynômes scindés ; relations entre coefficients et racines

On dit qu'un polynôme P est *scindé* s'il est produit de polynômes du premier degré. Alors P s'écrit $P = a\prod_{k=1}^{n}(X - x_k)$.

Soit $P = \prod_{k=1}^{n}(X - x_k)$ un polynôme unitaire scindé. Écrivons $P = X^n + \sum_{k=0}^{n-1} a_k X^k$. Alors on a

- somme des racines $\sum_{k=1}^{n} x_k = -a_{n-1}$;
- produit des racines $(-1)^n a_0 = \prod_{k=1}^{n} x_k$.
- Plus généralement, $(-1)^\ell a_{n-\ell} = \sum_{1\leqslant k_1<\ldots<k_\ell\leqslant n}\left(\prod_{j=1}^{\ell} x_{k_j}\right)$ est la somme de tous les produits de ℓ racines.
- Pour $n = 2$ on trouve $P = X^2 - SX + P$ où S est la somme et P le produit des racines.
- Pour $n = 3$ on trouve $P = X^3 - SX^2 + \Sigma_2 X - P$, où S est la somme, P le produit des racines et $\Sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$.

3.2.3 Dérivation des polynômes

Soit $P = \sum_{k=0}^{n} a_k X^k$. On définit sa dérivée : c'est le polynôme $P' = \sum_{k=1}^{n} k a_k X^{k-1}$.

3.12 Proposition. a) *Pour $P, Q \in K[X]$, on a $(PQ)' = P'Q + PQ'$.*

b) *Soient $P \in K[X]$ et $a \in K$ une racine de P. Alors a est une racine double de P si et seulement si $P'(a) = 0$.*

a) se vérifie pour $P = X^k$ et $Q = X^\ell$ et s'étend par linéarité.
Pour b), écrivons $P = (X-a)Q$ de sorte que (d'après a) $P' = Q+(X-a)Q'$, donc $Q(a) = P'(a)$. Alors a est racine double de P, si et seulement si c'est une racine de Q, *i.e.* si et seulement si $P'(a) = Q(a) = 0$.

3.13 Dérivées successives ; identité de Taylor. On définit aussi les dérivées successives en posant $P'' = (P')'$ *etc.* La dérivée k-ième se note $P^{(k)}$. On a $P^{(k)}(0) = k!a_k$, de sorte que, si K est de caractéristique nulle (et $\partial P \leqslant n$),

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k.$$

Plus généralement, soit $a \in K$. Les polynômes $(X - a)^k$ forment une base de $K[X]$ (car ils sont échelonnés). Posons $Q_k = \dfrac{(X-a)^k}{k!}$. On a $Q_k^{(j)} = Q_{k-j}$ si $k \geqslant j$ et $Q_k^{(j)} = 0$ si $k < j$. En particulier, $Q_k^{(j)}(a) = \delta_k^j$, et si P s'écrit $\sum_k b_k Q_k$, il vient $b_j = P^{(j)}(a)$, donc

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X - a)^k.$$

3.2.4 Polynômes irréductibles sur $\mathbb{R}$ et $\mathbb{C}$

Donnons sans démonstration le théorème fondamental suivant :

3.14 Théorème de d'Alembert-Gauss. *Tout polynôme non constant à coefficients complexes admet au moins une racine dans* $\mathbb{C}$.

Tout polynôme non constant est donc divisible par un $X - a$. Il en résulte immédiatement que les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes du premier degré : tout polynôme à coefficients complexes est donc scindé.

Soit maintenant $P \in \mathbb{R}[X]$ un polynôme irréductible. Considérons le comme polynôme à coefficients complexes. Il a une racine $z \in \mathbb{C}$. Si $z \in \mathbb{R}$, P est du premier degré. Si $z = a + ib \notin \mathbb{R}$, alors écrivons $P = BQ + R$ la division euclidienne de P par $B = (X - z)(X - \overline{z}) = X^2 - 2aX + (a^2 + b^2)$ (dans $\mathbb{R}[X]$). Alors $R \in \mathbb{R}[X]$ est de degré au plus 1 et s'annule en z : c'est le polynôme nul.

On trouve :

3.15 Corollaire. *Les polynômes irréductibles de* $\mathbb{R}[X]$ *sont les polynômes du premier degré et ceux du deuxième degré de discriminant strictement négatif.*

3.2.5 Racines et extensions de corps

Soient K un corps commutatif et $P \in K[X]$. Si L est une extension de K, on peut considérer P comme polynôme à coefficients dans L : en d'autres termes on identifie $K[X]$ à un sous-anneau de $L[X]$. En particulier, on peut définir

On note (P) l'idéal $PK[X]$ de $K[X]$. Puisque $K[X]$ est principal, tout idéal de $K[X]$ est de cette forme. Nous utiliserons le résultat suivant.

3.16 Proposition. *Soit* $P \in K[X]$ *un polynôme non nul. On a l'équivalence entre :*

(i) *Le polynôme* P *est irréductible ;*

(ii) *L'anneau quotient* $K[X]/(P)$ *est intègre ;*

(iii) *L'anneau quotient* $K[X]/(P)$ *est un corps.* □

Soit $P \in K[X]$ un polynôme irréductible. Notons $L = K[X]/(P)$ l'anneau quotient.

- On considère l'application $i : K \to L$ qui à un scalaire $a \in K$ associe la classe du polynôme constant $a \in K[X]$ dans le quotient. L'application i est un morphisme de corps (injectif) au moyen duquel on identifie K à un sous-corps de L et donc L à une extension de K.
- Notons aussi x la classe dans L du polynôme X dans le quotient $L = K[X]/(P)$. En d'autres termes, on a $x = \pi(X)$ où $\pi : K[X] \to L = K[X]/(P)$ est l'application quotient.
- Comme π est un homomorphisme d'anneaux, on $\pi(X^2) = x^2$ et plus généralement $\pi(X^n) = x^n$.
- Pour $a \in K$, on a $\pi(aX^0) = i(a)$, en d'autres termes, avec les identifications de $K \subset K[X]$ et $K \subset L$, la restriction de π à K est l'identité.
- On a donc $\pi(\sum_{k=0}^{n} a_k X^k) = \sum_{k=0}^{n} a_k x^k$; autrement dit, pour tout polynôme $Q \in K[X]$, on a $\pi(Q) = Q(x)$.
- En particulier, puisque $P \in \ker \pi = (P)$, on a $P(x) = 0$.

On a démontré :

3.17 Théorème. *Soient* K *un corps et* $P \in K[X]$ *un polynôme irréductible sur* K. *Il existe une extension* L *de* K *dans laquelle* P *a une racine.* □

3.18 Corollaire. *Soient* K *un corps et* $P \in K[X]$ *un polynôme non constant.*

a) Il existe une extension L *de* K *dans laquelle* P *a une racine.*

b) Il existe une extension L *de* K *dans laquelle* P *est scindé.*

Démonstration. a) Soit $P_0 \in K[X]$ un polynôme irréductible dans K divisant P. Par le théorème ci-dessus, il existe une extension L de K dans laquelle P_0 admet une racine ; celle-ci sera une racine de P.

b) On procède par récurrence sur le degré de P. On démontre par récurrence sur n l'énoncé suivant : $S(n)$: pour tout corps commutatif K et tout polynôme $P \in K[X]$ de degré n, il existe une extension L de K telle que P est scindé sur L.
- Pour $n = 1$: tout polynôme de degré 1 est scindé donc $S(1)$ est vraie.
- Supposons $S(n)$ démontrée et soit P un polynôme de degré $n+1$ sur un corps commutatif K. Par (a), il existe une extension L_1 de K dans laquelle P admet une racine α. Alors P vu comme polynôme de $L_1[X]$ s'écrit $P = (X-\alpha)Q$ où $Q \in L_1[X]$ est de degré n. Puisque $S(n)$ est vraie (hypothèse de récurrence), il existe une extension L de L_1 dans laquelle le polynôme Q est scindé. Alors L est une extension de K et le polynôme $P = (X-\alpha)Q$ est scindé dans L. □

3.3 Fractions rationnelles sur un corps commutatif K

3.19 Définition. Le corps des fractions de $K[X]$ se note $K(X)$. Ses éléments s'appellent des *fractions rationnelles.*

Si A, B, D sont des polynômes avec $BD \neq 0$, on a $\dfrac{AD}{BD} = \dfrac{A}{B}$. Donc pour chaque fraction rationnelle F il existe des polynômes A, B premiers entre eux $B \neq 0$ tels que $F = \dfrac{A}{B}\cdot$ Une écriture de $F = \dfrac{A}{B}$ avec A, B premiers entre eux s'appelle une *forme irréductible* de F.

Soit F une fraction rationnelle et $F = \dfrac{A}{B}$ une forme irréductible. Les racines de A s'appellent les *zéros* ou *racines* de F ; les racines de B s'appellent les *pôles* de F. L'*ordre de multiplicité* d'un zéro (*resp.* pôle) a est l'ordre de multiplicité de la racine a de A (*resp.* B).

Soit $F \in K(X)$. Notons $\mathcal{P} \subset K$ l'ensemble de ses pôles. Soit $x \in K - \mathcal{P}$. Il existe une écriture $F = \dfrac{A}{B}$ telle que $B(x) \neq 0$. On pose alors $F(x) = A(x)B(x)^{-1}$. Cet élément de K ne dépend pas de l'écriture $F = \dfrac{A}{B}$ (avec $B(x) \neq 0$).
L'application $x \mapsto F(x)$ de $K - \mathcal{P}$ dans K s'appelle la *fonction rationnelle* associée à F.

Décomposition en éléments simples

On va peu à peu essayer de décomposer une fraction rationnelle en une somme de termes plus simples.

a) ***Partie entière*** Le degré d'une fraction rationnelle $F = \dfrac{A}{B}$ est le nombre $\partial F = \partial A - \partial B (\in \mathbb{Z})$. Ce nombre est indépendant de l'écriture. On a $\partial(FG) = \partial F + \partial G$ et $\partial(F+G) \leqslant \max\{\partial F, \partial G\}$ (avec la convention $\partial 0 = -\infty$).
Soit $F = \dfrac{A}{B}$ une fraction rationnelle. Écrivons $A = BQ + R$ la division euclidienne de A par B. On trouve $F = Q + \dfrac{R}{B}$, où $Q \in K[X] \subset K(X)$ et $\dfrac{R}{B}$ est une fraction rationnelle de degré < 0 (ou nulle). Donc :
Toute fraction rationnelle $F \in K(X)$ se décompose de façon unique en une somme d'un polynôme Q et d'une fraction rationnelle F_1 de degré strictement négatif. Le polynôme Q de cette décomposition s'appelle la partie entière *de F.*

b) ***Parties primaires.*** Soit à présent $F = \dfrac{A}{B}$ une fraction rationnelle de degré < 0. Supposons que B s'écrive $B = B_1B_2$ où B_1 et B_2 sont des polynômes premiers entre eux. D'après le théorème de Bézout, il existe des polynômes C_1 et C_2 tels que $A = B_1C_2 + B_2C_1$. Écrivons $C_1 = QB_1 + A_1$ la division euclidienne de C_1 par B_1 et posons $A_2 = C_2 + QB_2$, de sorte que $A = A_2B_1 + A_1B_2$ avec $\partial A_1 < \partial B_1$. Notons qu'alors $A_2B_1 = A - A_1B_2$, de sorte que $\partial(A_2B_1) < \partial B$; il vient $\dfrac{A}{B} = \dfrac{A_1}{B_1} + \dfrac{A_2}{B_2}$ avec $\partial A_1 < \partial B_1$ et $\partial A_2 < \partial B_2$. On vérifie que cette décomposition est unique.

Décomposant B en produit $\displaystyle\prod_{i=1}^{k} P_i^{m_i}$ où les P_i sont des polynômes irréductibles distincts on obtient (par récurrence sur k) une décomposition unique

$$\frac{A}{B} = \sum_{i=1}^{k} \frac{A_i}{P_i^{m_i}}$$

avec $\partial A_i < m_i \partial P_i$.

c) ***Éléments simples.*** Considérons enfin le cas où $F = \dfrac{A}{P^m}$ où P est irréductible, $\partial A < m\partial P$. Supposons que $m \geqslant 2$, et notons $A = PQ + R$ la division euclidienne de A par P. On trouve $F = \dfrac{R}{P^m} + \dfrac{Q}{P^{m-1}}$. Par récurrence sur m, on trouve donc que F s'écrit

$$\sum_{k=1}^{m} \frac{R_k}{P^k}$$

avec $\partial R_k < \partial P$. Cette décomposition est encore unique.

d) Mettant tout cela ensemble, on trouve que toute fraction rationnelle $F = \dfrac{A}{B}$ s'écrit de façon unique sous la forme :

$$F = E + \sum_{i=1}^{k} \sum_{j=1}^{m_i} \frac{R_{i,j}}{P_i^j}$$

où $B = b\displaystyle\prod P_i^{m_i}$ est la décomposition de B en facteurs irréductibles (et $b \in K^*$), E et $R_{i,j}$ sont des polynômes avec $\partial R_{i,j} < \partial P_i$.
Cette décomposition s'appelle la *décomposition* de F *en éléments simples.*

Lorsque P_i est un polynôme du premier degré - c'est toujours le cas si $K = \mathbb{C}$ - les $R_{i,j}$ sont de degré nul, donc des éléments de K.

Dans le cas où $K = \mathbb{R}$, on peut avoir des P_i du deuxième degré ; on aura alors des termes du premier degré au numérateur.

3.4 Exercices

3.1 Exercice. *Racines rationnelles*
Soit $P = \displaystyle\sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients entiers. Soit $x = \dfrac{p}{q}$ une racine rationnelle de P écrite sous forme irréductible. Démontrer que $p|a_0$ et $q|a_n$.

3.2 Exercice. Factoriser le polynôme $P = X^5 - 4X^4 + 9X^3 - 21X^2 + 20X - 5$ sachant qu'il s'écrit comme un produit de trois polynômes à coefficients entiers.

3.3 Exercice. Décomposer en éléments simples dans $\mathbb{R}[X]$ la fraction rationnelle $F = \dfrac{X^2+2}{X^3(X-1)^2}$.

En déduire une primitive de l'application $t \mapsto \dfrac{t^2+2}{t^3(t-1)^2}$.

3.4 Exercice. Trouver un polynôme $P \in K[X]$ de degré 3 tel que $P(0) = 1$, $P'(0) = 0$, $P(1) = 0$ et $P'(1) = 1$. Quels sont les polynômes $Q \in K[X]$ qui vérifient $Q(0) = 1$, $Q'(0) = 0$, $Q(1) = 0$ et $Q'(1) = 1$?

3.5 Exercice. Calculer des primitives des fonctions

a) $x \mapsto \dfrac{1}{x^4-x^2-2}$; b) $x \mapsto \dfrac{x+1}{(x^2+1)^2}$; c) $x \mapsto \dfrac{x+1}{x(x-1)^6}$; d) $x \mapsto \dfrac{1}{\cos^3 x}$.

3.6 Exercice. Résoudre le système d'équations $\begin{cases} x+y+z=3 \\ xy+yz+zx=1 \\ x^3+y^3+z^3=15 \end{cases}$ d'inconnues $x, y, z \in \mathbb{C}$.

3.7 Exercice. Soit K un corps et $a, b \in \mathbb{N}$. On considère les polynômes $A = X^a - 1$ et $B = X^b - 1$ de $K[X]$.

1. On suppose $b \neq 0$. Quel est le reste de la division euclidienne de A par B ?
2. Quel est le PGCD D de A et B ?
3. Écrire une relation de Bézout $D = AU + BV$.
4. Autre méthode : décomposer A et B en facteurs irréductibles dans $\mathbb{C}$. Pourquoi cela donne-t-il le PGCD de A et B vus comme éléments de $\mathbb{Q}[X]$?

3.8 Exercice. Soit $P \in \mathbb{R}[X]$ un polynôme unitaire sans racines réelles.

1. Démontrer qu'il existe un polynôme $A \in \mathbb{C}[X]$ tel que $P = \overline{A}\,A$ et A et $\overline{A}$ soient premiers entre eux.

   Notons k le degré de A.
2. Démontrer qu'il existe un unique polynôme $J \in \mathbb{C}[X]$ de degré $< 2k$ tel que $J \equiv i\ [A]$ et $J \equiv -i\ [\overline{A}]$.
3. Démontrer que $J \in \mathbb{R}[X]$ et $J^2 \equiv -1\ [P]$.
4. Un espace vectoriel complexe peut être considéré comme $\mathbb{R}$-espace vectoriel. Inversement, soient E un $\mathbb{R}$-espace vectoriel et j un endomorphisme de E tel que $j^2 = -\mathrm{id}_E$.
   a) Démontrer qu'il existe une unique structure d'espace vectoriel sur E telle que, pour $s, t \in \mathbb{R}$ et $x \in E$ on ait $(s+it)x = sx + tj(x)$.
   b) Munissons E de cette structure. Démontrer que les endomorphismes du $\mathbb{C}$-espace vectoriel E sont les endomorphismes f du $\mathbb{R}$ espace vectoriel E tels que $j \circ f = f \circ j$.
5. Soit E un $\mathbb{R}$ espace vectoriel de dimension finie et f un endomorphisme de E sans valeurs propres réelles. Démontrer qu'il existe sur E une structure d'espace vectoriel complexe telle que f soit $\mathbb{C}$-linéaire.

3.9 Exercice. Soit $P \in K[X]$.

1. Décomposer $\dfrac{P'}{P}$ en éléments simples.
2. *Théorème de Lucas.* On suppose $K = \mathbb{C}$. Démontrer que l'ensemble des zeros de P' est inclus dans l'enveloppe convexe de l'ensemble des zéros de P.
3. *Ellipse de Steiner.* Soient $\alpha, \beta, \gamma \in \mathbb{C}$ les affixes de trois points non alignés et notons P le polynôme $P = (X-\alpha)(X-\beta)(X-\gamma)$. On veut démontrer qu'il existe une unique ellipse (appelée ellipse de Steiner) inscrite dans le triangle de sommets (α, β, γ) et tangente aux côtés du triangle en leur milieu dont les foyers sont les racines de P'.

a) Démontrer qu'il existe une unique application affine (sur $\mathbb{R}$) $\ell : \mathbb{C} \to \mathbb{C}$ telle que $\ell(1) = \alpha$, $\ell(j) = \beta$, $\ell(j^2) = \gamma$ (où $j = e^{\frac{2i\pi}{3}}$). Démontrer qu'il existe $a, b, c \in \mathbb{C}^2$ tels $\ell(z) = az + b\overline{z} + c$ pour tout $z \in \mathbb{C}$ et que l'on a $P = (X - c)^3 - 3ab(X - c) - a^3 - b^3$.

b) Démontrer qu'il existe une unique ellipse qui soit tangente au milieu des trois côtés du triangle (α, β, γ). Démontrer que les affixes des foyers de cette ellipse sont les racines de P'.

3.10 Exercice. *Hyperbole et triangle équilatère.* Dans le plan affine euclidien on considère une hyperbole équilatère H. Notons O son centre de symétrie. Soient P un point de H, P' son symétrique par rapport à O et $\mathcal{C}$ le cercle de centre P et de rayon PP'.

1. Démontrer que $\mathcal{C}$ et H se coupent en quatre points (avec la possibilité que P' soit un point double).
2. On note A, B, C les trois autres points d'intersection de $\mathcal{C}$ avec H. Démontrer que le centre de gravité du triangle ABC est P ; en déduire que c'est un triangle équilatéral.

3.11 Exercice. *Polynômes à racines de module* 1
Soit P un polynôme unitaire à coefficients entiers. Notons $x_1, \ldots, x_n$ les racines de P (comptées avec leur multiplicité).

1. On suppose que pour tout k, on a $|x_k| = 1$.
   a) Soit $\ell \in \mathbb{N}$. Démontrer qu'il existe un polynôme unitaire P_ℓ à coefficients entiers dont les racines sont les x_k^ℓ.
   b) Soit $Q = X^n + \sum_{j=0}^{n-1} a_j X^j$ un polynôme dont toutes les racines sont de module 1. Démontrer que $|a_j| \leqslant \binom{n}{j}$.
   c) En déduire qu'il existe ℓ et m tels que tels que $\ell \neq m$ et $P_\ell = P_m$.
   d) Démontrer qu'il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que, pour tout k on ait $x_k^\ell = x_{\sigma(k)}^m$.
   e) En déduire que pour tout $r \in \mathbb{N}$, on a $x_k^{\ell^r} = x_{\sigma^r(k)}^{m^r}$.
   f) Démontrer que toutes les racines de P sont des racines de 1.
2. On suppose que toutes les racines de P sont réelles comprises entre -2 et 2. Démontrer qu'elles sont de la forme $2\cos q\pi$ avec $q \in \mathbb{Q}$. (Considérer un polynôme Q tel que $Q(x) = x^n P(x + 1/x)$).
3. Soit A une matrice symétrique à coefficients entiers de norme < 2. Démontrer que les valeurs propres de A sont de la forme $2\cos q\pi$ avec $q \in \mathbb{Q}$.

3.12 Exercice. *Résultant de deux polynômes* Soit K un corps. Pour $n \in \mathbb{N}$, notons E_n l'espace vectoriel des polynômes de degré $< n$.

Soient $A, B \in K[X]$ des polynômes non nuls. Posons $m = \partial A$ et $n = \partial B$ et écrivons $A = \sum_{k=0}^{m} a_k X^k$, $B = \sum_{k=0}^{n} b_k X^k$. On considère l'application linéaire $f_{A,B} : E_n \times E_m \to E_{m+n}$ définie par $f_{A,B}(P, Q) =$

$AP + BQ$. Pour $k = 0, \ldots, n-1$, notons C_k la matrice colonne à $n+m$ lignes :

$$C_0 = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 0 \\ a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad C_k = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad C_{n-1} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}.$$

De même, pour $k = 0, \ldots, m-1$, notons D_k la matrice colonne à $n+m$ lignes :

$$D_0 = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 0 \\ b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad D_k = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad D_{m-1} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

(La matrice C_k commence par k lignes nulles et se termine par $n-1-k$ lignes nulles ; la matrice D_k commence par k lignes nulles et se termine par $m-1-k$ lignes nulles.)

1. Démontrer l'équivalence :
   (i) les polynômes A et B sont premiers entre eux (pour $K = \mathbb{C}$ les polynômes A et B n'ont pas de racine commune) ;
   (ii) l'application f est bijective ;
   (iii) le déterminant $\mathrm{Res}_{A,B}$ de la matrice carrée de colonnes $C_0, \ldots, C_{n-1}, D_0, \ldots, D_{m-1}$ n'est pas nul. Ce déterminant s'appelle le emphrésultant de A et B.
2. Pour $K = \mathbb{C}$ écrire une relation nécessaire et suffisante pour qu'un polynôme A possède des racines multiples.
3. Applications : calculer le résultant de A et B dans les cas suivant
   a) $A = aX^2 + bX + c$ et $B = A'$;
   b) $A = X^3 + pX + q$ et $B = A'$;
   c) A quelconque $B = X - b$.
4. Quelques formules sur le résultant. Démontrer que l'on a :
   a) $\mathrm{Res}_{B,A} = (-1)^{mn}\mathrm{Res}_{A,B}$ pour $A \in K[X]$ de degré m et $B \in K[X]$ de degré n ;
   b) $\mathrm{Res}_{A,bB} = b^m \mathrm{Res}_{A,B}$ pour $b \in K$;
   c) $\mathrm{Res}_{A,B_1B_2} = \mathrm{Res}_{A,B_1}\mathrm{Res}_{A,B_2}$;
   d) si $B = \prod_{i=1}^{n} X - y_i$, $\mathrm{Res}(A,B) = \prod_{i=1}^{n} A(y_i)$;

e) si $A = \prod_{i=1}^{m} X - x_i$, $\mathrm{Res}(A, B) = (-1)^{mn} \prod_{i=1}^{m} B(x_i)$;

f) si $A = \prod_{i=1}^{m} X - x_i$ et $B = \prod_{i=1}^{n} X - y_i$, $\mathrm{Res}(A, B) = \prod_{i,j} x_j - y_i$.

3.13 Exercice. On se propose de démontrer le :

Théorème de Sturm. *Soit $P \in \mathbb{R}[X]$ un polynôme sans racines multiples dans $\mathbb{C}$. Posons $P_0 = P$, $P_1 = P'$ et pour $k \geqslant 2$, supposant P_{k-2} et P_{k-1} construits, on écrit la division euclidienne de P_{k-2} par P_{k-1} sous la forme $P_{k-2} = Q_k P_{k-1} - P_k$. On note P_m le dernier P_k non nul. Notons A l'ensemble des nombres réels qui sont racine d'un P_k (au moins) pour $0 \leqslant k \leqslant m$. Pour $x \in \mathbb{R} \setminus A$, notons $n(x)$ le nombre de changements de signes de la suite $P_0(x), P_1(x), \ldots, P_m(x)$, c'est-à-dire le nombre de $i \in \{1, \ldots, m\}$ tels que $P_i(x)$ et $P_{i-1}(x)$ soient de signes contraires. Pour tous $a, b \in \mathbb{R} \setminus A$ tels que $a < b$, le nombre de racines de P dans l'intervalle $[a, b]$ est $n(a) - n(b)$.*

1. Démontrer que, pour tout $k < m$, P_k et P_{k+1} sont premiers entre eux. Démontrer que P_m est constant et non nul.
2. Démontrer que l'application $x \mapsto n(x)$ est constante sur tout intervalle contenu dans le complémentaire de A.

   Pour $x \in A$, on note $n_g(x)$ la limite à gauche de n en x et $n_d(x)$ sa limite à droite.
3. Soit x une racine de P_k avec $k > 0$.
   a) Démontrer que P_{k-1} et P_{k+1} ne s'annulent pas en x et sont de signes contraires. Démontrer qu'il existe un intervalle ouvert J contenant x tel que, pour $y \in J \setminus \{x\}$, le nombre de changements de signe dans la suite $P_{k-1}(y), P_k(y), P_{k+1}(y)$ soit égal à 1.
   b) Démontrer que si $x \in A$ n'est pas racine de $P_0 = P$, alors $n_g(x) = n_d(x)$.
4. Soit x une racine de P. Démontrer que $n_g(x) = n_d(x) + 1$.

   Indication : Les polynômes P et P' ont le même signe à droite de x et des signes contraires à gauche de x.
5. Établir le théorème de Sturm.

3.14 Exercice. *Résolution des équations du quatrième degré*

1. Soit $P \in K[X]$ un polynôme scindé unitaire de degré 4. Notons z_1, z_2, z_3, z_4 ses racines. Trouver un polynôme de degré 3 dont les racines sont $u_1 = z_1 z_2 + z_3 z_4$, $u_2 = z_1 z_3 + z_2 z_4$, $u_3 = z_1 z_4 + z_1 z_4$.
2. Si on sait résoudre les équations du troisième degré, on peut trouver u_1, u_2, u_3. Comment trouver alors les z_i ?

3.15 Exercice. Soit p un nombre premier.

1. Démontrer que dans $\mathbb{F}_p[X]$ on a l'égalité $X^p - X = \prod_{x \in \mathbb{F}_p} (X - x)$.
2. Démontrer le *théorème de Wilson* : $(p-1)! + 1 \equiv 0 \ \ [p]$.

3.16 Exercice. [Contenu d'un polynôme]

1. Soient $A, B \in \mathbb{Z}[X]$.

   Écrivons $A = \sum_{k=0}^{m} a_k X^k$, $B = \sum_{k=0}^{n} b_k X^k$ et $AB = \sum_{k=0}^{m+n} c_k X^k$. Soit p un nombre premier. On suppose que p divise tous les c_k. Démontrer que p divise tous les a_k ou tous les b_k.

   On appelle *contenu* d'un polynôme $P = \sum_{k=0}^{n} p_k X^k$ à coefficients dans $\mathbb{Z}$ et on note $c(P)$ le PGCD de ses coefficients $p_0, \ldots, p_n$.

2. Soient $A, B \in \mathbb{Z}[X]$. Démontrer que si $c(A) = c(B) = 1$, alors $c(AB) = 1$. En déduire que l'on a toujours $c(AB) = c(A)c(B)$.
3. Soit $P \in \mathbb{Z}[X]$ un polynôme non constant. Démontrer que si P est irréductible dans $\mathbb{Z}[X]$ il est irréductible dans $\mathbb{Q}[X]$.

3.17 Exercice. [Critère d'Eisenstein] Soient P un polynôme unitaire à coefficients entiers et p un nombre premier. On suppose que p divise tous les coefficients de P - sauf le coefficient dominant - et que $P(0)$ n'est pas divisible par p^2. Démontrer que P est irréductible sur $\mathbb{Z}$ - donc sur $\mathbb{Q}$.

Application. Démontrer que pour tout nombre premier p le polynôme $\Phi_p = \sum_{k=0}^{p-1} X^k$ est irréductible sur $\mathbb{Q}$.

3.18 Exercice. (**) *Comment trouver les racines d'un polynôme dans $\mathbb{F}_p$?*
On se donne $P \in K[X]$ dont on veut trouver les racines dans K.

1. Trouver une méthode pour isoler les racines multiples.

   Indication : On pourra utiliser la dérivée de P.
2. On suppose que $K = \mathbb{F}_p$ où p est un (grand !) nombre premier. Donner une méthode pour trouver un polynôme scindé à racines simples ayant les mêmes racines que P.

   Indication : Penser au polynôme $X^p - X$.
3. On suppose que P est scindé à racines simples.
   a) Ecrire $P = AB$ où les racines de A sont des carrés dans $\mathbb{F}_p$ et celles de B ne le sont pas.
   b) Soient a, b deux racines (qu'on ne connait pas). On veut les séparer, c'est à dire écrire $P = AB$ avec a racine de A et b de B. Pour cela, on cherche un polynôme Q dont a ou b est racine mais pas l'autre, puis on prend le PGCD de P et Q. (On dit que Q sépare a et b.) Soit $c \in \mathbb{F}_p$ - distinct de a et de b. On pose $Q = (X - c)^{\frac{p-1}{2}} - 1$. Démontrer que Q sépare a et b si et seulement si $\dfrac{c-a}{c-b}$ n'est pas un carré.
   En choisissant c au hasard, on a donc une chance sur 2 de séparer a et b.
   c) Esquisser une méthode qui va nous permettre de trouver toutes les racines de P (le degré de P est ici supposé petit par rapport à p).

3.19 Exercice. (****) *Polynômes irréductibles dans $\mathbb{F}_p[X]$.*

1. *Fonction de Moebius.* On définit la fonction de Moebius $\mu : \mathbb{N}^* \to \mathbb{Z}$ en posant $\mu(n) = 0$ si n a des facteurs carrés, $\mu(1) = 1$ et $\mu(p_1 p_2 \dots p_n) = (-1)^n$ si les p_i sont des nombres premiers distincts.
   a) Démontrer que si m, n sont premiers entre eux, on a $\mu(mn) = \mu(m)\mu(n)$.
   b) Soient $(a_n)_{n\in\mathbb{N}^*}$ et $(b_n)_{n\in\mathbb{N}^*}$ des suites de nombres réels. Démontrer que l'on a $a_n = \sum_{d|n} b_d$ pour tout n si et seulement si on a $b_n = \sum_{d|n} \mu(\frac{n}{d}) a_d$ pour tout n.
2. On note Q l'ensemble des polynômes unitaires à coefficients dans $\mathbb{F}_p$ et P l'ensemble des polynômes unitaires irréductibles. On note N_n le nombre de polynômes unitaires irréductibles de degré n.
   a) Démontrer que pour $t \in]-1/p, 1/p[$ on a
   $$\frac{1}{1-pt} = \sum_{A\in Q} t^{\partial A} = \prod_{R\in P} \frac{1}{1-t^{\partial R}} = \prod_{n=1}^{+\infty} (1-t^n)^{-N_n}.$$
   b) Démontrer que $p^n = \sum_{d|n} d N_d$.

Indication : Prendre le logarithme - ou la dérivée logarithmique.

c) En déduire que $nN_n = \sum_{d|n} \mu(\frac{n}{d}) p^d$.

d) Remarquant que n a au plus $\frac{n}{2}$ diviseurs distincts de n tous $\leqslant \frac{n}{2}$, en déduire que $nN_n \geqslant p^{n/2}(p^{n/2} - n/2)$, puis que $N_n > 0$ pour tout $n > 0$.

e) En déduire l'existence d'un corps à p^n éléments.