Université My Ismaïl
Faculté des Sciences–Meknès
Département de Mathématiques

A. U. 2020-2021
S. IV
Algébre 6

Série 1 (Corrigé/Indications)

Exercice 1

1. *On vérifie facilement que R_A est réflexive, symétrique et transitive et que pour tout $x \in E$, $\bar{x}^{R_A} = \bar{x}^R \cap A$.*
2. *On applique le théorème de décompostion d'une application à l'application $p_A = p_{|A} : A \to E/R$ laquelle est constante d'après (1) sur les classes de R_A.*

   Il existe donc une application $j_A : A/\mathcal{R}_{p_A} \to E/R$ qui vérifie $p_A = j_A \circ p$ avec $p : A \to A/\mathcal{R}_{p_A}$ la projection canonique de A sur le quotient relativement à la relation déquvalence $\mathcal{R}_{p_A}$ induite par p_A sur A ($x\mathcal{R}_{p_A}y \Leftrightarrow p_A(x) = p_A(y)$).

   D'autre part, on vérifie facilement que pour tout $x, y \in A$, on a : $x\mathcal{R}_{p_A}y \Leftrightarrow xR_Ay$ et par suite les deux relations déquivalences $\mathcal{R}_{p_A}$ et R_A sont identiques sur A.

   Il en ressort que $A/\mathcal{R}_{p_A} = A/R_A$ et donc que $q : A \to A/R_A$ est exactement $p : A \to A/\mathcal{R}_{p_A}$. D'où le résultat.
3. *Par sa construction, j_A est injective (car p_A est constante sur les classes) et elle est canonique (provient de la décomposition canonique de p_A).*

Exercice 2

Il est à noter tout d'abord que l'implication directe est évidente puisque tout groupe admet une élément neutre (à droite et à gauche) et tout élément admet un symétrique (à droite et à gauche).

Pour la réciproque, en remarque au début que $eTe = e$. Ensuite, si $x \in G$ vérifie $xTx = x$, alors en composant les deux membres (à gauche) par x', on obtient d'après (ii), l'associativité puis (i) que $x = e$ (noter que puisque T est une l.c.i, la composition préserve l'égalité). On en déduit que e est le seul élément idempotent de G.

Ensuite, on a par associativité et (i) : $(xTx')T(xTx') = xT(eTx') = xTx'$ et donc que xTx' est un idempotent, ce qui entraîne d'après ce qui précède que $xTx' = e$ et donc que x' est aussi un inverse à droite de x.

Enfin, par associativité et (i), on a : $xTe = xT(x'Tx) = (xTx')Tx = eTx = x$ et donc e est aussi un élément neutre à droite.

Exercice 3

1. *Il s'agit de trouver une condition nécessaire et suffisante sur G pour que φ soit un automorphisme. Remarquons alors que φ est un endomorphisme, si et seulement si $\forall x, y \in G,\ \varphi(xy) = \varphi(x)\varphi(y)$ si et seulement si $\varphi(xy) = \varphi(yx)$ car, (par définition de φ) on a : $\varphi(x)\varphi(y) = x^{-1}y^{-1} = (yx)^{-1} = \varphi(yx)$. On applique ensuite φ^{-1} et on obtient que $\forall x, y \in G,\ xy = yx$ c-à-d que G est commutatif.*

   Il est d'autre part évident que si G est commutatif, alors φ est un automorphisme. Par conséquent la C. N. S. est que G soit commutatif.
2. *Notons tout d'abord que par définition :*

$$a^k = \begin{cases} a \times \ldots \times a\ (k\ fois)\ si\ k \geq 0, \\ a^{-1} \times \ldots \times a^{-1}\ ((-k)\ fois)\ si\ k \leq 0. \end{cases} \tag{1}$$

   En particulier $a^0 = e$. Par suite, on a les relations suivantes :
   (a) : si $k \geq 0$, $a^k = a^{k-1}a = aa^{k-1}$, et donc $a^k a^{-1} = a^{k-1}$
   (b) : si $k \leq 0$, $a^k = (a^{-1})^{-k} = a^{k-1}a = aa^{k-1}$, et donc $a^{-1}a^k = (a^{-1})^{-k+1} = (a^{-1})^{-(k-1)} = a^{k-1}$
   (c) : $\forall k \in \mathbb{Z} : a^k = (a^{-k})^{-1}$. L'application $f : \mathbb{Z} \to G,\ k \mapsto a^k$ est un homomorphisme de groupes si

$\forall k,\ k' \in \mathbb{Z},\ a^{k+k'} = a^k a^{k'}$. *En utilisant les propriétés (a), (b) et (c), on a successivement :*
(i) si $k, k' \geq 0$, *alors*

$$a^k a^{k'} = a^k a^{-1} a a^{k'} = a^{k-1} a^{k'+1} = \ldots =^{HR} a^{k-i} a^{k'+i} = a^{k-i} a^{-1} a a^{k'+i} = a^{k-(i+1)} a^{k'+(i+1)} = \ldots =^{PR} a^{k+k'}. \quad (2)$$

(ii) si $k, k' \leq 0$, *il suffit de remplacer* a *par* a^{-1} *et appliquer (c).*
(iii) (i) si $k \geq 0$ *et* $k' \leq 0$,

$$a^k a^{k'} = a^k a a^{-1} a^{k'} = a^{k+1} a^{k'-1} = \ldots =^{HR} a^{k+i} a^{k'-i} = a^{k+i} a a^{-1} a^{k'-i} = a^{k+(i+1)} a^{k'-(i+1)} = \ldots =^{PR} a^{k+k'}. \quad (3)$$

Exercice 4

1. *Pour* $N_G(K)$, *on a successivement* $N_G(K) \subseteq G$ *(par définition) ;* $e \in N_G(K) \neq \emptyset$ *;* $\forall g, g' \in N_G(K)$ *:* $(gg')^{-1}K(gg') = (g')^{-1}(g^{-1}Kg)g' = (g')^{-1}Kg'$ *et par suite* $gg' \in N_G(K)$ *; enfin* $g^{-1}Kg = K \Rightarrow g(g^{-1}Kg)g^{-1} = gKg^{-1} \Rightarrow K = gKg^{-1} = (g^{-1})^{-1}Kg^{-1}$ *et donc* $g^{-1} \in N_G(K)$. *On conclut alors que* $N_G(K)$ *est un sous-groupe de* G *et on montre de même que* $C_G(K)$ *est aussi un sous-groupe de* G. *Enfin, l'inclusion* $C_G(K) \subseteq N_G(K)$ *se déduit de leurs définitions.*
2. *Supposons que* $N_G(K) = G$ *et montrons que* $K = \bigcup_{g\in G} g^{-1}Kg$. *Comme* $K = e^{-1}Ke$, *il reste à montrer que* $\bigcup_{g\in G} g^{-1}Kg \subseteq K$ *c. à. d. que* $\forall g \in G$, *on a* $g^{-1}Kg \subseteq K$, *en fait, de plus :* $\forall g \in G$, *on a alors* $g \in N_G(K)$ *et donc* $g^{-1}Kg = K$.
   Réciproquement, supposons que $K = \bigcup_{g\in G} g^{-1}Kg$ *et soit* $g \in G$ *un élément quelconque. Il faut montrer que* $g \in N_G(K)$. *On a évidemment* $g^{-1}Kg \subseteq K$. *D'autre part, tout* $k \in K$ *s'écrit* $k = (g^{-1})(gkg^{-1})g \in g^{-1}Kg$ *car* $gkg^{-1} = (g^{-1})^{-1}k(g^{-1}) \in (g^{-1})^{-1}K(g^{-1}) \subseteq K$ *(par hypothèse). Par suite,* $K \subseteq g^{-1}Kg$ *et donc* $g^{-1}Kg = K$.

Exercice 5
Supposons que HK *est un sous-groupe de* G *et montrons que* $HK = KH$. *Si* $x = hk \in HK$ *(qui est un sous-groupe), alors* $x^{-1} \in HK$ *et donc, il existe* $h' \in H, k' \in K$ *tel que* $x^{-1} = h'k'$. *D'où* $x = k'^{-1}h'^{-1} \in KH$ *(car* K *et* H *sont des sous-groupes de* G*). Ainsi, on a montré que* $HK \subseteq KH$. *Soit maintenant* $x = kh \in KH$, *son inverse* $x^{-1} = h^{-1}k^{-1} \in HK$ *qui est un sous-groupe et par suite* $x \in HK$. *D'où* $KH \subseteq HK$.

Supposons maintenant que $HK = KH$ *et montrons que* HK *est un sous-groupe de* G. *On a* $\emptyset \neq HK \subseteq G$ *et si* $x = hk,\ y = h'k' \in HK$, *alors* $xy = hkh'k' = h(kh')k' = h(h"k")k' = (hh")(k"k') \in HK$ *pour un certain couple* $h" \in H,\ k" \in K$ *issus de l'hypothèse* $HK = KH$. *D'autre part,* $x = hk \in HK = KH$ *s'écrit donc sous la forme* $x = k_1h_1$ *(dans* KH*) et donc* $x^{-1} = h_1^{-1}k_1^{-1} \in HK$. *Par conséquent* HK *est un sous-groupe de* G.

Exercice 6
Dans cet exercice, on appliquera le premier théorème d'isomorphisme pour un homomorphisme de groupes spécifique à chacune des deux questions.

1. *Dans ce cas, on écrit* $U = \{e^{2i\pi t},\ t \in \mathbb{R}\}$ *(c'est une écriture parmi d'autres, mais ici convenable). On considère alors l'application* $f : \mathbb{R} \to U$ *définie par* $f(t) = e^{2i\pi t}$. *Il est clair qu'elle est bien définie, surjective (par definition de* U*) et que c'est un homomorphisme de* $(\mathbb{R}, +)$ *dans* $(U, \times)$ *considéré comme sous-groupe de* $(\mathbb{C}^*, \times)$.
   $Ker(f) = \{t \in \mathbb{R} :\ e^{2i\pi t} = 1\}$. *Mais alors* $e^{2i\pi t} = 1 \Leftrightarrow 2\pi t = 0 + 2k\pi,\ k \in \mathbb{Z} \Leftrightarrow t \in \mathbb{Z}$. *D'où* $Ker(f) = \mathbb{Z}$ *et par le premier théorème d'isomorphisme, on déduit que* $\mathbb{R}/\mathbb{Z} \cong U$.
2. *Dans ce cas (très facile), considérer l'homomorphisme* $f : (\mathbb{C}^*, \times) \to (\mathbb{R}_+^*, \times)$ *donné par* $f(z) =\mid z \mid$ *(le module) et appliquer le premier théorème d'isomorphisme de groupes.*

Exercice 7
Soit Q_8 *le sous-groupe de* $\mathcal{GL}_2(\mathbb{C})$ *engendré par les deux matrices* $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *et* $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

1. *On vérifie facilement que* $A^2 = B^2 = -I_2$ *et donc* $A^3 = -A$ *et* $BA = -AB$.
2. *Montrons au début que*

$$Q_8 = H = \{\pm A^{i_1}B^{j_1}A^{i_2}B^{j_2}\ldots A^{i_n}B^{j_n}\ :\ i_k = k_k = -1,\ 0,\ ou\ +1\ et\ n \geq 0\}.$$

Il s'agit de montrer que H est le plus petit sous-groupe de $\mathcal{GL}_2(\mathbb{C})$ contenant A et B. Par définition de H, on a : $A,\ B \in H$ et $\emptyset \neq H \subseteq \mathcal{GL}_2(\mathbb{C})$. D'autre part, le produit de deux éléments de H est un élément de H. De même pour l'inverse. Finalement, si K est un sous-groupe de Q_8 contenant A et B, il contient leurs inverses A^{-1} et B^{-1} et donc tout produit $A^{i_1}B^{j_1}A^{i_2}B^{j_2}\dots A^{i_n}B^{j_n}$ et comme $A^2 = B^2 = -I_2$ et $BA = -AB$, un tel produit peut s'écrire sous la forme $\pm A^{i_1}B^{j_1}A^{i_2}B^{j_2}\dots A^{i_{n'}}B^{j_{n'}}$. Par conséquent $H \subseteq K$. D'où $Q_8 = H$.

Utilisant encore une fois de plus les relations $A^2 = B^2 = -I_2$ et $BA = -AB$ (celle-ci exprime l'anti-commutativité), on conclut que

$$Q_8 = H = \{\pm I_2,\ \pm A,\ \pm B,\ \pm AB\}.$$

Il en résulte que $Q_8 = H$ est un sous-groupe d'ordre 8. En dit que Q_8 ***est défini par les générateurs*** *A* ***et*** *B* ***et les relations*** *$A^2 = B^2 = -I_2$* ***et*** *$BA = -AB$.*

N.B ; Vous pouvez faire des recherches sur internet pour avoir d'autres définitions de Q_8 et de même pour le groupe des octonions.

Exercice 8

1. *La réponse est* **non** *grâce au contre exemple suivant :*

$$\mathbb{Z}_{p^\infty} = \bigcup_{k=0}^{k=\infty} \mathbb{Z}_{p^k};\ \text{où } \mathbb{Z}_{p^k} = \{e^{\frac{2i\pi m}{p^k}} :\ 0 \leq m \leq p^k - 1\}$$

En effet :

(i) Chaque $\mathbb{Z}_{p^k}$ est un sous-groupe cyclique de $U = \mathbb{S}^1$ qui est engendré par $e^{\frac{2i\pi}{p^k}}$. (facile).

(ii) $(\mathbb{Z}_{p^k})_{k\geq 0}$ est une suite croissante de sous-groupes de U :

Si $0 \leq k \leq k'$, alors $p^{k'} = p^k p^{k'-k}$ et donc $\frac{1}{p^k} = \frac{p^{k'-k}}{p^{k'}}$ ce qui entraine $e^{\frac{2i\pi m}{p^k}} = e^{\frac{2i\pi m p^{k'-k}}{p^{k'}}} = (e^{\frac{2i\pi m}{p^{k'}}})^{p^{k'-k}}$ et par suite $\mathbb{Z}_{p^k} \subseteq \mathbb{Z}_{p^{k'}}$.

(iii) $\mathbb{Z}_\infty$ est aussi un sous-groupe de U :

Pour cela : si $z_1,\ z_2 \in \mathbb{Z}_\infty$, il existe alors $k,\ k' \geq 0$ tels que $z_1 \in \mathbb{Z}_{p^k}$ et $z_1 \in \mathbb{Z}_{p^{k'}}$ et en supposant (par exemple) que $k \leq k'$, on obtient que $z_1,\ z_2 \in \mathbb{Z}_{p^{k'}}$ et donc $z_1(z_2)^{-1} \in \mathbb{Z}_{p^{k'}} \subseteq \mathbb{Z}_\infty$.

(iv) Tous les sous-groupes propres de $\mathbb{Z}_\infty$ sont finis :

Pour cela, remarquons tout d'abord que chaque élément de $\mathbb{Z}_\infty$ est d'ordre une puissance p^n ($n \geq 0$). Considérons H un sous-groupe propre de $\mathbb{Z}_\infty$ et supposons que l'ensemble des ordres de ses éléments est infini. Nécessairement, pour tout $z \in \mathbb{Z}_\infty$, il doit exister $z' \in H$ tel que $o(z') = p^{k'} > o(z) = p^k$ et donc $\mathbb{Z}_{p^k} \subseteq \mathbb{Z}_{p^{k'}} =< z' > \subseteq H$ par suite $\mathbb{Z}_\infty \subseteq H$ ce qui est une contradiction. Il en ressort que les éléments de H sont tous d'ordre fini et que $\exists h \in H$ d'ordre maximal égal à p^n. Par conséquent, $H = \mathbb{Z}_{p^n}$.

En conclusion, $\mathbb{Z}_\infty$ est un groupe infini dont tous les sous-groupes sont finis (et en fait tous cycliques).

2. *G est un groupe abélien. Montrons que l'ensemble de ses éléments d'ordre fini noté $T(G)$ est un sous-groupe de ce groupe.*

On a $T(G) \subseteq G$ et e est d'ordre 1 donc $e \in T(G)$, par suite, $T(G) \neq \emptyset$. Soient maintenant $x,\ y \in T(G)$ d'ordres respectifs $o(x) = n$ et $o(y) = m$. On a alors, puisque G est commutatif, $(xy)^{nm} = x^{nm}y^{nm} = e$ car $x^{nm} = (x^n)^m = e$ et de même $y^{nm} = (y^m)^n = e$ et donc $xy \in T(G)$. On a aussi $\forall k \geq 0,\ (x^{-1})^k x^k = e$ (par récurrence), donc, en particulier $(x^{-1})^n = (x^n)^{-1} = e$, par suite $x^{-1} \in T(G)$. Par conséquent, $T(G)$ est un sous-groupe de G.

Pour $T(T(G))$, remarquer que $T(T(G)) \subseteq T(G)$ et que puisque tous les éléments de $T(G)$ sont d'ordre fini alors $T(G) \subseteq T(T(G))$. D'où $T(T(G)) = T(G)$.

Exercice 9

Soit $(G, .)$ un groupe d'ordre fini n.

1. *Supposons que n est premier et montrons que G est cyclique. On sait d'après le Théorème de Lagrange que l'ordre de tout él'ement de G divise celui de G. Mais, comme n est premier (donc $n \geq 2$) ses seuls diviseurs sont 1 et n. Par suite, $G\backslash\{e\}$ contient un élément d'ordre n qu'on note x. Ainsi, le sous-groupe $< x >$ de G engendré par x est d'ordre n, et par conséquent, il est égal à G ; et donc G est cyclique.*

2. *Soit φ un endomorphisme de G. On sait que pour tout $x \in G$:*

$$o(x) = n \Leftrightarrow (x^n = e \text{ et } \forall k \geq 0,\ (x^k = e \Rightarrow n/k)).$$

(i) Supposons que φ est un automorphisme de G. On a alors pour tout $x \in G$ d'ordre $o(x) = n$, $(\varphi(x))^n = \varphi(x^n) = \varphi(e) = e$ et $\forall k \geq 0$; $(\varphi(x))^k = e \Rightarrow \varphi(x^k) = e \Rightarrow x^k = e \Rightarrow n/k$ (on a utilisé l'injectivité de φ). Par suite $o(x) = n \Rightarrow o(\varphi(x)) = n$. Inversement, en appliquant le même raisonnement à φ^{-1}, on a : $o(\varphi(x)) = n \Rightarrow o(\varphi^{-1}(\varphi(x))) = n \Rightarrow o(x) = n$. Donc $\forall x \in G,\ o(\varphi(x)) = o(x)$.
Réciproquement, supposons que $\forall x \in G,\ o(\varphi(x)) = o(x)$. $\forall x \in G$, on a $\varphi(x) = e \Rightarrow o(\varphi(x)) = 1 \Rightarrow x = e$ et par suite φ est injective. Mais comme par hypothèse G est fini, φ est aussi surjective (toute application entre deux ensembles finis de même cardinaux est injective ssi elle est surjective ssi elle est bijective).

(ii) D'après (i) il revient à montrer que $\forall x, y \in G,\ o(xy) = o(yx)$. Supposons donc que $o(xy) = n$ donc $(xy)^n = e$ et $\forall k \geq 0, (xk)^k = e \Rightarrow k/n$. Mais alors

$$(xy)^n = e \Rightarrow (xy)(xy)\dots(xy) = n \Rightarrow x(yx)(yx)\dots(yx)y = e \Rightarrow (yx)^{n-1} = x^{-1}y^{-1} = (yx)^{-1} \Rightarrow (yx)^n = e.$$

et de même $\forall k \geq 0\ (yx)^k = e \Rightarrow (xy)^k = e$, par suite puisque $o(xy) = n$, on a k/n et donc $o(yx) = n = o(xy)$. Idem, si $o(yx) = n$ alors $o(xy) = n$.

Exercice 10
Soit G un groupe cyclique d'ordre n et k un diviseur de n ; on écrit $n = kq$. Soit H un sous-groupe de G d'ordre k (on peut supposer que $k \geq 2$ sinon $H = \{e\}$ est alors unique). Montrons que $H =< x^q >$ (ce qui impliquera qu'il ne dépend que de n et k et donc qu'il est unique). On sait que tout sous-groupe d'un groupe cyclique est cyclique, donc il existe $y \in G$ tel que $H =< y >$. Or $y \in G$ donc $\exists l \geq 1 :\ y = x^l$. Ainsi

$$y^k = e \Rightarrow x^{lk} = e \Rightarrow n/lk \Rightarrow lk = nq + r,\ 0 \leq r < n.$$

Si $r \neq 0$, alors $x^{lk} = x^{nq}x^r = e \Rightarrow x^r = e \Rightarrow n/r$, ce qui est absurde et par suite $r = 0$ et donc $n = lk$ et comme $n = kq$ on obtient $l = q$. Par suite $H =< y >=< x^q >$.

Exercice 11
Soit G un groupe d'ordre 4. Si G est cyclique, alors $G \cong \mathbb{Z}/4\mathbb{Z}$. Supposons donc (pour compléter la disjonction des cas) que G n'est pas cyclique. Comme l'ordre d'un élément divise celui du groupe, alors $\forall x \in G\backslash\{e\},\ o(x) = 2$. Soient $x, y \in G$, comme $xy \in G$, on a alors $o(xy) = 2 \Rightarrow (xy)^2 = e \Rightarrow x(yx)y = \Rightarrow yx = x^{-1}y^{-1} = xy$ (car $x^2 = y^2 = e$). Par suite G est commutatif. Il en résutlte que $G = \{e, x, y, xy\} =< x >< y >= \{e, x\}\{e, y\}$. On considère

$$\begin{array}{rccc} g : & (G, .) & \to & (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +) \\ & e & \mapsto & (\bar{0}, \bar{0}) \\ & x & \mapsto & (\bar{1}, \bar{0}) \\ & y & \mapsto & (\bar{0}, \bar{1}) \\ & xy & \mapsto & (\bar{1}, \bar{1}). \end{array}$$

On vérifie facilement que g est bien définie et que c'est un isomorphisme de groupes.