100% ENTRAÎNEMENT

MATHS

MP/MPI

NOUVEAUX PROGRAMMES

Maxime Bailleul
François-Xavier Manoury
Stéphane Préteseille

ellipses

1 Groupes et anneaux

Maîtriser le cours

Exercice 1 – Le vrai/faux du début

1. L'ensemble des entiers relatifs pairs est un sous-groupe de $(\mathbb{Z}, +)$. ☐ Vrai ☐ Faux
2. L'ensemble des entiers relatifs impairs est un sous-groupe de $(\mathbb{Z}, +)$. ☐ Vrai ☐ Faux
3. L'ensemble des multiples de 7 est un sous-groupe de $(\mathbb{Z}, +)$. ☐ Vrai ☐ Faux

Exercice 2 –

Soit $(G, *)$ un groupe et I un ensemble non vide. Montrer que l'intersection d'une famille $(H_i)_{i\in I}$ de sous-groupes de G est un sous-groupe de G.

Exercice 3 –

Soit $n \in \mathbb{N}^*$ et $\xi = e^{2i\pi/n}$. Montrer que ξ est d'ordre fini dans $(\mathbb{C}^*, \times)$. Quel est le sous-groupe engendré par ξ ?

Exercice 4 –

Le but de cet exercice est de démontrer le théorème de Lagrange dans le cas d'un groupe commutatif : soit $(G, *)$ un groupe commutatif *fini* et x un élément de G. Alors x est d'ordre fini et l'ordre de x divise le cardinal de G.

Fixons x un élément de G.

1. Soit $f : G \to G$ l'application définie par :

$$\forall g \in G, f(g) = g * x$$

   Montrer que f est bijective.

2. Soit n le cardinal de G et $a_1, \dots, a_n$ les éléments de G. Considérons l'élément P de G défini par :

$$P = \prod_{i=1}^{n} a_i$$

   Montrer que :

$$P = P * (x^n)$$

3. En déduire la preuve du théorème de Lagrange.

Exercice 5 –
Soit $\varphi : (A, +_A, \cdot_A) \to (B, +_B, \cdot_B)$ un morphisme d'anneaux commutatifs. Montrer que le noyau de φ est un idéal de $(A, +_A, \cdot_A)$.

Maîtriser les méthodes fondamentales

Exercice 6 –
Soit p, q deux nombres premiers et x, y deux éléments d'ordres p et q d'un groupe abélien $(G, *)$. Montrer que $x * y$ est d'ordre pq.

Exercice 7 –
Soit $(G, *)$ un groupe et e son élément neutre.

1. Soit $x \in G$ tel que $x^{10} = e$ et $x^{21} = e$. Que peut-on dire de x ?
2. Soit $y \in G$ tel que $y^6 = e$ et $y^{22} = e$. Que peut-on dire de y^2 ?

Exercice 8 –
Soit $(\mathbb{K}, +, \cdot)$ un corps. Montrer que les seuls idéaux de ce corps sont $\{0_\mathbb{K}\}$ et $\mathbb{K}$.

Exercice 9 –

Posons $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ (a, b) \in \mathbb{Z}^2\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ est un anneau (pour les lois usuelles définies sur $\mathbb{R}$).
2. Soit $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{R}$ l'application définie par :

$$\forall (a, b) \in \mathbb{Z}^2,\ N(a + b\sqrt{2}) = a^2 - 2b^2$$

   Montrer que N est bien une application.
3. Montrer que pour tout $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$, $N(xy) = N(x)N(y)$.
4. En déduire les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$.

Exercice 10 –
Soit $(A, +, \cdot)$ un anneau commutatif.
On note 0 son élément neutre pour + et 1 son élément unité pour $\cdot$.
On dit qu'un élément x de A est nilpotent si il existe un entier naturel non nul n tel que $x^n = 0$.
On note $\mathrm{Nil}(A)$ l'ensemble des éléments nilpotents de A. Montrer que $\mathrm{Nil}(A)$ est un idéal de $(A, +, \cdot)$.

Pour aller plus loin

Exercice 11 –
Soit $(G, *)$ un groupe fini de cardinal impair et e son élément neutre.

1. Montrer que $f : G \to G$ définie par $f(g) = g^2$ est une bijection.
2. En déduire que l'équation $g^2 = e$, d'inconnue $g \in G$, admet une unique solution (à savoir e).

Exercice 12 –

Soit $(A, +, \cdot)$ un anneau de Boole, c'est-à-dire un anneau vérifiant la propriété suivante : pour tout $x \in A$, $x^2 = x$.

1. Montrer que, pour tout $x \in A$, $-x = x$.
2. Montrer que A est commutatif.

Exercice 13 – Le vrai/faux de la fin

Soit $n \geq 1$.

1. $\overline{5}$ génère $(\mathbb{Z}/17\mathbb{Z}, +)$. ☐ Vrai ☐ Faux
2. $\overline{5}$ génère $(\mathbb{Z}/15\mathbb{Z}, +)$. ☐ Vrai ☐ Faux
3. $(\mathbb{Z}/8\mathbb{Z}, +)$ contient 4 générateurs. ☐ Vrai ☐ Faux

Solution des exercices

Exercice 1 –

1. L'ensemble des entiers relatifs pairs est un sous-groupe de $(\mathbb{Z}, +)$. ☒ Vrai ☐ Faux
2. L'ensemble des entiers relatifs impairs est un sous-groupe de $(\mathbb{Z}, +)$. ☐ Vrai ☒ Faux
3. L'ensemble des multiples de 7 est un sous-groupe de $(\mathbb{Z}, +)$. ☒ Vrai ☐ Faux

🎓 Cours

On note pour tout entier $n \in \mathbb{N}$:

$$n\mathbb{Z} = \{nk,\ k \in \mathbb{Z}\}$$

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les ensembles $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Exercice 2 –

Vérifions les différents points de la caractérisation. Posons :

$$H = \bigcap_{i \in I} H_i$$

- Pour tout $i \in I$, H_i est inclus dans G donc H aussi.
- On note e l'élément neutre de G. Pour tout $i \in I$, $e \in H_i$ car H_i est un sous-groupe de G donc e appartient à H.
- Soit $x, y \in H$. Pour tout $i \in I$, x et y appartiennent à H_i qui est un sous-groupe de G donc $x * y^{-1} \in H_i$. Ainsi,

$$x * y^{-1} \in \bigcap_{i \in I} H_i = H$$

On en déduit que H est un sous-groupe de $(G, *)$.

À retenir

Soit $(G, *)$ un groupe et e son élément neutre.
H est un sous-groupe de $(G, *)$ si et seulement si :

- $H \subset G$.
- $e \in H$.
- $\forall x, y \in H,\ x * y^{-1} \in H$.

Exercice 3 –

On reconnait une racine n-ième de l'unité donc $\xi^n = 1$. De plus, pour tout $k \in \{1, \dots, n-1\}$,

$$0 < \frac{2\pi}{n} \leq 2\frac{k\pi}{n} \leq 2\frac{(n-1)\pi}{n} < 2\pi$$

donc :

$$\xi^k = \mathrm{e}^{2ik\pi/n} \neq 1$$

On en déduit ξ est d'ordre fini égal à n.

Cours

Un élément a d'un groupe $(G, *)$ est d'ordre fini si il existe un entier $k \in \mathbb{N}^*$ tel que a^k soit égal au neutre de G. L'ordre de a est alors le plus petit entier k vérifiant cette propriété.

Déterminons maintenant le sous-groupe engendré par ξ. On a :

$$< \{\xi\} >= \{\xi^k,\ k \in \mathbb{Z}\} = \{\xi^k,\ 0 \leq k \leq n-1\} = \mathbb{U}_n$$

Cours

Soit A une partie d'un groupe $(G, *)$.

- L'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G. C'est le plus petit (au sens de l'inclusion) contenant A. On l'appelle *sous-groupe engendré* par A et on le note $< A >$.
- Si $A = \{x\}$, où $x \in G$, alors :
$$< \{x\} >= \{x^k,\ k \in \mathbb{Z}\}$$

Exercice 4 –

1. Montrons que f est injective. Soit $(g, g') \in G^2$ tel que $f(g) = f(g')$. alors $g * x = g' * x$. On en déduit que :
$$(g * x) * x^{-1} = (g' * x) * x^{-1}$$
donc : Associativité de *
$$g * (x * x^{-1}) = g' * (x * x^{-1})$$
Or $x * x^{-1} = e$ (l'élément neutre de G) donc $g = g'$. Ainsi, f est injective.

Or G est un ensemble fini donc $f : G \to G$ est bijective.

G est fini donc $f : G \to G$ est injective si et seulement si elle est surjective si et seulement si elle est bijective

2. On sait que f est une bijection donc $f(G) = G$ donc $\{a_1, \dots, a_n\} = \{a_1 * x, \dots, a_n * x\}$. Or P est le produit de tous les éléments de G (ce terme a un sens car $*$ est commutative) donc :

$$P = \prod_{i=1}^{n} (a_i * x)$$

Par commutativité de $*$, on en déduit que :

$$P = \left(\prod_{i=1}^{n} a_i\right)\left(\prod_{i=1}^{n} x\right) = P * (x^n)$$

3. D'après la question précédente, on a :

$$P^{-1} * P = P^{-1} * (P * (x^n))$$

Or $*$ est associative et $P^{-1} * P = e$ donc $x^n = e$. On en déduit que x est d'ordre fini et que celui-ci est un diviseur de n, qui est le cardinal de G.

À retenir

Soit a un élément d'ordre fini d d'un groupe $(G, *)$ (dont on note e l'élément neutre). Alors pour tout entier relatif k,

$$a^k = e \iff d | k$$

Exercice 5 –

Cours

On appelle *morphisme* d'un anneau $(A, +_A, \cdot_A)$ dans un anneau $(B, +_B, \cdot_B)$ toute application $\varphi : A \to B$ vérifiant les propriétés suivantes :

- Pour tout $(x, y) \in A^2$, $\varphi(x +_A y) = \varphi(x) +_B \varphi(y)$.
- Pour tout $(x, y) \in A^2$, $\varphi(x \cdot_A y) = \varphi(x) \cdot_B \varphi(y)$.
- $\varphi(1_A) = 1_B$ (où 1_A et 1_B sont les unités des deux anneaux).

L'application φ est un morphisme d'anneaux donc en particulier un morphisme de groupes. Ainsi, $(\mathrm{Ker}(\varphi), +_A)$ est un sous-groupe de $(A, +_A)$.

Soit $a \in A$ et $x \in \mathrm{Ker}(\varphi)$. Alors :

$$\varphi(a \cdot_A x) = \varphi(a) \cdot_B \varphi(x) = \varphi(a) \cdot_B 0_B = 0_B$$

donc $a \cdot_A x \in \mathrm{Ker}(\varphi)$.

Ainsi, le noyau de φ est un idéal de $(A, +, \cdot)$.

Cours

Soit $(A, +, \cdot)$ un anneau commutatif et I une partie de A. On dit que I est un *idéal* de $(A, +, \cdot)$ si :

- $(I, +)$ est un sous-groupe de $(A, +)$.
- Pour tout $a \in A$ et tout $x \in I$, $a \cdot x \in I$.

Exercice 6 –

Notons e l'élément neutre de $(G, *)$. Par commutativité de $*$, on a :

$$(x * y)^{pq} = (x^p)^q * (y^q)^p = (e^q) * (e^p) = e$$

donc $x * y$ est d'ordre fini et son ordre divise pq. Soit $r \in \mathbb{N}^*$ tel que $(x * y)^r = e$. On a donc $(x^r) * (y^r) = e$ et en multipliant par y^{-1}, r fois à droite, on a :

$$x^r = (y^{-1})^r$$

puis :

$$x^{pr} = (y^{-1})^{pr}$$

Or $x^p = e$ donc $x^{pr} = e$ ce qui implique que $(y^{-1})^{pr} = e$. On en déduit que $y^{pr} = e$ donc q divise pr par propriété de l'ordre d'un élément.
Or p et q sont premiers entre eux donc q divise r. Lemme de Gauss
De même, on prouve que p divise r. Or p et q sont premiers entre eux donc pq divise r.

On en déduit que pq est l'ordre de xy.

Exercice 7 –

1. Par hypothèse x est d'ordre fini et en notant n son ordre, on sait que n divise 10 et n divise 21. Or le PGCD de 10 et 21 est 1. On en déduit que n divise 1 donc $n = 1$. Ainsi, $x^1 = e$ donc $x = e$.
2. Par hypothèse y est d'ordre fini et en notant m son ordre, on sait que m divise 6 et 22. Or le PGCD de 6 et 22 vaut 2. On en déduit que m divise 2 donc $m = 1$ ou $m = 2$.
   - Si $m = 1$ alors $y = e$ donc $y^2 = e$.
   - Si $m = 2$ alors $y^2 = e$.

   Ainsi, dans tous les cas, $y^2 = e$.

Exercice 8 –

Soit I un idéal de $(\mathbb{K}, +, \cdot)$. Si I est différent de $\{0_{\mathbb{K}}\}$, il contient au moins un élément y non nul de $\mathbb{K}$. Par définition d'un corps, on sait que y est inversible et $y^{-1} \in \mathbb{K}$. Par définition d'un idéal, en notant 1 l'élément unité du corps, on en déduit que $1 = y^{-1} \cdot y \in I$. De nouveau par définition d'un idéal, on a :

$$\forall x \in \mathbb{K}, x = x \cdot 1 \in I$$

Ainsi, $I = \mathbb{K}$.

Exercice 9 –

1. Il suffit de montrer que c'est un sous anneau de $(\mathbb{R}, +, \cdot)$.

- $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$.
- Soit $x, y \in \mathbb{Z}[\sqrt{2}]$. Il existe des entiers relatifs a, b, c et d tels que :

$$x = a + b\sqrt{2} \text{ et } y = c + d\sqrt{2}$$

Par simple calcul, on a :

$$x - y = (a - c) + (b - d)\sqrt{2} \text{ et } xy = ac + 2bd + (bc + ad)\sqrt{2}$$

Or $a-c, b-d, ac+2bd$ et $bc+ad$ sont des entiers relatifs donc $x-y$ et xy appartiennent à $\mathbb{Z}[\sqrt{2}]$.

- On a $1 = 1 + 0\sqrt{2}$ et $(1, 0) \in \mathbb{Z}^2$ donc $1 \in \mathbb{Z}[\sqrt{2}]$.

Ainsi, $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $(\mathbb{R}, +, \cdot)$.

Cours

Soit $(A, +, \cdot)$ un anneau (et 1_A son élément unité) et B une partie de A. Alors B est un sous-anneau de A si et seulement si :

$$\begin{cases} \forall (x, y) \in B^2,\ x - y \in B \text{ et } x \cdot y \in B \\ 1_A \in B \end{cases}$$

2. Soit a, b, c et d des entiers relatifs. Supposons que :

$$a + b\sqrt{2} = c + d\sqrt{2}$$

On en déduit que :

$$a - c = (d - b)\sqrt{2}$$

Sachant que $\sqrt{2}$ est irrationnel, et que $a - c$ et $d - b$ sont des entiers relatifs, on a $d = b$ et $a = c$. Finalement :

$$N(a + b\sqrt{2}) = N(c + d\sqrt{2})$$

L'application N est donc bien définie.

À retenir

Soit E et F deux ensembles. Une application $f : E \to F$ est bien définie si :

$$\forall x \in E,\ \exists! y \in F,\ f(x) = y$$

3. Soit $x, y \in \mathbb{Z}[\sqrt{2}]$. Il existe des entiers relatifs a, b, c et d tels que :

$$x = a + b\sqrt{2} \text{ et } y = c + d\sqrt{2}$$

On a déjà montré que :

$$xy = ac + 2bd + (bc + ad)\sqrt{2}$$

donc :

$$\begin{aligned} N(xy) &= (ac+2bd)^2 - 2(bc+ad)^2 \\ &= a^2c^2 + 4acbd + 4b^2d^2 - 2b^2c^2 - 4bcad - 2a^2d^2 \\ &= a^2c^2 + 4b^2d^2 - 2b^2c^2 - 2a^2d^2 \end{aligned}$$

Or on a :

$$\begin{aligned} N(x)N(y) &= (a^2-2b^2)(c^2-2d^2) \\ &= a^2c^2 - 2a^2d^2 - 2b^2c^2 + 4b^2d^2 \end{aligned}$$

ce qui donne l'égalité souhaitée.

4. Raisonnons par analyse-synthèse.

Analyse. Soit $x \in \mathbb{Z}[\sqrt{2}]$ inversible. Alors il existe $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. D'après la question précédente, on a donc :

$$N(x)N(y) = N(1) = 1$$

Or N est à valeurs dans $\mathbb{Z}$ donc $N(x) = \pm 1$.

Synthèse. Réciproquement, soit $x \in \mathbb{Z}[\sqrt{2}]$ tel que $N(x) = \pm 1$. Il existe $(a, b) \in \mathbb{Z}^2$ tel que :

$$x = a + b\sqrt{2}$$

et par hypothèse, $a^2 - 2b^2 = \pm 1$ donc $x \neq 0$ (si x est nul, $a = b = 0$ car $\sqrt{2}$ est irrationnel). On a alors :

$$\frac{1}{x} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \pm(a-b\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$$

Ainsi, x est inversible dans $\mathbb{Z}[\sqrt{2}]$.

Les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont donc les éléments de la forme $a + b\sqrt{2}$ où $(a, b) \in \mathbb{Z}^2$ et $a^2 - 2b^2 = \pm 1$.

Exercice 10 –

Vérifions les différents points de la caractérisation.

- $\mathrm{Nil}(A) \subset A$.
- 0 appartient à $\mathrm{Nil}(A)$ car $0^1 = 0$.
- Soit $x, y \in \mathrm{Nil}(A)$. Il existe deux entiers naturels non nuls n et m tels que $x^n = 0$ et $y^m = 0$. Pour tout entier $p \geq 1$, on a :

L'anneau est commutatif

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k \cdot y^{p-k}$$

Si chaque terme de la somme est nul, alors $x + y$ est nilpotent.