Université Aix-Marseille 2021–2022

Licence – Mathématiques
Algèbre 2

Examen
Correction

Exercice 1.

1. (a) Un groupe est un ensemble G muni d'une opération $* : G \times G \to G$ telle que :
   - $\forall g_1, g_2, g_3 \in G, (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ (associativité) ;
   - $\exists e \in G, \forall g \in G, e * g = g * e = g$ (existence d'un élément neutre) ;
   - $\forall g, \exists h \in G, g * h = h * g = e$ (existence d'inverses).

   (b) Une transposition est un cycle de longueur de deux, c'est-à-dire une permutation des éléments d'un ensemble donné fixant tous les éléments sauf deux, lesquels sont mutuellement envoyés l'un sur l'autre.

   (c) Un idéal d'un anneau A est une partie non vide I de A tel que :
   - $\forall b_1, b_2 \in I, b_1 - b_2 \in I$;
   - $\forall b \in I, \forall a \in A, ab \in I$ et $ba \in I$;

   c'est-à-dire un sous-groupe (pour l'addition) de A, stable par mutliplication par tout élément de A.

2. (a) On a $f(e_{G_1}) = e_{G_2}$, donc $e_{G_1} \in \mathrm{Ker}(f)$ qui est donc non vide. De plus, si $g_1, g_2 \in \mathrm{Ker}(f)$, on a $f(g_1 g_2^{-1}) = f(g_1)f(g_2)^{-1} = e_{G_2} e_{G_2}^{-1} = e_{G_2}$ et donc $g_1 g_2^{-1} \in \mathrm{Ker}(f)$. L'ensemble $\mathrm{Ker}(f)$ est donc un sous-groupe de G_1.

   Enfin, pour tout $h \in \mathrm{Ker}(f)$ et $g \in G_1$, on a $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e_{G_2}$ et donc $ghg^{-1} \in \mathrm{Ker}(f)$. L'ensemble $\mathrm{Ker}(f)$ est donc un sous-groupe distingué de G_1.

   (b) Soit $b, c \in A$ tels que $ab = ac$, on a alors $a(b - c) = ab - ac = 0_A$ et donc $b - c = 0_A$ puisque a n'est pas un diviseur de zéro. On en déduit donc que $b = c$.

Exercice 2.

1. Par calcul direct, on a
$$\sigma = (1, 3, 2, 6, 7)(4, 8, 9).$$

2. En tant que cycle de longueur 5, on a $(1, 3, 2, 6, 7)^5 = \mathrm{Id}$ et, en tant que cycle de longueur 3, $(4, 8, 9)^3 = \mathrm{Id}$. De plus, ces deux cycles étant à supports disjoints, ils commutent et on a donc
$$\sigma^{15} = (1, 3, 2, 6, 7)^{15}(4, 8, 9)^{15} = \mathrm{Id}$$
ainsi que
$$\sigma^{197} = \sigma^{13.15+2} = \sigma^2 = (1, 2, 7, 3, 6)(4, 9, 8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 6 & 9 & 5 & 1 & 3 & 4 & 8 \end{pmatrix}.$$

Exercice 3.

1. (a) Soit $k \in \mathbb{Z}$ tel que $\overline{k} \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$. L'entier k n'est donc pas un multiple de n, et puisque n est premier, k et n sont premiers entre eux. D'après le théorème de Bachet–Bézout, il existe donc $u, v \in \mathbb{Z}$ tels que $uk + vn = 1$. En prenant cette égalité modulo n, on obtient $\overline{u}\overline{k} = \overline{1}$. L'élement $\overline{u}$ est donc un inverse pour $\overline{k}$, qui est donc inversible.

   Tout élément non nul est donc inversible, et ne peut donc pas être un diviseur de zéro. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est donc intègre.

   (b) Soit $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $x^2 = \overline{1}$. Puisque $\mathbb{Z}/n\mathbb{Z}$ est commutatif, on a par identité remarquable
$$\overline{0} = x^2 - \overline{1} = (x - \overline{1})(x + \overline{1}).$$

Par intégrité de $\mathbb{Z}/_{n\mathbb{Z}}$, on en déduit que $x - \overline{1} = \overline{0}$ ou $x + \overline{1} = \overline{0}$, c'est-à-dire $x = \pm\overline{1}$.
Réciproquement, on vérifie directement que les carrés de $\overline{1}$ et $-\overline{1}$ sont bien égaux à $\overline{1}$. Enfin, n étant un nombre impair, on a bien $-\overline{1} \neq \overline{1}$. L'équation a donc bien deux solutions distinctes, à savoir $\overline{1}$ et $\overline{n-1}$.

(c) Soit $k \in [\![2, n-2]\!]$, on a alors $\overline{k} \neq \overline{0}$ donc $\overline{k}$ est inversible d'après la question (a), et on a $k \neq \overline{1}$ et $k \neq \overline{n-1}$ donc $\overline{k}^2 \neq \overline{1}$ d'après la question (b). En multipliant par $\overline{k}^{-1}$, on obtient bien $\overline{k} \neq \overline{k}^{-1}$.

(d) Considérons $\overline{(n-1)!} = \prod_{k=1}^{n-1} \overline{k}$. D'après la question précédente, les facteurs pour $k \in [\![2, n-2]\!]$ s'apparient deux à deux par paires inverses dont le produit vaut $\overline{1}$. On a donc $\overline{(n-1)!} = \overline{1}.\overline{n-1} = \overline{-1}$. On en déduit que $(n-1)!$ est congru à -1 modulo n.

(e) On a bien $(2-1)! = 1! = 1 \equiv -1 \mod 2$.

2. Puisque n n'est pas premier, il existe $\tilde{a}, b \in [\![2, n-1]\!]$ tels que $\tilde{a}b = n$, et quitte à échanger leurs rôles, on peut supposer $\tilde{a} \leq b$.

   Si $\tilde{a} \neq b$, alors en posant $a = \tilde{a}$, on a directement deux entiers distincts entre 2 et $n-1$ dont le produit est divisible par n car il vaut n.

   Supposons maintenant que $\tilde{a} = b$. On a $b > 2$ car sinon on aurait $\tilde{a} = b = 2$ et $n = 2.2 = 4$. On en déduit que $2\tilde{a} < b\tilde{a} = n$ et donc que $2\tilde{a} \in [\![2, n-1]\!]$. Puisque $\tilde{a} > 0$, on a de plus $2\tilde{a} \neq \tilde{a} = b$. En posant $a = 2\tilde{a}$, on a deux entiers distincts entre 2 et $n-1$ dont le produit est divisible par n puisqu'il vaut $2\tilde{a}b = 2n$.

3.
   - Si $n = 4$, alors $(n-1)! + 2 = 3! + 2 = 8$ qui est bien divisible par 4.
   - Si n est premier, alors $(n-1)! \equiv -1 \mod [n]$ d'après les questions 1.(d) et 1.(e) et donc n divise $(n-1)! - (-1) = (n-1)! + 1$.
   - Si n est non premier et différent de 4, alors il existe deux entiers distincts a et b entre 2 et $n-1$ dont le produit est divisible par n. Mais alors n divise également $(n-1)! = ab \prod_{\substack{1 \leq k \leq n-1 \\ k \notin \{a,b\}}} k$.

Exercice 4.

1. Soit $b_1, b_2 \in A$, on a

$$f_a(b_1 + b_2) = a(b_1 + b_2) = ab_1 + ab_2 = f(b_1) + f(b_2)$$

   puisque la multiplication est distributive sur l'addition dans A. L'application f_a est donc bien un morphisme de groupe.

   Soit $b \in \mathrm{Ker}(f)$, on a alors $ab = 0_A = a0_A$. Par intégrité de A, a étant non nul, on a $b = 0_A$ et donc $\mathrm{Ker}(f) = \{0_A\}$. Le morphisme de groupe f_a est donc injectif.

2. Soit $a \in A \setminus \{0_A\}$. D'après la question précédente, f_a est une application injective définie d'un ensemble fini dans un ensemble fini de même cardinal. L'application est donc aussi surjective et 1_A possède en particulier un antécédent $b \in A$. On a alors $ab = 1_A$.

   En raisonnant de même avec l'application

$$g_a : \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & xa \end{array}$$

   on montre qu'il existe $b' \in A$ tel que $b'a = 1_A$. On a alors

$$b' = b'1_A = b'ab = 1_Ab = b.$$

   L'élément a possède un inverse, et tout élément non nul est donc inversible.