Bouchaïb Radi
Abdelkhalak El Hami

MP
MP*

Maths

Cours, exercices
et problèmes de synthèse corrigés

NOUVEAUX PROGRAMMES

ellipses

Chapitre 1

Structures algébriques usuelles

1.1 Compléments sur les groupes

Théorème 1.1 (Caractérisation des sous-groupes) *Soit G un groupe et H une partie de G. Les assertions suivantes sont équivalentes :*

i) H *est un sous-groupe de* G.

ii) $e_G \in H$ *et* $\forall h,h' \in H$, *on a :* $h^{-1}h' \in H$.

Définition 1.1 (Sous-groupe engendré par une partie) *Soit G un groupe et S une partie de G. On appelle le sous-groupe de G engendré par S, l'intersection de tous les sous-groupes de G qui contiennent S. C'est le plus petit sous-groupe de G contenant S, on le note $\langle S \rangle$.*

Exemple 1.1 $\mathbb{Z} = \{n = n.1 \mid n \in \mathbb{Z}\} = \langle 1 \rangle$.

$U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \langle e^{2i\pi/n} \rangle$.

Théorème 1.2 *Toute intersection de sous-groupe de G est un sous-groupe de G.*

Définition 1.2 *S'il existe un élément x de G tel que $G = \langle x \rangle$,on dit que G est un groupe monogène.*

Définition 1.3 *Un groupe cyclique est un groupe monogène fini. Il est engendré par un seul élément.*

Théorème 1.3 *Les générateurs de $\mathbb{Z}/p\mathbb{Z}$ sont les $\bar{k}$ avec $k \wedge n = 1$.*

Théorème 1.4 *Si x est d'ordre fini, l'ordre de x est le cardinal du sous-groupe de G engendré par x.*

Théorème 1.5 *Si x est d'ordre fini d et si e désigne l'élément neutre de G, alors, pour n dans $\mathbb{Z}$, on a :* $x^n = e \Leftrightarrow d \mid n$.

Théorème 1.6 *L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.*

1.2 Compléments sur les anneaux

Définition 1.4 *si $(A_i)_{i\in I}$ est une famille d'anneaux, le produit cartésien $\prod_{i\in I} A_i$ peut être muni d'une structure d'anneau en définissant les opérations composante par composante, i.e.*

$$(a_i) + (b_i) = (a_i + b_i)(a_i)\dot{(}b_i) = (a_i\dot{b}_i)1_{\prod i\in IA_i} = (1_{A_i})_{i\in I}$$

On peut écrire : $\prod_{1\leq i\leq k} A_i$, sous la forme : $A_1 \times A_2 \times \cdot \times A_k$.

Définition 1.5 (Idéal d'un anneau commutatif) *Un idéal d'un anneau commutatif A est un sous-groupe I de $(A,+)$ tel que de plus :*

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

Définition 1.6 (Idéal engendré par un élément) *L'idéal engendré par un élément x est :*

$$xA = \{ax \mid x \in A\}$$

C'est le plus petit idéal qui contient x.

Définition 1.7 (Divisibilité dans un anneau commutatif intègre) *On dit, pour deux éléments a, b d'un anneau commutatif A, que a divise b (dans A) s'il existe q dans A tel que $aq = b$. Ce qui est particulier pour les anneaux intègres est que dans ce cas, si un élément non nul a divise b, alors l'élément q (le quotient) est toujours unique.*

1.3 Idéaux de $\mathbb{Z}$

Définition 1.8 *Tout idéal I de $\mathbb{Z}$ est de la forme $\mathbb{Z}x$ où x est un élément de $\mathbb{Z}$.*

Définition 1.9 (PGCD) *Le PGCD de deux nombres entiers non nuls est le plus grand entier qui les divise simultanément.*

Théorème 1.7 (Relation de Bézout) *Soient a et b deux entiers naturels non nuls. a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au + bv = 1$.*

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

Définition 1.10 ($\mathbb{Z}/n\mathbb{Z}$) *Pour tout entier $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ possède n éléments et*

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, n \bar{-} 1\}.$$

Théorème 1.8 (Anneaux $\mathbb{Z}/n\mathbb{Z}$) $(\mathbb{Z}/n\mathbb{Z}, +, \dot{)}$ *est un anneau commutatif et unitaire.*

Théorème 1.9 *Pour tout entier naturel n, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

Théorème chinois
Si m et n sont deux entiers premiers entre eux, les ensembles $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes.

Définition 1.11 (Indicatrice d'Euler) *On appelle indicatrice d'Euler d'un entier n l'entier $\phi(n)$ défini par :*

$$\phi(n) = card\{1 \leq k \leq n;\ k \text{ est premier avec } n\}.$$

$\phi(n)$ est aussi le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$, l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Théorème 1.10 *On a : $\phi(mn) = \phi(m)\phi(n)$ si m et n sont premiers entre eux.*

Théorème 1.11 *Si p est premier et $k \geq 1$, $\phi(p) = p - 1$ et $\phi(p^k) = p^k - p^{k-1}$.*

Calcul à l'aide de la décomposition en produits de facteurs premiers.

On peut calculer l'indicateur d'Euler $\phi(n)$ connaissant la décomposition en facteurs premiers de n. On a :

$$\begin{aligned} \phi(p_1^{k_1}) - \phi(p_r^{k_r}) &= (p_1^{k_1} - p_1^{k_1-1}) \times \cdots \times (p_r^{k_r} - p_r^{k_r-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_r}\right). \end{aligned}$$

Théorème d'Euler
Soit un entier $n > 1$. Si $k \in \mathbb{Z}$ vérifie $k \wedge n = 1$, alors

$$k^{\phi(n)} \equiv 1 \quad [n].$$

Le lien avec le petit théorème de Fermat est le suivant :

Théorème 1.12 *Soit p un nombre premier, et a un entier premier avec p. Alors a^{p-1} a pour reste 1 dans la division par p :*

$$a^{p-1} = 1 \quad mod\ p.$$

1.5 Anneaux $\mathbb{K}[X]$

Définition 1.12 *Soient $n \in \mathbb{N}^*$, $(P_1,\dots,P_n) \in (\mathbb{K}[X]-\{0\})^n$, il existe un polynôme et un seul D, unitaire, non nul, diviseur commun de $P_1,\dots,P_n$; D est appelé le plus grand commun diviseur de $P_1,\dots,P_n$ et noté* $\mathrm{PGCD}(P_1,\dots,P_n)$.

Identité de Bézout
Soit P et Q deux polynômes, P et Q sont premiers entre eux si et seulement s'il existe deux polynômes M et N tels que :

$$PM + QN = 1.$$

Lemme de Gauss
Etant donné trois polynômes P, Q et R tels que

$$P \mid QR \quad P \wedge Q = 1 \text{ alors } \quad P \mid R.$$

Définition 1.13 (Polynôme irréductible) *Un polynôme P de $\mathbb{K}[X]$ est dit irréductible sur le corps $\mathbb{K}$ s'il est non inversible et si les seuls diviseurs dans $\mathbb{K}[X]$ sont les polynômes associés à P, et les éléments de $\mathbb{K}\backslash\{0\}$.*

Théorème de décomposition
Tout polynôme non-constant P (non-inversible) peut s'écrire d'une manière unique sous la forme :

$$P = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_r^{\alpha_r}$$

avec $\lambda \in \mathbb{K}^* = \mathbb{K}\backslash\{0\}$; $P_1,P_2,\dots,P_r$ des polynômes irréductibles et $\alpha_1,\dots,\alpha_r$ des entiers naturels.

Corollaire 1.1 *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un et les polynômes de degré deux de discriminant srictement négatif.*

Théorème 1.13 *Les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré* 1.

1.6 Algèbres

Définition 1.14 *Soit E un ensemble, muni de deux lois internes $+$, $\times$ et d'une loi externe à opérateurs dans $\mathbb{K}$. Alors $(E, + , \times ,.)$ est un $\mathbb{K}-$algèbre lorsque :*

1) *$(E, + , \times ,.)$ est un $\mathbb{K}-$espace vectoriel.*
2) *La loi $\times$ est associative et admet un élément neutre (qu'on note 1_E).*
3) *La loi $\times$ est distributive sur la loi $+$.*
4) *Pour tous $u,v \in E$, et tout $\lambda \in \mathbb{K}$, $(\lambda u) \times v = u \times (\lambda v) = \lambda(u \times v)$.*

Définition 1.15 (Sous-algèbre) *Un sous-algèbre d'un $\mathbb{K}-$algèbre $(E,+,\times,.)$, est une partie F de E qui contient 1_E et qui est stable pour chacune des trois lois, c'est-à-dire :*

1) $1_E \in F$

2) $\forall (u,v) \in F^2,\ u+v \in F$ *et* $u \times v \in F$

3) $\forall u \in \mathbb{K},\ \forall \lambda \in \mathbb{K},\ \lambda u \in F.$

Définition 1.16 (Morphisme d'algèbre) *Soient $(E,+,\times,\dot{)}$ et $(F,+,\times,\dot{)}$ deux $\mathbb{K}-$algèbres. Soit $\phi\colon E \to F$. On dit que ϕ est un morphisme de $\mathbb{K}-$algèbres si les assertions suivantes sont vérifiées :*

1) $\forall (u,v) \in E^2,\ \phi(u+v) = \phi(u) + \phi(v)$

2) $\forall (u,v) \in E^2,\ \phi(u \times v) = \phi(u) \times \phi(v)$

3) $\forall u \in E,\ \forall \lambda \in \mathbb{K},\ \phi(\lambda u) = \lambda \phi(u)$

4) $\phi(1_E) = 1_F.$

1.7 Exercices résolus

Exercice 1.1 *Soit $G = \mathbb{R}^\star \times \mathbb{R}$ et $\star$ la loi de composition interne définie sur G par*

$$(x,y) \star (x',y') = (xx',xy'+y)$$

1) Montrer que $(G,\star)$ est un groupe non commutatif.

2) Montrer que $\mathbb{R}_+^\star \times \mathbb{R}$ est un sous-groupe de $(G,\star)$.

Solution.

1) La loi $\star$ est bien définie, on montre que $*$ est associative, $(1,0)$ est l'élément neutre et $(\frac{1}{x},-\frac{y}{x})$ est le symétrique de (x,y). Soient $(x,y)\,,(x',y')\,,(x'',y'') \in G$

a) Associativité :

$$\begin{aligned}(x,y) \star (x',y') \star (x'',y'') &= (xx',xy'+y) \star (x'',y'') \\ &= (xx'x'',xx'y''+xy'+y)\end{aligned}$$

et

$$\begin{aligned}(x,y) \star ((x',y') \star (x'',y'')) &= (x,y) \star (x'x'',x'y''+y') \\ &= (xx'x'',xx'y''+xy'+y)\end{aligned}$$

donc $\star$ est associative.

b) Elément neutre :

$$(x,y) \star (1,0) = (x,y) \quad \text{et} \quad (1,0) \star (x,y) = (x,y)$$

donc $(1,0)$ est élément neutre.

c) Symétrie :

$$(x,y) \star (1/x, -y/x) = (1,0) \quad \text{et} \quad (1/x, -y/x) \star (x,y) = (1,0)$$

donc tout élément est symétrisable.

Finalement d'après a), b) et c), on a : $(G,\star)$ est un groupe.

$(1,2)\star(3,4) = (3,6)$ et $(3,4)\star(1,2) = (3,10)$ donc le groupe n'est pas commutatif.

2) $H = \mathbb{R}_+^\star \times \mathbb{R}$ est inclus dans G.

$(1,0) \in H$.

$$\forall (x,y)\,,\ (x',y') \in H,\ (x,y) \star (x',y') \in H$$

car $xx' > 0$

$$\forall (x,y) \in H,\ (x,y)^{-1} = (1/x, -y/x) \in H$$

car $1/x > 0$.

D'où H est un sous groupe de $(G,\star)$.

Exercice 1.2 *1) Montrer que $\mathbb{Z}^2$ n'est pas monogène.*

2) Est-ce que $(\mathbb{Z}/10\mathbb{Z}) \times (\mathbb{Z}/21\mathbb{Z})$ est monogène ?

Solution.

1) Soit $(a,b) \in \mathbb{Z}^2$. Le sous-groupe de $\mathbb{Z}^2$ engendré par (a,b) est l'ensemble $A = \{(na,nb)\ ;\ n \in \mathbb{Z}\}$.

bullet Si $(a,b) = (0,0)$, il est clair que $A \neq \mathbb{Z}^2$.

- Sinon, on suppose par exemple $b \neq 0$. Alors $(1,0) \notin A$ puisque

$$nb = 0 \Rightarrow n = 0.$$

Dans tous les cas $A \neq \mathbb{Z}^2$, donc $\mathbb{Z}^2$ n'est pas monogène.

2) Le groupe $(\mathbb{Z}/10\mathbb{Z}) \times (\mathbb{Z}/21\mathbb{Z})$ est isomorphe à $\mathbb{Z}/210\mathbb{Z}$ puisque 10 et 21 sont premiers entre eux $(21 - 2 \times 10 = 1)$.

Exercice 1.3 *1) L'ensemble des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a,b,c,d \in \mathbb{R}$ tels que $ad - bc \neq 0$ et $a^2 - b^2 - c^2 - d^2 \leq 1$ est-il un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$?*

2) L'ensemble des matrices $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$ est-il un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$?

3) Existe-t-il une valeur $M \in \mathbb{R}$ telle que l'ensemble des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a,b,c,d \in \mathbb{R}$ tels que $ad - bc \neq 0$ et $a \leq M$ forme un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$?

Solution.

1) L'ensemble G des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a,b,c,d \in \mathbb{R}$ tels que $ad - bc \neq 0$ et $a^2 - b^2 - c^2 - d^2 \leq 1$ n'est pas un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$. En effet, les deux matrices $\begin{pmatrix} 1 & 1 \\ 0 & \frac{1}{2} \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 1 & \frac{1}{2} \end{pmatrix}$ appartiennent à G et leur produit $\begin{pmatrix} 2 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{4} \end{pmatrix}$ n'appartient pas à G.

2) L'ensemble H des matrices $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$ est un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$. En effet,
   - I_2 élément neutre de $\mathcal{G}l_2(\mathbb{R})$ appartient à H.
   - Soient $M = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ et $M' = \begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix}$ deux éléments de H alors $MM' = \begin{pmatrix} ac & ad+bc^{-1} \\ 0 & (ac)^{-1} \end{pmatrix}$ donc le produit de deux éléments de H appartient à H.
   - Soit $M = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$. Alors $M^{-1} = \begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix}$ appartient à H.

3) Soit K_M l'ensemble des matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ avec $a,b,c,d \in \mathbb{R}$ tels que $ad - bc \neq 0$ et $a \leq M$. On montre, en raisonnant par l'absurde, qu'il n'existe pas de valeur $M \in \mathbb{R}$ telle que K_M forme un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$.
   Soit $M \in \mathbb{R}$ tel que K_M forme un sous-groupe de $\mathcal{G}l_2(\mathbb{R})$. Alors I_2 appartient à K_M donc $M \geq 1$. Ainsi, les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et, pour tout $n \in \mathbb{N}$, $A_n = \begin{pmatrix} 1 & 1 \\ n & 1 \end{pmatrix}$ appartiennent à K_n donc le produit $AA_n = \begin{pmatrix} 1+n & 0 \\ 0 & 1 \end{pmatrix}$ appartient à K_n. En conséquence, pour tout $n \in \mathbb{N}$, on a : $1 + n \leq M$, ce qui est absurde.

Exercice 1.4 *Soit G un groupe, H et K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.*

Solution.

- Si $H \subset K$ alors $H \cup K = K$, qui est un sous-groupe de H. Même chose si $K \subset H$.
- Réciproquement, supposons que $H \cup K$ est un sous-groupe de G. Par l'absurde supposons que $H \not\subset K$ et $K \not\subset H$. Alors il existe $x \in H \setminus K$ et $y \in K \setminus H$. Comme $x,y \in H \cup K$ et que $H \cup K$ est un groupe alors $x.y \in H \cup K$. Donc $x.y \in H$ ou $x.y \in K$. Par exemple supposons $x.y \in H$ alors comme $x \in H$, $x^{-1} \in H$ et donc comme H est un groupe $x^{-1}.x.y \in H$ et donc $y \in H$. Ce qui est en contradiction avec l'hypothèse $y \in K \setminus H$. En conclusion, parmi les sous-groupes H et K l'un est inclus dans l'autre.

Exercice 1.5 *Soit H un groupe abélien. Un élément $x \in H$ est dit d'ordre fini lorsqu'il existe $n \in \mathbb{N}$ tel que la somme $x + \cdots + x$ (n-fois) soit égale à 0. Montrer que l'ensemble des éléments d'ordre fini de H est un sous-groupe abélien de H.*

Solution. On note G l'ensemble des éléments d'ordre fini de H. On montre que G est un sous-groupe de H.
- $G \subset H$ et $0 \in G$.
- Si $x \in G$ alors $(-x)+(-x)+\cdots+(-x) = -(x+x+\cdots+x) = 0$. Donc $-x \in G$.

– Si $x,y \in G$ alors $(x+y)+\cdots+(x+y) = (x+\cdots+x)+(y+\cdots+y) = 0+0 = 0$. Donc $x+y \in G$.

On a montré que G est un sous-groupe de H. De plus, comme H est commutatif alors G l'est aussi.

Exercice 1.6 *Soient G un groupe et $x \in G$ un élément d'ordre n. Quel est l'ordre de x^2 ?*

Solution. On rappelle d'abord que pour x un élément d'ordre n, alors

$$x^q = e \Rightarrow n|q.$$

– Si n est pair alors $\mathrm{ord}(x^2) = n/2$: en effet $(x^2)^{\frac{n}{2}} = x^n = e$ et pour $p \geq 1$ tel que $(x^2)^p = e$ alors $x^{2p} = e$ et $n|2p$ donc $p \geq \frac{n}{2}$. Donc $n/2$ est le plus petit des entiers q (non nul) tel que $x^q = e$ et par conséquent $n/2$ est l'ordre de x.
– Si n est impair alors $\mathrm{ord}(x) = n$. Tout d'abord $(x^2)^n = (x^n)^2 = e$ et pour p tel que $(x^2)^p = e$ alors $n|2p$ mais 2 et n sont premiers entre eux donc d'après le théorème de Gauss, $n|p$ et en particulier $p \geq n$.

Exercice 1.7 *1) Soient G un groupe et $x,y \in G$ des éléments qui commutent et d'ordres respectifs m et n premiers entre eux. Montrer que xy est d'ordre mn. Montrer que l'hypothèse m et n premiers entre eux est indispensable.*

2) Montrer que $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ sont des éléments d'ordres finis et que AB n'est pas d'ordre fini.

Solution.

1) On a $(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = e.e = e$. Soit p tel que $(xy)^p = e$, alors $e = (xy)^{mp} = x^{mp}y^{mp} = y^{mp}$, et donc mp est divisible par l'ordre de y, c'est-à-dire n. Comme m et n sont premiers entre eux alors d'après le théorème de Gauss n divise p. Un raisonnement semblable à partir de $(xy)^{np} = e$ conduit à : m divise p. Finalement $m|p$ et $n|p$ donc $mn|p$ car m et n sont premiers entre eux.

   On propose un contre-exemple dans le cas où m et n ne sont pas premiers entre eux : dans le groupe $\mathbb{Z}/12\mathbb{Z}$: $\bar{2}$ est d'ordre 6, $\bar{4}$ est d'ordre 3, mais $\bar{2}+\bar{4} = \bar{6}$ est d'ordre $2 \neq 3 \times 6$.

2) A est d'ordre 4, B est d'ordre 3, $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ n'est jamais la matrice identité pout $n \geq 1$.

Exercice 1.8 *Le groupe $(\mathbb{Q},+)$ est-il monogène ?*

Solution. On propose une démonstration par l'absurde. Supposons que $(\mathbb{Q},+)$ est engendré par un seul élément $\frac{p}{q}$ (p et q premiers entre eux) alors tout élément de $\mathbb{Q}$ s'écrit $n\frac{p}{q}$ avec $n \in \mathbb{Z}$. Il s'ensuit que $\frac{p}{2q}$ (qui appartient à $\mathbb{Q}$) doit s'écrire $n\frac{p}{q}$, mais alors $2n = 1$ avec $n \in \mathbb{Z}$ ce qui est impossible. Par conséquent, $(\mathbb{Q},+)$ n'est pas monogène.

Exercice 1.9 *Montrer que les groupes multiplicatifs $\mathbb{R} \setminus \{0\}$ et $\mathbb{C} \setminus \{0\}$ ne sont pas isomorphes.*