Lycée Louis-Le-Grand, Paris 2014/2015
MPSI 4 – Mathématiques
A. Troesch

# Algèbre 2 – Structures algébriques

**Exercice 1 – (Produit semi-direct)**
Soit $G$ un groupe

1. Montrer que $\mathrm{Aut}(G)$ muni de la composition est un groupe.
2. Soit $G$ et $H$ deux groupes, et $\varphi : H \longrightarrow \mathrm{Aut}(G)$ un homomorphisme de groupe. On définit, pour tout $(g,h) \in G \times H$ :

$$(g,h) \star (g',h') = (g \cdot \varphi(h)(g'), hh').$$

Montrer que $(G \times H, \star)$ est un groupe. Ce groupe est appelé produit semi-direct de $G$ par $H$ relativement à $\varphi$ et est noté $G \rtimes_\varphi H$, ou plus simplement $G \rtimes H$, lorsqu'il n'y a pas d'ambiguïté possible.

**Exercice 2 – (Théorème de Cayley)**
En considérant les permutations de $G$ définies par $x \mapsto gx$, montrer que tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique.

**Exercice 3** – Soit $G$ un ensemble muni d'une loi de composition $\times$ associative telle que pour tout $x$ et $y$ de $G$, il existe un unique $z$ et un unique $z'$ de $G$ tels que $x \times z = y$ et $z' \times x = y$. Montrer que $G$ est un groupe.

**Exercice 4** – Soit $G$ un ensemble muni d'une loi de composition $/$ vérifiant, pour tout $(a,b,c) \in G^3$ :
- $a/a = b/b$
- $a/(b/b) = a$
- $(a/a)/(b/c) = c/b$
- $(a/c)/(b/c) = a/b$.

En interprétant la loi $/$ comme une « division », construire sur $G$ une structure de groupe.

**Exercice 5** – Soit $G$ un groupe non réduit à son élément neutre. Montrer que $G$ n'admet aucun sous-groupe propre si et seulement si $G$ est cyclique d'ordre $p$ premier.

**Exercice 6** – Soit $G$ un groupe fini. Montrer que la relation $H < K$ (sous-groupe) définit un ordre total sur l'ensemble des sous-groupes de $G$ si et seulement si $G$ est cyclique d'ordre $p^\alpha$.

**Exercice 7 – (Exposant d'un groupe)**
Soit $G$ un groupe fini abélien.

1. Montrer que pour tout $x$ et $y$ d'ordre $a$ et $b$, il existe un élément $z$ dans $G$ d'ordre $a \vee b$
2. Montrer qu'il existe dans $G$ un élément d'ordre égal au ppcm de l'ordre de tous les éléments. Cet ordre est appelé exposant du groupe $G$.
3. Le résultat reste-t-il vrai si $G$ n'est pas supposé abélien ?

**Exercice 8 – (Idempotents)**
Soit $(E, \star)$ un magma . On dit que $x \in E$ est idempotent si $x \star x = x$.

1. Montrer que si tout élément de $E$ est régulier et si $\star$ est distributive par rapport à elle-même, alors tout élément est idempotent.
2. Montrer que si tout élément de $E$ est régulier et si $\star$ est associative, alors $E$ admet au plus un idempotent.

**Exercice 9** – Soit $(E, \cdot)$ un magma associatif tel qu'il existe $n \in \mathbb{N}$, supérieur ou égal à 2, tel que pour tout $(x,y) \in E^2$, $(xy)^n = yx$. montrer que $\cdot$ est commutative.

**Exercice 10** – Soit $(E, \cdot)$ un monoïde commutatif. Soit $(x, y) \in E^2$. On suppose que $xy$ est symétrisable. Montrer que $x$ et $y$ le sont aussi.

**Exercice 11** – Montrer que $\mathbb{R} \times \mathbb{R}$ muni de la loi $\star$ définie par

$$(x, y) \star (x', y') = (x + x', y\mathrm{e}^{x'} + y'\mathrm{e}^{x})$$

est un groupe.

**Exercice 12 – (groupe des inversibles d'un monoïde)**
Soit $(E, \cdot)$ un monoïde, et $S(E)$ l'ensemble des éléments symétrisables de $E$. Montrer que $S(E)$ est stable par $\cdot$, et que la loi induite munit $S(E)$ d'une structure de groupe.

**Exercice 13** – Soit $E$ un ensemble fini muni d'une loi de composition interne $\cdot$ associative, pour laquelle tous les éléments de $E$ sont réguliers. Montrer que $(E, \cdot)$ est un groupe.

**Exercice 14 – (Caractérisation des couples de sous-groupes dont l'union est un groupe)**
Soit $G$ un groupe et $H$ 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 $K \subset H$. Peut-on généraliser cela à une union de $n$ sous-groupes ?

**Exercice 15 – (Autour du produit HK)**
Soit $(G, \times)$ un groupe, et $H$ et $K$ deux sous-groupes de $G$. Les questions sont indépendantes.

1. Montrer que si $G$ est abélien, alors $HK$ est un groupe, et que c'est le plus petit sous-groupe de $G$ contenant $H \cup K$.
2. Dans le cas général, montrer que les propriétés suivantes sont équivalentes :
   (i) $HK$ est un sous-groupe de $G$
   (ii) $KH$ est un sous-groupe de $G$
   (iii) $HK \subset KH$
   (iv) $KH \subset HK$
3. Soit $H, K, L$ trois sous-groupes de $G$ tels que $HK = KH$ et $H \subset L$. Montrer que

$$H(K \cap L) = (K \cap L)H = (HK) \cap L.$$

**Exercice 16 – (Groupes cycliques)**

1. Montrer que tout groupe cyclique est abélien, et isomorphe à un groupe $\mathbb{Z}/n\mathbb{Z}$.
2. Montrer que tout sous-groupe d'un groupe cyclique est cyclique.

**Exercice 17** – Soit $n \in \mathbb{N}$. Déterminer tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

**Exercice 18** –

1. Déterminer (à isomorphisme près) tous les groupes d'ordre $p$ premier.
2. Soit $G$ un groupe abélien tel que tous ses sous-groupes propre soient cycliques. Est-ce que $G$ est cyclique ?

**Exercice 19 – (ENS)**
Caractériser les groupes dont l'ensemble des sous-groupes est fini.

**Exercice 20 – (ENS)**
Soit $G$ un groupe abélien d'ordre $pq$, où $p$ et $q$ sont deux nombres premiers distincts. Montrer que $G$ est cyclique.

**Exercice 21** – Soit $(G, \times)$ un groupe, de neutre $e$. On suppose que pour tout $x \in E$, $x^2 = e$.

1. Montrer que $G$ est abélien et que s'il n'est pas réduit à $\{e\}$, son cardinal est pair.
2. Montrer que si $G$ est fini, $|G|$ est une puissance de 2.

**Exercice 22** – Soit $f : G \to H$ un morphisme de groupes (noté additivement).

1. Montrer que pour tout sous-groupe $G'$ de $G$, $f(G')$ est un sous-groupe de $H$
2. Montrer que pour tout sous-groupe $H'$ de $H$, $f^{-1}(H')$ est un sous-groupe de $H$.
3. L'image par $f$ d'un sous-groupe distingué de $G$ est-elle un sous-groupe distingué de $H$ ?
4. L'image réciproque par $f$ d'un sous-groupe distingué de $G$ est-elle un sous-groupe distingué de $F$ ?

**Exercice 23** –

1. Soit $f : G \to H$ un morphisme de groupes. Montrer que $\mathrm{Ker}(f)$ est un sous-groupe distingué de $f$.
2. Réciproquement, montrer que tout sous-groupe distingué de $G$ est le noyau d'un certain morphisme de groupes $f : G \to H$.

**Exercice 24** – Soit $H$ et $K$ deux sous-groupes de $G$ d'ordres finis respectifs $\alpha$ et $\beta$ tels que $\alpha \wedge \beta = 1$. Montrer que $H \cap K = \{e\}$, où $e$ est le neutre de $G$.

**Exercice 25** – Soit $(G, \times)$ un groupe.

1. On définit le centre $Z$ de $G$ par $Z = \{a \in G \mid \forall g \in G, ag = ga.\}$. Montrer que $Z$ est un sous-groupe de $G$.
2. Montrer que si $G/Z$ est cyclique, alors $G$ est abélien.
3. Soit $G$ un groupe abélien de neutre $e$, et $x$ deux éléments de $G$ d'ordre $p$, tel que $y$ ne soit pas dans le sous-groupe monogène $< x >$ engendré par $x$. Montrer que $< x > \cap < y >= \{e\}$.
4. En déduire que si $p$ est un entier premier, tout groupe d'ordre $p^2$ est isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$, soit à $(\mathbb{Z}/p\mathbb{Z})^2$.

**Exercice 26** – Soit $(A, +, \times)$ un anneau. Montrer que $U(A)$ l'ensemble des éléments inversibles de $A$ est stable par $\times$, et est un groupe pour cette loi de composition interne.

**Exercice 27** – Soit $A$ un anneau, et $a \in A$. On suppose que $a$ admet un unique inverse à droite. Montrer que $a$ est régulier à gauche, puis que $a$ est inversible. Quel est son inverse ?

**Exercice 28** – Soit $A$ un anneau. Montrer que l'intersection de deux sous-anneaux de $A$ est encore un anneau.

**Exercice 29** – Soit $X$ un ensemble non vide.

1. Montrer que $(\mathcal{P}(X), \triangle, \cap)$ est un anneau. Quels sont les éléments neutres ? Est-ce un corps ?
2. (a) Soit $Y \subset X$. $\mathcal{P}(Y)$ est-il un sous-anneau de $\mathcal{P}(X)$ ?
   (b) Montrer que $\mathcal{P}(Y)$ peut être muni à l'aide des lois induites d'une structure d'anneau.
3. Soit $\{I_1, \dots, I_n\}$ une partition de $X$, et $A = \left\{\bigcup_{j \in J} I_j, \quad J \in \mathcal{P}([\![1, n]\!])\right\}$. Montrer que $A$ est un sous-anneau de $\mathcal{P}(X)$.
4. Réciproquement, montrer que tout sous-anneau de $\mathcal{P}(X)$ est de cette forme.

**Exercice 30** – Soit $J = (a_{i,j})_{1 \leqslant i,j \leqslant n}$ la matrice de $\mathcal{M}_n(\mathbb{R})$ définie par

$$a_{i,j} = \begin{cases} 1 & \text{si } i + j = n + 1 \\ 0 & \text{sinon.} \end{cases}$$

$A = \{aI_n + bJ, \quad (a, b) \in \mathbb{R}^2\}$ est-il un sous-groupe $\mathcal{M}_n(\mathbb{R})$ ? un sous-anneau ?

**Exercice 31** – Soit $A$ un anneau et $a$ un élément nilpotent de $A$. Montrer que $1 - a$ est inversible, et exprimer son inverse en fonction des puissances successives de $a$.

$^*$**Exercice 32** – **(Exponentielle et logarithme d'un élément nilpotent)**
Soit $A$ un anneau tel que tout élément $n = n \times 1_A$ ($n \in \mathbb{N}^*$) est inversible. Ces éléments commutant de façon évidente avec tout autre élément de $A$, on s'autorise à écrire la multiplication par $n^{-1}$ sous forme d'une fraction. On définit, pour tout élément nilpotent $a$ :

$$\exp(a) = \sum_{n=0}^{+\infty} \frac{a^n}{n!} \qquad \text{et} \qquad \ln(1 - a) = -\sum_{n=1}^{+\infty} \frac{a^n}{n},$$

ces sommes étant bien définies, puisqu'elles ne comportent qu'un nombre fini de termes non nuls.

1. Montrer que pour tout $a$ et $b$ nilpotents tels que $ab = ba$, $\exp(a+b) = \exp(a)\exp(b)$.
2. Montrer que pour tout élément nilpotent $a$, $\exp(a)$ est inversible, et donner son inverse.
3. Montrer que pour tout élément nilpotent $a$, $\exp(\ln(1-a)) = 1-a$

   Indication : on pourra mener de front le calcul de $\exp(\ln(1-a))$ dans $A$ et un développement limité à un ordre assez grand de $\exp(\ln(1-x))$ dans $\mathbb{R}$, et comparer ensuite les coefficients obtenus.
4. Montrer que pour tout élément nilpotent $a$, $\ln(\exp(a)) = a$.

**Exercice 33** – Soit $A$ un anneau, et $a$ et $b$ deux éléments de $A$. Montrer que si $ab$ est nilpotent, alors $ba$ aussi.

**Exercice 34** – Soit $A$ un anneau commutatif. Soit $N$ l'ensemble des éléments nilpotents de $A$. Soit $B = \{1+x,\ x \in N\}$. Montrer que $(B, \times)$ est un groupe.

**Exercice 35** – Soit $A$ un anneau, $a$ un élément nilpotent de $A$, et $B = \{1 + aP(a),\ P \in \mathbb{Z}[X]\}$. Montrer que $B$ est stable par $\times$, et que $(B, \times)$ est un groupe.

**Exercice 36** – Soit $A$ un anneau. Pour tout $x \in A$, on définit

$$x^{(0)} = 1, \qquad x^{(1)} = x, \qquad x^{(2)} = x(x-1), \qquad \dots \qquad x^{(n)} = x(x-1)\dots(x-n+1).$$

1. Soit $P$, $Q$ dans $\mathbb{Z}[X]$. Montrer que si $x$ et $y$ commutent, alors $P(x)$ et $Q(y)$ aussi.
2. Montrer que pour tout $x$ et $y$ de $A$, si $xy = yx$, alors :

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

**Exercice 37** – Soit $A$ un anneau, et $a$ et $b$ deux éléments de $A$ tels que $ab$ soit inversible et $ba$ ne soit pas diviseur de zéro. Montrer que $a$ et $b$ sont inversibles.

**Exercice 38** – **(Anneaux euclidiens et anneaux principaux)**
Soit $A$ un anneau. On dit que $A$ est euclidien si $A$ est intègre, et s'il existe une fonction $v : A \setminus \{0\} \to \mathbb{N}$, appelée stathme, telle que :

$$\forall (a,b) \in (A \setminus \{0\})^2, \quad \exists (q,r) \in A^2, \quad a = bq + r \text{ et } (r = 0 \text{ ou } v(r) < v(b)).$$

1. Justifier que $\mathbb{Z}$, $\mathbb{R}[X]$ sont euclidiens.
2. Soit $\mathbb{Z}[\mathrm{i}] = \{(a + \mathrm{i}\, b),\ (a,b) \in \mathbb{Z}\}$ (entiers de Gauss) En considérant $v : z \mapsto |z|^2$, montrer que $\mathbb{Z}[\mathrm{i}]$ est euclidien.
3. Montrer qu'un anneau euclidien est principal.

**Exercice 39** – Soit $K$ un corps

1. Montrer que si la caractéristique de $K$ est $p$ premier, il existe un morphisme de corps injectif $i : \mathbb{F}_p \to K$.
2. Montrer que si la caractéristique de $K$ est nulle, il existe un morphisme de corps injectif $i : \mathbb{Q} \to K$.

**Exercice 40** – **(Caractérisation d'un corps parmi les anneaux par ses idéaux)**
Soit $A$ un anneau commutatif non réduit à $\{0\}$. Montrer que $A$ est un corps si et seulement si les seuls idéaux de $A$ sont $\{0\}$ et $A$.

**Exercice 41** – **(Un corps de nombres)**
Soit $a \in \mathbb{Q}_+^*$ tel que $\sqrt{a} \notin \mathbb{Q}$. On définit :

$$\mathbb{Q}(\sqrt{a}) = \{\lambda + \mu\sqrt{a}\}, \quad (\lambda, \mu) \in \mathbb{Q}^2.$$

1. Montrer que $\mathbb{Q}(\sqrt{a})$ est un sous-corps de $\mathbb{R}$.
2. Les corps $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ sont-ils isomorphes ?