Anneaux et arithmétique

Compléments sur les anneaux

1. Produit fini d'anneaux.
2. Idéal d'un anneau commutatif. Idéal engendré par un élément. Noyau d'un morphisme d'anneaux commutatifs.
3. Divisibilité dans un anneau commutatif intègre et interprétation en termes d'idéaux.

Idéaux de $\mathbb{Z}$

4. Idéaux de $\mathbb{Z}$.
5. PGCD de n entiers relatifs : définition en termes d'idéaux et relation de Bézout.

Anneaux $\mathbb{K}[X]$ où $\mathbb{K}$ est un sous-corps de $\mathbb{C}$

6. Idéaux de $\mathbb{K}[X]$.
7. PGCD de n polynômes : définition en termes d'idéaux et relation de Bézout. Par convention, le PGCD est unitaire.
8. Irréductibles de $\mathbb{K}[X]$, et en particulier irréductibles de $\mathbb{C}[X]$, irréductibles de $\mathbb{R}[X]$.
9. Existence et unicité de la décomposition en facteurs irréductibles unitaires.

Anneaux $\mathbb{Z}/n\mathbb{Z}$

10. Inversibles de $\mathbb{Z}/n\mathbb{Z}$. Condition nécessaire et suffisante pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Notation $\mathbb{F}_p$.
11. Théorème chinois : isomorphisme naturel de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si $m \wedge n = 1$. Généralisation à plus de deux facteurs. Application aux systèmes de congruences et à la résolution de systèmes d'équations dans $\mathbb{Z}/n\mathbb{Z}$.
12. Indicatrice d'Euler φ. Calcul à l'aide de la décomposition en produits de facteurs premiers (après avoir établi les expressions de $\varphi(p^k)$ pour p premier, et $\varphi(mn)$ pour $m \wedge n = 1$).
13. Théorème d'Euler et lien avec le petit théorème de Fermat.

Algèbres

14. Algèbre et sous-algèbre. Exemples : $\mathbb{K}[X]$, $\mathscr{L}(E)$, $\mathcal{M}_n(\mathbb{K})$, $\mathcal{F}(X, \mathbb{K})$.
15. Morphisme d'algèbres.

Sauf mention explicite du contraire, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

1 Révisions

Définition 1

Soit A un ensemble muni de deux lois de composition internes : une loi notée additivement, $+$, et une loi notée multiplicativement, $\times$. On dit que $(A, +, \times)$ est un *anneau* lorsque

— $(A, +)$ est un groupe commutatif, d'élément neutre noté 0_A ou 0,

— $\times$ est une loi associative,

— $\times$ admet un élément neutre 1_A ou 1,

— $\times$ est distributive par rapport à $+$

Un élément $a \in A$ est dit *inversible* lorsqu'il est inversible pour la loi $\times$. Un anneau $(A, +, \times)$ est dit *commutatif* lorsque $\times$ est commutative.

Par exemple,

- $(\mathbb{C}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$ et $(\mathbb{Z}, +, \times)$ sont des anneaux commutatifs.
- $(\mathcal{M}_n(\mathbb{R}), +, \times)$ est un anneau de neutres 0_n et I_n.
- Si E est un $\mathbb{K}$-espace vectoriel, $(\mathscr{L}(E), +, \circ)$ est un anneau de neutres $0_{\mathscr{L}(E)}$ et Id_E.
- Si $(A, +, \times)$ est un anneau et X est un ensemble, l'ensemble $\mathcal{F}(X, A)$ des fonctions de X dans A, muni des lois $+$ et $\times$ définies par

$$\begin{aligned} \forall f, g \in \mathcal{F}(X, A),\ \forall x \in X,\ (f+g)(x) &= f(x) + g(x), \\ (f \times g)(x) &= f(x) \times g(x) \end{aligned}$$

  est un anneau. En particulier, $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$ et $(\mathbb{R}^{\mathbb{N}}, +, \times)$ sont des anneaux commutatifs.
- $\{0\}$ est un anneau. Dans cet anneau, $0_A = 1_A$.

Pour la multiplication dans un anneau, on omet souvent le signe $\times$. Vous avez eu l'habitude avec les matrices : $A \times B$ était notée AB.

Propriété 1 – calculs élémentaires

Soit $(A, +, \times)$ un anneau. Pour a et b dans A, on a

$$\begin{array}{lll} & 0_A \times a = 0_A \quad \text{et} \quad a \times 0_A = 0_A & \\ \forall n \in \mathbb{Z}, & (n \cdot a)\, b = a\, (n \cdot b) = n \cdot (ab) & \text{et en particulier, } -(ab) = (-a)b = a(-b) \\ & (-a)(-b) = ab & \text{et en particulier, } (-1_A)^2 = 1_A \end{array}$$

Propriété 2

Soit $(A, +, \times)$ un anneau et $a, b \in A$ tels que $a \times b = b \times a$. Alors, pour tout $n \in \mathbb{N}$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot \left(a^{n-k} \times b^k\right) \quad \text{et} \quad a^n - b^n = (a-b) \times \left[\sum_{k=0}^{n-1} a^{(n-1)-k} \times b^k\right]$$

Définition 2

On dit qu'un élément $a \in A$ est nilpotent lorsqu'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.

✎ Exercice 1 : Montrer que si x est nilpotent, alors $1 - x$ est inversible.

Définition 3

Un élément a de l'anneau $(A, +, \times)$ est inversible s'il existe $b \in A$ tel que

$$ab = ba = 1$$

Cet élément b est alors unique, on l'appelle inverse de a et on le note a^{-1}.

Propriété 3 – groupe des unités

L'ensemble $U(A)$ des éléments inversibles de l'anneau A est un groupe pour la multiplication.

Par exemple, $U(\mathbb{Z}) =$, $U(\mathbb{K}) =$, $U(\mathcal{M}_n(\mathbb{K})) =$, $U(\mathscr{L}(E)) =$

Exercice 2 : Déterminer l'ensemble des éléments inversibles de $\mathbb{K}[X]$.

Définition 4

On dit qu'un anneau $(A, +, \times)$ est *intègre* lorsque c'est un anneau commutatif non nul dans lequel on a l'implication :

$$a \times b = 0 \Rightarrow (a = 0 \text{ ou } b = 0)$$

$\mathbb{Z}$ et $\mathbb{K}[X]$ sont des anneaux intègres.

Exercice 3 :

1. Montrer que $\mathcal{M}_3(\mathbb{R})$ n'est pas un anneau intègre.
2. Montrer que l'anneau $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$ n'est pas intègre.

Définition 5

Soit $(A, +, \times)$ un anneau et B une partie de A. On dit que B est un *sous-anneau* de A lorsque B est stable à la fois pour $+$ et pour $\times$, B contient 1_A et $(B, +, \times)$ est un anneau.

Votre œil de lynx aura remarqué qu'il ne suffit pas de demander que B soit un anneau contenu dans A...

Propriété 4

Soit $(A, +, \times)$ un anneau et B une partie de A.

$$B \text{ est un sous-anneau de } A \Leftrightarrow \begin{cases} 1_A \in B \\ B \text{ est stable par différence :} & \forall x, y \in B,\ x - y \in B \\ B \text{ est stable par produit :} & \forall x, y \in B,\ xy \in B \end{cases}$$

Exercice 4 : Soit A un anneau. Montrer que l'ensemble (appelé centre de A) $C(A) = \{a \in A \,|\, \forall b \in A,\ ab = ba\}$ est un sous-anneau de A.

Définition 6

On appelle *corps* tout anneau commutatif non nul dans lequel tout élément non nul est inversible.

Muni des lois usuelles d'addition et de multiplication, $\mathbb{C}$ est un corps, de même que $\mathbb{R}$ et que $\mathbb{Q}$. Tout corps est intègre.

Définition 7

Soient A et B deux anneaux et $f : A \to B$. f est un *morphisme d'anneaux* si :

$$f(1_A) = 1_B, \qquad \forall x, y \in A,\ f(x+y) = f(x) + f(y) \quad \text{et } f(xy) = f(x)f(y)$$

Si f est un morphisme d'anneaux, f est un morphisme de groupes pour l'addition, donc

$$f(0_A) = 0_B \quad f(-x) = -f(x) \quad \text{et pour } n \in \mathbb{Z},\ f(nx) = nf(x)$$

Comme dans le cas des groupes, la composée de deux morphismes d'anneaux est un morphisme d'anneaux et l'image directe/réciproque d'un sous-anneau par un morphisme d'anneau est un sous-anneau. On définit également les notions d'isomorphisme d'anneaux, d'automorphisme d'anneau et d'anneaux isomorphes. Il reste vrai que la composée de deux isomorphismes est un isomorphisme et que la réciproque d'un isomorphisme est un isomorphisme.

Exercice 5 : Soit $P \in \mathrm{GL}_n(\mathbb{K})$. Montrer que $f : M \mapsto P^{-1}MP$ est un morphisme d'anneaux de $\mathcal{M}_n(\mathbb{K})$.

2 Produit fini d'anneaux

Soient $(A_1, +, \times), \ldots, (A_n, +, \times)$ des anneaux et $A = A_1 \times A_2 \times \cdots \times A_n$. On définit des lois $+$ et $\times$ sur A en posant :

$$\begin{aligned}(x_1, \ldots, x_n) + (y_1, \ldots, y_n) &= (x_1 + y_1, \ldots, x_n + y_n)\\ (x_1, \ldots, x_n) \times (y_1, \ldots, y_n) &= (x_1 \times y_1, \ldots, x_n \times y_n)\end{aligned}$$

Propriété 5

L'ensemble A muni des lois $+$ et $\times$ définies ci-dessus est un anneau de neutres

$$0_A = (0_{A_1}, \ldots, 0_{A_n}) \quad \text{et} \quad 1_A = (1_{A_1}, \ldots, 1_{A_n})$$

Dans cet anneau produit, un élément $(a_1, \ldots, a_n)$ est inversible si, et seulement si, $a_1, \ldots, a_n$ sont inversibles. Dans ce cas, on a :

$$(a_1, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1})$$

On a donc $U(A) = U(A_1) \times U(A_2) \times \cdots \times U(A_n)$.

Par exemple, $(\mathbb{R}^n, +, \times)$ est un anneau d'éléments neutres $(0, \ldots, 0)$ et $(1, \ldots, 1)$.

3 Idéal d'un anneau commutatif

Définition 8

Soit $(A, +, \times)$ un anneau commutatif. Une partie I de A est un *idéal* de A si

$$\begin{cases} I & \text{est un sous-groupe de } (A, +) \\ I & \text{est absorbant : pour tout } (a, x) \in A \times I,\ a \times x \in I \end{cases}$$

Par exemple, $\{0\}$ est un idéal de A. Dès qu'un idéal contient 1_A, il est égal à

Exercice 6 : Montrer que pour I et J idéaux de A, la somme $I + J$ est un idéal.
On montre de même facilement que pour I et J idéaux de A, l'intersection $I \cap J$ est un idéal.

Définition - propriété 1

Soit $\varphi : A \to A'$ un morphisme d'anneaux commutatifs. Le noyau de φ est

$$\ker \varphi = \{x \in A \mid \varphi(x) = 0_{A'}\}$$

Le noyau de φ est un idéal de A.

Définition - propriété 2

Soit x un élément d'un anneau commutatif A. L'ensemble :

$$xA = \{xa \mid a \in A\}$$

est le plus petit idéal de A contenant x. C'est l'intersection de tous les idéaux de A qui contiennent x. On l'appelle *idéal engendré par* x.

4 Divisibilité dans un anneau commutatif intègre

Soit $(A, +, \times)$ un anneau commutatif intègre.

Définition 9

Soient a et b deux éléments de A.
On dit que a divise b (ou que b est multiple de a) s'il existe $u \in A$ tel que $b = au$. On note alors $a|b$.

On retrouve des divisibilités déjà connues : $2|8$ dans $\mathbb{Z}$, $(X-1)|(X^2-1)$ dans $\mathbb{R}[X]$.
La relation de divisibilité est réflexive et transitive, mais en général, elle n'est ni symétrique ni antisymétrique.

Propriété 6

$$x|y \quad \Leftrightarrow \quad yA \subset xA$$

Par conséquent, deux éléments engendrent le même idéal si, et seulement si, ils se divisent mutuellement. On dit qu'ils sont *associés*.

Exercice 7 : Pour a et b éléments de A anneau commutatif intègre, montrer que si a divise b et b divise a (a et b sont associés), alors il existe u inversible de A tel que $b = ua$.

5 L'anneau $\mathbb{Z}$ et ses idéaux

Propriété 7

Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, pour $n \in \mathbb{N}$.

Remarque :
$n\mathbb{Z} = m\mathbb{Z} \Leftrightarrow (n|m \text{ et } m|n) \Leftrightarrow n = \pm m$. Avec n et m dans $\mathbb{N}$, $n\mathbb{Z} = m\mathbb{Z}$ si et seulement si $n = m$.

Propriété 8 – plus grand diviseur commun

Soit $a, b \in \mathbb{Z}$.
Il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On a pour $k \in \mathbb{Z}$:

$$k|d \quad \Leftrightarrow \quad (k|a \text{ et } k|b)$$

d est appelé PGCD de a et b et noté $a \wedge b$. On a une relation de Bézout :

$$\exists (u, v) \in \mathbb{Z}^2, \quad au + bv = d$$

Les diviseurs communs à a et b sont donc exactement les diviseurs de d. Et lorsque a ou b est non nul, d est le plus grand parmi tous les diviseurs positifs communs à a et b.
Cette définition du PGCD est équivalente à la définition du PGCD vue en première année.

Propriété 9

Pour $a_1, \dots, a_n$ entiers relatifs, il existe un unique entier naturel d tel que

$$d\mathbb{Z} = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$$

Pour tout $k \in \mathbb{Z}$,

$$k|d \quad \Leftrightarrow \quad (\forall i \in [\![1, n]\!],\ k|a_i)$$

d est le PGCD de $a_1, \dots, a_n$.

Propriété 10

Pour $a_1, \dots, a_n$ entiers relatifs, il existe un unique entier naturel m, appelé PPCM de $a_1, \dots, a_n$, tel que

$$m\mathbb{Z} = a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}$$

6 L'anneau $\mathbb{K}[X]$

Définition - propriété 3

Soient P et Q deux polynômes de $\mathbb{K}[X]$. Ces polynômes sont *associés* s'ils vérifient une des assertions équivalentes suivantes :

1. $P|Q$ et $Q|P$
2. il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$

Par exemple, tout polynôme non nul de $\mathbb{K}[X]$ est associé à un unique polynôme unitaire, le polynôme obtenu par

6.1 l'anneau $\mathbb{K}[X]$ et ses idéaux

Propriété 11

Les idéaux de $\mathbb{K}[X]$ sont les $P\mathbb{K}[X]$ avec $P \in \mathbb{K}[X]$.

$$P\mathbb{K}[X] = Q\mathbb{K}[X] \Leftrightarrow (P|Q \text{ et } Q|P) \Leftrightarrow (P \text{ et } Q \text{ sont associés}) \Leftrightarrow (\exists \lambda \in \mathbb{K}^* \text{ tel que } P = \lambda Q)$$

Propriété 12

Soit $(P, Q) \in \mathbb{K}[X]^2$. On appelle PGCD de P et Q tout polynôme $D \in \mathbb{K}[X]$ tel que

$$P\mathbb{K}[X] + Q\mathbb{K}[X] = D\mathbb{K}[X]$$

Il existe un unique PGCD unitaire ou nul de P et Q. On le note $P \wedge Q$.

Cette définition du PGCD est équivalente à la définition du PGCD vue en première année. Le théorème de Bézout découle directement de cette nouvelle définition.

Propriété 13

Soit $(P_1, \dots, P_n) \in (\mathbb{K}[X])^n$.

- On appelle PGCD de $P_1, \dots, P_n$ tout polynôme $D \in \mathbb{K}[X]$ tel que

  $$P_1\mathbb{K}[X] + P_2\mathbb{K}[X] + \cdots + P_n\mathbb{K}[X] = D\mathbb{K}[X]$$

  Il existe un unique PGCD unitaire ou nul de $P_1, \dots, P_n$, on le note $P_1 \wedge \cdots \wedge P_n$.
- On appelle PPCM de $P_1, \dots, P_n$ tout polynôme $M \in \mathbb{K}[X]$ tel que

  $$P_1\mathbb{K}[X] \cap P_2\mathbb{K}[X] \cap \cdots \cap P_n\mathbb{K}[X] = M\mathbb{K}[X]$$

  Il existe un unique PPCM unitaire ou nul de $P_1, \dots, P_n$, on le note $P_1 \vee \cdots \vee P_n$.

Soit E un espace vectoriel de dimension finie et $u \in \mathscr{L}(E)$. L'ensemble des polynômes annulateurs de u est le noyau du morphisme d'algèbres

$$\begin{pmatrix} \mathbb{K}[X] & \longrightarrow & \mathscr{L}(E) \\ P & \longmapsto & P(u) \end{pmatrix}$$

C'est un idéal de $\mathbb{K}[X]$, appelé *idéal annulateur* de u. L'idéal annulateur de u admet un unique générateur unitaire appelé *polynôme minimal* de u, noté π_u.

$$\{P \in \mathbb{K}[X],\ P(u) = 0_{\mathscr{L}(E)}\} = \pi_u\,\mathbb{K}[X]$$

6.2 polynômes irréductibles de $\mathbb{K}[X]$

Définition 10

On dit qu'un polynôme $P \in \mathbb{K}[X]$ NON CONSTANT est *irréductible* lorsque ses seuls diviseurs sont les polynômes associés à 1 ou à P.

Concrètement, P est irréductible lorsque $P = QH$ implique $Q \in \mathbb{K}$ ou $H \in \mathbb{K}$.
Un polynôme est réductible lorsqu'on peut le factoriser sous la forme d'un produit de deux polynômes de degré au moins 1.

Propriété 14 – irréductibilité des polynômes de degré 1

Pour $\alpha \in \mathbb{K}$, $X - \alpha$ est irréductible dans $\mathbb{K}[X]$.

Théorème 1

1. Les polynômes irréductibles unitaires de $\mathbb{C}[X]$ sont les polynômes : $X - \alpha$ avec $\alpha \in \mathbb{C}$.
2. Les polynômes irréductibles unitaires de $\mathbb{R}[X]$ sont :
   (a) Les polynômes de degré 1 de la forme $X - \alpha$ avec $\alpha \in \mathbb{R}$.
   (b) Les polynômes de degré 2 de la forme $X^2 + pX + q$ avec $p^2 - 4q < 0$.

Théorème 2

Soit P un polynôme non nul de $\mathbb{K}[X]$.
Il existe $\lambda \in \mathbb{K}^*$, $n \in \mathbb{N}^*$, $P_1, \dots, P_n$ polynômes irréductibles unitaires deux à deux distincts, $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$ tels que

$$P = \lambda \prod_{i=1}^{n} P_i^{\alpha_i}$$

Cette décomposition est unique à l'ordre près des facteurs.

Pour $A = \lambda P_1^{\alpha_1} \dots P_k^{\alpha_k}$ et $B = \mu P_1^{\beta_1} \dots P_k^{\beta_k}$ polynômes non nuls, décomposés comme ci-dessus, on a :

— $B|A$ si, et seulement si, pour tout i, $\beta_i \leqslant \alpha_i$

— $A \wedge B = D =$ et $A \vee B = M =$

— $AB = \lambda\mu MD$

7 L'anneau $\mathbb{Z}/n\mathbb{Z}$

n désigne un entier naturel non nul.

7.1 éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Nous avons déjà vu (chapitre Groupes) que $(\mathbb{Z}/n\mathbb{Z}, +)$ était un groupe commutatif. On définit, en vérifiant que la classe de congruence de $k\ell$ modulo n ne dépend que des classes de k et ℓ, une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ par :

$$\overline{k} \times \overline{\ell} = \overline{k\ell}$$

Propriété 15

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif, d'éléments neutres $\overline{0}$ et $\overline{1}$.
Les éléments inversibles sont les classes des éléments premiers avec n :

$$U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{k} \mid k \wedge n = 1\}$$

Pour trouver l'inverse de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z}$, il suffit de trouver un couple de Bézout (u, v) tel que $ku+nv = 1$. Dans cette situation, $\overline{k} \times \overline{u} = \overline{1}$.

Exercice 8 :

1. Montrer que $\mathbb{Z}/12\mathbb{Z}$ n'est pas un anneau intègre.
2. $\overline{9}$ est-il inversible dans $\mathbb{Z}/12\mathbb{Z}$? Si oui, déterminer son inverse. Mêmes questions pour $\overline{7}$.
3. Résoudre dans $\mathbb{Z}$ l'équation $7x \equiv 11[12]$.

Propriété 16

$\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier. Le corps $\mathbb{Z}/p\mathbb{Z}$ est aussi noté $\mathbb{F}_p$.

Exercice 9 : Modernisons quelques démonstrations d'arithmétique.

1. Compléter, dans $\mathbb{Z}/6\mathbb{Z}$,

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
x^2						
$x(x^2-1)$						

   On en déduit que pour tout $n \in \mathbb{N}$, 6 divise $n(n-1)(n+1)$. Pourquoi ? Proposer une démonstration arithmétique comme en MPSI.
2. Retrouver le lemme d'Euclide grâce à la propriété précédente.
3. Retrouver le lemme de Gauß.
4. Retrouver le petit théorème de Fermat grâce à la propriété précédente.

7.2 théorème chinois

Théorème 3 – théorème chinois

Soit $(m,n) \in (\mathbb{N}^*)^2$ un couple d'entiers premiers entre eux. Les anneaux $\mathbb{Z}/(mn)\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes par le morphisme d'anneaux :

$$\varphi : \left(\begin{array}{ccc} \mathbb{Z}/(mn)\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{k} & \longmapsto & \left(\overline{\overline{k}}, \overline{\overline{k}}\right) \end{array} \right)$$

Corollaire 1 – théorème des restes chinois

Soit $(m,n) \in (\mathbb{N}^*)^2$ un couple d'entiers premiers entre eux. Pour tous $a, b \in \mathbb{Z}$, le système

$$\begin{cases} k & \equiv a \ [n] \\ k & \equiv b \ [m] \end{cases}$$

admet une infinité de solutions. Si k_0 est une solution particulière, les solutions sont exactement les entiers congrus à k_0 modulo mn.

Méthode – restes chinois

On détermine une relation de Bézout $mu+nv=1$. Cela nous fournit $k_1 = mu$ et $k_2 = nv$ vérifiant :

$$\begin{cases} k_1 & \equiv 1 \ [n] \\ k_1 & \equiv 0 \ [m] \end{cases} \qquad \begin{cases} k_2 & \equiv 0 \ [n] \\ k_2 & \equiv 1 \ [m] \end{cases}$$

$k_0 = ak_1 + bk_2$ est une solution particulière au système des restes chinois. Les solutions sont exactement les entiers congrus à k_0 modulo mn.

Exercice 10 : Résoudre dans $\mathbb{Z}$ le système (S) : $\begin{cases} n \equiv 1 & [5] \\ n \equiv 3 & [11] \end{cases}$.

Propriété 17 – généralisation du théorème chinois

Étant donné $n_1, \ldots, n_r$ premiers entre eux deux à deux, les anneaux

$$\mathbb{Z}/(n_1 \ldots n_r)\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/n_1\mathbb{Z} \times \ldots \mathbb{Z}/n_r\mathbb{Z}$$

sont isomorphes.

Exercice 11 : Ce sont les calculs en astronomie, ainsi que des problèmes de répartition de grains, qui ont donné lieu, très probablement, à la naissance des congruences.
Le plus ancien problème de restes (ou, dit de façon moderne, de congruence) dont nous ayons la trace, est le problème de Sunzi, paru dans le *Classique mathématique de Sunzi.*
Problème 3-26 du Sunzi suanjing
Suppose que l'on ait un nombre inconnu d'objets. S'ils sont comptés par 3, il en reste 2, s'ils sont comptés par 5, il en reste 3 et s'ils sont comptés par 7, il en reste 2. Combien d'objets y a-t-il ?

8 Indicatrice d'Euler

Définition 11

Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire encore le nombre d'entiers de $[\![0, n-1]\!]$ premiers avec n.
L'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est appelée *indicatrice d'Euler*.

$\varphi(n)$ est aussi le nombre d'entiers de $[\![1, n]\!]$ premiers avec n.

Propriété 18 – indicatrice d'Euler d'une puissance de nombre premier

Soient p un nombre premier et $k \in \mathbb{N}^*$ Alors $\varphi(p^k) = p^k - p^{k-1}$.

Propriété 19

Si n et m sont deux entiers naturels non nuls premiers entre eux alors

$$\varphi(nm) = \varphi(n)\varphi(m)$$

Propriété 20

Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec $p_1, \dots, p_r$ nombres premiers distincts deux à deux et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$, on a

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

Exercice 12 : Calculer $\varphi(12)$ et $\varphi(15)$.

Théorème 4 – théorème d'Euler

Soit $n \in \mathbb{N}^*$. Pour a entier relatif premier avec n, on a :

$$a^{\varphi(n)} \equiv 1\ [n]$$

Lorsque p est premier, $\varphi(p) = p - 1$ et on retrouve le petit théorème de Fermat : pour $a \wedge p = 1$, $a^{p-1} \equiv 1\ [p]$.

9 Algèbres

Définition 12

Soient $\mathbb{K}$ un corps et $\mathcal{A}$ un ensemble muni de deux lois internes $+$ et $\times$ ainsi que d'une loi externe $.$, c'est-à-dire d'une application :

$$\begin{pmatrix} \mathbb{K}\times\mathcal{A} & \longrightarrow & \mathcal{A} \\ (\lambda,x) & \longmapsto & \lambda.x \end{pmatrix}$$

On dit que $(\mathcal{A},+,\times,.)$ est une $\mathbb{K}$-*algèbre* ou tout simplement *une algèbre* si

(i) $(\mathcal{A},+,.)$ est un $\mathbb{K}$-espace vectoriel

1. $(\mathcal{A},+,\times)$ est un anneau
2. $\forall(\lambda,x,y)\in\mathbb{K}\times\mathcal{A}^2$, $\lambda.(x\times y)=(\lambda.x)\times y=x\times(\lambda.y)$.

Lorsque l'anneau est commutatif, l'algèbre est dite commutative.

Exemples :

— $\mathbb{K}$, $\mathbb{K}^{\mathbb{N}}$, $\mathcal{F}(X,\mathbb{K})$ (pour X ensemble quelconque), $\mathbb{K}[X]$, $\mathbb{K}(X)$ sont des algèbres commutatives.

— Si E est un $\mathbb{K}$-espace vectoriel, $(\mathscr{L}(E),+,\circ,.)$ est une algèbre. Elle est non commutative dès que $\dim E\geqslant 2$.

— $(\mathcal{M}_n(\mathbb{K}),+,\times,.)$ est une algèbre. Elle est non commutative dès que $n\geqslant 2$.

Définition 13

On appelle *sous-algèbre* d'une $\mathbb{K}$-algèbre $(\mathcal{A},+,\times,.)$, toute partie $\mathcal{B}$ de $\mathcal{A}$ qui est un sous-anneau de $(A,+,\times)$ et un sous-espace vectoriel de $(A,+,.)$.

Nous admettons qu'une sous-algèbre d'une $\mathbb{K}$-algèbre est une $\mathbb{K}$-algèbre.

Par exemple, l'ensemble des matrices diagonales de $\mathcal{M}_n(\mathbb{K})$ est une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{K})$. L'ensemble des matrices triangulaires supérieures/inférieures de $\mathcal{M}_n(\mathbb{K})$ est une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$. Si I est un intervalle de $\mathbb{R}$, pour tout $k\in\mathbb{N}\cup\{\infty\}$, $\mathcal{C}^k(I,\mathbb{K})$ est une sous-algèbre de $\mathcal{F}(I,\mathbb{K})$.

Définition 14

Soient $\mathcal{A}$ et $\mathcal{B}$ deux $\mathbb{K}$-algèbres. Un *morphisme d'algèbres* de $\mathcal{A}$ dans $\mathcal{B}$ est une application linéaire de $\mathcal{A}$ dans $\mathcal{B}$ qui est également un morphisme d'anneaux.

Il y a donc 3 conditions à satisfaire pour que $f:\mathcal{A}\to\mathcal{B}$ soit un morphisme d'algèbre, qui sont :

1.

2.

3.

Par exemple, l'application $z\in\mathbb{C}\mapsto\overline{z}$ est un morphisme de la $\mathbb{R}$-algèbre $\mathbb{C}$ dans elle-même.

10 Annexe : quelques éléments de démonstrations

Propriété 3 (première année)

Pour une fois, nous ne pouvons pas montrer que $U(A)$ est un sous-groupe d'un groupe connu plus gros car nous n'avons pas de groupe connu plus gros à proposer.

— La loi $\times$ est-elle une loi interne de $U(A)$?
Oui car pour x et y inversibles, on a $y^{-1}x^{-1}xy = y^{-1}1_A y = y^{-1}y = 1_A$ et de même, $xyy^{-1}x^{-1} = 1_A$, donc xy est inversible.

— La loi $\times$ est-elle associative ?
Oui car A est un anneau.

— La loi $\times$ possède-t-elle un élément neutre dans $U(A)$?
Oui car $1_A \times 1_A = 1_A$ donc $1_A \in U(A)$ et 1_A est par ailleurs un élément neutre.

— Tout élément a-t-il un inverse dans $U(A)$?
Oui car si $x \in U(A)$, x est inversible et $xx^{-1} = 1_A = x^{-1}x$, donc x^{-1} est aussi inversible. $x^{-1} \in U(A)$.

Définition-propriété 2

Notons $I = xA$.

- I est un idéal.
  On a $(A, +)$ groupe et on a vu au chapitre Groupes que xA était un sous-groupe de A. Donc $(I, +)$ est un groupe.
  Et pour $xa \in I$ (où $a \in A$) et $a' \in A$, on a $a'xa = xa'a \in xA = I$.

- I contient x.
  Car $x = x1_A$ et $1_A \in A$.

- I est le plus petit idéal contenant x.
  Soit J un idéal contenant x. Par définition d'un idéal, tous les xa avec $a \in A$, sont dans J, donc $xA \subset J$, soit $I \subset J$.

- I est l'intersection de tous les idéaux de A qui contiennent x.
  Comme I contient x, $\bigcap_{K \text{ idéal de } A \text{ contenant x}} K \subset I$.
  Par le point précédent, pour tout J idéal contenant x, $I \subset J$ donc $I \subset \bigcap_{K \text{ idéal de } A \text{ contenant x}} K$.

Définition-propriété 1

Soit $I = \ker \varphi$, où $\varphi : A \to A'$ est un morphisme d'anneaux (avec A et A' anneaux commutatifs).
On sait déjà (vu en première année) qu'un morphisme d'anneaux est un morphisme de groupes pour l'addition, et que le noyau d'un morphisme de groupes est un sous-groupe, donc $(I, +)$ est un sous-groupe de A. Vérifions que I est absorbant :
Soit $x \in I$ et $a \in A$.
$\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a).0_{A'} = 0_{A'}$, donc $ax \in I$.

Remarque pour moi : le noyau d'un morphisme d'anneaux n'est pas un anneau ! En effet, $\varphi(1_A) = 1_{A'} \neq 0_{A'}$ (quand l'anneau n'est pas réduit à $\{0\}$).
Par contre, l'image d'un morphisme d'anneaux est un anneau.

Propriété 6

• Supposons que $x|y$. Il existe $a \in A$ tel que $y = ax$.
Soit $z \in yA$. Il existe $b \in A$ tel que $z = yb$, et donc $z = xab$ (on rappelle que A est supposé commutatif). Donc $z \in xA$.
• Supposons que $yA \subset xA$.
$y = y1_A \in yA$, donc $y \in xA$, donc il existe $a \in A$ tel que $y = xa$. Donc $x|y$.

Propriété 7

On sait déjà que les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$. Donc tout idéal de $\mathbb{Z}$ est de cette forme. Réciproquement, les $n\mathbb{Z}$ sont bien des idéaux (ce sont des idéaux engendrés par un élément).

Propriété 8

$a\mathbb{Z} + b\mathbb{Z}$ étant un idéal de $\mathbb{Z}$, il existe un unique (on l'a vu en remarque) d entier naturel tel que cet idéal soit égal à $d\mathbb{Z}$.
Comme $d \in d\mathbb{Z}$, on a une relation de Bézout : il existe u et v tels que $d = au + bv$.
Si k divise a et b, dans la relation précédente, k divise d.
Et si k divise d, alors $d\mathbb{Z} \subset k\mathbb{Z}$. Donc $a\mathbb{Z} \subset d\mathbb{Z} \subset k\mathbb{Z}$, et k divise a. De même pour b.

Remarque : si on a une relation de Bézout de la forme $au + bv = 1$, alors $1 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, donc $d\mathbb{Z}$ est un idéal qui contient 1 : c'est $\mathbb{Z}$. Donc $d = 1$. On retrouve là un résultat de première année avec une approche par idéaux.

Propriété 11

Soit I un idéal de $\mathbb{K}[X]$. Si $I = \{0\}$, on a $I = 0.\mathbb{K}[X]$. Sinon, l'ensemble $\{\deg P,\ P \in \mathbb{K}[X] \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$. Elle admet un plus petit élément. On considère $P_0 \in I$ ayant ce degré minimal.
Comme I est absorbant, $P_0\mathbb{K}[X] \subset I$.
Réciproquement, soit $A \in I$. On effectue la division euclidienne de P par P_0. Il existe Q et R tels que

$$A = QP_0 + R \qquad \text{et } \deg(R) < \deg(P_0)$$

On constate que $R = A - P_0Q$. Comme I est absorbant, $P_0Q \in I$. Comme $(I, +)$ est un groupe, $A - P_0Q \in I$. Donc $R \in I$, avec $\deg(R) < \deg(P_0)$. Donc $R = 0$, et $A \in P_0\mathbb{K}[X]$. $I = P_0\mathbb{K}[X]$.

Propriété 12

Par la propriété précédente, on a l'existence d'un PGCD. Et on a réexpliqué que $D\mathbb{K}[X] = C\mathbb{K}[X]$ si et seulement si C et D sont associés, si et seulement s'il existe $T \in U(\mathbb{K}[X])$ tel que $C = TD$.

Propriété 14

Si $X - \alpha = QH$, alors $1 = \deg(Q) + \deg(H)$, donc $\begin{cases}\deg(Q) & = 1\\ \deg(H) & = 0\end{cases}$ ou $\begin{cases}\deg(H) & = 1\\ \deg(Q) & = 0\end{cases}$. Donc $Q \in \mathbb{K}$ ou $H \in \mathbb{K}$.

Théorème 1

Dans $\mathbb{C}[X]$, tout polynôme non constant admet une racine (théorème de d'Alembert-Gauss). Aussi un polynôme de degré supérieur ou égal à 2 peut se factoriser sous la forme $(X - a)Q(X)$ avec $\deg(Q) \geqslant 1$, et n'est donc pas irréductible. On a par ailleurs déjà vu que les polynômes $X - \alpha$, avec $\alpha \in \mathbb{C}$, sont irréductibles. Donc ce sont les seuls polynômes irréductibles dans $\mathbb{C}[X]$.
Dans $\mathbb{R}[X]$, on a déjà vu que les polynômes $X - \alpha$ étaient irréductibles. Les polynômes de la forme $X^2 + pX + q$ avec $p^2 - 4q < 0$ le sont aussi. En effet, si un tel polynôme était réductible, il serait divisible par un polynôme de degré 1, qui aurait donc une racine réelle. On aurait une racine réelle pour $X^2 + pX + q$, ce qui est exclu.
Soit un polynôme de degré au moins 3 dans $\mathbb{R}[X]$. En tant que polynôme de $\mathbb{C}[X]$, P admet une racine λ. Si λ est réel, $(X - \lambda)$ divise P dans $\mathbb{R}[X]$, et P est réductible. Si λ n'est pas réel, comme P est à coefficients réels, nous avons appris que $\overline{\lambda}$ était aussi racine de P. $(X - \lambda)(X - \overline{\lambda}) = X^2 - 2\,\mathrm{Re}(\lambda)X + |\lambda|^2$ divise P dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$ (*). P est réductible.

(*) Si $Q \in \mathbb{R}[X]$ divise $P \in \mathbb{R}[X]$ dans $\mathbb{C}[X]$, alors Q divise P dans $\mathbb{R}[X]$. En effet, s'il existe $R \in \mathbb{C}[X]$ tel que $P = QR$, alors on en conjuguant les coefficients, on trouve (le polynôme « conjugué » est celui dont on a conjugué tous les coefficients) :

$$QR = P = \overline{P} = \overline{QR} = Q\overline{R}$$

et par intégrité de $\mathbb{C}[X]$, ayant $Q \neq 0$, on a $R = \overline{R}$, et donc $R \in \mathbb{R}[X]$.

Théorème 2

• $\mathcal{P}_n$: « tout polynôme de degré n est produit d'irréductibles » se montre facilement par récurrence forte.
Soit A un polynôme non nul de $\mathbb{K}[X]$.

• Si A est constant, c'est terminé.
Sinon, A s'écrit comme produit d'irréductibles. En factorisant par leur coefficient dominant, on se ramène à des irréductibles unitaires. En les regroupant, on trouve les α_i. Voilà pour l'existence.

• Unicité. Comme les P_i sont unitaires, λ est unique : c'est le coefficient dominant de A. Écrivons, avec des a_P et b_P entiers naturels éventuellement nuls

$$A = \lambda \prod_{P\text{unitaire}} P^{a_P} = \lambda \prod_{P\text{unitaire}} P^{b_P}$$

et condidérons un polynôme Q unitaire pour lequel $a_Q \leqslant b_Q$. On met en facteur et on simplifie dans $\mathbb{K}[X]$ intègre :

$$\prod_{P\text{unitaire autre que } Q} P^{a_P} = Q^{b_Q - a_Q} \prod_{P\text{unitaire autre que } Q} P^{b_P}$$

Le membre de gauche est premier avec Q (produit de polynômes premiers avec Q) donc $b_Q - a_Q = 0$.

Propriété 15

• La multiplication est bien définie. Si $\begin{cases}k' & \equiv k\ [n]\\ \ell' & \equiv \ell\ [n]\end{cases}$ alors $k'\ell' \equiv k\ell\ [n]$.
• On a déjà vu que $(\mathbb{Z}/n\mathbb{Z}, +)$ était un groupe commutatif.
• $\times$ est bien associative, commutative, distributive par rapport à $+$. On a $\overline{1} \times \overline{k} = \overline{k} = \overline{k} \times \overline{1}$.
Ainsi on a un anneau. Cet anneau n'est en général pas intègre. Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2} \times \overline{3} = \overline{2 \times 3} = \overline{0}$ sans que ni 2 ni 3 ne soient congrus à 0 modulo 6.

• $\overline{k} \times \overline{\ell} = 1$ si et seulement si $\exists m \in \mathbb{Z}/\ k\ell = 1 + mn$ si et seulement si il existe $(\ell, -m)$ couple de Bézout pour (k, n), si et seulement si (théorème de Bézout) $k \wedge n = 1$.

Propriété 16

On rappelle que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.
Si n est premier, tous les entiers k de 1 à $n-1$ sont premiers avec n. Par la propriété 15, $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Tous les éléments non nuls sont inversibles, et $\mathbb{Z}/n\mathbb{Z}$ est un corps.
Et si n n'est pas premier, il peut s'écrire ab avec $2 \leqslant a \leqslant n-1$. On a $\overline{a} \times \overline{b} = \overline{ab} = \overline{0}$. $\mathbb{Z}/n\mathbb{Z}$ n'est alors pas intègre, et ne peut pas être un corps.

Théorème chinois et théorème des restes chinois

• Vérifions que l'application φ est bien définie.
Si $\overline{k} = \overline{\ell}$, alors nm divise $k - \ell$. Donc n divise $k - \ell$ et m divise $k - \ell$. Et donc, dans $\mathbb{Z}n\mathbb{Z}$, $\overline{\overline{k}} = \overline{\overline{\ell}}$ et dans $\mathbb{Z}/m\mathbb{Z}$, $\overline{\overline{k}} = \overline{\overline{\ell}}$.
• Par la définition des lois dans l'anneau produit, on arrive facilement à

$$\varphi(\overline{1}) = 1_{\text{anneau produit}} \qquad \varphi(\overline{k} + \overline{\ell}) = \varphi(\overline{k}) + \varphi(\overline{\ell}) \qquad \varphi(\overline{k\ell}) = \varphi(\overline{k})\varphi(\overline{\ell})$$

• Soit $k \in \ker \varphi$. On a $\overline{\overline{k}} = \overline{\overline{0}}$ donc $m|k$. Et $\overline{\overline{k}} = \overline{\overline{0}}$ donc $n|k$. Et comme m et n sont premiers entre eux, $mn|k$, puis $\overline{k} = \overline{0}$.
Donc φ est injective.
Enfin, $\text{Card}(\mathbb{Z}/mn\mathbb{Z}) = nm = \text{Card}(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ donc φ est bijective.
La surjectivité de φ apporte le théorème des restes chinois.

Propriété 18

On va compter le nombre d'entiers n de $[\![1, p^k]\!]$ qui ne sont **pas** premiers avec p^k. n et p^k ont un diviseur commun entier naturel autre que 1 si et seulement si n est multiple de p. Les entiers de $[\![1, p^k]\!]$ qui ne sont **pas** premiers avec p^k sont donc :

$$p, 2p, 3p, \ldots, p^k$$

Il y en a p^{k-1}.
Le nombre d'entiers n de $[\![1, p^k]\!]$ qui **sont** premiers avec p^k est donc

$$\varphi(p^k) = \text{Card}[\![1, p^k]\!] - p^{k-1} = p^k - p^{k-1}$$

Propriété 19

Lemme 1

Si F et G sont deux anneaux isomorphes, alors $|U(F)| = |U(G)|$, où $U(A)$ désigne l'ensemble des éléments inversibles de l'anneau A, et $|A|$ désigne le cardinal de l'ensemble A.

Notons $\varphi : F \to G$ un isomorphisme d'anneaux de F dans G.
Si a est inversible dans F alors il existe $b \in F$ tel que $ab = 1_F$. Par l'isomorphisme φ, on a $\varphi(a)\varphi(b) = 1_G$ et $\varphi(a) \in U(G)$.
Réciproquement, soit $x \in U(G)$.
Par surjectivité de φ, il existe $a \in A$ tel que $x = \varphi(a)$, et en notant y l'inverse de x, il existe $b \in A$ tel que $\varphi(b) = y$. On a

$$\varphi(1_F) = 1_G = xy = \varphi(ab)$$

donc par injectivité de φ, $ab = 1_F$ et a est inversible, et $x \in \varphi(U(F))$.
Donc $\varphi(U(F)) = U(G)$.
Comme φ est bijective, $U(F)$ et $\varphi(U(F))$ ont même cardinal.
Finalement, $|U(F)| = |U(G)|$.

Retour à la démonstration. Par le théorème chinois, l'anneau $\mathbb{Z}/mnZ$ est isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Il y a donc autant d'éléments inversibles dans $\mathbb{Z}/mn\mathbb{Z}$ que dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

$$|U(\mathbb{Z}/mn\mathbb{Z})| = |U((\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}))|$$

Mais par propriété sur les produits d'anneaux, $U(A_1 \times A_2) = U(A_1) \times U(A_2)$, donc

$$|U(\mathbb{Z}/mn\mathbb{Z})| = |U(\mathbb{Z}/n\mathbb{Z})| \times |U(\mathbb{Z}/m\mathbb{Z})|$$

Enfin, il y a exactement $\varphi(mn)$ éléments inversibles dans $\mathbb{Z}/mn\mathbb{Z}$, $\varphi(m)$ éléments inversibles dans $\mathbb{Z}/m\mathbb{Z}$ et $\varphi(n)$ éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$.
Donc $\varphi(mn) = \varphi(m)\varphi(n)$.

Propriété 20
Par les deux propriétés précédentes,

$$\begin{aligned}\varphi(n) &= (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \dots (p_r^{\alpha_r} - p_r^{\alpha_r-1}) = p_1^{\alpha_1}(1 - \frac{1}{p_1}) \dots p_r^{\alpha_r}(1 - \frac{1}{p_r}) \\ &= p_1^{\alpha_1} \dots p_r^{\alpha_r}(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_r})\end{aligned}$$

Théorème d'Euler
Soit a un entier premier avec $n \in \mathbb{N}^*$.
Puisque $a \wedge n = 1$, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Autrement dit, $\overline{a} \in U(\mathbb{Z}/n\mathbb{Z})$, groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$, qui est de cardinal $\varphi(n)$. Dans un groupe fini, tout élément est d'ordre fini et son ordre divise le cardinal du groupe. Donc

$$\overline{a}^{\varphi(n)} = \overline{1}$$