Arithmétique

Parties du programme abordées : Parties 3.1 (extensions de la notion de nombre) et 3.2 (anneaux et corps).

Leçons concernées : 101, 103, 104, 106, 110, 159, 165, 169, 302, 304, 305, 306, 310, 349, 351, 357.

Références
COMBES, François, *Algèbre et géométrie*, Bréal.
DEMAZURE, Michel, *Cours d'algèbre*, Cassini.
FRANCINOU-GIANELLA, *Exercice de mathématiques pour l'agrégation, Algèbre 1*, Masson.
FRANCINOU-GIANELLA-NICOLAS, *Oraux X-ENS, algèbre 1 et 2*, Cassini.
KETRANE-ELINEAU, *Épreuve orale d'exemples et d'exercices*, Dunod.
DE KONINCK, MERCIER, *Introduction à la théorie de nombres*, Modulo.
MADERE, *Préparation à l'oral de l'agrégation*, Ellipses.
PERRIN, Daniel, *Cours d'algèbre*, ellipses.

Dans cette feuille, un anneau A est par défaut muni des lois $+$ et $\times$, avec les conventions usuelles de notation, les neutres sont notés 0 et 1, le groupe multiplicatif des éléments inversibles de A est noté $U(A)$.

On note $\mathrm{Div}\,(a)$ l'ensemble des diviseurs d'un élément a de A et aA l'ensemble de ses multiples, qui est l'idéal de A engendré par a (noté parfois (a)).

Pour tout entier $n \geq 2$, on note $\phi(n)$ le nombre l'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ (la fonction ϕ est l'indicatrice d'Euler). On montre par comptage que pour tout nombre premier p et tout entier $r \geq 1$, on a $\phi(p^r) = p^r - p^{r-1}$, puis l'isomorphisme du théorème chinois donne $\phi(p_1^{r_1} \dots p_k^{r_k}) = (p_1^{r_1} - p_1^{r_1 - 1}) \dots (p_k^{r_k} - p_k^{r_k - 1})$ où les p_i sont des nombres premiers deux à deux distincts.

Arithmétique dans les anneaux. Les fondamentaux.

Exercice 1

Montrer que dans un anneau fini, tout élément non nul est soit un diviseur de zéro, soit un inversible. En déduire qu'un anneau fini est un corps si et seulement si il est intègre.

Exercice 2

Soit A un anneau. On dit que deux éléments a, a' de A sont associés s'il existe un inversible e de A tel que $a' = ea$. C'est une relation d'équivalence sur A.

1. On suppose que A est intègre. Montrer l'équivalence entre les propriétés suivantes :

a. $a|a'$ et $a'|a$,

b. $aA = a'A$ (a et a' ont même multiples),

c. $\mathrm{Div}\,(a) = \mathrm{Div}\,(a')$ (a et a' ont mêmes diviseurs),

d. a et a' sont associés.

2. Quelles équivalences de la question précédente subsistent dans le cas où l'anneau A n'est pas intègre ? Donner un contre-exemple le cas échéant.

Exercice 3 *Identité de Bezout dans un anneau principal*

Soit A un anneau principal. Soient $a, b, c \in A$.

1. Montrer l'équivalence suivante :

$$\mathrm{Div}\,(a) \cap \mathrm{Div}\,(b) = \mathrm{Div}\,(c) \;\Leftrightarrow\; aA + bA = cA.$$

(relation de "dualité" entre les diviseurs et les multiples.)

2. En déduire que toute ensemble fini d'éléments d'un anneau principal possède un p.g.c.d. Que peut-on dire de l'unicité du p.g.c.d. ?

Conclusion : On dit que a et b sont premiers entre eux si $\mathrm{Div}\,(a) \cap \mathrm{Div}\,(b) = \{1\}$. D'après la première question, dans un anneau principal, c'est donc équivalent à $aA + bA = A$, donc à $1 \in aA + bA$, c'est-à-dire à l'identité de Bezout.

Exercice 4

Montrer que l'ensemble des décimaux $\mathbb{D} = \bigcup_{n \in \mathbb{N}} 10^{-n}\mathbb{Z}$ est un anneau pour $+$ et $\times$. Quels sont ses inversibles ?

Exercice 5 *Des anneaux non principaux*

1. Soit A un anneau. Montrer que $A[X]$ est principal si et seulement si A est un corps.

2. Donner des idéaux non principaux dans $\mathbb{R}[X, Y]$ et dans $\mathbb{Z}[X]$.

Exercice 6 *Inversibles dans $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[i\sqrt{2}]$*

On considère $\mathbb{Z}[\sqrt{2}] = \{P(\sqrt{2}),\ P \in \mathbb{Z}[X]\}$.

1. Montrer que $\mathbb{Z}[\sqrt{2}]$ est le sous-anneau de $\mathbb{C}$ engendré par $\sqrt{2}$ et que ses éléments sont de la forme $a + b\sqrt{2}$, $a, b \in \mathbb{Z}$. Montrer qu'il est intègre.

Pour tout $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, on note $\overline{a + b\sqrt{2})} = a - b\sqrt{2}$ et $N(a + b\sqrt{2}) = a^2 - 2b^2$.

2. Montrer que $x \mapsto \overline{x}$ et $x \mapsto N(x)$ sont multiplicatives (de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{2}]$ et de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}$ respectivement).

3. Montrer que $x \in \mathbb{Z}[\sqrt{2}]$ est inversible si et seulement si $N(x) = \pm 1$.

4. Montrer qu'il y a une infinité d'éléments inversibles dans $\mathbb{Z}[\sqrt{2}]$.

5. Que se passe-t-il si on remplace $\sqrt{2}$ par $i\sqrt{2}$?

Exercice 7 *$\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel*

On considère l'anneau $\mathbb{Z}[i\sqrt{5}] = \{P(i\sqrt{5}),\ P \in \mathbb{Z}[X]\}$.

En s'inspirant de l'exercice précédent, définir une norme sur cet anneau et montrer que l'élément 9 possède deux écritures non équivalentes comme produit d'éléments irréductibles. En déduire que cet anneau n'est pas factoriel.

On étudiera plus loin l'anneau $\mathbb{Z}[i]$, appelé anneau des entiers de Gauss, pour étudier l'équation diophantienne $x^2 + y^2 = p$, avec p premier.

Les algorithmes de base et applications.

Exercice 8 *Algorithme d'Euclide étendu (théorie)*

Pour tous entiers $x, y \in \mathbb{Z}$, $y \neq 0$, on note $q(x,y)$ et $r(x,y)$ le quotient et le reste de la division euclidienne de x par y.

1. Montrer que pour tout $a, b \in \mathbb{Z}$, $a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + r(a,b)\mathbb{Z}$.

Soient a et b deux entiers tels que $a \geq b > 0$.

On considère les suites récurrentes $(r_n)_{n\geq -1}$, $(u_n)_{n\geq -1}$, $(v_n)_{n\geq -1}$, $(q_n)_{n\geq 1}$, définie de la manière suivante (algorithme d'Euclide étendu) :

1. $r_{-1} = a,\ r_0 = b, u_{-1} = 1,\ u_0 = 0,\ v_0 = 0,\ v_{-1} = 1,$
2. $\forall n \in \mathbb{N}$, si $r_n \neq 0$, alors
   (a) $q_{n+1} = q(r_{n-1}, r_n)$,
   (b) $r_{n+1} = r(r_{n-1}, r_n) = r_{n-1} - q_{n+1} r_n$,
   (c) $u_{n+1} = u_{n-1} - q_{n+1} u_n$,
   (d) $v_{n+1} = v_{n-1} - q_{n+1} v_n$,

   sinon $r_{n+1} = q_{n+1} = u_{n+1} = u_{n+1} = 0$.

2. Montrer que la suite $(r_n)_{n\geq -1}$ est strictement décroissante jusqu'à un rang N à partir duquel elle est identiquement nul.

3. Montrer que pour tout entier n compris entre -1 et N, on a $a\mathbb{Z} + b\mathbb{Z} = r_{n-1}\mathbb{Z} + r_n\mathbb{Z} = r_{N-1}\mathbb{Z}$.

4. Montrer que pour tout $n \geq -1$, on a $r_n = u_n a + v_n b$. Laquelle de ces égalités est une identité de Bezout pour a et b ?

Exercice 9 *Algorithme d'Euclide étendu (application)*

1. Pour chacunes des familles suivantes dans $\mathbb{Z}$, déterminer le pgcd et une identité de Bezout :

a. 126 et 230. **b.** 427 et 715. **c.** 180, 606 et 750. **d.** 342, 405 et 720.

2. Pour chacunes des familles suivantes dans $\mathbb{R}[X]$, déterminer le pgcd unitaire et une identité de Bezout :

a. X^2+1 et X^2+X+1. **b.** $X^6-2X^5+2X^4-3X^3+3X^2-2X$ et $X^4-2X^3+X^2-X+1$.

c. $X^4+X^3-X^2-2X-2$ et $X^5+X^4+X^3-3X^2-3X-3$.

Exercice 10 *Deux algorithmes d'Euclide*

Soient $a, b \in \mathbb{N}$. Montrer que $\mathrm{pgcd}\,(X^a-1, X^b-1) = X^{\mathrm{pgcd}\,(a,b)} - 1$.

Exercice 11 *Décomposition en facteurs premiers ou algorithme d'Euclide ?*

1. Trouver les factorisations en nombres premiers de 1961 et 2027. Donner le nombre de divisions euclidiennes effectuées. En déduire pgcd(1961,2027).

2. Comparer le nombre de divisions effectuées par cette méthode et par l'algorithme d'Euclide pour calculer le pgcd de ces deux nombres.

Exercice 12 *Coût de l'algorithme d'Euclide et suite de Fibonacci*

A. Une majoration simple.

Pour tous entiers $x, y \in \mathbb{N} \setminus \{0\}$, on note $r(x, y)$ le reste de la division euclidienne de x par y.

1. Montrer que si $x \geq y$, alors $r(x, y) < \frac{x}{2}$.

Soient a et b deux entiers tels que $a \geq b > 0$. On considère la suite récurrente suivante (algorithme d'Euclide pour calculer le pgcd de a et b) :

$$r_{-1} = a, \; r_0 = b$$
$$\forall n \in \mathbb{N}, \text{ si } r_n \neq 0, \text{ alors } r_{n+1} = r(r_{n-1}, r_n), \text{ sinon } r_{n+1} = 0.$$

2. Montrer que pour tout entier $k \geq 1$, on a $r_{2k} < \frac{b}{2^k}$.

On note N le nombre de divisions effectuées dans l'algorithme d'Euclide pour a et b, c'est-à-dire le plus petit entier k tel que $r_k = 0$ dans la suite définie précédemment, et L le nombre de chiffres de l'écriture en base 2 de b.

3. Montrer que $2^{L-1} \leq b < 2^L$ et que $N < 2L$.

Cette inégalité exprime que le temps de calcul d'un pgcd par l'algorithme d'Euclide contrôlé par le double du nombre de chiffres en écriture binaire du plus petit des deux entiers. La suite du problème améliore ce résultat à l'aide d'une majoration par la suite de Fibonacci.

B. Le théorème de Lamé, 1845 [Demazure, p.25].

On considère la suite de Fibonacci $(F_n)_{n \in \mathbb{N}}$ définie par :

$$F_0 = 1, \; F_1 = 1$$
$$\forall n \in \mathbb{N}, \; F_{n+2} = F_n + F_{n+1}.$$

4. Montrer que pour tout n tel que $0 \leq n \leq N - 1$, on a $r_n \geq F_{N-n}$. En déduire que $b \geq F_N$.

5. Sachant que $F_n = \frac{1}{\sqrt{5}}(\phi^n - (1 - \phi)^n)$ avec $\phi = \frac{\sqrt{5}+1}{2}$, en déduire que $N \leq \frac{3}{2}L + 1$.

Exercice 13 *Calcul de puissance : exponentiation rapide vs théorème d'Euler*

A. Dans cete partie on se place dans l'anneau $\mathbb{Z}/91\mathbb{Z}$.

1. Calculer $\overline{2}^{1032}$ à l'aide de l'algorithme d'exponentiation rapide.

2. Montrer que $\overline{2}$ est inversible dans $\mathbb{Z}/91\mathbb{Z}$ et déterminer l'ordre de $\overline{2}$ dans le groupe $(\mathbb{Z}/91\mathbb{Z})^*$. Comment peut-on en déduire que 91 n'est pas un nombre premier ?

B. Dans cette partie on se place dans l'anneau $\mathbb{Z}/201\mathbb{Z}$.

3. Calculer à l'aide de l'algorithme d'exponentiation rapide $\overline{2}^{261}$.

4. a. Calculer $\phi(201)$.

b. Montrer que $\overline{2}$ est inversible dans $\mathbb{Z}/201\mathbb{Z}$, déterminer l'ordre de $\overline{2}$ dans le groupe $U(\mathbb{Z}/201\mathbb{Z})$ et calculer $\overline{2}^{261}$.

Exercice 14 *Théorème des restes chinois (1)*

On considère l'application suivante :

$$\begin{array}{rccc} \Phi : & \mathbb{Z}/20\mathbb{Z} & \to & \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z} \\ & \overline{x} & \mapsto & (\overline{x},\overline{x}) \end{array}$$

où $\overline{x}$ désigne la classe de l'entier x dans l'anneau considéré.

1. Donner les images par Φ de tous les éléments de $\mathbb{Z}/20\mathbb{Z}$ et constater que Φ est bien une bijection.

2. Résoudre :

a. $\left\{\begin{array}{lll} x & \equiv & 2 \ [4] \\ x & \equiv & 4 \ [5] \end{array}\right.$ **b.** $\left\{\begin{array}{lll} x & \equiv & 1 \ [4] \\ x & \equiv & 2 \ [5] \end{array}\right.$

On rappelle que $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ muni des lois $+$ et $\times$ produits, définies par

$$(x,y)+(x',y')=(x+x',y+y'),\ (x,y)\times(x',y')=(x\times x',y\times y'),$$

est un anneau, dont les inversibles sont $U(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z})=U(\mathbb{Z}/4\mathbb{Z})\times U(\mathbb{Z}/5\mathbb{Z})$.

3. Déterminer les éléments inversibles de $\mathbb{Z}/20\mathbb{Z}$ et ceux de $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$, et constater qu'ils sont en relation par Φ.

4. Trouver l'inverse de $\overline{13}$ dans $\mathbb{Z}/20\mathbb{Z}$ en utilisant l'image par Φ de $\overline{13}$ dans $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$.

Exercice 15 *Théorème des restes chinois (2)*

1. Résoudre les systèmes suivants en $x\in\mathbb{Z}$:

a. $\left\{\begin{array}{lll} x & \equiv & 3 \ [8] \\ x & \equiv & 6 \ [27] \end{array}\right.$ **b.** $\left\{\begin{array}{lll} x & \equiv & 1 \ [2] \\ x & \equiv & 2 \ [3] \\ x & \equiv & 3 \ [4] \\ x & \equiv & 4 \ [5] \end{array}\right.$ **c.** $\left\{\begin{array}{lll} x & \equiv & 5 \ [6] \\ x & \equiv & 7 \ [9] \end{array}\right.$

d. $\left\{\begin{array}{lll} x & \equiv & 4 \ [6] \\ x & \equiv & 7 \ [9] \end{array}\right.$ **e.** $\left\{\begin{array}{lll} x & \equiv & 38 \ [60] \\ x & \equiv & 14 \ [42] \end{array}\right.$

2. Donner une condition nécessaire et suffisante pour que le système : $\left\{\begin{array}{lll} x & \equiv & a \ [n] \\ x & \equiv & b \ [m] \end{array}\right.$ ait une solution et décrire l'ensemble des solutions.

Exercice 16 *Le protocole RSA [FGFPM], [Ketrane,Elineau]*

Soient p, q deux nombres premiers distincts.

1. Montrer que pout tout $a\in\mathbb{Z}$ non divisible par p ou q, on a $a^{(p-1)(q-1)}\equiv 1\ [pq]$.

2. Soit $d\in\{1,\ldots,(p-1)(q-1)\}$ premier avec $(p-1)(q-1)$. Montrer qu'il existe $e\in\{1,\ldots,(p-1)(q-1)\}$ tel que $ed\equiv 1\ [(p-1)(q-1)]$.

3. Montrer que pout tout $a\in\mathbb{Z}$, on a $a^{de}\equiv a\ [pq]$.

Exercice 17 *Indicatrice d'Euler et factorisation*

1. Déterminer $\phi(10836)$.

2. **a.** Soient p,q deux nombres premiers distincts et $n=pq$. Déterminer p et q en fonction de n et $\phi(n)$.

b. Sachant que $\phi(17063)=16800$, factoriser 17063.

Arithmétique des entiers.

Exercice 18

Soient $a,b\in\mathbb{N}$. Montrer que 2^a-1 divise $2^{ab}-1$. En déduire que pour tout entier naturel p, si 2^p-1 est premier, alors p est premier.

Exercice 19

1. Quels sont les entiers relatifs de la forme $3k+5l$, avec $k,l \in \mathbb{Z}$?

2. Montrer que tous les entiers supérieurs ou égaux à 8 sont de la forme $3k+5l$, avec $k,l \in \mathbb{N}$.

Exercice 20

Soit $n \in \mathbb{Z}$. Quelle est la classe de $(n-1)!$ modulo n ?

Exercice 21

Montrer que $2^{2005}+5^{2005}$ est divisible par 41.

Exercice 22 *Équations diophantiennes de degré 1.*

1. Résoudre les équations diophantiennes suivantes :

a. $7x-9y=1$ **b.** $11x+17y=5$ **c.** $21x-49y=12$ **d.** $21x-49y=14$.

2. Un restaurant propose des menus à 13 et 19 euros. Si la recette de la journée est de 1000 euros, peut-on connaître le nombre de clients ayant choisi le menu à 13 euros et le nombre de clients ayant pris celui à 19 euros ?

3. Résoudre les équations suivantes dans $\mathbb{Z}/24\mathbb{Z}$:

a. $\overline{7}x=\overline{4}$ **b.** $\overline{15}x=\overline{5}$ **c.** $\overline{10}x=\overline{4}$.

Exercice 23 *L'équation diophantienne $x^2-y^2=n$.*

1. Résoudre l'équation diophantienne $x^2-y^2=p$ en $x,y \in \mathbb{Z}$, avec p premier.

2. Résoudre l'équation diophantienne $x^2-y^2=15$ en $x,y \in \mathbb{Z}$.

Exercice 24 *L'équation diophantienne $x^2+y^2=p$. Entiers de Gauss.*

Le problème est de déterminer les entiers qui s'écrivent comme somme de deux carrés. On se restreindra ici au cas des entiers premiers, le cas général s'en déduisant (voir [Perrin] p.56).

Soit $\Sigma = \{n \in \mathbb{N} \mid n = x^2+y^2,\ x,y \in \mathbb{N}\}$.

1. Déterminer les carrés de $\mathbb{Z}/4\mathbb{Z}$ et en déduire que si $n \in \Sigma$, alors $n \not\equiv 3\ [4]$.

2. Montrer que $2 \in \Sigma$ et que 2 n'est pas irréductible dans $\mathbb{Z}[i]$.

Pour mimer la méthode de l'exercice précédent dans $\mathbb{Z}$, on est naturellement conduit à étudier les éléments irréductibles de $\mathbb{Z}[i]$.

A. *La norme et les inversibles de $\mathbb{Z}[i]$.*

On considère l'application $N : \mathbb{Z}[i] \to \mathbb{N}$, appelée "norme", définie par $N(a+ib)=a^2+b^2$.

3. Montrer que N est multiplicative : pour tout $z,z' \in \mathbb{Z}[i]$, on a $N(z\,z')=N(z)\,N(z')$.

4. Déterminer $U(\mathbb{Z}[i])$.

5. En déduire qu'un nombre premier p appartient à Σ si et seulement si il n'est pas irréductible dans $\mathbb{Z}[i]$.

B. *L'anneau $\mathbb{Z}[i]$ est euclidien (donc principal, donc factoriel).*

6. Montrer que tout nombre complexe z est à distance euclidienne inférieure ou égale à $\frac{\sqrt{2}}{2}$ d'un élément de $\mathbb{Z}[i]$.

7. En déduire qu'il existe une division euclidienne dans $\mathbb{Z}[i]$ relativement à la norme N :

$$\forall a,b \in \mathbb{Z}[i],\ b \neq 0,\ \exists c,r \in \mathbb{Z}[i] \text{ tels que } a=bc+r \text{ et } N(r)<N(b)$$

(sans nécessairement unicité).

8. Faire la division euclidienne de $3+2i$ par $1-3i$ dans $\mathbb{Z}[i]$.

C. *Quotient par l'idéal engendré par un élément non irréductible.*

Soit p un nombre premier.

9. Montrer que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $\mathbb{Z}[i]/(p)$ est intègre (indication : utiliser le fait que l'anneau $\mathbb{Z}[i]$ est euclidien, donc factoriel).

10. En utilisant l'isomorphisme $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2+1)$ (voir exercice en fin de feuille), en déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si le polynôme X^2+1 n'a pas de racine dans $\mathbb{F}_p$.

11. En déduire pour tout nombre premier p impair l'équivalence des propriétés suivantes :

a. p appartient à Σ

b. -1 est un carré dans $\mathbb{F}_p$

c. $(-1)^{\frac{p-1}{2}} = 1$

d. $p \equiv 1$ [4].

Les nombres premiers qui appartiennent à Σ sont donc 2 et les nombres premiers p tels que $p \equiv 1$ [4].

Exercice 25 *Témoins de non primalité (1)*

Soit $(N_n)_{n\in\mathbb{N}}$ une suite d'entiers produits de deux nombres premiers distincts p_n et q_n. On suppose que p_n et q_n tendent vers l'infini quand n tend vers l'infini. Montrer que la probabilité qu'un entier $a < N_n$ ne soit pas premier à N_n tend vers 0 quand n tend vers l'infini.

Exercice 26 *Témoins de Fermat (2) [Demazure]*

Soit n un entier non premier. On dit que a est un *témoin de Fermat* de non-primalité de n si $n \wedge a = 1$ et $a^{n-1} \not\equiv 1$ $[n]$.

On suppose que $n = pq$ où p et q sont deux nombres premiers distincts tels que $\operatorname{pgcd}(p-1, q-1) = 2$. Montrer que 2 est un témoin de Fermat de n.

Exercice 27 *Témoins de Fermat (3) [Demazure]*

Soit $n \geq 2$ un entier. Montrer que soit n ne possède aucun témoin de Fermat, soit il en possède au moins $\frac{n}{2}$ (indication : utiliser un sous-groupe de $U(\mathbb{Z}/n\mathbb{Z})$.

Arithmétique et groupes

Exercice 28 *Sous-groupes finis de $\mathbb{K}^*$ (1) [FGN p.41]*

Soit G un groupe abélien fini. Pour tout $x \in G$, on note $\operatorname{ord}(x)$ l'ordre de x dans G.

1. Soient $x, y \in G$, $m = \operatorname{ord}(x)$, $n = \operatorname{ord}(y)$. Montrer que si $\operatorname{pgcd}(n, m) = 1$, alors $\operatorname{ord}(xy) = nm$.

2. Soient $m, n \in \mathbb{N} \setminus \{0\}$. Montrer qu'il existe $m', n' \in \mathbb{N} \setminus \{0\}$ tels que $\operatorname{pgcd}(n', m') = 1$ et $\operatorname{ppcm}(n, m) = n'm'$.

3. Montrer qu'il existe $u \in G$ tel que $\operatorname{ord}(u)$ est égal au ppcm des ordres des éléments de G (appelé exposant de G).

4. Montrer que tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif) est cyclique.

Exercice 29 $n = \sum_{d|n} \psi(n)$

Soit $n \geq 2$ un entier. On va montrer que $n = \sum_{d|n} \psi(n)$ de deux manières différentes.

A. Comptage dans les groupes cycliques

1. Montrer que tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est de cardinal un diviseur d de n.

2. Réciproquement, pour tout $d|n$, montrer qu'il existe un unique sous-groupe de cardinal d de $\mathbb{Z}/n\mathbb{Z}$, et que ce sous-groupe est cyclique.

3. Montrer que le groupe $\mathbb{Z}/d\mathbb{Z}$ possède exactement $\psi(d)$ générateurs.

4. En déduire que $n = \sum_{d|n} \psi(n)$.

5. Déterminer tous les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ et vérifier la formule précédente.

B. Comptage dans les fractions rationnelles

Exercice 30 *Sous-groupes finis de $\mathbb{K}^*$ (2) [Perrin, p.74]*

Déduire de la formule de l'exercice précédent que tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif) est cyclique.

Arithmétique des polynômes.

Exercice 31 *Anneau des polynômes sur le corps fini $\mathbb{F}_p$.*

Soit p un nombre premier.

1. Montrer l'égalité suivante dans l'anneau des polynômes à coefficients dans le corps $\mathbb{Z}/p\mathbb{Z}$:

$$\prod_{i=0}^{n-1}(X-\bar{i}) = X^p - X.$$

2. En déduire que $(p-1)! \equiv -1$ $[p]$ (théorème de Wilson).

3. En déduire également que $(X+\bar{1})^p = X^p+\bar{1}$ (indication : montrer que $(X+\bar{1})^p-(X+\bar{1}) = X^p-X$).

Exercice 32 *Racines d'un polynôme de $\mathbb{Z}[X]$ ou $\mathbb{Q}[X]$*

Soit $P(X) = a_nX^n + \cdots + a_0$ un polynôme de $\mathbb{Q}[X]$ dont les coefficients $a_0, \ldots, a_n$ sont entiers.

1. Montrer que si un rationnel $x = \frac{p}{q}$ est racine de P, où p et q sont des entiers premiers entre eux, alors p divise a_0 et q divise a_n.

2. Les polynômes suivants de $\mathbb{Q}[X]$ ont-ils des racines dans $\mathbb{Q}$?

a. $5X^3 + X^2 - 1$ **b.** $X^4 + 3X^3 - 3X^2 - 12X - 4$

Exercice 33 *Un algorithme de factorisation dans $\mathbb{Z}[X]$ [ref ?]*

On considère le polynôme $P(X) = X^5 + X^4 + 2X^2 - 1$.

1. Montrer que si P est irréductible dans $\mathbb{Z}[X]$, alors il existe un polynôme de degré au plus deux qui divise P dans $\mathbb{Z}[X]$.

2. Soit $Q \in \mathbb{Z}[X]$ un polynôme de degré au plus 2 et qui divise P. Calculer $P(0)$, $P(1)$ et $P(-1)$. En déduire toutes les valeurs possibles pour $Q(0)$, $Q(1)$ et $Q(-1)$, donc toutes les valeurs possibles de Q.

3. Factoriser P dans $\mathbb{Z}[X]$.

Exercice 34 *(irréductibilité par réduction modulo 2 et 3)*

On considère le polynôme $P(X) = X^5 - 6X^3 + 2X^2 - 4X + 5$ de $\mathbb{Z}[X]$.

En le réduisant modulo 2 et 3, montrer que ce polynôme est irréductible.

Exercice 35 *Anneau des polynômes sur un anneau non intègre et lemme chinois.*

1. Déterminer les racines du polynôme $X^2 - \bar{1}$ de $(\mathbb{Z}/15\mathbb{Z})[X]$, en remarquant qu'une racine est un élément de $U(\mathbb{Z}/15\mathbb{Z})$.

2. Soit n un entier impair, $n \geq 3$. Montrer que le nombre de racines du polynôme $X^2-\bar{1}$ de $(\mathbb{Z}/n\mathbb{Z})[X]$ est 2^k où k est le nombre de facteurs premiers de la décomposition de n (indication : réduire l'équation $x^2 - 1 \equiv 0$ $[n]$ aux diviseurs de n).

Exercice 36 *Isomorphismes et quotients.*

Pour tout $\omega \in \mathbb{C}$, on note $\mathbb{Z}[\omega] = \{P(\omega),\ P \in \mathbb{Z}[X]\}$.

1. Décrire les éléments de $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Z}[j]$, $\mathbb{Z}[\pi]$.

2. Montrer que les anneaux suivants sont isomorphes :

a. $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[X]/(X^2 - 2)$. **b.** $\mathbb{Z}[i]$ et $\mathbb{Z}[X]/(X^2 + 1)$.

3. Décrire $\mathbb{Z}[j]$, $\mathbb{Z}[1 + i]$ comme des quotients de l'anneau $\mathbb{Z}[X]$.

4. Décrire l'anneau $\mathbb{Z}[X]/(10X - 1)$ comme un sous-anneau de $\mathbb{C}$.

5. Montrer les isomorphismes suivants pour p premier et d entier, $d \geq 1$:

$$\mathbb{Z}[i\sqrt{d}]/(p) \simeq \mathbb{Z}[X]/(X^2 + d, p) \simeq \mathbb{F}_p[X]/(X^2 + d).$$