Algèbre 2, L3
Examen du 15/01/2024 à 9h
Documents/calculatrices interdits
Durée : 3h

Exercice 1. Définir les notions d' anneau intègre, factoriel, euclidien, principal, Noethérien, et donner les relations d'implication entre ces propriétés.

Exercice 2. On considère la permutation $\sigma \in \mathcal{S}_{10}$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 6 & 8 & 7 & 2 & 5 & 10 & 3 & 1 & 9 \end{pmatrix}.$$

1. Décomposer σ en produit de cycles disjoints.
2. Calculer l'ordre de σ dans $\mathfrak{S}_{10}$.
3. Calculer σ^{4781}.
4. Calculer la signature de σ.

Solution : cf TD.

Exercice 3. On considère le groupe $(\mathbb{Z}/17\mathbb{Z})^\times$ des inversibles dans l'anneau $\mathbb{Z}/17\mathbb{Z}$.

1. Montrer que tout élément non nul de $\mathbb{Z}/17\mathbb{Z}$ est inversible. Quel est l'ordre de $(\mathbb{Z}/17\mathbb{Z})^\times$?
2. On rappelle que $(\mathbb{Z}/17\mathbb{Z})^\times$ est cyclique. Rappeler le théorème qui décrit tous les sous-groupes d'un groupe cyclique.
3. Montrer que $(\mathbb{Z}/17\mathbb{Z})^\times$ a exactement un sous-groupe d'ordre 8 et donner les deux descriptions vues en cours de ce sous-groupe.
4. Soit $\overline{x} \in \mathbb{Z}/17\mathbb{Z}$ non nul. Montrer que $\overline{x}$ est un carré si et seulement si $\overline{x}^8 = \overline{1}$.
5. Soit $\overline{x}$ une racine de $P(X) = X^6 + X^4 + X^2 + \overline{1}$ dans $\mathbb{Z}/17\mathbb{Z}$. Montrer que $\overline{x}^8 = \overline{1}$ puis que $\overline{x}$ est un carré dans $\mathbb{Z}/17\mathbb{Z}$.
6. Déterminer les racines de P et écrire P comme produit de facteurs irréductibles dans $\mathbb{Z}/17\mathbb{Z}[X]$.

Solution :

1. Soit $x \in \mathbb{Z}$ tel que $\overline{x} \neq \overline{0} \in \mathbb{Z}/17\mathbb{Z}$ non nul. Alors x n'est pas multiple de 17 qui est premier, donc il est premier à 17. D'après la relation de Bezout, soit $a, b \in \mathbb{Z}$ tels que $ax + 17b = 1$. Réduisant modulo 17, on obtient $\overline{a}\,\overline{x} = \overline{1}$, de sorte que $\overline{x}$ est inversible dans $\mathbb{Z}/17\mathbb{Z}$.
2. Soit G cyclique d'ordre n et d un diviseur de n. Il existe un unique sous-groupe de G d'ordre d, notons le H_d. Notant $\varphi_k : G \to G$ l'application définie par $\varphi_d(x) = x^k$, on a $H_d = \text{Im}\,(f_{n/d}) = \ker(f_d)$.
3. Comme $(\mathbb{Z}/17\mathbb{Z})^\times$ est un groupe cyclique d'ordre 16, il a exactement un sous-groupe d'ordre 8 qu'on a noté H_8. D'après la question précédente,
$$H_8 = \{\overline{x}^2 \,|\, \overline{x} \in (\mathbb{Z}/17\mathbb{Z})^\times\} = \{\overline{x} \,|\, \overline{x}^8 = 1\}.$$
4. Les deux conditions données dans la question sont les conditions pour que $\overline{x} \in H_8$.
5. Soit $\overline{x}$ une racine de $P(X) = X^6 + X^4 + X^2 + \overline{1}$ dans $\mathbb{Z}/17\mathbb{Z}$. On a alors $\overline{x}^6 = -\overline{x}^4 - \overline{x}^2 - \overline{1}$, donc $\overline{x}^8 = -\overline{x}^6 - \overline{x}^4 - \overline{x}^2 = (\overline{x}^4 + \overline{x}^2 + \overline{1}) - \overline{x}^4 - \overline{x}^2 = \overline{1}$. Comme $\overline{x}^8 = 1$, $\overline{x}$ est un carré d'après la question précédente.
   On peut aussi utiliser le fait que $(X^2 - 1)(X^6 + X^4 + X^2 + 1) = X^8 - 1$: si $\overline{x}$ vérifie $\overline{x}^6 + \overline{x}^4 + \overline{x}^2 + \overline{1} = 0$, alors il vérifie $(\overline{x}^6 + \overline{x}^4 + \overline{x}^2 + \overline{1})(\overline{x}^2 - \overline{1}) = 0$, soit $\overline{x}^8 - \overline{1} = 0$.
6. On voit que $\overline{2}, \overline{4}, \overline{8}, \overline{9}, \overline{13}, \overline{15}$ sont des racines de P. Ce sont donc toutes les racines de P. (Pour déterminer ces racines, il n'est pas nécessaire de tester tous les éléments de $\mathbb{Z}/17\mathbb{Z}$: on peut se limiter aux carrés, d'après la question précédente, et de plus on peut utiliser le fait que $\overline{x}$ est une racine si et seulement si $-\overline{x}$ est une racine.) D'après le cours, on sait qu'on peut factoriser P par tous les facteurs $X - \overline{2}, X - \overline{4}, X - \overline{8}, X - \overline{9}, X - \overline{13}, X - \overline{15}$. On obtient
$$P(X) = (X - \overline{2})(X - \overline{4})(X - \overline{8})(X - \overline{9})(X - \overline{13})(X - \overline{15}),$$
tous ces facteurs étant irréductibles puisque de degré 1.

Exercice 4. Donner la liste de tous les groupes abéliens d'ordre 240 écrits selon leur décomposition cyclique.

Solution : La décomposition de 240 en produit de nombres premiers est $240 = 2^4 * 3 * 5$. Soit G un groupe abélien d'ordre 240. Puisque les partitions de 4 sont $(4), (3,1), (2,2), (2,1,1), (1,1,1,1)$, la partie 2-primaire de G est l'un des 5 groupes $\mathbb{Z}/16\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4Z, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2Z \times \mathbb{Z}/4Z, (\mathbb{Z}/2\mathbb{Z})^4$. La partie 3-primaire de G est $\mathbb{Z}/3\mathbb{Z}$ et sa partie 5-primaire est $\mathbb{Z}/5\mathbb{Z}$. Le groupe G est donc l'un des 5 groupes $\mathbb{Z}/240\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/60Z, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2Z \times \mathbb{Z}/60Z, (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/30\mathbb{Z}$, qui sont écrits là selon leur décomposition cyclique.

Exercice 5. Soit p un nombre premier ($p \geq 2$) et $\mathbb{Z}[i\sqrt{p}] \subset \mathbb{C}$ l'ensemble des nombres de la forme $a + bi\sqrt{p}$ avec $a, b \in \mathbb{Z}$.

1. Montrer que $\mathbb{Z}[i\sqrt{p}]$ est un sous-anneau de l'anneau $(\mathbb{C}, +, \times)$.
2. Montrer que $\mathbb{Z}[i\sqrt{p}]$ est intègre.
3. Pour $z \in \mathbb{Z}[i\sqrt{p}]$, on note $\overline{z}$ le conjugué complexe de z. Montrer que si $\overline{x} \,|\, \overline{y}$ dans $\mathbb{Z}[i\sqrt{p}]$, alors $x|y$ dans $\mathbb{Z}[i\sqrt{p}]$.
4. On note $N(z) = z\overline{z}$. Déterminer $N(a + bi\sqrt{p})$ en fonction de a et b.
5. Montrer que $\forall x, y \in \mathbb{Z}[i\sqrt{p}]$, on a $N(xy) = N(x)N(y)$.
6. Soit $x \in \mathbb{Z}[i\sqrt{p}]$. Montrer que x est inversible dans $\mathbb{Z}[i\sqrt{p}]$ si et seulement si $N(x) = 1$.
7. En déduire que $\mathbb{Z}[i\sqrt{p}]^\times = \{-1, 1\}$.
8. Soit $x \in \mathbb{Z}[i\sqrt{p}]$. Montrer que si $N(x)$ est un nombre premier, alors x est irréductible.
9. On suppose dans cette question que $p = 7$.
   (a) Montrer que si x n'est pas inversible, et non nul, alors $N(x) \geq 4$.
   (b) Montrer que $1 + i\sqrt{7}, 1 - i\sqrt{7}$ et 2 sont irréductibles (on pourra calculer $N(1 + i\sqrt{7}), N(1 - i\sqrt{7})$ et $N(2)$ et utiliser la question précédente).
   (c) En écrivant 8 comme produits d'éléments irréductibles de $\mathbb{Z}[i\sqrt{7}]$, montrer que $\mathbb{Z}[i\sqrt{7}]$ n'est pas factoriel.
10. On suppose dans cette question que $p = 2$. On rappelle qu'on a vu en cours que $\mathbb{Z}[i\sqrt{2}]$ est euclidien. **Cette question est plus difficile que les précédentes.**
    (a) Montrer que $\mathbb{Z}[i\sqrt{2}]$ est factoriel.
    (b) Soit $z \in \mathbb{Z}[i\sqrt{2}]$ non inversible. Montrer qu'il existe un entier $\ell \geq 1$ et des éléments $x_i \in \mathbb{Z}[i\sqrt{2}]$ irréductibles et tels que :
    - $z = x_1 \cdots x_\ell$;
    - $\forall i \geq 2$, $\mathrm{Re}(x_i) \geq 0$;
    - Si $i \leq j$ alors $N(x_i) \leq N(x_j)$;
    - Si $i \leq j$ et $N(x_i) = N(x_j)$ alors $|\mathrm{Re}(x_i)| < |\mathrm{Re}(x_j)|$.

    Montrer de plus que l'entier ℓ et les éléments x_i sont uniques.
    (c) Soit $x \in \mathbb{Z}[i\sqrt{2}]$ tel que $N(x)$ est un nombre premier. Montrer que x est premier dans l'anneau $\mathbb{Z}[i\sqrt{2}]$.
    (d) Soit $x \in \mathbb{Z}[i\sqrt{2}]$ tel que $N(x)$ est un nombre premier et $y \in \mathbb{Z}[i\sqrt{2}]$ tel que $N(x)|N(y)$ dans $\mathbb{Z}$. Montrer que $x|y$ ou que $\overline{x} \,|\, y$ dans $\mathbb{Z}[i\sqrt{2}]$.
    (e) Soit p un entier premier, et soit $x, y \in \mathbb{Z}[i\sqrt{2}]$ tels que $N(x) = N(y) = p$. Montrer que $x = \pm y$ ou que $x = \pm\overline{y}$.
    (f) Donner l'unique décomposition de l'élément $7 - 17i\sqrt{2}$ en produit de facteurs irréductibles dont il est question dans la question (b).

Solution :

1. On vérifie que $\mathbb{Z}[i\sqrt{p}]$ est un sous-groupe de $(\mathbb{C}, +)$ et que le produit de deux éléments de $\mathbb{Z}[i\sqrt{p}]$ est encore dans $\mathbb{Z}[i\sqrt{p}]$.
2. Soit $x, y \in \mathbb{Z}[i\sqrt{p}]$ tels que $xy = 0$. Condiérant ce produit comme un produit d'éléments de $\mathbb{C}$, on a donc $x = 0$ ou $y = 0$. Ainsi, $\mathbb{Z}[i\sqrt{p}]$ est intègre, comme d'ailleurs tout sous-anneau d'un anneau intègre.
3. Si $\overline{x} \,|\, \overline{y}$ dans $\mathbb{Z}[i\sqrt{p}]$, alors, par définition, il existe $z \in \mathbb{Z}[i\sqrt{p}]$ tel que $\overline{y} = z\overline{x}$. Alors, $y = \overline{z}x$, donc $x|y$.
4. On a $N(a + bi\sqrt{p}) = a^2 + pb^2$.

5. Cette relation est vraie dans $\mathbb{C}$, elle est donc vraie en particulier si $x, y \in \mathbb{Z}[i\sqrt{5}]$. Autre argument possible : $N(xy) = (xy)\overline{(xy)} = xy\overline{x}\,\overline{y} = x\overline{x}y\overline{y} = N(x)N(y)$.
6. Soit x inversible. Soit donc $y \in \mathbb{Z}[i\sqrt{p}]$ tel que $xy = 1$. On trouve $1 = N(1) = N(xy) = N(x)N(y)$, et puisque $N(x)$ et $N(y)$ sont des entiers naturels, $N(x) = N(y) = 1$.
7. Si on écrit $x = a + bi\sqrt{p}$, on en déduit $a^2 + pb^2 = 1$, donc $a = \pm 1$ et $b = 0$. Inversement, 1 et -1 sont bien sûr inversibles.
8. Soit $x \in \mathbb{Z}[i\sqrt{p}]$ tel que $N(x)$ est un nombre premier. Ecrivons $x = yz$ et montrons que y ou z est inversible. En effet, nous avons alors $N(x) = N(y)N(z)$. Comme $N(x)$ est premier, ceci implique $N(y) = 1$ ou $N(z) = 1$. Donc y est inversible ou z est inversible.
9. On suppose $p = 7$.
   (a) Si $x = a + bi\sqrt{7}$ n'est pas inversible, on a $b \neq 0$, et donc $N(x) \geq 7b^2 \geq 7$, ou $b = 0$ et $|a| > 1$, et donc $N(x) \geq 2^2 = 4$. Dans tous les cas, $N(x) \geq 4$.
   (b) Ecrivons $1 + i\sqrt{7} = xy$ et montrons que x ou y est inversible. On a $8 = N(1 + i\sqrt{7}) = N(x)N(y)$. Si x et y sont tous les deux non inversibles, alors $N(x), N(y) \geq 4$, ce qui est contradictoire. Le même argument vaut pour $1 - i\sqrt{7}$ et 2, puisque $N(1 - i\sqrt{7}) = 8$ et $N(2) = 4$.
   (c) $8 = 2 \times 2 \times 2 = (1 + i\sqrt{7})(1 - i\sqrt{7})$. Or $2, 1 + i\sqrt{7}$ et $1 - i\sqrt{7}$ sont irréductibles. Si $\mathbb{Z}[i\sqrt{7}]$ était factoriel, la décomposition de 8 en produit d'éléments irréductibles serait unique, et en particulier le nombre de facteurs irréductibles ne dépendrait pas de la décomposition. Or, on a une décomposition avec 3 facteurs et une autre avec 2 facteurs, donc $\mathbb{Z}[i\sqrt{7}]$ n'est pas factoriel.
10. On suppose $p = 2$.
   (a) Un anneau euclidien est factoriel, donc $\mathbb{Z}[i\sqrt{2}]$ est factoriel.
   (b) Soit $z \in \mathbb{Z}[i\sqrt{2}]$ non inversible. Soit $z = x_1 \cdots x_\ell$ une écriture de z comme produit d'irréductibles de $\mathbb{Z}[i\sqrt{2}]$. Quitte à réordonner les x_i, on peut supposer que les normes des x_i sont croissantes : si $i \leq j$ alors $N(x_i) \leq N(x_j)$. On peut de plus supposer la dernière propriété vraie : si $i \leq j$ et $N(x_i) = N(x_j)$ alors $|\mathrm{Re}(x_i)| < |\mathrm{Re}(x_j)|$ (quitte à réordonner à nouveau). Soit enfin $i \geq 2$. Si $\mathrm{Re}(x_i) < 0$, on peut remplacer x_1 par $-x_1$ et x_i par $-x_i$, de manière à avoir $\mathrm{Re}(x_i) \geq 0$. Ceci montre l'existence des x_i.
   De plus, comme l'anneau $\mathbb{Z}[i\sqrt{2}]$ est factoriel, on sait qu'on a unicité de la décomposition. Si donc on écrit $z = x'_1 \cdots x'_m$ avec les x'_i vérifiant les propriétés de la question, alors on sait que $\ell = m$ et qu'il existe une bijection σ telle que x'_i est associé à $x_{\sigma(i)}$, ce qui implique d'après la question 6 que $x'_i = \pm x_{\sigma(i)}$. Ainsi on a $N(x'_i) = N(x_{\sigma(i)})$ et $|\mathrm{Re}(x'_i)| = |\mathrm{Re}(x_{\sigma(i)}|$. Les propriétés de croissance impliquent alors que $\sigma(i) = i$ et donc $x'_i = \pm x_i$. Finalement, la propriété que x_i et x'_i sont tous deux de partie réelle strictement positive lorsque $i \geq 2$ implique que $x_i = x'_i$ lorsque $i \geq 2$. Mais alors, l'égalité $z = x_1 \cdots x_\ell = x'_1 \cdots x'_\ell$ implique qu'on a aussi $x_1 = x'_1$.
   (c) Soit $x \in \mathbb{Z}[i\sqrt{2}]$ tel que $N(x)$ est un nombre premier. On sait déjà que x est irréductible. Mais, dans un anneau principal ($\mathbb{Z}[i]$ est euclidien donc principal), irréductible implique premier. Donc, x est premier.
   (d) Soit $x \in \mathbb{Z}[i\sqrt{2}]$ tel que $N(x)$ est un nombre premier et $y \in \mathbb{Z}[i\sqrt{2}]$ tel que $N(x)|N(y)$ dans $\mathbb{Z}$. On a $N(x) = x\overline{x}$ et $N(y) = y\overline{y}$. Donc $x\overline{x} \,|\, y\overline{y}$ dans $\mathbb{Z}$ donc dans $\mathbb{Z}[i\sqrt{2}]$. Ainsi $x \,|\, y\overline{y}$. Comme x est premier, $x|y$ ou $x \,|\, \overline{y}$. D'après la question 2, dans le deuxième cas de figure, $\overline{x} \,|\, y$. On a donc $x|y$ ou $\overline{x} \,|\, y$.
   (e) Soit p un entier premier, et soit $x, y \in \mathbb{Z}[i\sqrt{2}]$ tels que $N(x) = N(y) = p$. D'après la question précédente, x divise y ou x divise $\overline{y}$. Supposons d'abord que x divise y. Soit donc z tel que $y = xz$. Alors $N(y) = p = N(xz) = N(x)N(z) = pN(z)$, de sorte que $N(z) = 1$ donc $z = \pm 1$. Ainsi, $y = \pm x$. Si x divise $\overline{y}$, on a de même $x = \pm\overline{y}$.
   (f) Soit $z = 7 - 17i\sqrt{2}$. On a $N(z) = 627 = 3 * 11 * 19$. Soit $x = 1 + i\sqrt{2}$: $N(x) = 3$ est premier et divise $N(z)$. D'après la question (e), $x|z$ ou $\overline{x}|z$. Or

$$\frac{z}{x} = \frac{z\overline{x}}{N(x)} = \frac{27 + 24i\sqrt{2}}{3} = 9 + 8i\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$$

alors que

$$\frac{z}{\overline{x}} = \frac{zx}{N(x)} = \frac{-41 + 10i\sqrt{2}}{3} \notin \mathbb{Z}[i\sqrt{2}],$$

ce qui montre que x divise z dans $\mathbb{Z}[i\sqrt{2}]$, mais pas $\overline{x}$. De la même manière, on observe que $3 - i\sqrt{2}$ (de norme 11) divise z mais pas $3 + i\sqrt{2}$, et que $1 + 3i\sqrt{2}$ (de norme 19) divise z mais pas $1 - 3i\sqrt{2}$. On obtient

$$z = -(1 + i\sqrt{2})(3 - i\sqrt{2})(1 + 3i\sqrt{2}) = (-1 - i\sqrt{2})(3 - i\sqrt{2})(1 + 3i\sqrt{2}),$$

ce qui est la décomposition souhaitée.