Université Aix-Marseille 2018–2019

Licence – Mathématiques
Algèbre 2

Seconde session
corrigé

Exercice 1.

1. (a) Deux entiers $k_1, k_2 \in \mathbb{Z}$ sont congrus modulo $n \in \mathbb{N}^*$ si et seulement si n divise $k_2 - k_1$.
   (b) Dans un groupe G, on appelle conjugué de $g \in G$ par $h \in G$ l'élément $h.g.h^{-1}$.
   (c) Un anneau A est intégre si 0_A est le seul diviseur de zéro, c'est-à-dire si, pour tout $a_1, a_2 \in A \setminus \{0_A\}$, on a $a_1.a_2 \neq 0_A$.
2. Le premier théorème d'isomorphisme pour les groupes dit que tout morphisme de groupes $f : G_1 \to G_2$ induit un isomorphisme de groupes $\overline{f} : {G_1}/{\mathrm{Ker}(f)} \to \mathrm{Im}(f)$. Pour le démontrer, on commence par remarquer que, $\mathrm{Ker}(f)$ étant un sous-groupe distingué de G_1, ${G_1}/{\mathrm{Ker}(f)}$ est bien un groupe, de même que $\mathrm{Im}(f) \subset G_2$, et que pour toute classe $[g] \in {G_1}/{\mathrm{Ker}(f)}$, on peut définir $\overline{f}([g]) = f(g) \in \mathrm{Im}(f)$. En effet, si $g' \in [g]$, on a alors $g'.g^{-1} \in \mathrm{Ker}(f)$ et donc $f(g') = f(g'.g^{-1}.g) = f(g'.g^{-1}).f(g) = f(g)$. De plus, $\overline{f}$ est un morphisme de groupes car on a, pour tous $g_1, g_2 \in G_1$, $\overline{f}([g_1.g_2]) = f(g_1.g_2) = f(g_1).f(g_2) = \overline{f}([g_1]).\overline{f}([g_2])$, et ce morphisme est surjectif sur $\mathrm{Im}(f)$ par construction. Enfin, si pour $g_1, g_2 \in G$, on a $\overline{f}([g_1]) = \overline{f}([g_2])$, c'est que $f(g_1) = f(g_2)$ et donc que $f(g_1.g_2^{-1}) = f(g_1).f(g_2)^{-1} = e_{G_2}$, impliquant de fait que $[g_1] = [g_2]$ et donc l'injectivité de $\overline{f}$. Au final, l'application $\overline{f}$ est donc bien un isomorphisme de groupes.
3. Commençons par vérifier que la multiplication est bien une opération interne pour les éléments inversibles, c'est-à-dire qu'un produit de deux élément inversible est bien inversible. Pour cela, on considère a_1 et a_2 deux éléments inversibles et on constate que $a_2^{-1}.a_1^{-1}$ est bien un inverse pour $a_1.a_2$. En effet, on a $a_2^{-1}.a_1^{-1}.a_1.a_2 = a_2^{-1}.a_2 = 1$ et pareil pour $a_1.a_2.a_2^{-1}.a_1^{-1}$. Dès lors, l'associativité est vérifié par définition d'un anneau, l'existence d'un élément neutre l'est par définition du caractére unitaire d'un anneau, et l'existence d'un inverse l'est par définition d'un élément inversible.

Exercice 2.

1. (a) Soit $e^{\frac{2ia_1\pi}{p^{k_1}}}, e^{\frac{2ia_2\pi}{p^{k_2}}} \in U_p$, alors

$$e^{\frac{2ia_1\pi}{p^{k_1}}}.\left(e^{\frac{2ia_2\pi}{p^{k_2}}}\right)^{-1} = e^{\frac{2ia_1\pi}{p^{k_1}}}.e^{-\frac{2ia_2\pi}{p^{k_2}}} = e^{\frac{2ia_1\pi}{p^{k_1}}-\frac{2ia_2\pi}{p^{k_2}}} = e^{\frac{2i(p^{k_2}.a_1-p^{k_1}.a_2)\pi}{p^{k_1+k_2}}} \in U_p.$$

   Le sous-ensemble U_p de $\mathbb{C}$ est donc bien un sous-groupe, donc un groupe.
   (b) La suite $\left(e^{\frac{2i\pi}{p^k}}\right)_{k\in\mathbb{N}}$ donne une suite infini d'éléments de U_p qui sont tous distincts, le groupe U_p est donc d'ordre infini. Par contre, pour tout $e^{\frac{2ia\pi}{p^k}} \in U_p$, on a $\left(e^{\frac{2ia\pi}{p^k}}\right)^{p_k} = e^{2ia\pi} = 1$, montrant que $e^{\frac{2ia\pi}{p^k}}$ est d'ordre fini.
   (c) Supposons par l'absurde que U_p est monogène, alors il est engendré par un élément d'ordre fini et est donc lui-même d'ordre fini, ce qui contredit la question précédente. On en déduit donc que U_p n'est pas monogène.
   Remarque : on pourrait montrer que U_p n'est même pas finiment engendré, c'est-à-dire engendré par un nombre fini d'éléments.
2. (a) Si $k_1 \leq k_2 \in \mathbb{N}$, alors $e^{\frac{2i\pi}{p^{k_1}}} = e^{\frac{2ip^{k_2-k_1}\pi}{p^{k_2}}} = \left(e^{\frac{2i\pi}{p^{k_2}}}\right)^{p^{k_2-k_1}} \in G_{k_2}$ et donc, $G_{k_1} = \langle e^{\frac{2i\pi}{p^{k_1}}}\rangle \subset G_{k_2}$.
   (b) On a clairement $\cup_{k\in\mathbb{N}} G_k \subset U_p$. Réciproquement, pour tout $e^{\frac{2ia\pi}{p^k}} \in U_p$, on a $e^{\frac{2ia\pi}{p^k}} = \left(e^{\frac{2i\pi}{p^k}}\right)^a \in G_k \subset \cup_{k\in\mathbb{N}} G_k$. Par double inclusion, on a donc $\cup_{k\in\mathbb{N}} G_k = U_p$.
   (c) On considère l'application

$$\varphi_k : \begin{array}{ccc} \mathbb{Z} & \to & G_k \\ a & \mapsto & e^{\frac{2ia\pi}{p^k}} \end{array}.$$

C'est un morphisme de groupes car on a, pour tout $a_1, a_2 \in \mathbb{Z}$, $\varphi(a_1+a_2) = e^{\frac{2i(a_1+a_2)\pi}{p^k}} = e^{\frac{2ia_1\pi}{p^k}}.e^{\frac{2ia_2\pi}{p^k}} = \varphi(a_1).\varphi(a_2)$. Ce morphisme est surjectif car G_k est engendré par $\varphi(1) = e^{\frac{2i\pi}{p^k}}$ et son noyau vaut $\left\{a \in \mathbb{Z} \mid \frac{a}{p^k} \in \mathbb{Z}\right\} = p^k\mathbb{Z}$. Par le premier théorème d'isomorphisme, on en déduit que G_k est isomorphe à $\mathbb{Z}/p^k\mathbb{Z}$.

(d) i. α. Puisque $H \subset U_p = \cup_{k\in\mathbb{N}} G_k$, il existe nécessairement un $k \in \mathbb{N}$ tel que $x \in G_k$. L'ensemble $\{k \in \mathbb{N} \mid x \in G_k\}$ est donc un ensemble non vide d'entiers naturels, il possède donc un plus petit élément.

β. Comme $x \in G_{k_x}$, il existe $a \in \mathbb{Z}$ tel que $x = \left(e^{\frac{2i\pi}{p^{k_x}}}\right)^a = e^{\frac{2ia\pi}{p^{k_x}}}$. Si $k_x = 0$, alors $x = e^{2ia\pi} = 1 = e^{2i\pi}$, et on peut remplacer a par 1 qui est bien premier avec p. Autrement, supposons par l'absurde que a n'est pas premier avec p, alors puisque p est premier, on a $a = a'.p$ avec $a' \in \mathbb{Z}$ et donc $x = e^{\frac{2ia'p\pi}{p^{k_x}}} = e^{\frac{2ia'\pi}{p^{k_x-1}}} \in G_{k_x-1}$, ce qui contredit la minimalité de k_x. On en déduit que a est premier avec p.

γ. Puisque a est premier avec p, il l'est également avec p^{k_x}, et d'après le théorème de Bachet–Bezout, il existe donc $u, v \in \mathbb{Z}$ tels que $a.u + v.p^{k_x} = 1$. On a alors $e^{\frac{2i\pi}{p^{k_x}}} = e^{\frac{2i(au+vp^{k_x})\pi}{p^{k_x}}} = e^{\frac{2aui\pi}{p^{k_x}}}.e^{2iv\pi} = \left(e^{\frac{2ai\pi}{p^{k_x}}}\right)^u = x^u \in H$ et donc $G_{k_x} \subset H$ puisque G_{k_x} est engendré par $e^{\frac{2i\pi}{p^{k_x}}}$.

ii. Supposons par l'absurde que $H \neq U_p = \cup_{k\in\mathbb{N}} G_k$. L'ensemble $\{k \in \mathbb{N} \mid G_k \not\subset H\}$ est donc non vide et on peut considérer son plus petit élément k_0. On a $k_0 > 0$ car $G_0 = \{1\} \subset H$ et, par minimalité de k_0, $G_{k_0-1} \subset H$. Or, par hypothèse, $H \neq G_{k_0-1}$, il existe donc $x \in H \setminus G_{k_0-1}$. D'après la question précédente, on a alors $G_{k_x} \subset H$. Mais $k_x \geq k_0$ car $x \notin G_{k_0-1}$, et d'après la question (a), on a $G_{k_0} \subset G_{k_x} \subset H$, ce qui contredit la définition de k_0.

(e) D'après la question (c), tous les G_k sont cycliques et d'après la question (d), U_p est le seul sous-groupe de U_p à ne pas être égal à un G_k. On en déduit donc que, parmi tous les sous-groupes de U_p, seul U_p n'est pas cyclique.

Exercice 3.

1. (a) On a

$$(a-b).(a'-b') = a.a' + b.b' - a.b' - b.a' \equiv a.a' - 3.b.b' - a.b' - b.a' \mod 4.$$

(b) Pour montrer que A est un sous-anneau de $\mathbb{C}$, il faut montrer qu'il est stable par somme, opposé et inverse. Soit $\frac{a+i\sqrt{3}b}{2}, \frac{a'+i\sqrt{3}b'}{2} \in A$, avec donc $a \equiv b \mod 2$ et $a' \equiv b' \mod 2$:

- $\frac{a+i\sqrt{3}b}{2} + \frac{a'+i\sqrt{3}b'}{2} = \frac{(a+a')+i\sqrt{3}(b+b')}{2} \in A$ car $a + a' \equiv b + b' \mod 2$;
- $-\frac{a+i\sqrt{3}b}{2} = \frac{-a-i\sqrt{3}b}{2} \in A$ car $-a \equiv -b \mod 2$;
- $\frac{a+i\sqrt{3}b}{2}.\frac{a'+i\sqrt{3}b'}{2} = \frac{a.a'-3.b.b'+i\sqrt{3}(a.b'+b.a')}{4} = \frac{\frac{a.a'-3.b.b'}{2}+i\sqrt{3}\frac{a.b'+b.a'}{2}}{2}$, or $a.a' \equiv b.b' \equiv 3.b.b' \mod 2$ et $a.b' \equiv b.a' \equiv -b.a' \mod 2$, donc $a.a' - 3.b.b'$ et $a.b' + b.a'$ sont tous les deux pairs et $\frac{a.a'-3.b.b'}{2}, \frac{a.b'+b.a'}{2} \in \mathbb{Z}$; de plus, 2 divise $a - b$ et $a' - b'$ par hypothèse, 4 divise donc $(a-b).(a'-b')$ ainsi que $a.a' - 3.b.b' - a.b' - b.a'$ d'après la question précédente, et on en déduit que 2 divise $\frac{a.a'-3.b.b'}{2} - \frac{a.b'+b.a'}{2}$ et donc que $\frac{a+i\sqrt{3}b}{2}.\frac{a'+i\sqrt{3}b'}{2} \in A$.

2. On a $e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \in A$.
3. Par stabilité par produit, si un anneau contient $e^{\frac{2i\pi}{3}}$, il contient également $e^{\frac{4i\pi}{3}} = \left(e^{\frac{2i\pi}{3}}\right)^2$. Et par stabilité par somme et inverse, il contient également $-(e^{\frac{2i\pi}{3}} + e^{\frac{4i\pi}{3}}) = -\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2} - \frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = 1$ et $e^{\frac{2i\pi}{3}} - e^{\frac{4i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} + \frac{1}{2} + i\frac{\sqrt{3}}{2} = i\sqrt{3}$.
4. L'intersection de tous les sous-anneaux de $\mathbb{C}$ contenant $e^{\frac{2i\pi}{3}}$ est un sous-anneau de $\mathbb{C}$ contenant $e^{\frac{2i\pi}{3}}$, inclu dans tous les sous-anneau de $\mathbb{C}$ contenant $e^{\frac{2i\pi}{3}}$. Il existe donc bien un plus petit sous-anneau de $\mathbb{C}$ contenant $e^{\frac{2i\pi}{3}}$. D'après la question précédente, ce dernier contient 1 et $i\sqrt{3}$, donc par combinaison linéaire, il contient tous les $a + ib\sqrt{3}$, avec $a, b \in \mathbb{Z}$, autrement dit tous les $\frac{a+ib\sqrt{3}}{2}$ avec $a, b \in \mathbb{Z}$ et $a \equiv b \equiv 0 \mod 2$. Et en sommant tous ces derniers avec $e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, il contient également tous les $\frac{a+ib\sqrt{3}}{2}$ avec $a, b \in \mathbb{Z}$ et $a \equiv b \equiv 1 \mod 2$. On en déduit qu'il contient

A. Mais par ailleurs, A est lui-même un sous-anneau de $\mathbb{C}$ contenant $e^{\frac{2i\pi}{3}}$, c'est donc bien le plus petit sous-anneau de $\mathbb{C}$ contenant $e^{\frac{2i\pi}{3}}$.