Université Paris-Sud 2016-2017
L2/S4 M204 Mathématiques : Algèbre

Feuille d'exercices n^{0}1

Exercice 1
Pour chacun de ces ensembles, déterminer s'il est un groupe ou non : $(\mathbb{R},+)$, $(\mathbb{R},\times)$, $(\mathbb{C}^*,\times)$, $([0,1],+)$, $(\mathbb{Q}[\sqrt{2}]^*,\times)$ et $(\mathbb{R}^*\times\mathbb{R},*)$ où $*$ est définie par $(x,y)*(x',y')=(xx',xy'+yx'^n)$.

Exercice 2
Montrer que la loi de composition interne $*$ sur $]-1,1[$ donnée par

$$x*y=\frac{x+y}{1+xy}$$

est bien définie, et que $(]-1,1[,*)$ est un groupe abélien.

Exercice 3 (Groupe des transformations affines de $\mathbb{R}$)
Montrer que la loi de composition interne $*$ sur $\mathbb{R}^*\times\mathbb{R}$ donnée par

$$(a,b)*(a',b')=(aa',ab'+b)$$

munit $\mathbb{R}^*\times\mathbb{R}$ d'une structure de groupe, et expliquer le titre de l'exercice.

Exercice 4

1. Montrer qu'une partie $H\subset\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ si et seulement s'il existe $d\in\mathbb{N}$ tel que
$$H=d\mathbb{Z}=\{dz;z\in\mathbb{Z}\}.$$
2. Soient a et b deux entiers relatifs. Montrer que l'ensemble
$$D=\{ax+by;(x,y)\in\mathbb{Z}^2\}$$
est un sous-groupe de $\mathbb{Z}$ et que l'entier d tel que $D=d\mathbb{Z}$ est le pgcd de a et b.
3. Soient a et b deux entiers relatifs. Montrer que $a\mathbb{Z}\cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ et que l'entier m tel que $a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z}$ est le ppcm de a et b.

Exercice 5
Soit $(G,\cdot)$ un groupe fini et A, B deux sous-groupes de G. On note $AB=\{a\cdot b\mid a\in A,b\in B\}$. Montrer que AB est un sous-groupe de G si et seulement si AB=BA.

Exercice 6
Donner le groupe des isométries d'un triangle équilatéral dans le plan. (Faire la liste des éléments du groupe, les décrire géométriquement, et donner la table de multiplication.)

Exercice 7 (Somme et intersection d'idéaux)

1. Déterminer tous les idéaux de $\mathbb{Z}$.
2. Vérifier que si I et J sont deux idéaux de $\mathbb{Z}$, alors $I\cap J$ et $I+J=\{i+j;(i,j)\in I\times J\}$ sont des idéaux de Z.
3. Montrer plus généralement que si I et J sont deux idéaux d'un anneau commutatif A, alors $I\cap J$ et $I+J=\{i+j;(i,j)\in I\times J\}$ sont des idéaux de A.

Exercice 8 (Algorithme d'Euclide)
Si a_0 et a_1 sont deux entiers relatifs donnés, on appelle algorithme d'Euclide l'algorithme suivant : Pour $n \in \mathbb{N}$,

- si $a_{n+1} \neq 0$, a_{n+2} est le reste de la division euclidienne de a_n par a_{n+1}
- si $a_{n+1} = 0$, STOP.

1. Montrer que l'algorithme se termine, i.e. qu'il existe $n_f \in \mathbb{N}$ tel que $a_{n_f+1} = 0$.
2. Montrer que a_{n_f} est le pgcd de a_0 et a_1.
3. Montrer que pour tout $n \leq n_f$, il existe des entiers u_n et v_n tels que
$$a_n = u_n a_0 + v_n a_1.$$
4. Donner une formule permettant de calculer u_{n+1} et v_{n+1} en fonction de u_n et v_n. En déduire un algorithme pour déterminer deux entiers u et v tels que
$$a_0 \wedge a_1 = ua_0 + va_1.$$
(Les entiers u et v sont appelés des *coefficients de Bézout* pour a_0 et a_1; sont-ils uniques ?)
5. Calculer des coefficients de Bézout pour les couples $(27, 23)$, $(1789, 1969)$, $(1965, 135)$.

Exercice 9
Pour $n \in \mathbb{N}^*$, nous nous intéressons dans cet exercice à l'ensemble $\{0, \ldots, n-1\}$ que nous noterons $\mathbb{Z}/n\mathbb{Z}$ et sur lequel nous allons définir une structure de groupe, puis une structure d'anneau.

1. *Structure de groupe*
   (a) Pour a et b dans $\mathbb{Z}/n\mathbb{Z}$, on définit $a \bar{+} b \in \mathbb{Z}/n\mathbb{Z}$ comme le reste de la division euclidienne de $a + b$ (addition dans $\mathbb{Z}$) par n. Montrer que $(\mathbb{Z}/n\mathbb{Z}, \bar{+})$ est un groupe abélien.
   (b) Vérifier que $(\mathbb{Z}/n\mathbb{Z}, \bar{+})$ est cyclique; quels sont ses générateurs ?
2. *Structure d'anneau*
   (a) Pour a et b dans $\mathbb{Z}/n\mathbb{Z}$, on définit $a \bar{*} b \in \mathbb{Z}/n\mathbb{Z}$ comme le reste de la division euclidienne de ab (multiplication dans $\mathbb{Z}$) par n. Montrer que $(\mathbb{Z}/n\mathbb{Z}, \bar{+}, \bar{*}))$ est un anneau commutatif.
   (b) Quels sont les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, \bar{+}, \bar{*})$? À quelle condition l'anneau est-il intègre ? À quelle condition est-il un corps ?