AG3 2017-2018

FEUILLE D'EXERCICES 13.

Révision.

Exercice 1. *Réviser les définitions de*

- *Groupe groupe abélien, sous-groupe, groupe cyclique, classe à gauche suivant un sous-groupe, groupe quotient, ordre d'un groupe, ordre d'un élément, morphisme de groupe, noyau d'un morphisme, indice d'un sous-groupe H dans G, groupe symétrique, transposition, signature, groupe alterné, action de groupe, action triviale, orbite, stabilisateur*
- S_n, A_n, D_n, $Aut(G)$ *(ou G est un groupe),* G/H *(G est un groupe et H est un sous-groupe),* $K[X]$, $pgcd(P,Q)$, $GL(2,\mathbb{R})$, $SL(2,\mathbb{R})$, $Hom_K(V,W)$ *où V et W espaces vectoriels sur K.*
- *Anneau, anneau commutatif, sous-anneau, corps, idéal à gauche (à droite, bilatère), diviseurs de zéro, anneau intègre, idéal principal, morphisme d'anneaux, noyau d'un morphisme d'anneau, anneau quotient, idéal premier, idéal maximal, caractéristique d'un anneau (d'un corps), corps des fractions.*
- *Polynôme à coéfficients d'un corps K, une fonction polynôme, corps algébriquement clos, polynôme irreductible.*
- *Espace vectoriel sur un corps K, sous-espace vectoriel, vecteurs linéairement dépendants et linéairement dépendants, une base d'un espace vectoriel, un espace vectoriel de dimension finie (et de dimension infinie), application linéaire, noyau et image.*

Exercice 2. *Décider pour chaque énoncé s'il est vrai ou faux. Justifier vos réponses.*

(1) *Soit* $S = \{x + \pi y \mid x, y \in \mathbb{Q}\}$.

(a) S *est un sous-groupe de* $(\mathbb{R}, +)$;
Réponse : C'est vrai. En effet, $0 = 0 + \pi \cdot 0 \in S$; *soit* $x, y \in S$, *il suffit de montrer* $x - y \in S$. *On peut écrire* $x = x_1 + \pi \cdot x_2$ *et* $y = y_1 + \pi \cdot y_2$ *avec* $x_1, x_2, y_1, y_2 \in \mathbb{Q}$, *et* $x - y = (x_1 - y_1) + \pi(x_2 - y_2)$. *Comme* $x_1 - y_1, x_2 - y_2 \in \mathbb{Q}$, *on a* $x - y \in S$.

(b) S *est un sous-groupe de* $(\mathbb{R}, \cdot)$;
Réponse : C'est faux. S n'est pas stable par multiplication, et 0 *n'a pas d'inverse multiplicatif.*

(c) S *est un idéal du corps* $(\mathbb{R}, +\cdot)$;
Réponse : C'est faux. S n'est pas stable par multiplication par $\mathbb{R}$.

(d) S est un sous-anneau de $\mathbb{R}, +, \cdot)$;
Réponse : C'est faux. S n'est pas stable par multiplication.

(e) $(S, +, \cdot)$ est un corps.
Réponse : C'est faux. S n'est pas stable par multiplication.

(f) S est un espace vectoriel sur $\mathbb{R}$.
Réponse : C'est faux. S n'est pas stable par multiplication par les éléments de $\mathbb{R}$. Par contre S est un espace vectoriel sur $\mathbb{Q}$.

(2) Il existe un morphisme de groupe $\phi : (\mathbb{R}, +) \to (\mathbb{R}, +)$

(a) tel que $\phi(2) = 3$ et $\phi(-2) = 2$;
Réponse : C'est faux. Tout morphisme de groupe f de $\mathbb{R}$ dans $\mathbb{R}$ satisfait $f(0) = 0$, et $f(x+y) = f(x)+f(y)$. Si ϕ est un morphisme, on a $0 = \phi(0) = \phi(2 + (-2)) = \phi(2) + \phi(-2) = 3 + 2 = 5$, donc absurde.

(b) tel que $\phi(x) \geq 0$ pour tout $x \in \mathbb{R}$;
Réponse : C'est vrai. Un tel morphisme est unique, c'est le morphisme de groupes trivial, i.e. tel que $\phi(x) = 0$ pour tout $x \in \mathbb{R}$;

(c) tel que $\phi(a) = b$ pour un $a \in \mathbb{R}$ et un $b \in \mathbb{R}$.
Réponse : C'est faux. Si $a = 0$ et $b \neq 0$ un tel morphisme n'existe pas. Par contre, si $a \neq 0$ et $b \neq 0$, on prend $\phi(x) = \frac{b}{a}x$; si $a = b = 0$, on prend $\phi(x) = kx$ pour un $k \in \mathbb{R}$.

(3) $\mathbb{Z}/2\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}/4\mathbb{Z}$;
Réponse : C'est faux. $\mathbb{Z}/2\mathbb{Z}$ n'est pas un sous-ensemble de $\mathbb{Z}/4\mathbb{Z}$.

(4) $\mathbb{Z}/2\mathbb{Z}$ est isomorphe à un sous-groupe de $\mathbb{Z}/4\mathbb{Z}$;
Réponse : C'est vrai. $\mathbb{Z}/2\mathbb{Z}$ est isomorphe à un sous-groupe $H = \{\bar{0}, \bar{2}\}$ de $\mathbb{Z}/4\mathbb{Z}$.

(5) $G = 5\mathbb{Z}$ est un sous-groupe distingué de Z ;
Réponse : C'est vrai. G est un sous-groupe de $\mathbb{Z}$, et comme Z est abélien, tout son sous-groupe est distingué.

(6) $SL(2, \mathbb{R})$ est un sous-groupe distingué de $GL(2, \mathbb{R})$;
Réponse : C'est vrai, on a fait le calcul en TD.

(7) Tout groupe cyclique d'ordre 20 a un sous-groupe d'ordre 5 ;
Réponse : C'est vrai. Soit x un générateur de ce groupe. Alors x est d'ordre 20. Soit $y = x^4$, alors $|y| = 5$. Le sous-groupe engendré par y est d'ordre 5.

(8) S_4 est abélien ;
Réponse : C'est faux. On a montré en cours que S_n n'est pas abélien à pour $n \geq 3$.

(9) Si un idéal I d'un anneau A contient 1_A, alors $I = A$.
Réponse : C'est vrai. Si $1_A \in I$ et $x \in A$, alors par définition de idéal, $x \cdot 1_A \in I$, d'où $x \in I$ pour tout $x \in A$ et donc $A = I$.

(10) *Tout sous-anneau S de A est un idéal bilatère de A.*
Réponse : C'est faux. Par exemple, $I = Z$ est un sous-anneau de $A = \mathbb{Q}$, mais ce n'est pas un idéal.

(11) *Le corps $\mathbb{Z}/7\mathbb{Z}$ n'est pas algébriquement clos.*
Réponse : C'est vrai. On a vu en cours et en TD que un corps fini n'est jamais algébriquement clos.

(12) *L'anneau $\mathbb{Q}[X]$ est intègre.*
Réponse : C'est vrai. On a vu en cours que $K[X]$ est intègre.

(13) *Polynôme $P = 1 + X + X^2 + X^3 + X^4$ est irréductible dans*

(a) $\mathbb{R}[X]$
Réponse : C'est faux. Par exemple, $P = (1 - \frac{2}{1+\sqrt{5}}X + X^2)(1 + \frac{1+\sqrt{5}}{2}X + X^2)$. Pour trouver ces polynômes de degré 2 on commence par écrire $P = (a_0 + a_1X + a_2X^2)(b_0 + b_1X + b_2X^2)$. On obtient le système d'équations $a_0b_0 = 1$, $a_2b_2 = 1$, $a_0b_1 + a_1b_0 = 1$, $a_0b_2 + a_1b_1 + a_2b_0 = 1$ et $a_1b_2 + a_2b_1 = 1$. Il y a une infinité de solutions en fait, par exemple $a_0 = b_0 = a_2 = b_2 = 1$, $a_1 = -\frac{2}{1+\sqrt{5}}$ et $b_1 = \frac{1+\sqrt{5}}{2}$.
Une autre méthode : Si P a une racine dans $\mathbb{R}$, c'est bon, P n'est pas irréductible. Sinon P a une racine $\alpha \in \mathbb{C} \setminus \mathbb{R}$. On a $P(\alpha) = 0$ et donc $\overline{P(\alpha)} = 0$. Comme les coéfficients de P sont réels, $\overline{P(\alpha)} = P(\bar{\alpha})$, et donc $\bar{\alpha}$ est aussi une racine de P. Le polynôme $(X - \alpha)(X - \bar{\alpha}) = (X^2 - 2Re(\alpha)X + |\alpha|^2)$ est à coéfficients réels et il divise P. Donc P n'est pas irreductible. Cet argument montre que si $P \in \mathbb{R}[X]$ et de degré ≥ 3, alors P n'est pas irreductible.

(b) $\mathbb{Z}/5\mathbb{Z}[X]$
Réponse : C'est faux. $P(1) = 0$ mod 5, donc P a une racine dans $\mathbb{Z}/5\mathbb{Z}$.

(c) $\mathbb{Z}/2\mathbb{Z}[X]$.
Réponse : C'est vrai. On vérifie d'abord que $P(0) = 1$ mod 2 et $P(1) = 1$ mod 2, donc il n'y a pas de racines. Donc si P n'st pas irreductible, alors $P = P_1P_2$ où P_1 et P_2 sont des polynômes de degré 2. On suppose qu'il existent tels polynômes P_1 et P_2 , et on pose $P_1 = a_0 + a_1X + a_2X^2$ et $P_2 = b_0 + b_1X + b_2X^2$ et on essaie de determiner les coéfficients. En multipliant P_1 et P_2 on trouve que $a_0b_0 = 1$ et $a_2b_2 = 1$. Ca implique $a_0 = b_0 = a_2 = b_2 = 1$. Mais on a aussi $a_1 + b_1 = 1$ et $a_1b_1 = 1$. Ce système n'a pas de solutions dans $\mathbb{Z}/2\mathbb{Z}$.

(14) *$GL(2, \mathbb{R})$ est un espace vectoriel sur $\mathbb{R}$.*
Réponse : C'est faux. $GL(2, \mathbb{R})$ n'est pas stable par l'addition. Par exemple, $A = I_2$ et $B = -I_2$ sont deux éléments dans $GL(2, \mathbb{R})$, mais $A + B = 0$ et la matrice 0 n'est pas inversible.

(15) *Soit K un corps. L'espace vectoriel K^n est de dimension n.*
Réponse : C'est vrai. Vecteurs

$$e_1 = (1_K, 0_K, \dots, 0_K), e_2 = (0_K, 1_K, 0_K, \dots, 0_K), \dots, e_n = (0_K, \dots, 1_K)$$

dans K^n forment une base de K^n.

(16) *Fonctions $f_1, f_2 : K \to K$ définies par $f_1(t) = t$ et $f_2(t) = t^6$ sont linéairement indépendants sur tout corps K.*
Réponse : C'est faux. Contre exemple : $K = \mathbb{Z}/2\mathbb{Z}$. $f_1(\bar{0}) = f_2(\bar{0}) = \bar{0}$ et $f_1(\bar{1}) = f_2(\bar{1}) = 1$, donc $f_1 = f_2$.

Exercice 3. *Trouver tous les sous-groupes finis de $(\mathbb{R}, +)$.*
Réponse : Les éléments d'un groupe fini sont d'ordre fini. Si $x \in \mathbb{R}$, x est d'ordre fini si il existe $n \in \mathbb{N}^*$ avec $nx = 0$. Le seul élément d'ordre fini dans $(\mathbb{R}, +)$ est $x = 0$. Donc le seul sous-groupe fini de $(\mathbb{R}, +)$ est le sous-groupe trivial.

Exercice 4. *Trouver tous les sous-groupes de $G = \mathbb{Z}/6\mathbb{Z}$ et $G' = \mathbb{Z}/7\mathbb{Z}$.*
Réponse : Sous-groupes de G : $\{\bar{0}\}, G, \{\bar{0}, \bar{2}, \bar{4}\}, \{\bar{0}, \bar{3}\}$. Sous-groupes de G' : $\{\bar{0}\}$ et G. Il n'y a pas d'autres car l'ordre d'un sous-groupe divise l'ordre du groupe, et l'ordre de G' est 7.

Exercice 5. *Soit*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 6 & 2 & 4 & 1 \end{pmatrix}$$

(1) *Décomposer σ en produit des cycles à support disjoint.*
Réponse : $\sigma = (1\,3\,7)(4\,6)(2\,5)$

(2) *Décomposer σ en produit des transpositions.*
Réponse : Par exemple, $\sigma = (1\,7)(1\,3)(4\,6)(2\,5)$.

(3) *Déterminer la signature de σ.*
Réponse : D'après la question précédent, σ se décompose en produit de nombre paire de transpositions, donc $\epsilon(\sigma) = 1$.

Exercice 6. *Soit $G = S_3$. G agit sur lui-même par conjugaison. Trouver toutes les orbites pour cette action.*
Réponse : on a déjà fait cet exercice en TD pour S_3 (la question devait etre pour S_4). Les orbites pour S_3 sont :

$$\{(1\,2), (1\,3), (2\,3)\}, \{(1\,2\,3), (1\,3\,2)\} \text{ et } \{Id\}$$

Exercice 7. *Soit A un anneau de Boole (pour tout $x \in A$ on a $x^2 = x$). Montrer que si A n'est pas trivial, alors A est de caractéristique 2.*
Réponse : Il faut montrer que $1_A + 1_A = 0_A$. Montrons en fait que $x + x = 0_A$ pour tout $x \in A$. On a

$$x + x = (x + x)^2 = x^2 + x + x + x^2 = x + x + x + x$$

d'où $x + x = 0_A$.

Exercice 8. *Soit A un anneau commutatif. On dit qu'un élément $x \in$ est nilpotent si il existe $n > 0$ tel que $x^n = 0_A$. Montrer que l'ensemble I des éléments nilpotents de A est un idéal de A.*
Réponse : D'abord, 0_A est nilpotent, donc $0_A \in I$. Soit $x, y \in I$, alors $x^n = 0$ et $y^m = 0$.

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

Si $k \leq n$ alors $m+n-k \geq m$ et donc $y^{m+n-k} = 0_A$. Si $k \geq n$, alors $x^k = 0_A$. Donc $x^k y^{m+n-k} = 0_A$ pour tout $0 \leq k \leq m+n$, d'où $(x+y)^{n+m} = 0_A$. On a montré que $x + y \in I$. Soit $x \in I$ et $c \in A$. Soit $n > 0$ tel que $x^n = 0_A$. Alors $(cx)^n = c^n x^n = c^n 0_A = 0_A$, donc $cx \in I$. On a montré que I est un idéal de A.

Exercice 9. *Soit V un espace vectoriel sur un corps K, et V_1, V_2 deux sous-espaces vectoriels de V.*

— *Montrer que $V_1 \cap V_2$ est un sous-espace vectoriel de V.*
Réponse : Il faux montrer que $V_1 \cap V_2$ contient le zéro, stable pas addition, et stable par multiplication par les éléments de K.
  (1) $0 \in V_1$ *et* $0 \in V_2$ *donc* $0 \in V_1 \cap V_2$ *;*
  (2) Soit $x, y \in V_1 \cap V_2$, alors $x, y \in V_1$ et $x, y \in V_2$. Donc $x + y \in V_1$ et $x + y \in V_2$ d'où $x + y \in V_1 \cap V_2$;
  (3) Soit $c \in K$ et $x \in V_1 \cap V_2$. Comme $x \in V_1$, on a $cx \in V_1$. Pareil pour V_2. Donc $cx \in V_1 \cap V_2$.

— *Montrer que*

$$V_1 + V_2 = \{u + w \,| u \in V_1, w \in V_2\}$$

est un sous-espace vectoriel de V.
Réponse :
  (1) $0 \in V_1$ *et* $0 \in V_2$ *donc* $0 = 0 + 0 \in V_1 + V_2$ *;*
  (2) Soit $x, y \in V_1 + V_2$, alors $x = x_1 + x_2, y = y_1 + y_2$ où $x_1, y_1 \in V_1$ et $x_2, y_2 \in V_2$. Donc $x_i + y_i \in V_i$ pour $i = 1, 2$, d'où $x + y \in V_1 + V_2$;
  (3) Soit $c \in K$ et $x \in V_1 + V_2$. Soit $x = x_1 + x_2$ avec $x_i \in V_i$. On a $cx_i \in V_i$ pour $i = 1, 2$. Donc $cx = cx_1 + cx_2 \in V_1 + V_2$.

Exercice 10. *(*) Montrer que tout groupe d'ordre 6 est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ou à S_3.*

Exercice 11. *(*) Montrer que l'anneau quotient $K[X]/I$ est un corps si et seulement si I est irréductible.*

Exercice 12. *(*) Sout G un groupe. Montrer que tout sous-groupe $H < G$ d'indice 2 est distingué.*