UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Feuille n°5 : groupes de permutations, entiers de Gauss

Exercices à savoir faire chez soi

Exercice 1

Vrai ou faux ? L'écriture $3+3\,i = 1.(1+2\,i)+(2+i)$ est une division euvclidienne de $3+3i$ par $1+2i$.

Exercice 2

Vrai ou faux ? Soit $\sigma \in \mathfrak{S}_n$ un élément d'ordre r. Alors pour tout entier k vérifiant $1 \leqslant k \leqslant r-1$ et tout $d \in \{1,\dots,n\}$ on a $\sigma^k(d) \neq d$.

Exercice 3

Le raisonnement est-il correct ? Comme $(1,2,3)$ est d'ordre 3, $(1,2)$ est d'ordre 2, et 2 et 3 sont premiers entre eux, $\sigma = (1,2,3)(1,2)$ est d'ordre 6.

Exercice 4

Pour chacun des couples (a,b) d'éléments de $\mathbf{Z}[i]$ donnés ci-dessous, calculer un pgcd δ de a et b et déterminer un couple (u,v) d'éléments de $\mathbf{Z}[i]$ tel que $\delta = a\,u + b\,v$: $(6+3\,i, -1+7\,i)$, $(35, 9+6\,i)$, $(10,14)$.

Exercices à savoir faire

Exercice 5

1 Soit $\sigma \in \mathfrak{S}_{12}$ défini par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 4 & 12 & 1 & 7 & 10 & 11 & 9 & 3 & 6 & 2 & 8 \end{pmatrix}$$

Déterminer la décomposition de σ en produit de cycles à supports disjoints, une décomposition de σ en produit de transpositions, l'ordre de σ, l'inverse de σ et la signature de σ.

2 Mêmes questions avec $\sigma \in \mathfrak{S}_{16}$ défini par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 5 & 4 & 10 & 9 & 11 & 16 & 15 & 12 & 2 & 7 & 8 & 14 & 6 & 3 & 1 & 13 \end{pmatrix}$$

Exercice 6

Déterminer la décomposition en cycles à supports disjoints et la signature de $\sigma \in \mathfrak{S}_n$ définie par $\sigma(i) = n+1-i$.

Exercice 7

Cet exercice s'intéresse aux éléments irréductibles de $\mathbf{Z}[i]$.

1 Rappeler la définition d'un élément irréductible.

2 Soit p un nombre premier impair. Montrer qu'il existe un élément $z \in \mathbf{Z}[i]$ de norme p si et seulement si p est congru à 1 modulo 4.

Quelles sont par ailleurs les normes possibles d'un élément de $\mathbf{Z}[i]$ qui divise p ?

En déduire que p est irréductible dans $\mathbf{Z}[i]$ si et seulement si p est congru à 3 modulo 4.

3 Soit z_1, z_2 et z_3 des éléments de $\mathbf{Z}[i]$ avec z_1 irréductible. On suppose que z_1 divise $z_2\,z_3$. Montrer que z_1 divise z_2 ou z_3 . *Indication :* c'est en fait une question de cours !

4 Soit z un élément irréductible de $\mathbf{Z}[i]$. Montrer qu'il existe un nombre premier p tel que z divise p dans $\mathbf{Z}[i]$. En déduire que les irréductibles de $\mathbf{Z}[i]$ sont exactement les éléments qui s'écrivent $\alpha\,p$ avec p nombre premier congru à 3 modulo 4 et $\alpha \in \{1, -1, i, -i\}$ ou $a + i\,b$ avec $a, b \in \mathbf{Z}$ et $a^2 + b^2$ premier.

5 Décomposer en produit d'irréductibles dans $\mathbf{Z}[i]$ l'élément $-9 + 123\,i$. *Indication :* supposons la décomposition écrite ; que peut-on dire de la norme des éléments intervenant dans la décomposition ?

Exercice 8

Soit $p = 13$. En appliquant la méthode vue en cours, décomposer p en somme de deux carrés. Plus précisément :

1. déterminer $c \in \mathbf{Z}$ tel que $c^2 \equiv -1 \quad [p]$;
2. calculer à l'aide de l'algorithme d'Euclide $\mathrm{pgcd}(p, c + i)$.

Même question avec $p = 641$.

Exercice 9

Pour traiter cet exercice, on s'inspirera de la méthode utilisée en cours pour étudier $\mathbf{Z}[i]$ et les nombres premiers qui s'écrivent comme somme de deux carrés.

1 Montrer que

$$\{a + i\,b\sqrt{2}, \quad (a, b) \in \mathbf{Z}^2\}$$

est un sous-anneau de $\mathbf{C}$. On le note $\mathbf{Z}[i\sqrt{2}]$. Dessiner les éléments de $\mathbf{Z}[i\sqrt{2}]$.

2 Pour tout élément z de $\mathbf{Z}[i\sqrt{2}]$, on pose $N(z) = z\,\overline{z}$. Déterminer les éléments inversibles de $\mathbf{Z}[i\sqrt{2}]$.

3 Montrer que $\mathbf{Z}[i\sqrt{2}]$ admet une division euclidienne similaire à celle existant sur $\mathbf{Z}[i]$.

4 Soit p un nombre premier qui s'écrit $a^2 + 2\,b^2$ avec $a, b \in \mathbf{Z}$. Chercher des exemples (au moins trois) de tels nombres premiers. Montrer que si p vérifie cette propriété alors -2 est un carré dans $\mathbf{F}_p$.

5 Soit p un nombre premier impair tel que -2 est un carré dans $\mathbf{F}_p$. Soit $c \in \mathbf{Z}$ tel que p divise $c^2 + 2$. En considérant l'application qui à $a + ib\sqrt{2}$ associe $[a - c\,b]_p$, montrer que p s'écrit $a^2 + 2\,b^2$ avec $a, b \in \mathbf{Z}$.

Remarques : On peut démontrer que si p est un nombre premier impair, alors -2 est un carré modulo p si et seulement si p est congru à 1 ou 3 modulo 8. Un petit complément à cet exercice est donné par l'exercice 13 ci-dessous.

Exercice 10

1 Montrer que l'ensemble

$$\{a + b\sqrt{5}, \quad (a, b) \in \mathbf{Z}^2\}$$

est un sous-anneau de $\mathbf{R}$. On le note $\mathbf{Z}[\sqrt{5}]$.

2 Soit $(a, b, a', b') \in \mathbf{Z}^4$. Montrer que si on a $a + b\sqrt{5} = a' + b'\sqrt{5}$ alors $a = a'$ et $b = b'$. Ceci justifie la définition suivante : si $x = a + b\sqrt{5} \in \mathbf{Z}[\sqrt{5}]$, on pose $N(x) = a^2 - 5\,b^2$.

3 Montrer que pour $x, x' \in \mathbf{Z}[\sqrt{5}]$ on a $N(x\,x') = N(x)N(x')$.

4 En déduire que $x \in \mathbf{Z}[\sqrt{5}]$ est inversible si et seulement si $N(x) = 1$ ou $N(x) = -1$.
5 Existe-t-il des éléments $x \in \mathbf{Z}[\sqrt{5}]$ qui sont de norme 2 ? (on pourra réduire modulo 5)
6 Montrer que 2 et $3 + \sqrt{5}$ sont irréductibles et premiers entre eux dans $\mathbf{Z}[\sqrt{5}]$.
7 En considérant par exemple l'égalité $2.2 = (3+\sqrt{5})(3-\sqrt{5})$, montrer que le lemme d'Euclide ne vaut pas dans $\mathbf{Z}[\sqrt{5}]$ (ceci montre qu'il ne peut pas exister de division euclidienne dans $\mathbf{Z}[\sqrt{5}]$).

Exercices à chercher

Exercice 11

On rappelle que $\mathfrak{S}_n$ est engendré par les transpositions.
1 En déduire que $\mathfrak{S}_n$ est engendré par les n transpositions

$$\{(1,2),(1,3),\ldots,(1,n)\}$$

Indication : pour tout $\sigma \in \mathfrak{S}_n$ et toute transposition (i,j) on a $\sigma(i,j)\sigma^{-1} = (\sigma(i),\sigma(j))$; essayer d'utiliser cette formule pour montrer que n'importe quelle transposition s'écrit comme le produit de transpositions de la forme $(1,i)$.
2 En déduire que $\mathfrak{S}_n$ est engendré par les $n-1$ transpositions

$$\{(1,2),(2,3),(3,4)\ldots,(n-1,n)\}.$$

Indication : calculer le produit $(1,2)(2,3)\ldots(i-2,i-1)$ utiliser ensuite la formule de conjugaison pour montrer que n'importe quelle transposition de la forme $(1,i)$ est dans le groupe engendré par l'ensemble ci-dessus.
3 En déduire que $\mathfrak{S}_n$ est engendré par les 2 éléments

$$\{(1,2,3,\ldots,n),(1,2)\}.$$

Indication : si $c = (1,2,3,\ldots,n)$, que vaut $c^k\,(1,2)\,c^{-k}$?

Exercice 12

1 Décrire les éléments de $\mathfrak{A}_3$. À quel groupe « connu » $\mathfrak{A}_3$ est-il isomorphe ?
2 Décrire les éléments de $\mathfrak{A}_4$. Vérifier que

$$K = \{\mathrm{Id},(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$$

est un sous-groupe commutatif de $\mathfrak{A}_4$, distinct de $\mathfrak{A}_4$.

Vérifier que K est distingué dans $\mathfrak{A}_4$, c'est-à-dire

$$\forall\sigma \in \mathfrak{A}_4, \quad \forall\tau \in K, \quad \sigma\tau\sigma^{-1} \in K.$$

Ainsi $\mathfrak{A}_4$ n'est pas simple.

Montrer que K est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. On pourra considérer deux éléments σ et τ de K distincts de Id et l'application $(n,m) \to \sigma^n\,\tau^m$ où $(n,m) \in \mathbf{Z}^2$.
3 Déterminer les classes de conjugaison dans $\mathfrak{A}_4$.

Exercice 13

Cet exercice fait suite à l'exercice 9. On a vu dans le cours (respectivement dans l'exercice 9) qu'un nombre premier p s'écrivait $a^2 + b^2$ (respectivement $a^2 + 2\,b^2$) avec $(a, b) \in \mathbf{Z}^2$ si et seulement si -1 (respectivement -2) est un carré dans $\mathbf{F}_p$.

1 Il est également vrai qu'un nombre premier p s'écrit $a^2 + 3\,b^2$ avec $(a, b) \in \mathbf{Z}^2$ si et seulement si -3 est un carré dans $\mathbf{F}_p$.

Montrer que cette dernière condition est effectivement nécessaire.

Expliquer cependant pourquoi on *ne* peut *pas* appliquer la stratégie du cours ou de l'exercice 9 à l'anneau $\mathbf{Z}[i\sqrt{3}] = \{a + i\,b\,\sqrt{3}\}$ afin de montrer que la condition est suffisante.

2 Soit c un entier strictement positif. Soit p un nombre premier. Montrer que si p s'écrit $a^2 + c\,b^2$ avec $(a, b) \in \mathbf{Z}^2$ alors $-c$ est un carré modulo p.

Contrairement à ce que pourraient laisser supposer les exemples de $c = 1$, 2 ou 3, la condition « $-c$ est un carré modulo p » n'est en général pas une condition suffisante pour l'existence de $(a, b) \in \mathbf{Z}^2$ vérifiant $p = a^2 + c\,b^2$, même si on suppose que c n'a pas de facteur carré.

Par exemple, on vérifiera que 113 est premier, qu'on a $72^2 \equiv -14 \quad [113]$ et que pourtant il n'existe pas $(a, b) \in \mathbf{Z}^2$ tel que $113 = a^2 + 14\,b^2$.