CHAPITRE

16

Entiers

Amalie Emmy Noether (23 mars 1882 -– 14 avril 1935) est une mathématicienne allemande spécialiste d'algèbre abstraite et de physique théorique. Décrite par Albert Einstein comme « le génie mathématique créatif le plus considérable produit depuis que les femmes ont eu accès aux études supérieures », elle a révolutionné les théories des anneaux, des corps et des algèbres. En physique, le théorème de Noether explique le lien fondamental entre la symétrie et les lois de conservation et est considéré comme aussi important que la théorie de la relativité.

Au printemps 1915, Noether est invitée à Göttingen. Un membre de la faculté proteste : « Que penseront nos soldats, quand ils [...] verront qu'ils doivent apprendre aux pieds d'une femme ? ». Hilbert s'indigne : « je ne vois pas pourquoi le sexe de la candidate serait un argument contre son admission comme Privatdozent. Après tout, nous sommes une université, pas des bains publics. »

Bien que le théorème de Noether ait un profond effet sur la physique, elle est mieux connue parmi les mathématicien(ne)s pour ses contributions fondatrices en algèbre générale.

« Le développement de l'algèbre abstraite, qui est l'une des innovations les plus caractéristiques des mathématiques du vingtième siècle, est largement redevable [à Emmy Noether], par les articles qu'elle a publiés, par ses conférences et son influence personnelle sur ses contemporains. »

– Nathan Jacobson.

Programme

- Idéaux de $\mathbf{Z}$. Interprétation de la divisibilité en termes d'idéaux.
- L'anneau $\mathbf{Z}/n\mathbf{Z}$, inversibles de $\mathbf{Z}/n\mathbf{Z}$. L'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est premier. Théorème chinois, application aux systèmes de congruences. Indicatrice d'Euler φ, calcul à l'aide de la décomposition de n en facteurs premiers, théorème d'Euler.
- Anneau, produit fini d'anneaux, sous-anneaux. Morphisme d'anneaux, image et noyau d'un morphisme. Isomorphisme d'anneaux.
- Algèbre. Exemples : $\mathbf{K}[X]$, $\mathscr{L}(E)$, $\mathscr{M}_n(\mathbf{K})$, $\mathcal{F}(X,\mathbf{K})$. Sous-algèbre, morphisme d'algèbres.
- Anneau intègre, corps, sous-corps.
- Idéal d'un anneau commutatif. Le noyau d'un morphisme d'anneaux est un idéal. Relation de divisibilité dans un anneau commutatif intègre.

Dans ce chapitre A est un anneau et $\mathbf{K}$ est un corps. Nous supposerons, en accord avec le programme, que les éléments neutres de A sont distincts, autrement dit que A n'est pas l'anneau nul. En l'absence d'ambiguïté on note

- xy au lieu de $x \cdot y$
- 0 et 1 les éléments neutres de A, au lieu de 0_A et 1_A.

Programme

Un bi-magma pourvu des mêmes axiomes à l'exception de l'existence d'un élément unité pour la multiplication est appelé pseudo-anneau. Dans certains anciens écrits, les pseudo-anneaux sont appelés anneaux et les anneaux du programme sont qualifiés d'anneaux unifères. Nous n'utiliserons pas la notion de pseudo-anneau et tous nos anneaux possèderont donc un élément unité pour la multiplication.

Introduction

L'ensemble des entiers naturels n'est pas un anneau, ni même un groupe. En effet on ne peut pas soustraire n'importe quel entier naturel d'un autre et obtenir un résultat positif. L'ensemble des entiers relatifs est en quelque sorte le groupe canoniquement associé à $\mathbf{N}$. On peut le voir comme un ensemble de couples (a,b) d'entiers naturels. L'entier relatif, que l'on notera par la suite $b-a$, est défini comme la classe d'équivalence des couples (a,b) pour la relation (d'équipollence)

$$(a,b)\mathcal{R}(c,d) \Leftrightarrow a+d=b+c\,.$$

On voit que cette définition ne fait appel qu'à l'addition.

Comme $\mathbf{N}$ est muni de deux lois, la multiplication étant une addition itérée, on peut vouloir étendre l'a multiplication à $\mathbf{Z}$. Cela résulte de la règle des signes, qui elle-même résulte de la distributivité : $2a+(-1)a=(2-1)a=1a=a$ et donc $(-1)a=-a$.

De la même façon, le corps des rationnels est le corps canoniquement associé à $\mathbf{Z}$ de la façon suivante : le rationnel r que l'on note a/b est la classe d'équivalence de couples d'entiers relatifs (a,b), avec b non nul, pour la relation (d'équipollence)

$$(a,b)\mathcal{R}(c,d) \Leftrightarrow ad=bc\,.$$

On a vu que l'ensemble des fonctions d'un ensemble X dans un groupe commutatif G est muni d'une structure de groupe, donnée par la loi sur G. Si on note cette loi $+$, de sorte que $(G,+)$ est un groupe abélien, alors G^X est un groupe pour la loi $\oplus$ donnée par

$$\forall (f_1,f_2)\in G^X\times G^X \quad f_1\oplus f_2\in G^X \quad \text{avec } \forall x\in X \quad (f_1\oplus f_2)(x)=f_1(x)+f_2(x)\ .$$

Si, de plus, $X=G$, alors on peut munir cet ensemble d'une autre loi, la loi de composition, de sorte que G^G est un anneau.

Si on impose des conditions supplémentaires aux fonctions, comme par exemple celles d'être un homomorphisme, on garde la structure d'anneau, et c'est pourquoi si G est un groupe, alors $\mathrm{End}(G)$ est un anneau. Par exemple pour le groupe additif $(\mathbf{R},+)$

$$\mathrm{End}(\mathbf{R})=\left\{f:\mathbf{R}\to\mathbf{R}\ \middle|\ \forall (x,y)\in\mathbf{R}^2, f(x+y)=f(x)+f(y)\right\}\ .$$

1 Arithmétique des entiers

Rappel

Idéal

Soit I une partie de $\mathbf{Z}$. On dit que I est un idéal de $\mathbf{Z}$ si c'en est un sous-groupe additif et qu'il est stable par multiplication externe par $\mathbf{Z}$, i.e.

$$\forall x\in I\ ,\ \forall a\in A\ ,\quad ax\in I\ .$$

Théorème 16 - 1

Les idéaux de $\mathbf{Z}$ sont exactement les ensembles de la forme $n\mathbf{Z}$ avec n dans $\mathbf{Z}$ et on a, pour a et b entiers relatifs, $a\mathbf{Z}=b\mathbf{Z}$ si et seulement si $a=\pm b$.

Démonstration. On a déjà vu que tous les sous-groupes additifs de $\mathbf{Z}$ sont de la forme $n\mathbf{Z}$, avec n dans $\mathbf{Z}$. Comme un idéal est un sous-groupe additif, il en résulte qu'un idéal de $\mathbf{Z}$ est nécessairement de cette forme. La vérification du fait que $n\mathbf{Z}$ est un idéal est directe et la dernière assertion résulte du fait que si a est un multiple de b et réciproquement, on peut écrire $a=kb$ et $b=k'a$, avec k et k' entiers, et qu'alors $kk'=1$, ce qui entraîne $|k|\leq 1$ puis $|k|=1$. □

Aparté

On dit que les idéaux de $\mathbf{Z}$ sont principaux et que $\mathbf{Z}$ est un anneau principal.

Définition 16 - 1

Soit a et b dans $\mathbf{Z}$. On dit que a **divise** b, et on note $a\mid b$, si b appartient à l'idéal engendré par a, autrement dit s'il existe k dans $\mathbf{Z}$ tel que $b=ka$. On dit aussi que b est un **multiple** de a et que a est un **diviseur** de b.

Remarque 16 - 1

Avec les notations précédentes, l'élément k est unique sauf si $a=0$ (et donc b est nul aussi), puisque tous les éléments de $\mathbf{Z}$ sont réguliers (i.e. $\mathbf{Z}$ est intègre).

On a donc $a\mid b\Leftrightarrow aA\supset bA$.

Proposition 16 - 1

Soit a et b dans $\mathbf{Z}$. Il existe c dans $\mathbf{Z}$ tel que $a\mathbf{Z} \cap b\mathbf{Z} = c\mathbf{Z}$.

On dit que c est un plus petit commun multiple, ou **ppcm**, de a et b. On peut choisir c de façon canonique en imposant c nul ou strictement positif. On dit alors que c est **le ppcm** de a et b, et on note $c = \text{ppcm}(a, b)$ ou encore $c = a \vee b$.

Par ailleurs si a et b sont non nuls, c ne l'est pas non plus.

De plus si, pour x dans $\mathbf{Z}$, $a \mid x$ et $b \mid x$, alors $c \mid x$.

Démonstration. Puisque l'intersection de deux sous-groupes en est un et que l'intersection de deux parties stables par multiplication par $\mathbf{Z}$ l'est aussi, $a\mathbf{Z} \cap b\mathbf{Z}$ est un idéal de $\mathbf{Z}$ et la première assertion en découle.

On a déjà vu que le générateur positif de $c\mathbf{Z}$ est défini de façon unique. Ce générateur n'est nul que si l'idéal est nul.

L'intersection contient au moins ab et n'est donc réduite à $\{0\}$ que si a ou b est nul.

Enfin la dernière assertion n'est qu'une reformulation de l'égalité $a\mathbf{Z} \cap b\mathbf{Z} = c\mathbf{Z}$. □

Proposition 16 - 2

Soit a et b sont dans $\mathbf{Z}$. On note $a\mathbf{Z} + b\mathbf{Z} = \left\{ax + by \mid (x, y) \in \mathbf{Z}^2\right\}$. Alors $a\mathbf{Z} + b\mathbf{Z}$ est un idéal de $\mathbf{Z}$ et c'est le plus petit idéal de $\mathbf{Z}$ contenant a et b. On le note également (a, b).

Démonstration. Soit I un idéal de $\mathbf{Z}$ contenant a et b, alors il contient $a\mathbf{Z}$ et $b\mathbf{Z}$ par stabilité par multiplication par $\mathbf{Z}$ et donc aussi $a\mathbf{Z} + b\mathbf{Z}$ par stabilité par addition. On vérifie directement que $a\mathbf{Z} + b\mathbf{Z}$ est un idéal de $\mathbf{Z}$ et l'assertion s'ensuit. □

Proposition 16 - 3

Soit a et b sont dans $\mathbf{Z}$, il existe d dans $\mathbf{Z}$ tel que $(a, b) = d\mathbf{Z}$.

On dit que d est un plus grand commun diviseur, ou **pgcd**, de a et b. On peut choisir d de façon canonique en imposant d nul ou strictement positif. On dit alors que d est **le pgcd** de a et b, et on note $d = \text{pgcd}(a, b)$ ou encore $d = a \wedge b$.

Par ailleurs si a ou b est non nul, d ne l'est pas non plus.

De plus si, pour x dans $\mathbf{Z}$, $x \mid a$ et $x \mid b$, alors $x \mid d$.

Démonstration. Puisque (a, b) est un idéal de $\mathbf{Z}$, il est de la forme $d\mathbf{Z}$. Pour x dans $\mathbf{Z}$, si $x \mid a$ et $x \mid b$, alors $x\mathbf{Z}$ contient $a\mathbf{Z}$ et $b\mathbf{Z}$ et donc aussi $a\mathbf{Z} + b\mathbf{Z}$ puisque $x\mathbf{Z}$ est stable par addition. Ainsi il contient $d\mathbf{Z}$, i.e. $x \mid d$.

Le reste est similaire (ou identique) à la démonstration précédente. □

Définition 16 - 2

On dit que deux éléments de A sont premiers entre eux, et on écrit $a \wedge b = 1$, si l'idéal qu'ils engendrent est A.

Théorème 16 - 2

Théorème de Bézout

Soit a et b deux éléments de $\mathbf{Z}$. Ils sont premiers entre eux si et seulement si

$$\exists (u, v) \in \mathbf{Z}^2 , \quad au + bv = 1 .$$

Une telle relation est appelée relation de Bézout.

Démonstration. C'est une simple reformulation de $(a, b) = a\mathbf{Z} + b\mathbf{Z}$. □

Théorème 16 - 3

Lemme de Gauss

Soit a, b et c dans $\mathbf{Z}$ tels que $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Démonstration. On a $a\mathbf{Z} + b\mathbf{Z} = \mathbf{Z}$ et donc $ac\mathbf{Z} + bc\mathbf{Z} = c\mathbf{Z}$. Or $ac\mathbf{Z} \subset a\mathbf{Z}$ et $bc\mathbf{Z} \subset a\mathbf{Z}$ puisque $a \mid bc$. Par conséquent $ac\mathbf{Z} + bc\mathbf{Z} \subset a\mathbf{Z}$ par définition de l'idéal engendré comme plus petit idéal contenant une partie. D'où $c\mathbf{Z} \subset a\mathbf{Z}$, i.e. $a \mid c$. □

Exemples 16 - 1

Soit a et b premiers entre eux, alors

1. $a + b$ et b sont premiers entre eux ;
2. $a + b$ et ab sont premiers entre eux ;
3. pour p et q dans $\mathbf{N}$, a^p et b^q sont premiers entre eux.

Définition 16 - 3

On appelle nombre premier tout entier naturel p dont les diviseurs naturels sont exactement 1 et p. En particulier $p \neq 1$.

Exercice

Soit $(p_k)_{k\in\mathbf{N}^*}$ la liste des nombres premiers, i.e. $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ etc. En considérant $p_1 p_2 \cdots p_n + 1$, montrer qu'il existe une infinité de nombres premiers.

En remarquant que le dernier nombre considéré est congru à 3 modulo 4, en déduire qu'il existe une infinité de nombres premiers de la forme $4k + 3$ avec k entier.

En changeant légèrement la méthode, montrer qu'il existe une infinité de nombres premiers de la forme $6k + 5$ avec k entier.

Trouver d'autres exemples simples.

Le théorème de Gauss permet d'obtenir

Théorème 16 - 4

Existence et unicité de la décomposition en facteurs premiers

Soit n un entier relatif non nul et $\mathcal{P}$ l'ensemble des nombres premiers.

Il existe un unique couple formé d'une suite presque nulle $(v_p(n))_{p\in\mathcal{P}}$ et d'une unité ε de $\mathbf{Z}^\times$ (i.e. $\varepsilon = \pm 1$) tels que

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

Les produits sont donc finis.

Démonstration. L'existence se démontre par récurrence sur $|n|$ (dans $\mathbf{N}^*$).

— Si $|n| = 1$, alors on pose $v_p(n) = 0$ pour tout p dans $\mathcal{P}$ et $\varepsilon = n$.

— Si $|n|$ est premier, alors on pose $v_p(n) = \delta_p(n)$ pour tout p dans $\mathcal{P}$ et $\varepsilon = \dfrac{n}{|n|}$.

— Si $|n|$ n'est pas premier, on dispose de n_1 et n_2 dans $\mathbf{Z}$ tels que $n = n_1 n_2$ avec $|n_1|$ et $|n_2|$ strictement inférieurs à $|n|$. Si on dispose de décompositions pour n_1 et n_2, il vient

$$n = n_1 n_2 = \varepsilon_1 \varepsilon_2 \prod_{p\in\mathcal{P}} p^{v_p(n_1)+v_p(n_2)} .$$

L'unicité est une conséquence du théorème de Gauss. Soit ε et ε' deux unités dans $\mathbf{Z}^\times$, (a_p) et (b_p) deux suites presque nulles dans $\mathbf{N}^{(\mathcal{P})}$ tels que

$$\varepsilon \prod_{p\in\mathcal{P}} p^{a_p} = \varepsilon' \prod_{p\in\mathcal{P}} p^{b_p} .$$

Si les suites (a_p) et (b_p) sont distinctes, on dispose de p dans $\mathcal{P}$ que $a_p \neq b_p$ et en divisant les deux membres de l'égalité par $p^{\min(a_p,b_p)}$, on obtient deux entiers relatifs. L'un est divisible par p puisque $\min(a_p,b_p) < \max(a_p,b_p)$ et donc l'autre aussi. Mais ceci contredit le théorème de GAUSS puisqu'on a affaire à un produit (fini) de nombres premiers à p. On en déduit $(a_p) = (b_p)$ et donc aussi $\varepsilon = \varepsilon'$. □

Définition 16 - 4

On reprend les notations du théorème précédent. Les entiers $v_p(n)$ s'appellent les **valuation p-adique** de n. On étend ces valuations à $\mathbf{N}$ en posant $v_p(0) = +\infty$.

Théorème 16 - 5

Si m et n sont deux entiers relatifs, on a $m \mid n \Leftrightarrow \forall p \in \mathcal{P},\ v_p(m) \leq v_p(n)$. De plus, pour m et n non nuls,

$$m \vee n = \prod_{p\in\mathcal{P}} p^{\max(v_p(n),v_p(m))} \text{ et } m \wedge n = \prod_{p\in\mathcal{P}} p^{\min(v_p(n),v_p(m))}\ .$$

Il en résulte $mn = \varepsilon(m \vee n)\cdot(m \wedge n)$ pour un certain ε dans $\mathbf{Z}^\times$ (unique si $mn \neq 0$).

Démonstration. Soit m, n et k trois entiers relatifs non nuls. D'après le théorème précédent, on a, pour tout p dans $\mathcal{P}$, $v_p(n) = v_p(m) + v_p(k)$ et donc $v_p(n) \geq v_p(m)$. Réciproquement si pour tout p dans $\mathcal{P}$ on a $v_p(n) \geq v_p(m)$, alors en posant $k = \prod_{p\in\mathcal{P}} p^{v_p(n)-v_p(m)}$, on a $|n| = k\,|m|$ et donc $m \mid n$. La première assertion en résulte puisqu'elle est directe dans le cas $m = 0$ ou $n = 0$.

Les deux suivantes sur le pgcd et le ppcm s'ensuivent puisque, pour tous entiers naturels a, b et c, on a

$$(c \leq a \text{ et } c \leq b) \Leftrightarrow c \leq \min(a,b)$$

et

$$(a \leq c \text{ et } b \leq c) \Leftrightarrow \max(a,b) \leq c\ .$$

La dernière résulte du fait qu'on a $(m \vee n)\cdot(m \wedge n) = |mn|$ si $mn \neq 0$ et $m \vee n = 0$ si $mn = 0$. □

2 Les anneaux $\mathbf{Z}/n\mathbf{Z}$

Définition 16 - 5

Soit n un entier naturel non nul et a et b dans $\mathbf{Z}$. On dit que a et b sont congrus modulo n, et on écrit $a \equiv b \pmod{n}$, si $a - b \in n\mathbf{Z}$, i.e. $a + n\mathbf{Z} = b + n\mathbf{Z}$.

On a donc

$$(a \equiv b \pmod{n}) \Leftrightarrow (n \mid (b-a))\ .$$

Proposition 16 - 4

La relation de congruence modulo n est une relation d'équivalence. Les classes, appelées **classes de congruence**, sont au nombre de n et, plus précisément, un ensemble de représentants est donné par les classes de $0, 1, \ldots, n-1$.

Démonstration. Les propriétés des relations d'équivalence se vérifient directement. On remarquera qu'on n'utilise que le fait que $n\mathbf{Z}$ est un groupe additif.

La définition par $n \mid (b-a)$ montre que $0, 1, \ldots, n-1$ ne sont pas dans la même classe (deux à deux) puisque leurs différences respectives sont comprises strictement entre $-n$ et n.

Le fait que ce soit un ensemble complet de représentants résulte de la division euclidienne : soit a dans $\mathbf{Z}$ et $a = nq + r$ la division euclidienne de a par n, alors $a \equiv r \pmod{n}$ et $0 \leq r \leq n-1$. □

Notation

L'ensemble des classes de congruences modulo n se note $\mathbf{Z}/n\mathbf{Z}$. Si k appartient à $\mathbf{Z}$, on note (en l'absence d'ambiguïté) $\overline{k}$ la classe de congruence de k modulo n.

Théorème 16 - 6

Pour tout entier naturel non nul n, $\mathbf{Z}/n\mathbf{Z}$ est un anneau pour les lois induites par l'addition et la multiplication sur $\mathbf{Z}$, i.e. pour α et β dans $\mathbf{Z}/n\mathbf{Z}$, soit a et b tels que $\alpha = \overline{a}$ et $\beta = \overline{b}$, on peut poser

$$\alpha + \beta = \overline{a+b} \quad \text{et} \quad \alpha \cdot \beta = \overline{ab}$$

et ces deux lois munissent $\mathbf{Z}/n\mathbf{Z}$ d'une structure d'anneau commutatif.

La projection canonique $a \mapsto \overline{a}$ est un morphisme surjectif d'anneaux de $\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$.

Démonstration. On vérifie que les lois sont bien définies : si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors $(a+b) - (a'+b') = (a-a') + (b-b') \in n\mathbf{Z}$ par stabilité d'un idéal par addition, et

$$ab - a'b' = \begin{vmatrix} a & b \\ a' & b' \end{vmatrix} = \begin{vmatrix} a-a' & b-b' \\ a' & b' \end{vmatrix} \in n\mathbf{Z}$$

puisque $n\mathbf{Z}$ est stable par multiplication externe par $\mathbf{Z}$ et par addition.

Les propriétés d'anneau sont induites de celles de $\mathbf{Z}$: on a $0_{\mathbf{Z}/n\mathbf{Z}} = \overline{0}$, $1_{\mathbf{Z}/n\mathbf{Z}} = \overline{1}$, $-\overline{a} = \overline{-a}$ et la distributivité et les commutativités sont immédiates.

La définition même des lois montre que la projection canonique est un morphisme d'anneaux puisque $\overline{1}$ est bien élément neutre dans $\mathbf{Z}/n\mathbf{Z}$. Il est surjectif par définition. □

Rappel

Soit A un anneau commutatif. On dit qu'il est intègre (resp. que c'est un corps) si tous ses éléments non nuls sont réguliers (resp. inversibles dans A). En particulier un corps est intègre.

Théorème 16 - 7

L'anneau $\mathbf{Z}/n\mathbf{Z}$ a les propriétés suivantes :

1. $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si n est premier.
2. $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est premier.
3. Si a est dans $\mathbf{Z}$, $\overline{a}$ est inversible dans $\mathbf{Z}/n\mathbf{Z}$ si et seulement si $a \wedge n = 1$.
4. Soit α dans $\mathbf{Z}/n\mathbf{Z}$, α est inversible si et seulement si c'est un générateur du groupe additif $\mathbf{Z}/n\mathbf{Z}$.

Démonstration. Avec les notations précédentes, l'intégrité s'écrit $\alpha\beta = \alpha\beta' \Rightarrow (\alpha = \overline{0} \vee \beta = \beta')$ ou encore $\alpha\beta = \overline{0} \Rightarrow (\alpha = \overline{0} \vee \beta = \overline{0})$, soit $p \mid ab \Rightarrow (p \mid a \vee p \mid b)$. Il s'agit

du lemme d'EUCLIDE (que l'on peut voir comme conséquence du lemme de GAUSS) lorsque p est premier.

Réciproquement, si p n'est pas premier, on l'écrit $p = ab$ avec $0 < a, b < p$ et on a $\overline{a}\overline{b} = \overline{0}$ bien que $\overline{a}$ et $\overline{b}$ ne soient pas nuls.

Comme un corps est intègre, il est nécessaire que n soit premier pour que $\mathbf{Z}/n\mathbf{Z}$ soit un corps. Réciproquement si $0 < a < n$ avec n premier, alors a est premier avec n puisque n n'a pas de diviseurs dans $[\![2; n-1]\!]$. Si $au + nv = 1$ est une relation de BÉZOUT dans $\mathbf{Z}$, alors on a $\overline{au} = \overline{1}$ et ceci montre que $\overline{a}$ est inversible dans $\mathbf{Z}/n\mathbf{Z}$. Et il en résulte que $\mathbf{Z}/n\mathbf{Z}$ est un corps.

La démonstration précédente montre que si $a \wedge n = 1$, alors $\overline{a} \in (\mathbf{Z}/n\mathbf{Z})^\times$. Réciproquement si $a \wedge n = d$ avec $d > 1$, alors $d \mid a$ et donc $n \mid a(n/d)$. En posant $m = n/d$, on a $m \in \mathbf{Z}$ et $\overline{am} = \overline{0}$ et donc $\overline{a}$ est un diviseur de 0 dans $\mathbf{Z}/n\mathbf{Z}$, aussi n'est-il pas inversible.

Pour α dans $\mathbf{Z}/n\mathbf{Z}$, α est un générateur si et seulement si $\overline{1}$ appartient à $\alpha\mathbf{Z}/n\mathbf{Z}$, i.e. si et seulement s'il existe k dans $\mathbf{Z}$ tel que $k\alpha = \overline{1}$. Par définition de la loi sur $\mathbf{Z}/n\mathbf{Z}$, cette dernière propriété s'écrit $\overline{k}\alpha = \overline{1}$ et est équivalente à l'inversibilité de α. □

Définition 16 - 6

Si A est un anneau, on note $A^\times$ le groupe multiplicatif de ses éléments inversibles (dans A). On note $\varphi(n)$ le cardinal de $(\mathbf{Z}/n\mathbf{Z})^\times$. Cette fonction est appelée fonction indicatrice d'EULER.

Exemple 16 - 2

On a $\mathbf{Z}^\times = \{\pm 1\}$ et $\mathbf{K}[X]^\times = \mathbf{K}^*$ si $\mathbf{K}$ est un corps. D'après ce qui précède, on a

$$\varphi(n) = \text{Card}\left(\{a \in [\![1; n-1]\!] \mid a \wedge n = 1\}\right) .$$

En particulier si $n = p^k$, avec p premier, on a $\varphi(p^k) = p^k - p^{k-1} = n\left(1 - \dfrac{1}{p}\right)$ car $a \wedge n = 1 \iff a \wedge p = 1$.

Définition 16 - 7

Soit A et B deux anneaux. On appelle morphisme d'anneaux toute application $\varphi : A \to B$ telle que

1. $\varphi(1_A) = 1_B$,
2. $\forall (a, b) \in A^2$, $\varphi(a + b) = \varphi(a) + \varphi(b)$,
3. $\forall (a, b) \in A^2$, $\varphi(ab) = \varphi(a)\varphi(b)$.

On note $\text{Hom}(A, B)$ l'ensemble de ces morphismes. Si $A = B$, on parle d'endomorphismes d'anneaux et on note $\text{End}(A)$ leur ensemble.

Exemple 16 - 3

Le morphisme canonique π_n de $\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ est un morphisme d'anneaux.

Définition 16 - 8

On appelle isomorphisme d'anneaux de A sur B tout morphisme bijectif et on note $\text{Isom}(A, B)$ leur ensemble. L'écriture $A \cong B$ signifie qu'il existe un isomorphisme de A sur B. On appelle automorphisme de l'anneau A tout endomorphisme bijectif de A et on note $\text{Aut}(A)$ leur ensemble.

Comme un morphisme d'anneaux est en particulier un morphisme de groupes, il est surjectif si et seulement si $\text{Im}(f) = B$ et injectif si et seulement si $\text{Ker}(f) = \{0_A\}$.

Remarque 16 - 2

Si f est un isomorphisme d'anneaux entre A et B, alors f induit un isomorphisme de groupes entre $A^\times$ et $B^\times$ puisqu'alors $xy = 1_A \iff f(x)f(y) = 1_B$.

Propriété 16 - 1

Sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ (♠)

Les sous-groupes de $(\mathbf{Z}/n\mathbf{Z}, +)$ sont cycliques.

Les idéaux $\mathbf{Z}/n\mathbf{Z}$ sont principaux. Par contre, par définition d'un anneau principal, un anneau principal est intègre et donc $\mathbf{Z}/n\mathbf{Z}$ n'est un anneau principal que si c'est un corps et alors ses idéaux sont l'idéal nul et lui-même.

Démonstration. Soit H un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ et π_n le morphisme canonique de $\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$. L'image réciproque $\pi_n^{-1}(H)$ est un sous-groupe de $\mathbf{Z}$, donc de la forme $p\mathbf{Z}$. Par surjectivité de π_n, on a $H = \pi_n\left(\pi_n^{-1}(H)\right)$ et puisque $p\mathbf{Z}$ est monogène engendré par p, H est engendré par $\pi_n(p)$ et est donc monogène. Comme il est évidemment fini, H est cyclique. Plus précisément, $H = \overline{p}\,(\mathbf{Z}/n\mathbf{Z})$, ce qui démontre que H est principal. □

Remarque 16 - 3

On peut écrire $\pi_n^{-1}(H) \supset \mathrm{Ker}(\pi_n) = n\mathbf{Z}$ et donc $p \mid n$. Il en résulte

$$H = \overline{p}\ \mathbf{Z}/n\mathbf{Z} \cong (p\mathbf{Z})/(n\mathbf{Z}) \cong \mathbf{Z}/(n/p)\mathbf{Z}$$

et en particulier $\mathrm{Card}(H) = n/p$.

Proposition 16 - 5

Premier théorème d'isomorphisme (♠)

Soit A un anneau et f dans $\mathrm{Hom}(\mathbf{Z}, A)$. Si le noyau de f contient $n\mathbf{Z}$, on peut factoriser f par le morphisme canonique π_n de $\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$, i.e. il existe $\overline{f} \in \mathrm{Hom}(\mathbf{Z}/n\mathbf{Z}, A)$ tel que $f = \overline{f} \circ \pi_n$. On dit que $\overline{f}$ est induit par f par **passage au quotient**.

Démonstration. Cela résulte directement du fait qu'on a $\mathrm{Ker}(\pi_n) \subset \mathrm{Ker}(f)$. □

Théorème 16 - 8

Théorème (des restes) chinois

Soit p et q deux entiers naturels non nuls et **premiers entre eux**. On a un isomorphisme d'anneaux

$$\mathbf{Z}/pq\mathbf{Z} \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$$

induit par l'homomorphisme canonique de $\mathbf{Z}$ dans $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$.

En particulier

$$(\mathbf{Z}/pq\mathbf{Z})^\times \cong (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times \ .$$

Démonstration. Soit $\pi_p \in \mathrm{Hom}(\mathbf{Z}, \mathbf{Z}/p\mathbf{Z})$ et $\pi_q \in \mathrm{Hom}(\mathbf{Z}, \mathbf{Z}/q\mathbf{Z})$ les morphismes canoniques et f le morphisme donné par $f(a) = (\pi_p(a), \pi_q(a))$.

Puisque pq est dans le noyau des morphismes π_p et π_q, il est dans celui de f, de sorte que f passe au quotient et induit un morphisme $\overline{f}$ dans $\mathrm{Hom}(\mathbf{Z}/pq\mathbf{Z}, \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z})$.

Ce morphisme est injectif d'après le lemme de Gauss : en effet si $\overline{f}(\alpha) = (\overline{0}, \overline{0})$ et si $\alpha = \overline{a}$, alors $p \mid a$ et $q \mid a$ et donc, puisque p et q sont premiers entre eux, $pq \mid a$, i.e. $\alpha = \overline{0}$. Mézalor, puisque ces deux anneaux sont de cardinal pq, $\overline{f}$ est aussi surjectif, donc bijectif. Le dernier point résulte du fait qu'un isomorphisme préserve les éléments inversibles. □

Remarque 16 - 4

La démonstration ne fournit pas une méthode constructive. Néanmoins il suffit de trouver un antécédent à $(\overline{1},\overline{0})$ et $(\overline{0},\overline{1})$ pour construire l'application réciproque. En effet si a et b dans $\mathbf{Z}/pq\mathbf{Z}$ vérifient $\overline{f}(a)=(\overline{1},\overline{0})$ et $\overline{f}(b)=(\overline{0},\overline{1})$, alors pour tout (m,n) dans $\mathbf{Z}^2$, $\overline{f}(ma+nb)=(\overline{m},\overline{n})$. Or si $up+vq=1$ est une relation de BÉZOUT entre p et q, alors $a=\overline{vq}$ et $b=\overline{up}$ conviennent. Autrement dit $f(nup+mvq)=(\overline{m},\overline{n})$.

Exemple 16 - 4

Par exemple pour $p=5$ et $q=7$. On écrit $-4\times 5+3\times 7=1$ et donc pour trouver un entier naturel x tel que $x\equiv \mathbf{4} \pmod 5$ et $x\equiv \mathbf{2} \pmod 7$, il suffit de poser

$$x=-4\times 5\times \mathbf{2}+3\times 7\times \mathbf{4}=44$$

et on peut même prendre $x=9$ puisque c'est la même chose modulo 35. C'est d'ailleurs un fait général, cette méthode donne rarement un x optimal au sens que sa valeur absolue est la plus petite possible ou qu'il est compris entre 1 et pq (ce qui n'est d'ailleurs pas la même chose).

Attention ! Il faut multiplier la partie en p par le nombre à atteindre modulo q et vice-versa.

Corollaire 16 - 1

Calcul de la fonction indicatrice d'EULER

La fonction φ est multiplicative au sens suivant :

$$p\wedge q=1\Rightarrow \varphi(pq)=\varphi(p)\varphi(q)\ .$$

En particulier $\varphi(n)=n\prod_{p|n}\left(1-\frac{1}{p}\right)$.

Démonstration. C'est une conséquence directe de l'isomorphisme

$$(\mathbf{Z}/pq\mathbf{Z})^\times\cong(\mathbf{Z}/p\mathbf{Z})^\times\times(\mathbf{Z}/q\mathbf{Z})^\times$$

en prenant les cardinaux, et du calcul de $\varphi(n)$ dans le cas où n est une puissance d'un nombre premier. □

3 Propriétés générales des anneaux et des algèbres

Dans ce paragraphe A est un anneau ou une $\mathbf{K}$-algèbre associative.

Proposition 16 - 6

L'élément nul est absorbant : $\forall x\in A,\ x\cdot 0=0\cdot x=0$.

Démonstration. Soit x dans A, on a $0\cdot x=(1-1)x=x-x=0$ et de même $x\cdot 0=0$. □

Définition 16 - 9

Unités

Un élément a de A est dit **inversible** (dans A) s'il admet un inverse b dans A, i.e. $ab=ba=1_A$. On le note alors a^{-1}. Les éléments inversibles dans A sont appelés unité de A. On note leur ensemble $\mathcal{U}(A)$ ou encore $A^\times$.

Remarque 16 - 5

Si x est inversible dans A, x^{-1} aussi et on a $\left(x^{-1}\right)^{-1} = x$. Si, de plus y est inversible dans A, xy l'est aussi et son inverse est $y^{-1}x^{-1}$. Comme $1 \in A^\times$, $A^\times$ est un sous-magma de A, stable par passage à l'inverse, i.e. est un groupe.

Danger

On note $A^\times$ l'ensemble des unités, mais souvent on le note plutôt A^* et cette notation se mélange avec la coutume qui est que l'exposant * signifie « privé de 0 ». Ces deux notations représentent la même notion dans le cas d'un corps, mais pas pour un anneau général, notamment dans $\mathbf{Z}$. Le plus souvent le contexte sera explicite et on gardera en général la notation $A^\times$ pour des anneaux abstraits, de sorte que $\mathbf{Z}^*$ aura quasiment toujours le sens d'ensemble des entiers relatifs non nuls.

Définition 16 - 10

Diviseurs de 0

Un élément a de A est dit **diviseur de** 0 à gauche (respectivement à droite) s'il est non nul et s'il existe x dans A, non nul, tel que $ax = 0$ (respectivement $xa = 0$). Un anneau commutatif ne possédant aucun diviseur de 0 est dit intègre.

Remarque 16 - 6

Les éléments inversibles sont réguliers et il y a équivalence entre ne pas être un diviseur de 0 est être régulier puisque, pour a, x et y dans A, on a $ax = ay \iff a(x-y) = 0$ et, de même à droite.

Définition 16 - 11

Nilpotents

On définit les **itérés** de a selon les lois $+$ et $\cdot$: ka pour $k \in \mathbf{Z}$ et a^n pour $n \in \mathbf{N}$, voire pour $n \in \mathbf{Z}$ si a est inversible.

L'élément a est dit **nilpotent** s'il existe n dans $\mathbf{N}^*$ tel que $a^n = 0$. Dans ce cas l'**indice de nilpotence** de a est le plus petit entier p qui réalise cette propriété : $p = \min\{n \in \mathbf{N}^* \mid a^n = 0\}$.

Exercice

Exhiber, s'il en existe, des diviseurs de 0 et des éléments nilpotents dans $\mathscr{M}_n(\mathbf{K})$ et $C(I, \mathbf{R})$.

Proposition 16 - 7

Soit a, b, b_1, $\cdots$, b_n des éléments de A. On a par distributivité

$$a \cdot \left(\sum_{i=1}^{n} b_i\right) = \sum_{i=1}^{n} (a \cdot b_i) \quad \text{et} \quad \left(\sum_{i=1}^{n} b_i\right) \cdot a = \sum_{i=1}^{n} (b_i \cdot a)\ .$$

La règle des signes $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ en résulte et, comme on a $(n \cdot 1)b = nb$ la loi de composition externe de $\mathbf{Z}$ sur A s'interprète comme une loi de composition interne en identifiant l'élément n de $\mathbf{Z}$ à $n \cdot 1_A$. Et, plus généralement, on a $\forall n \in \mathbf{Z}$, $(na) \cdot b = a \cdot (nb) = n(a \cdot b)$.

Démonstration. On a, par distributivité, $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$ et donc $(-a) \cdot b = -a \cdot b$. De même $a \cdot (-b) = -a \cdot b$, d'où le résultat. Le reste est une conséquence de la distributivité et de la règle des signes (avec $b_1 = \cdots = b_n = b$ et éventuellement $a = 1_A$). □

Notation

Si a et b sont dans A, on note $[a,b]$ leur défaut de commutation, i.e. $[a,b] = ab-ba$. Par conséquent a et b commutent (i.e. $ab=ba$) si et seulement si $[a,b]=0$. Attention ! Cette notation n'est pas officiellement au programme, même si elle est très courante notamment dans la théorie des algèbres de LIE (Sophus LIE, 1842–1899).

Théorème 16 - 9

Soit a et b dans A et commutant entre eux (i.e. $ab=ba$), on a

1. Pour tout couple d'entiers naturels (p,q), on a $[a^p, b^q]=0$.
2. Formule du binôme de NEWTON

$$(a+b)^n = \sum_{\substack{k_1+\cdots+k_p=n \\ 0\leq k_1, 0<k_2,\ldots,k_p}} a^{k_1}b^{k_2}a^{k_3}\cdots = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}\ .$$

3. Formule de Jacob BERNOULLI (identité remarquable)

$$a^n - b^n = \sum_{k=0}^{n-1} a^k(a-b)b^{n-1-k} = (a-b)\left(\sum_{k=0}^{n-1}a^k b^{n-1-k}\right)\ .$$

Les formules médianes sont vraies **même si a et b ne commutent pas**.

Démonstration. Par récurrence sur p, on obtient le résultat pour $q=1$, grâce à la formule $[a^{p+1},b] = a^{p+1}b - ba^{p+1} = a(a^pb-ba^p)+(ab-ba)a^p$. On a donc, pour p dans $\mathbf{N}$, $[a^p,b]=0$ et aussi $[b,a^p]=0$. Ce qu'on vient juste de démontrer donne immédiatement le résultat. Il résulte de ce qui précède qu'un produit de k termes égaux à a et ℓ termes égaux à b est indépendant de l'ordre dans lequel est effectué le produit, et les deux formules en découlent. □

Proposition 16 - 8

Cas particuliers de la formule de BERNOULLI

Somme d'une progression géométrique Pour a dans A et n entier naturel non nul, on a puisque 1 et a commutent

$$1-a^n = (1-a)\sum_{k=0}^{n-1}a^k = \left(\sum_{k=0}^{n-1}a^k\right)(1-a)\ .$$

En particulier si a un élément de A **nilpotent** d'indice inférieur à p, alors $1-a$ est **inversible** d'inverse donné par

$$(1-a)^{-1} = \sum_{k=0}^{p-1}a^k\ .$$

Exercice

Établir la formule du multinôme, valable pour $a_1, a_2, \cdots, a_p$ commutant deux à deux :

$$\forall n\in\mathbf{N},\ (a_1+a_2+\cdots+a_p)^n = \sum_{\substack{(\alpha_1,\alpha_2,\ldots,\alpha_p)\in\mathbf{N}^p \\ \alpha_1+\alpha_2+\cdots+\alpha_p=n}} \frac{n!}{\alpha_1!\,\alpha_2!\cdots\alpha_p!}a_1^{\alpha_1}a_2^{\alpha_2}\cdots a_p^{\alpha_p}.$$

On a différents moyens de construire un anneau : partir d'un anneau et regarder à l'intérieur, mettre ensemble des anneaux ou les transformer.

Définition 16 - 12

Sous-anneau

Une partie B de A en est un sous-anneau si, muni des mêmes lois (i.e. de leurs birestrictions à B), B est un anneau d'unité 1_A. De façon équivalente, B est un sous-anneau de A si et seulement si $1_A \in B$ et pour tout (x, y) dans B^2, $x - y$ et xy appartiennent à B.

On remarquera que 0_A appartient nécessairement à B.

Définition 16 - 13

Sous-algèbre

Si A est une $\mathbf{K}$-algèbre, une partie B de A en est une sous-$\mathbf{K}$-algèbre si c'en est un sous-espace vectoriel et un sous-magma unifère pour la multiplication, i.e. si et seulement si $1_A \in B$ et pour tous (x, y) dans B^2 et (λ, μ) dans $\mathbf{K}^2$, $\lambda x + \mu y$ et xy appartiennent à B.

Exemples 16 - 5

L'anneau A lui-même est un sous-anneau (trivial) de A.

Par contre $\{0_A\}$ n'est pas un anneau, donc pas non plus un sous-anneau.

L'ensemble des matrices diagonales 2×2 de la forme $\mathrm{diag}(x, 0)$ avec $x \in \mathbf{K}$ n'est pas un sous-anneau de l'anneau $\mathscr{M}_2(\mathbf{K})$ car il ne contient pas son unité et pourtant, muni des lois induites, c'est un anneau, d'unité $\mathrm{diag}(1, 0)$.

Remarque 16 - 7

L'intersection de sous-anneaux de A en est un et on peut, tout comme pour les groupes, définir l'anneau engendré par une partie. Néanmoins cette notion n'a que peu d'intérêt et on lui préfère celle d'idéal engendré par une partie, comme nous le verrons.

La réunion de deux sous-anneaux n'a aucune raison d'en être un.

Définition 16 - 14

Si A et B sont deux anneaux, on peut munir le produit cartésien $A \times B$ d'une structure d'anneau en effectuant les opérations composantes par composantes. Son élément neutre est le couple formé des éléments neutres respectifs de A et B.

Exemple 16 - 6

Si A' et B' sont des sous-anneaux respectifs de A et B, $A' \times B'$ est un sous-anneau de $A \times B$.

Définition 16 - 15

Soit A et B des $\mathbf{K}$-algèbres. On appelle morphisme d'algèbres une application linéaire qui est multiplicative.

Remarque 16 - 8

Soit φ un homomorphisme d'anneaux (ou de $\mathbf{K}$-algèbres) de A dans B. On a $\varphi(0_A) = 0_B$. Pour a dans A on a $\varphi(-a) = -\varphi(a)$ et, pour n dans $\mathbf{N}$, $\varphi(na) = n\varphi(a)$ et $\varphi(a^n) = \varphi(a)^n$. La première propriété est encore vraie pour n dans $\mathbf{Z}$. La seconde l'est aussi si, de plus, a est inversible.

Exemples 16 - 7

L'application identique est un endomorphisme pour tout anneau. L'application $z \mapsto \overline{z}$ appartient à $\mathrm{End}(\mathbf{C})$. L'application $a+ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ appartient à $\mathrm{Hom}(\mathbf{C}, \mathscr{M}_2(\mathbf{R}))$.

Tout comme pour les groupes, on peut utiliser une bijection ensembliste de A sur un ensemble E pour munir, **par transport de structure**, E d'une structure d'anneau.

Propriété 16 - 2

L'image directe par un morphisme d'anneaux d'un sous-anneau de A est un sous-anneau de B et l'image réciproque d'un sous-anneau de B est un sous-anneau de A. En particulier si f est un morphisme d'anneaux, $\mathrm{Im}(f)$ est un sous-anneau de l'anneau d'arrivée.

Remarque 16 - 9

Par contre $\mathrm{Ker}(f)$ n'est jamais un sous-anneau de l'anneau source car il ne contient pas 1_A.

Exemple 16 - 8

Soit $\varphi : \mathbf{Z} \to A$ qui à l'entier naturel n associe $n1_A$. C'est un homomorphisme d'anneaux. Mais attention ! ce morphisme n'est pas injectif en général, de sorte que l'on ne peut pas penser $\mathbf{Z}$ comme un sous-anneau de A. Néanmoins cette propriété universelle de $\mathbf{Z}$, qui permet d'envoyer tout élément de $\mathbf{Z}$ dans A, est une propriété forte. On dit que $\mathbf{Z}$ est un objet initial dans la catégorie des anneaux.

Remarque 16 - 10

L'ensemble $\mathrm{Aut}(A)$ est un sous-groupe de S_A.

Définition 16 - 16

Si A est commutatif et si $A^\times = A\backslash\{0\}$, on dit que A est un corps (commutatif). En particulier un corps est intègre.

Exemples 16 - 9

Les anneaux $(\mathcal{F}(X,K),+,\times)$, $(\mathscr{L}(E),+,\circ)$ et $(\mathscr{M}_n(\mathbf{K}),+,\times)$ ne sont pas intègres. Les anneaux $(\mathbf{Z},+,\times)$ et $(\mathbf{K}[X],+,\times)$ sont intègres mais ne sont pas des corps. Bien sûr $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$ sont des corps, tout comme $\mathbf{Q}[\sqrt{2}]$ défini par $\mathbf{Q}[\sqrt{2}] = \left\{a+b\sqrt{2} \;\middle|\; (a,b) \in \mathbf{Q}^2\right\}$ est un corps. Plus subtil : un anneau intègre fini est un corps car l'application $x \mapsto ax$ est surjective.

Définition 16 - 17

Sous-corps

On appelle sous-corps d'un corps $\mathbf{K}$ tout sous-anneau possédant la structure de corps. Une partie $\mathbf{L}$ d'un corps $\mathbf{K}$ en est un sous-corps si et seulement si $1_{\mathbf{K}} \in \mathbf{L}$ et $\forall (x,y) \in \mathbf{L}^2$, $x-y \in \mathbf{L}$ et, si $y \neq 0$, $xy^{-1} \in \mathbf{L}$.

Remarque 16 - 11

L'intersection de sous-corps de $\mathbf{K}$ en est un, mais la réunion de sous-corps n'a aucune raison d'en être un.

Définition 16 - 18

Un morphisme de corps n'est rien d'autre qu'un morphisme d'anneaux entre deux corps.

Théorème 16 - 10

Soit $\mathbf{K}$ et $\mathbf{L}$ deux corps et f dans $\mathrm{Hom}(\mathbf{K},\mathbf{L})$. Alors

1. pour tout x dans $\mathbf{K}^*$, on a $f(x^{-1}) = f(x)^{-1}$;
2. f est injectif et $\mathrm{Im}(f)$ est un sous-corps de $\mathbf{L}$ isomorphe à $\mathbf{K}$. De plus ces deux propriétés sont encore valides si $\mathbf{L}$ est anneau.

Démonstration. Puisque f est un morphisme de magmas entre les groupes $\mathbf{K}^*$ et $\mathbf{L}^*$, c'est un morphisme de groupes et donc il préserve l'inverse. Plus généralement si x est non nul, on a $f(xx^{-1}) = f(1) = 1$ et $f(x^{-1}x) = f(1) = 1$, donc $f(x)$ est inversible, d'inverse $f(x)^{-1}$ et ceci que $\mathbf{L}$ soit un corps ou simplement un anneau. Il en résulte que si x est non nul, $f(x)$ aussi et donc $\mathrm{Ker}(f)$ est réduit à $\{0\}$, i.e. f est injectif. En conséquence f réalise une bijection de $\mathbf{K}$ sur son image. □

4 Arithmétique

On a vu qu'un noyau de morphisme d'anneaux n'est pas un sous-anneau, on pourrait s'intéresser à sa structure de pseudo-anneau, mais en fait elle est plus riche que cela. C'est un idéal. Le mot idéal est un vocabulaire emprunté à Ernst Kümmer (1810–1893) et Richard Dedekind (1831–1916) : ils étaient à la recherche de nombres idéaux permettant de retrouver l'unicité de la décomposition en facteurs premiers dans des contextes plus généraux que les entiers. Par exemple dans $\mathbf{Z}[i\sqrt{5}]$ on a $6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ et chacun des deux facteurs ne peut pas être décomposé plus avant. L'idée est donc d'inventer, tout comme on a inventé un nombre de carré -1, des nombres tels que $2 = ab$, $3 = cd$, $1 + i\sqrt{5} = ac$ et $1 - i\sqrt{5} = bd$. Ce sont ces nombres qui sont qualifiés d'idéaux.

In fine il se révèle que ces nombres sont des ensembles (mais les autres nombres ne sont-ils pas eux aussi des ensembles ?!).

Rappel

Idéal

Soit A un anneau **commutatif** et I une partie de A. On dit que I est un idéal de A si c'en est un sous-groupe additif et qu'il est stable par multiplication externe par A, i.e.

$$\forall x \in I\,,\ \forall a \in A\,,\quad ax \in I\,.$$

Remarques 16 - 12

Si 1_A appartient à I, alors $I = A$, par stabilité par multiplication externe par des éléments de A. En particulier I est aussi un sous-anneau si et seulement si $I = A$.

Si A est un corps, alors $I = A$ ou $I = \{0\}$. En effet si x est non nul et appartient à I, alors x^{-1} appartient à A et donc $x^{-1}x \in I$, i.e. $1 \in I$.

La notation (hors-programme) A/I, où A est un anneau et I en est un idéal, généralise celle adoptée pour $\mathbf{Z}/n\mathbf{Z}$ et on peut montrer que A/I peut être canoniquement muni d'une structure d'anneau. La démonstration est identique à celle effectuée pour $\mathbf{Z}/n\mathbf{Z}$.

Exemple 16 - 10

L'ensemble des multiples d'un élément a, noté aA ou Aa, est un idéal de A.
Quand A est intègre, ou si a n'est pas un diviseur de 0, les éléments de aA s'écrivent de façon unique sous la forme ab avec b dans A. Dans ce cas l'idéal est en bijection avec l'anneau total.

♠

On appelle idéal principal un idéal de la forme aA.
Un anneau **intègre** dont tous les idéaux sont principaux est dit principal. Par exemple $\mathbf{Z}$ et $\mathbf{K}[X]$ le sont. En fait l'existence d'une division euclidienne (on parle alors d'anneau euclidien) entraîne l'existence d'une décomposition essentiellement unique en facteurs premiers (on parle d'anneau factoriel) et celle-ci entraîne à son tour que tous les idéaux sont principaux.

Définition 16 - 19

Divisibilité dans A
Lorsque A est intègre, pour a et b dans A, on dit que a divise b ou que b est un multiple de a si $b \in aA$. On note $a \mid b$.

Remarque 16 - 13

On a $a \mid b \iff bA \subset aA$.

Pour aller plus loin

Une intersection (quelconque) d'idéaux de A est un idéal. Si J est une partie d'un anneau A, on définit l'idéal engendré par J, et on le note (J), comme l'intersection de tous les idéaux de A contenant J. On a également

$$(J) = \left\{ x \in A \;\middle|\; \exists n \in \mathbf{N}^*,\ \exists (x_i)_{1\leq i\leq n} \in J^n,\ \exists (a_i)_{1\leq i\leq n} \in A^n \quad x = \sum_{i=1}^{n} a_i x_i \right\} .$$

Proposition 16 - 9

Noyau d'un morphisme d'anneaux
Si $f : A \to B$ est un morphisme d'anneaux, avec A commutatif, alors $\mathrm{Ker}(f)$ est un idéal de A.

Démonstration. Soit a dans A et x dans $\mathrm{Ker}(f)$, on a $f(ax) = f(a)f(x) = f(a)\cdot 0 = 0$ et donc $ax \in \mathrm{Ker}(f)$.
Comme f est aussi un morphisme de groupes, $\mathrm{Ker}(f)$ est un sous-groupe de A et donc, finalement, c'en est un idéal. □

Exemple 16 - 11

L'évaluation d'un polynôme, par exemple en 0 est un morphisme : soit f de $\mathbf{K}[X]$ dans $\mathbf{K}$ qui au polynôme P associe $P(0)$, on a $\mathrm{Ker}(f) = X\mathbf{K}[X]$, i.e. $\mathrm{Ker}(f)$ est formé des multiples de X.

Il y a un autre corollaire de la factorisation d'un morphisme, dans le cas des corps :

Théorème 16 - 11

Caractéristique d'un corps (♠)
Soit $\mathbf{K}$ un corps et f le morphisme canonique de $\mathbf{Z}$ dans $\mathbf{K}$. Son noyau est soit nul, soit de la forme $p\mathbf{Z}$ avec p premier.

Démonstration. Si $\mathrm{Ker}(f)$ n'est pas nul, on l'écrit $p\mathbf{Z}$ et si p n'est pas premier, on écrit $p = ab$. Mézalor a et b n'appartiennent pas à $\mathrm{Ker}(f)$, donc $f(a)$ et $f(b)$ sont non nuls. Or $f(a)f(b) = f(ab) = f(p) = 0$ et ceci contredit le fait qu'un corps est intègre. □

Pour aller plus loin

Plus conceptuellemment : on note $A = \mathbf{Z}$, $I = \mathrm{Ker}(f) = n\mathbf{Z}$ et on a un homomorphisme induit $\overline{f}$ dans $\mathrm{Hom}(A/I, \mathbf{K})$. Par définition du noyau ce morphisme est injectif et, par restriction, $\overline{f}^{|f(A)}$: $A/I \cong f(A)$. Comme $\mathbf{K}$ est un corps et que $f(A)$ en est un sous-anneau, ce dernier est en fait intègre. Par isomorphie A/I est également intègre et n est premier.

Définition 16 - 20

Caractéristique d'un corps (♠)

Si le noyau du morphisme précédent est $p\mathbf{Z}$, avec p premier, on dit que $\mathbf{K}$ est de **caractéristique** p. Sinon on dit qu'il est de caractéristique nulle.

Dans ce dernier cas, le morphisme canonique dans $\mathrm{Hom}(\mathbf{Z}, \mathbf{K})$ est injectif et $\mathbf{K}$ est infini.

Aparté

On appelle idéal premier d'un anneau A tout idéal I vérifiant

$$\forall (x, y) \in A^2,\ \big(xy \in I \Rightarrow (x \in I \text{ ou } y \in I)\big)\ .$$

On dit que a est premier dans A si aA l'est.

On dit que a est irréductible dans A si a n'est pas une unité et si, pour tout couple (b, c) d'éléments de A, on a $a = bc \Rightarrow (b \in A^\times \vee c \in A^\times)$. Il revient au même de demander à ce que l'idéal aA soit maximal pour l'inclusion, i.e. si $aA \subset bA$, alors soit $bA = aA$, soit $bA = A$.

Ces notions sont évidemment très proches et se confondent lorsque A est principal, donc en particulier lorsque $A = \mathbf{Z}$ ou $A = \mathbf{K}[X]$.

Un idéal $n\mathbf{Z}$ de $\mathbf{Z}$ est premier si et seulement $|n|$ est premier. Un idéal $P\mathbf{K}[X]$ est premier si et seulement si P est irréductible.

Exemple 16 - 12

Les corps $\mathbf{F}_p$ définis par $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ pour p premier sont de caractéristique p. Les corps de nombres $\mathbf{Q}$, $\mathbf{Q}[\sqrt{2}]$, $\mathbf{Q}[i]$, $\mathbf{R}$, $\mathbf{C}$ etc. sont de caractéristique nulle.

Remarque 16 - 14

On peut mettre une structure de corps sur V_4 (on rappelle que ce groupe est le groupe de Klein, ou Vierergruppe, à savoir $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$). Si on note ses éléments 0, 1, x et y (de sorte que $y = x+1$, $x = y+1$, $x+y = 1$, $x+x = y+y = 1+1 = 0$), alors on peut poser $x^2 = y$, $y^2 = x$ et $xy = yx = 1$. On note ce corps $\mathbf{F}_4$ et on peut vérifier que c'est le seul corps à quatre éléments (à isomorphisme près). On remarquera que $\mathbf{F}_4^\times$ est cyclique : c'est $\mathbf{Z}/3\mathbf{Z}$, ce qui était prévisible puisqu'il n'y a qu'un seul groupe à trois éléments et que $\mathbf{F}_4^\times$ est un tel groupe... mais c'est un phénomène général : le groupe des inversibles d'un corps fini est toujours cyclique.

Recherche

Donner un sens à la phrase suivante :

$$\mathbf{F}_4 \cong \mathbf{F}_2[X]/\left(X^2+X+1\right)$$

et la démontrer.

Plus fort ? Montrer que si p est premier et congru à 3 modulo 4, alors

$$\mathbf{F}_{p^2} = \mathbf{Z}[i]/(p)$$

est un corps à p^2 éléments (et c'est le seul à isomorphisme près).

Pour aller plus loin

Il n'existe pas de corps gauches finis : autrement dit la commutativité est automatique dans le cas des corps finis ! C'est un théorème de Joseph WEDDERBURN (1882 – 1948).

Exemples 16 - 13

1. On peut penser à chercher les sous-anneaux de $\mathbf{Z}$, mais à cause de la propriété de $\mathbf{Z}$ comme objet initial, tout sous-anneau de $\mathbf{Z}$ contient $\mathbf{Z}$ et lui est donc égal.
2. Si on cherche des sous-anneaux de $\mathbf{R}$, il faut aussi commencer par inclure $\mathbf{Z}$. Le plus simple est de considérer l'ensemble $\mathbf{Z}[\sqrt{2}]$ des nombres de la forme $a+b\sqrt{2}$, avec a et b entiers. On note aussi cet anneau $\mathbf{Z} \oplus \sqrt{2}\mathbf{Z}$.
3. Si on cherche maintenant dans $\mathbf{C}$, un exemple est fourni par les entiers de GAUSS, $\mathbf{Z}[i]$. Il s'agit des nombres complexes de la forme $a+ib$ avec a et b entiers. Puisque $i^2=-1$, c'est bien un anneau. Il a été utilisé par GAUSS pour faire de l'arithmétique. Par exemple pour étudier l'équation diophantienne $x^2+y^2=z^2$, pour x, y et z entiers. On peut l'écrire $(x+iy)(x-iy)=z^2$ et, si on admet que les entiers de GAUSS ont des propriétés arithmétiques proches de celles des entiers, on peut en déduire que $x+iy$ et $x-iy$ n'admettent aucun diviseur commun en dehors de $1\pm i$ et trouver toutes les solutions.
4. Pour étudier l'équation de FERMAT $x^3+y^3=z^3$, toujours avec des inconnues entières, on peut utiliser un anneau semblable, à savoir $\mathbf{Z}[\rho]$, avec $\rho = e^{2i\pi/3}$. On a $1+\rho+\rho^2=0$ et donc $\rho^2=-1-\rho$, ce qui prouve que l'on obtient bien un anneau en considérant les nombres de la forme $a+b\rho$. En effet $(a+b\rho)(c+d\rho)=(ac-bd)+(ad+bc-bd)\rho$. Pour étudier l'équation de FERMAT, on utilise la factorisation $x^3+y^3=(x+y)(x+\rho y)(x+\rho^2 y)$.

En étudiant les éléments inversibles de ces anneaux, on voit apparaître les groupes $\mathbf{Z}/n\mathbf{Z}$, ce qui est encore une manifestation de propriétés arithmétiques :

1. $\mathbf{Z}^\times = \{\pm 1\} = U_2(\mathbf{C}) \cong \mathbf{Z}/2\mathbf{Z}$,
2. $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\} = U_4(\mathbf{C}) \cong \mathbf{Z}/4\mathbf{Z}$,
3. $\mathbf{Z}[\rho]^\times = \left\{\pm 1, \pm\rho, \pm\rho^2\right\} = U_6(\mathbf{C}) \cong \mathbf{Z}/6\mathbf{Z}$.

5 Rappels et compléments

5 1 Rappels

Définition 16 - 21

Soit A un ensemble muni de deux lois internes, notées $\intercal$ et $\perp$ (A est donc un multi-magma). On dit que A est un **anneau** si $(A, \intercal)$ est un groupe commutatif (abélien) et si la loi $\perp$ vérifie les propriétés d'associativité, de distributivité (par rapport à $\intercal$) et admet un élément neutre. On note 0 l'élément neutre de $(A, \intercal)$ et 1 celui de $(A, \perp)$.

Une **algèbre** sur un corps $\mathbf{K}$, ou $\mathbf{K}$-algèbre, est un $\mathbf{K}$-espace vectoriel muni d'une multiplication interne qui est bilinéaire. Dans le cadre du programme, on demande en sus que $(A, \times)$ soit unifère. Autrement dit $(A, +, \times)$ est un anneau où l'axiome d'associativité de la multiplication est remplacé par

$\forall \lambda \in \mathbf{K}, \forall (x, y) \in A^2 \ \lambda \star (x \times y) = (\lambda \star x) \times y = x \times (\lambda \star y)$.

5 2 Commutativité

On peut définir une structure plus générale de corps, mais le programme stipule que seuls les corps commutatifs seront manipulés. Lorsqu'un corps n'est pas commutatif, on parle de corps gauche.

De même le programme se restreint aux idéaux des anneaux commutatifs. Mais en l'absence de commutativité, on pourrait être conduit à considérer des idéaux à gauche, à droite ou bilatères. C'est cette dernière notion qui sert beaucoup en arithmétique car elle correspond aux propriétés d'un noyau. Toutefois les deux premières sont également très utiles et permettent de manipuler les anneaux un peu comme des scalaires dans un objet qui ressemble à un espace vectoriel. On parle alors de module.

Le plus souvent les modules sont considérés sur des anneaux principaux. Par exemple : $\mathscr{M}_n(\mathbf{Z})$ ou $\mathscr{M}_n(\mathbf{K}[X])$ sont des modules particulièrement intéressants. Le second est même crucial pour comprendre la réduction et interpréter correctement le polynôme caractéristique.

5 3 Arithmétique dans un anneau principal

Les définitions du ppcm et du pgcd s'étendent sans changer un iota au cas où A est principal, à ceci près qu'il n'y a en général pas de façon canonique de choisir un générateur de l'intersection de deux idéaux ou de l'idéal engendré par deux idéaux, i.e. de parler *du* ppcm ou *du* pgcd.

Autrement dit, en toute généralité $a \vee b$ et $a \wedge b$ ne sont pas définis de façon unique, mais à une unité près de l'anneau A.

Le théorème d'existence et d'unicité de la décomposition en irréductibles peut se reformuler en termes d'idéaux : si I et J sont deux idéaux, on pose $I \cdot J = (I \cup J)$. On a en particulier $I \cdot J = J \cdot I$ et on peut définir I^k pour k entier naturel etc. Alors, pour J idéal de $\mathbf{Z}$ ou de $\mathbf{K}[X]$, on a l'existence et l'unicité d'une décomposition

$$J = \prod_{I \in \mathcal{P}} I^{v_I(J)}$$

où $\mathcal{P}$ désigne l'ensemble des idéaux premiers de $\mathbf{Z}$ ou de $\mathbf{K}[X]$ et $(v_I(J))_{I \in \mathcal{P}}$ est une suite presque nulle dans $\mathbf{N}^{(\mathcal{P})}$. Le produit est donc un produit fini. On peut aussi reformuler l'expression des pgcd et des ppcm en utilisant des idéaux.

Exercices

Entiers

16 - 1 Ⓢ ★ Suite de nombres composés †

Montrer que pour tout entier n, il existe n entiers consécutifs non premiers.

16 - 2 Ⓢ ★★ Série harmonique †

Soit n un entier supérieur à 2. Montrer que $1+\frac{1}{2}+\cdots+\frac{1}{n}$ n'est pas un entier.

16 - 3 Ⓢ M 2018 ★★ Nombres de Mersenne

a. Soit p et q deux entiers supérieurs ou égaux à 2. Montrer que si q^p-1 est premier, alors p est premier et $q=2$.

b. Soit p un nombre premier impair et k un diviseur premier de 2^p-1. Montrer $k\equiv 1 \pmod{2p}$.

16 - 4 Ⓢ ★★

Soit a et b deux entiers naturels non nuls et n un entier supérieur à 2. Montrer que si a^n+b^n est premier, alors n est une puissance de 2 ou bien $a=b=1$.

Indication : Bernoulli.

16 - 5 Ⓢ ★★ Nombres de Fermat

Soit, pour $n\in\mathbf{N}$, $F_n=2^{2^n}+1$.

a. Pour n dans $\mathbf{N}$, montrer $\prod_{k=0}^{n}F_k=F_{n+1}-2$.

b. En déduire que, pour n et m entiers naturels distincts, $F_n\wedge F_m=1$.

c. En déduire que l'ensemble des nombres premiers est infini.

16 - 6 Ⓢ ★★ Puissances

Soit k un entier naturel supérieur à 2. Montrer que le produit $n(n+1)(n+2)$ de trois entiers consécutifs n'est pas une puissance k^{e}.

Indication : par l'absurde, montrer que $n(n+2)$ et $n+1$ sont des puissances k^{e}, puis comparer $n(n+2)$ et $(n+1)^2$.

16 - 7 Ⓢ C 2011 ★★ Arithmétique et polynômes

Soit P et Q dans $\mathbf{Z}[X]$ premiers entre eux en tant que polynômes de $\mathbf{Q}[X]$. On pose, pour n entier, $u_n=\text{pgcd}(P(n),Q(n))$. Montrer que (u_n) est périodique.

16 - 8 Ⓢ ★★★ Équation diophantienne

On s'intéresse à l'équation diophantienne cubique $x^3=y^2+2$, avec x et y dans $\mathbf{Z}$.

a. Montrer que y et x sont impairs.

b. Déterminer un sous-anneau de $\mathbf{C}$ dans lequel le membre de droite de cette équation se factorise.

c. À l'aide de la division dans $\mathbf{C}$, construire un tel anneau A de sorte qu'il ait une division euclidienne, i.e. $\forall(a,b)\in A\times A\setminus\{0\}$, $\exists(q,r)\in A^2$, $a=bq+r$ avec $|r|<|b|$.

d. On admet que dans un tel anneau, tout nombre se décompose en facteurs « premiers ». Montrer que 2 n'est pas premier dans A, mais qu'il est produit d'exactement deux nombres premiers.

e. Montrer que, si (x,y) est solution de l'équation diophantienne, alors x^3 est produit de deux facteurs premiers entre eux et donc produit de deux cubes.

f. Donner toutes les solutions de l'équation.

16 - 9 Ⓢ X 2018 ★★★ Équation de Pell-Fermat

Soit d dans $\mathbf{Z}$ et (E) l'équation $x^2-dy^2=1$ dont on cherche les solutions dans $\mathbf{Z}^2$.

a. **i.** On suppose $d\leq 0$. Résoudre (E).

ii. On suppose $\sqrt{d}\in\mathbf{N}$. Résoudre (E).

On suppose dans la suite $d>0$ et $\sqrt{d}\notin\mathbf{N}$.

b. **i.** Soit (x_0,y_0) une solution de (E) telle que $y_0\neq 0$. On pose $z=x_0+y_0\sqrt{d}$. Montrer $|z|\neq 1$ et qu'on peut construire une suite (x_n,y_n) d'entiers telle que pour tout entier naturel n on ait $z^{n+1}=x_n+\sqrt{d}y_n$.

ii. En déduire que l'équation (E) admet une infinité de solutions.

c. On admet que, pour tout réel irrationnel α, il existe une infinité de rationnels $r=\frac{p}{q}$ avec p et q premiers entre eux, tels que $0<|\alpha-r|<\frac{1}{q^2}$. Montrer qu'il existe une solution (x_0,y_0) de l'équation (E) telle que $y_0\neq 0$.

16 - 10 ★★★ Approximation forte

Soit p un nombre premier.

a. Montrer que l'on peut étendre la fonction valuation p-adique, notée v_p à $\mathbf{Q}^*$.

b. On pose $N_p(x)=p^{-v_p(x)}$ pour x dans $\mathbf{Q}^*$ et $N_p(0)=0$. Montrer qu'on a

a. $\forall x\in\mathbf{Q}$, $N_p(x)=0\iff x=0$.

b. $\forall(x,y)\in\mathbf{Q}^2$, $N_p(xy)=N_p(x)N_p(y)$.

c. $\forall(x,y)\in\mathbf{Q}^2$, $N_p(x+y)\leq N_p(x)+N_p(y)$.

On se donne $(p_i)_{1\leq i\leq n}$ des nombres premiers et on pose $d_0(x,y)=|x-y|$ et, pour $1\leq i\leq n$,

$d_i(x,y) = N_{p_i}(x-y)$. On note $d(x,y) = \sum_{i=0}^{n} d_i(x,y)$ et enfin on note Δ l'application diagonale de $\mathbf{Q}^{n+1}$ dans $\mathbf{Q}$, i.e. $\Delta(x) = (x,\dots,x)$.

c. Montrer que $\Delta(\mathbf{Q})$ est dense dans $\mathbf{Q}^{n+1}$, i.e.

$$\forall a \in \mathbf{Q}^{n+1}\ ,\ \forall \varepsilon \in \mathbf{R}_+^*\ ,\ \exists x \in \mathbf{Q} \quad d(a,\Delta(x)) \leq \varepsilon\ .$$

16 - 11 ★★★ Théorème de Fermat $n = 4$

On souhaite établir que, pour x, y et z dans $\mathbf{Z}$, on a $x^4 + y^4 = z^4 \Longrightarrow xyz = 0$.

a. Soit x, y et u dans $\mathbf{N}^*$ premiers dans leur ensemble et tels que $x^4 + y^4 = u^2$. Montrer que u est impair.

b. Se ramener au cas où il existe a et b dans $\mathbf{N}^*$ tels que $x^2 = 2ab$, $y^2 = a^2 - b^2$ et $u = a^2 + b^2$.

c. Montrer que a est impair et b est pair.

d. Montrer qu'il existe d et f dans $\mathbf{N}^*$ tels que $a = d^2$ et $b = 2f^2$, puis qu'on a $(2f^2)^2 + y^2 = (d^2)^2$.

e. Construire alors r et s dans $\mathbf{N}^*$ tels que $r^4 + s^4 = d^2$ et $d < u$.

f. Conclure

16 - 12 ★★★★ Théorème de Fermat $n = 3$

On souhaite établir que, pour x, y et z dans $\mathbf{Z}$, on a $x^3 + y^3 = z^3 \Longrightarrow xyz = 0$.

a. Se ramener au cas où ces trois nombres sont premiers entre eux deux à deux.

b. Démontrer alors que l'un d'eux est divisible par 3. On pourra établir $x+y = z \pmod 3$ et $3xy(x+y) = 0 \pmod 9$.

On conclut par une descente infinie en construisant un triplet plus petit vérifiant la même identité. Soit $A = \mathbf{Z}[\rho]$.

c. Montrer que A est un anneau euclidien pour le stathme donné par $N(a+b\rho) = |a+b\rho|^2 = a^2 - ab + b^2$.

d. Montrer que la décomposition en facteurs premiers dans A de 3 est $(-\rho^2)(1-\rho)^2$.

e. Se ramener à résoudre $x^3 + y^3 + z^3 = 0$ avec x, y, z dans A, premiers entre eux deux à deux et l'un d'eux divisible par $1-\rho$.

f. On étudie l'équation $u_1x^3 + u_2y^3 + u_3z^3 = 0$ avec u_i des unités de A.

i. Se ramener au cas où z est divisible par $1-\rho$ mais pas $x-y$.

ii. Montrer que si $x-1$ est divisible par $1-\rho$, alors $x^3 - 1$ l'est par $(1-\rho)^4$.

iii. En considérant $u_1x^3 + u_2y^3$, se ramener au cas $u_1 = u_2 = 1$.

iv. Montrer qu'on a $x + y = (1-\rho)u_1'X^3$, $x + \rho y = (1-\rho)u_2'Y^3$ et $x + \rho^2 = (1-\rho)u_3'Z^3$.

v. Conclure.

$\mathbf{Z}/n\mathbf{Z}$

16 - 13 Ⓢ ★ ♥

Résoudre en nombres entiers le système $\begin{cases} x \wedge y = 18 \\ x \vee y = 540\ . \end{cases}$

16 - 14 Ⓢ ★

Résoudre dans $\mathbf{Z}$ l'équation $10x \equiv 14 \pmod{18}$.

16 - 15 Ⓢ ★★ ♥

Résoudre dans $\mathbf{Z}$ le système : $\begin{cases} x \equiv 2 \pmod{88} \\ x \equiv 1 \pmod{27} \\ x \equiv 3 \pmod{35}\ . \end{cases}$

16 - 16 Ⓢ ★★ ♥

Déterminer le dernier chiffre de l'écriture décimale de 2^{2016} puis les deux derniers.

16 - 17 Ⓢ M 2011 ★★ Division euclidienne

Donner le reste de la division euclidienne de 2011^{2011} par 13.

16 - 18 Ⓢ ★★ Théorème de Wolstenholme

Pour p premier on note $\mathbf{F}_p$ le corps fini $\mathbf{Z}/p\mathbf{Z}$.

a. Factoriser le polynôme $X^p - X$ dans $\mathbf{F}_p[X]$.

b. En déduire le théorème de Wilson : p premier $\Longleftrightarrow (p-1)! \equiv -1 \pmod p$.

c. Établir de même : p premier $\Longleftrightarrow (p-2)! \equiv 1 \pmod p$.

d. Soit $\frac{a}{b}$ l'écriture irréductible de $\sum_{k=1}^{p-1} \frac{1}{k}$. Montrer, pour $p \geq 3$, $p \mid a$.

16 - 19 Ⓢ ADS X 2007 ★★ Un théorème de Lagrange †

Soit p un nombre premier distinct de 2 et b et c deux entiers non divisibles par p. Montrer qu'il existe deux entiers u et v tel que p divise $u^2 + bv^2 + c$.

16 - 20 Ⓢ ★★

Soit p premier impair et q un diviseur premier de $2^p - 1$. Montrer $q \equiv 1 \pmod{2p}$.

Indication : on s'intéressera à $\langle\overline{2}\rangle$ dans $(\mathbf{Z}/q\mathbf{Z})^*$.

16 - 21 M 2017 ★★ Groupe des inversibles

Soit a un nombre impair positif et n un entier supérieur à 3. Montrer $a^{2^{n-2}} \equiv 1 \pmod{2^n}$. En déduire les entiers n pour lesquels le groupe des inversibles de l'anneau $\mathbf{Z}/2^n\mathbf{Z}$ est cyclique.

16 - 22 Ⓢ **MR 2018** ★★ **Points rationnels**

Soit $X = \{(x,y) \in \mathbf{R}^2 \mid x^2+y^2=3\}$.

a. Décrire géométriquement X.

b. Démontrer $X \cap \mathbf{Q}^2 = \emptyset$. On pourra étudier les solutions entières de l'équation $x^2+y^2-3z^2=0$.

16 - 23 Ⓢ **TPE 2011** ★★★ **Équation du second degré**

Résoudre $x^2+x+1=0$ dans les anneaux $\mathbf{Z}/7\mathbf{Z}$ et $\mathbf{Z}/6\mathbf{Z}$. Que dire dans $\mathbf{Z}/n\mathbf{Z}$?

16 - 24 Ⓢ **X 2015** ★★★ **Somme quadratique de Gauss**

Soit z une racine n-ième primitive de l'unité, avec n impair. Montrer, pour $d \geq 1$, $z^{(k+n)^d} = z^{k^d}$ et en déduire le module de $\displaystyle\sum_{k=0}^{n-1} z^{k^2}$.

16 - 25 Ⓢ ★★★ **Sommes de deux carrés**

a. Soit p un entier naturel impair somme de deux carrés. Montrer $4 \mid (p-1)$. La réciproque est-elle vraie ?

b. On se propose de montrer la réciproque dans le cas où p est premier. Soit donc p un nombre premier vérifiant $4 \mid (p-1)$.

i. Montrer que $\mathbf{Z}/p\mathbf{Z} \setminus \{0\}$ contient exactement $\dfrac{p-1}{2}$ carrés qui sont les racines dans $\mathbf{Z}/p\mathbf{Z}$ du polynôme $X^{(p-1)/2}-1$.

ii. Montrer l'existence d'un entier m tel que m^2+1 soit divisible par p.

iii. Montrer qu'il existe (a,b) dans $\mathbf{Z}^2$ tel que $|bm-ap| \leq \sqrt{p}$ et $0 < b < \sqrt{p}$.

iv. Conclure.

Arithmétique et polynômes

16 - 26 Ⓢ ★

Montrer que X^3+X+1 n'a pas de racine rationnelle et en déduire qu'il est irréductible dans l'anneau $\mathbf{Q}[X]$.

16 - 27 Ⓢ ★

Trouver tous les polynômes P de $\mathbf{R}[X]$ tels que $P(X^2) = P(X)P(X+1)$.

16 - 28 Ⓢ ★ **Fonctions symétriques élémentaires**

Soit n un entier supérieur à 2 et $x_1, x_2, \ldots, x_n$ des nombres entiers. On note $\sigma_1, \sigma_2, \ldots, \sigma_n$ leurs fonctions symétriques élémentaires, i.e.

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k} = \sum_{\substack{I \subset [\![1;n]\!] \\ \mathrm{Card}(I)=k}} \prod_{i \in I} x_i \,.$$

a. Montrer que, pour tout i, x_i^n appartient à l'idéal engendré par les σ_k et en déduire que tout nombre premier divisant tous les σ_k divise également tous les x_i.

b. En déduire $\wedge_{i=1}^n x_i = 1 \iff \wedge_{k=1}^n \sigma_k = 1$.

c. Soit k un entier compris entre 1 et n et p un nombre premier. Montrer que p divise au moins k des entiers $(x_i)_{1 \leq i \leq n}$ si et seulement si p divise σ_n, σ_{n-1}, …, σ_{n-k+1}, et retrouver le résultat précédent.

16 - 29 Ⓢ ★★

Trouver tous les entiers naturels non nuls n tels que $1-X+X^2-X^3+X^4$ divise $1-X^n+X^{2n}-X^{3n}+X^{4n}$ dans $\mathbf{C}[X]$.

16 - 30 Ⓢ **Magistère 2017** ★★

Montrer $\forall P \in \mathbf{K}[X]$, $P - X \mid P \circ P - X$.

16 - 31 Ⓢ **X** ★★ $P' \mid P$ ♥

Trouver les P de $\mathbf{C}[X]$ tels que P' divise P.

16 - 32 Ⓢ ★★ ♠

Le polynôme X^4-14X^2+1 est-il irréductible dans l'anneau $\mathbf{Q}[X]$?

16 - 33 Ⓢ ★★ ♠

On pose $A = \mathbf{Z}[X]$ et $I = \{P \in A \mid 3 \mid P(0)\}$. Montrer que I est un idéal de A mais qu'il n'est pas principal, i.e. I n'est pas de la forme xA avec x dans A.

16 - 34 Ⓢ **X 2015** ★★ **Polynômes entiers**

Soit Z_n l'ensemble des zéros des polynômes unitaires de degré n, à coefficients entiers dont toutes les racines sont de module au plus égal à 1.

a. Montrer que Z_n est fini.

b. Montrer que, si α appartient à Z_n, alors, pour tout entier k, α^k aussi.

c. Qu'en déduit on ?

Indication : utiliser une matrice compagnon.

16 - 35 Ⓢ **X 2011** ★★ **Polynômes et diviseurs**

Soit P dans $\mathbf{Z}[X]$ non constant. Montrer que l'ensemble des nombres premiers p tels qu'il existe n dans $\mathbf{Z}$ vérifiant $P(n) \neq 0$ et p divise $P(n)$, est infini.

Indication : considérer $\dfrac{1}{b}P(a+bmX)$ *pour* a, b *et* m *bien choisis.*

16 - 36 Ⓢ **C 2015** ★★ **Transformée de Fourier**

Soit $n \geq 1$ et $\omega = \exp(2i\pi/n)$. Pour P dans $\mathbf{C}[X]$, on définit

$$\mathcal{F}(P) = \sum_{k=0}^{n-1} P(\omega^k) X^k \quad \text{et} \quad \overline{\mathcal{F}}(P) = \sum_{k=0}^{n-1} P(\omega^{-k}) X^k \,.$$

a. Montrer que $\mathcal{F}$ et $\breve{\mathcal{F}}$ définissent des endomorphismes de $\mathbf{C}[X]$.

b. Calculer $\breve{\mathcal{F}} \circ \mathcal{F}$ et en déduire que $\mathcal{F}$ est un automorphisme de $\mathbf{C}_{n-1}[X]$ dont on précisera la réciproque.

c. Soit $P \in \mathbf{Z}[X]$ tel que

— pour tout z dans $\mathbf{U}_n$, on ait $|P(z)| \leq 1$;

— il existe une racine de P dans $\mathbf{U}_n$.

Montrer que $X^n - 1$ divise P.

16 - 37 Ⓢ ★★★ Polynôme minimal de $2^{1/q}$ ♠

a. Pour $n \geq 2$, le polynôme $X^n - 2$ est-il irréductible dans $\mathbf{Q}[X]$?

b. Soit P dans $\mathbf{Z}[X]$ avec $P(0)$ impair et soit α une racine réelle de P. Montrer que α n'est pas une puissance rationnelle positive de 2, i.e. $\ln(\alpha)/\ln(2) \notin \mathbf{Q}_+^*$.

Indication : on pourra se ramener au cas où $\alpha = 2^{1/q}$ et P est de degré strictement inférieur à q.

16 - 38 Ⓢ ★★★ Polynômes hyperboliques

On appelle polynôme hyperbolique un polynôme à coefficients réels dont toutes les racines sont réelles. Dans la suite on note P et Q deux tels polynômes. On écrit $P = \sum_{k=0}^{n} a_k X^k$ avec $n = \deg(P) \geq 1$.

a. Montrer que $\sum_{k=0}^{n} a_k Q^{(k)}$ est hyperbolique.

b. On suppose de plus que Q n'a pas de racine dans l'intervalle $[0; n]$. Montrer que $\sum_{k=0}^{n} a_k Q(k) X^k$ est hyperbolique.

Indication : Traiter le cas $n = 1$ et en déduire le cas général par itération.

16 - 39 Ⓢ ★★★ Théorème de Fermat – Polynômes

a. Soit A, B et C dans $\mathbf{C}[X]$ premiers entre eux dans leur ensemble, non constants, et vérifiant $A+B=C$. Montrer que le nombre total de leurs racines (comptées sans multiplicités) est strictement supérieur au plus grand de leurs degrés.

b. Soit maintenant n un entier supérieur à 3. Montrer qu'il n'existe aucun triplet de polynômes (A, B, C) de $\mathbf{C}[X]$, non proportionnels, satisfaisant à $A^n + B^n = C^n$.

16 - 40 Ⓢ ★★★ Théorème de Dirichlet

a. Soit n dans $\mathbf{N}^*$ et Φ_n le polynôme unitaire de $\mathbf{C}[X]$ dont les racines (simples) sont les racines primitives n^{e} de l'unité. Montrer $\Phi_n \in \mathbf{Z}[X]$.

b. On se donne p premier, m naturel non multiple de p et a un entier naturel tel que p divise $\Phi_m(a)$. Montrer que p ne divise pas a et que m est le plus petit entier naturel non nul tel que $a^m \equiv 1 \pmod{p}$.

c. Que dire des nombres premiers p appartenant à la progression arithmétique de raison m et de terme initial 1 ? (On pourra démontrer ou utiliser le résultat de l'exercice 16 - 35.)

Anneaux généraux

16 - 41 Ⓢ ★

Pour $m \in \mathbf{N}^*$, déterminer tous les morphismes d'anneaux de $\mathbf{Z}^m$ dans $\mathbf{Z}$.

16 - 42 ★★

Déterminer tous les sous-anneaux de $\mathbf{Z}^2$ et préciser lesquels sont intègres.

Indication : utiliser l'application $(u, v) \mapsto u - v$.

16 - 43 Ⓢ ★★ †

Soit $(a, b) \in A^2$ où A est un anneau. On suppose que $1 - ba$ est inversible. Montrer qu'il en est de même de $1 - ab$.

Indication : on pourra s'inspirer de l'identité

$$(1-x)^{-1} = \sum_{k=0}^{+\infty} x^k \, .$$

16 - 44 Ⓢ ★★★ Anneaux de Boole

Soit A un anneau de Boole, i.e. un anneau dans lequel tout élément x de A vérifie $x^2 = x$.

a. Montrer que A est commutatif.

b. Soit $\mathcal{R}$ la relation dans A définie par $x\mathcal{R}y \equiv xy = x$. Montrer que $\mathcal{R}$ est une relation d'ordre. On note $\leq$ cet ordre.

c. Montrer que, si A est fini, il est isomorphe à $(\mathscr{P}(E), \Delta, \cap)$ pour un certain ensemble fini E que l'on caractérisera par rapport à l'ordre précédent.

Idéaux

16 - 45 Ⓢ ★ Classes d'association

Soit A un anneau intègre. On pose $a\mathcal{R}b \equiv aA = bA$, i.e. $a\mathcal{R}b \equiv \big(\exists \varepsilon \in A^\times \; a = \varepsilon b\big)$. Cette relation s'appelle relation d'association.

a. Vérifier que c'est une relation d'équivalence. Ses classes d'équivalence sont appelées **classes d'association**.

b. Montrer que l'application $a \mapsto aA$ induit un isomorphisme d'ensembles ordonnés entre l'ensemble des classes d'association muni de la divibilité et l'ensemble des idéaux principaux de A muni de l'inclusion inverse.

16 - 46 Ⓢ ★★

Déterminer tous les idéaux de $\mathbf{K}^n$, où $\mathbf{K}$ est un corps et n un entier naturel non nul.

16 - 47 Ⓢ **M 2007** ★★★ ♠

Soit p un nombre premier. On pose $\mathbf{Q}_{(p)} = \{a/b \,|\, (a,b) \in \mathbf{Z} \times \mathbf{Z}^*, a \wedge b = 1 \text{ et } p \wedge b = 1\}$. Montrer que $\mathbf{Q}_{(p)}$ est un anneau principal et un sous-anneau de $\mathbf{Q}$.

16 - 48 Ⓢ ★★★ **Valeur absolue ultramétrique**

Soit φ une application d'un corps $\mathbf{K}$ dans $\mathbf{R}_+$ telle que, pour x et y dans $\mathbf{K}$, on ait $\varphi(x) = 0 \iff x = 0$, $\varphi(xy) = \varphi(x)\varphi(y)$ et

$$\varphi(x+y) \leq \max(\varphi(x), \varphi(y)) \ .$$

a. On pose $A = \{x \in \mathbf{K} \,|\, \varphi(x) \leq 1\}$. Montrer que A est un sous-anneau de $\mathbf{K}$.

b. On pose $B = \{x \in \mathbf{K} \,|\, \varphi(x) < 1\}$. Montrer que B est un idéal de A.

c. Soit $\mathcal{R}$ la relation sur A définie par $x\mathcal{R}y \equiv x - y \in B$. Montrer que c'est une relation d'équivalence et que l'ensemble des classes d'équivalences a une structure naturelle de corps.

16 - 49 Ⓢ ★★★ **Entiers de Gauss**

Soit $\mathbf{Z}[i] = \left\{a + ib \;\middle|\; (a,b) \in \mathbf{Z}^2\right\}$.

a. Montrer que $\mathbf{Z}[i]$ est un sous anneau de $\mathbf{C}$.

b. On note $N(a) = a\overline{a}$. En utilisant la division dans $\mathbf{C}$ (en fait dans $\mathbf{Q}[i]$), montrer qu'on peut le munir d'une division euclidienne de stathme N : pour (a,b) dans $\mathbf{Z}[i]^2$, avec $b \neq 0$, il existe un couple (q,r) dans $\mathbf{Z}[i]^2$ tel que $a = bq + r$ et $0 \leq N(r) < N(b)$.

c. En déduire que $\mathbf{Z}[i]$ est principal.

d. Soit a dans $\mathbf{Z}[i]$, montrer que si $N(a)$ est premier dans $\mathbf{Z}$ alors a est irréductible dans $\mathbf{Z}[i]$, mais que la réciproque est fausse en général.

16 - 50 ★★★ **Anneau factoriel** ♠

Soit A un anneau principal. On note $\mathcal{P}$ un ensemble de représentants des classes d'association des éléments irréductibles (voir exercice 16 - 45).

a. Montrer que toute suite croissante $(I_n)_{n\in\mathbf{N}}$ d'idéaux de A est stationnaire : $\exists n_0 \in \mathbf{N}, \forall n \geq n_0, I_n = I_{n_0}$.

b. Soit a un élément non nul de $A \setminus A^\times$. Montrer que a possède au moins un diviseur irréductible d.

c. Montrer que tout a de $A \setminus \{0\}$ admet une unique décomposition primaire : il existe un unique couple (u,α) où $u \in A^\times$ et $\alpha \in \mathbf{N}^{(\mathcal{P})}$ avec

$$a = u \prod_{p\in\mathcal{P}} p^{\alpha(p)} \ .$$

(On dit que A est factoriel.)

16 - 51 Ⓢ ★★★★ **Anneau Noethérien**

Soit A un anneau. Montrer que les trois propriétés suivantes sont équivalentes :

a. Tout idéal de A est engendré par un nombre fini d'éléments.

b. Toute suite croissante d'idéaux de A est stationnaire.

c. Tout ensemble non vide d'idéaux de A possède un élément maximal (pour l'inclusion).

Corps

16 - 52 Ⓢ ★ ♠

Soit $\mathbf{K}$ un corps fini de caractéristique p.

a. Montrer qu'il existe un plus petit corps inclus dans $\mathbf{K}$ et qu'il est égal à $\mathbf{F}_p$.

b. En déduire que $\mathbf{K}$ a une structure de $\mathbf{F}_p$-espace vectoriel et qu'il existe un entier naturel non nul n tel que $|\mathbf{K}| = p^n$.

c. Qu'en est-il si $\mathbf{K}$ est un corps infini ?

16 - 53 Ⓢ ★★ †

Déterminer les automorphismes de corps de $\mathbf{R}$ dans $\mathbf{R}$.

Indication : on montrera qu'ils sont nécessairement croissants.

16 - 54 **M 2015** ★★ **Matrices sur un corps fini**

Soit p un nombre premier et $\mathbf{K} = \mathbf{Z}/p\mathbf{Z}$.

a. Calculer le cardinal de $\mathbf{K}_2[X]$.

b. Montrer qu'il existe des polynômes de $\mathbf{K}_2[X]$ non constants qui ne soient pas scindés.

c. En déduire qu'il existe des matrices dans $\mathscr{M}_2(\mathbf{K})$ non trigonalisables.

16 - 55 **C 2017** ★★ **Carrés modulo p**

Soit p un nombre premier, on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$, $\mathbf{F}_p^*$ son groupe des inversibles.

a. Montrer $\overline{x} = \overline{y} \Longrightarrow e^{2i\pi x/p} = e^{2i\pi y/p}$.

b. Pour a dans $\mathbf{F}_p^*$ on note $\tau(a) = \sum_{k\in\mathbf{F}_p} ak^2$. Montrer que si a est un carré, alors $\tau(a) = \tau(1)$ et sinon $\tau(a) + \tau(1) = 0$.

16 - 56 ★★★ **Anneau des entiers**

Soit A un anneau intègre, et B un sous anneau de A satisfaisant à la propriété suivante :

$$\forall x \in A\,,\ \exists P \in B[X]\,,\ P \text{ normalisé et } P(x) = 0.$$

Établir l'équivalence : A est un corps $\iff$ B est un corps.

16 - 57 Ⓢ ★★★ **Automorphismes de $\mathbf{Q}[\sqrt{2}]$**

Déterminer les automorphismes du corps $\mathbf{Q}[\sqrt{2}]$.

16 - 58 Ⓢ ★★★ ♠

Soit $\mathbf{K}$ le $\mathbf{Q}$-espace vectoriel engendré par 1, $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{6}$ (vu comme sous-espace vectoriel du $\mathbf{Q}$-espace vectoriel $\mathbf{R}$, par exemple). Montrer que c'est un corps. Existe-t-il α dans $\mathbf{K}$ tel que $\mathbf{K} = \mathbf{Q}[\alpha] = \{P(\alpha) \,|\, P \in \mathbf{Q}[X]\}$?

16 - 59 Ⓢ ★★★ **$\mathbf{K}^*$ pour $\mathbf{K}$ corps fini**

Le but est de montrer que le groupe des éléments inversibles d'un corps fini est cyclique. Pour n entier naturel, on note D_n l'ensemble des diviseurs de n.

a. Soit G un groupe fini d'ordre n. Soit d divisant n, on note $A_d = \{x \in G \,|\, \mathrm{ord}_G(x) \mid d\}$. On suppose que G possède la propriété (P) suivante :

$$\forall d \in D_n \ \ \mathrm{Card}(A_d) \leq d \,.$$

i. Soit $\psi(d) = \mathrm{Card}\,\{x \in G \,|\, \mathrm{ord}_G(x) = d\}$. Montrer $\forall d \in \mathcal{D}_n$, $\psi(d) \leq \varphi(d)$, où φ est l'indicatrice d'Euler.

ii. Montrer $\sum_{d\in\mathcal{D}_n} \psi(d) = n$.

iii. Montrer $\sum_{d\in\mathcal{D}_n} \varphi(d) = n$.

iv. Montrer $\forall d \in \mathcal{D}_n$, $\psi(d) = \varphi(d)$.

v. En déduire que G est cyclique.

b. Soit $\mathbf{K}$ un corps fini commutatif. Montrer que $(\mathbf{K}^*, \cdot)$ est cyclique.

16 - 60 ★★★ **Théorème de Wedderburn**

Soit A un anneau de cardinal fini tel que $A^\times = A \setminus \{0\}$. On désire montrer que A est commutatif (i.e. que tout corps fini est commutatif). Dans cet exercice on appelle corps fini un tel anneau, qu'il soit ou non commutatif.

a. Soit x dans A. On note C_x le commutant de x, i.e. $C_x = \{y \in A \,|\, xy = yx\}$. Montrer que c'est un sous-corps fini de A. En déduire que le centre Z de A défini par $Z = \cap_{x\in A} C_x$ est un corps fini commutatif. On note $|Z| = q$.

b. Soit x dans A. Montrer que A et C_x sont des Z-espaces vectoriels et en déduire qu'on dispose de n et n_x dans $\mathbf{N}^*$ tels qu'on ait $|A| = q^n$ et $|C_x| = q^{n_x}$.

c. En considérant la relation d'équivalence donnée par $x\mathcal{R}y$ si et seulement s'il existe a dans $A^\times$ tel que $x = aya^{-1}$, montrer que $\dfrac{q^n - 1}{q^{n_x} - 1}$ est un entier et en déduire $n_x \mid n$.

d. Montrer qu'on a

$$q^n - 1 = q - 1 + \sum_{i=1}^{t} \frac{q^n - 1}{q^{n_i} - 1}$$

pour certains entiers n_i tels que $\dfrac{q^n - 1}{q^{n_i} - 1}$ soit un entier strictement supérieur à 1.

e. Soit d un entier. On note Φ_d le polynôme unitaire de $\mathbf{C}[X]$ dont les racines sont les racines primitives d^{e} de l'unité. Montrer $X^n - 1 = \prod_{d|n} \Phi_d$ et en déduire que Φ_d est à coefficients entiers et que son coefficient constant est de valeur absolue égale à 1.

f. En déduire que, si on a $d \mid n$ alors $\Phi_n(q) \mid \dfrac{q^n - 1}{q^d - 1}$.

g. Montrer que, pour $d \in \mathbf{N}^*$ et λ une racine de Φ_d, on a $|q - \lambda|^2 > |q - 1|$ et en déduire $n = 1$. Conclure.