UNIVERSITÉ DE PARIS 7
Année 2000-2001, DEUG 2ème année
Groupes et arithmétique (MT282)

1 Relations d'équivalence, notion de groupe, propriétés élémentaires de $\mathbb{Z}$

1.1

Soit X un ensemble. On note $\mathcal{P}(X)$ l'ensemble des parties de X. Soit $\mathcal{P} \subset \mathcal{P}(X)$. $\mathcal{P}$ est une *partition* de X si :

$$i) \qquad \bigcup_{Y \in \mathcal{P}} Y = X.$$

$$ii) \quad Y \cap Y' = \emptyset \quad (Y, Y' \in \mathcal{P},\ Y \neq Y')$$

$$iii) \qquad \emptyset \notin \mathcal{P}.$$

Montrer que si $\mathcal{R}$ est une relation d'équivalence sur X alors les éléments de $X/\mathcal{R}$ forment une partition de X.
Réciproquement montrer que si $\mathcal{P}$ est une partition de X il existe une unique relation d'équivalence dont $\mathcal{P}$ soit l'ensemble des classes.
Application : Combien y-a-t-il de relations d'équivalence sur un ensemble à 4 éléments ?

1.2

On considère sur $\mathbb{R}^2$ les relations $\mathcal{R}_1$ et $\mathcal{R}_2$ définies par

$$(x, y)\mathcal{R}_1(x', y') \text{ si et seulement si } xy = x'y'$$

$$(x, y)\mathcal{R}_2(x', y') \text{ si et seulement si } xy = x'y' \text{ et } xx' \geq 0\ .$$

Sont-elles des relations d'équivalence ? Si oui, décrire les classes d'équivalence (on pourra faire un dessin).

1.3

Soient A un ensemble et B une partie de A. On définit sur $\mathcal{P}(A)$ la relation $\mathcal{R}$ suivante

$$X\mathcal{R}Y \text{ si et seulement si } X \cap B = Y \cap B\ .$$

Montrer que $\mathcal{R}$ est une relation d'équivalence et montrer qu'il existe une bijection entre l'ensemble quotient pour cette relation et l'ensemble $\mathcal{P}(B)$ des parties de B.
Indication : Considérer l'application

$$\begin{array}{ccc} \mathcal{P}(A) & \longrightarrow & \mathcal{P}(B) \\ X & \longmapsto & X \cap B \end{array}$$

et montrer qu'elle se factorise par $\mathcal{R}$.

1.4

1. On considère sur $\mathbb{R}$ la relation $\mathcal{R}$ définie par

$$x\mathcal{R}x' \text{ si et seulement si } x - x' \in \mathbb{Z}$$

   (a) Montrer que $\mathcal{R}$ est une relation d'équivalence.
   (b) $\mathbb{U}$ étant l'ensemble des nombres complexes de module 1, $f : \mathbb{R} \to \mathbb{U}$ est définie par $f(t) = e^{2i\pi t}$. Montrer que f se factorise en une application $\overline{f}$ de $\mathbb{R}/\mathcal{R}$ dans $\mathbb{U}$.
   (c) Montrer que $\overline{f}$ est une bijection.

2. On considère sur l'intervalle $I=[0,1]$ la partition (A_x) (où x parcourt $]0,1]$); $A_x=\{x\}$ quand x est différent de 1, $A_1=\{0;1\}$. $\mathcal{R}'$ est la relation d'équivalence définie par cette partition. Construire une bijection entre $I/\mathcal{R}'$ et $\mathbb{U}$.

3. Soit i l'inclusion de I dans $\mathbb{R}$. Montrer qu'il existe une unique application $\tilde{\imath}$ de $I/\mathcal{R}'$ vers $\mathbb{R}/\mathcal{R}$ vérifiant
$$\tilde{\imath}\circ\pi'=\pi\circ i$$
où π et π' sont les projections canoniques. Montrer que $\tilde{\imath}$ est une bijection.

1.5 Construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$

On se propose dans cet exercice de construire de manière axiomatique l'ensemble des nombres rationnels à partir de $\mathbb{Z}$.
On définit sur l'ensemble $\mathbb{Z}\times(\mathbb{Z}-\{0\})$ la relation $\sim$ suivante :

$$(a,b)\sim(a',b') \text{ si et seulement si } ab'=a'b$$

1. Montrer que $\sim$ est une relation d'équivalence. L'ensemble quotient $\mathbb{Z}\times(\mathbb{Z}-\{0\})/\sim$ est l'ensemble des nombres rationnels, noté $\mathbb{Q}$.

2. Proposer un système de représentants dans $\mathbb{Z}\times(\mathbb{Z}-\{0\})$ des nombres rationnels.

3. Soit $\phi:\mathbb{Z}\longrightarrow\mathbb{Q}$ l'application définie par
$$\forall a\in\mathbb{Z},\ \phi(a)=\overline{(a,1)}$$
Montrer que ϕ est injective. Ainsi, l'identification de $\mathbb{Z}$ avec $\phi(\mathbb{Z})$ permet de voir $\mathbb{Z}$ comme un sous-ensemble de $\mathbb{Q}$.

4. Montrer que l'application
$$\begin{array}{ccc}(\mathbb{Z}\times(\mathbb{Z}-\{0\}))\times(\mathbb{Z}\times(\mathbb{Z}-\{0\})) & \longrightarrow & \mathbb{Q}\\ ((a,b),(a',b')) & \longmapsto & \overline{(ab'+a'b,bb')}\end{array}$$
se factorise par $\sim$ et définit ainsi une application de $\mathbb{Q}\times\mathbb{Q}$ dans $\mathbb{Q}$, notée $+$, qui prolonge l'addition sur $\mathbb{Z}$.

5. Montrer que $(\mathbb{Q},+)$ est un groupe et que $(\mathbb{Z},+)$ en est un sous-groupe.

6. Montrer que l'application
$$\begin{array}{ccc}(\mathbb{Z}\times(\mathbb{Z}-\{0\}))\times(\mathbb{Z}\times(\mathbb{Z}-\{0\})) & \longrightarrow & \mathbb{Q}\\ ((a,b),(a',b')) & \longmapsto & \overline{(aa',bb')}\end{array}$$
se factorise par $\sim$ et définit ainsi une application de $\mathbb{Q}\times\mathbb{Q}$ dans $\mathbb{Q}$, notée $\times$, qui prolonge la multiplication sur $\mathbb{Z}$.

1.6

Soient $n\in\mathbb{N}^*$ et $\mathcal{M}_n(\mathbb{R})$ l'ensemble des matrices réelles carrées de taille $n\times n$.

1. $(\mathcal{M}_n(\mathbb{R}),\times)$ est-il un groupe?

2. Soit $GL_n(\mathbb{R})$ le sous-ensemble de $\mathcal{M}_n(\mathbb{R})$ des matrices inversibles. $(GL_n(\mathbb{R}),\times)$ est-il un groupe ?

1.7

Soit E un ensemble et G l'ensemble des bijections de E dans E. Pour tout couple (f, g) d'éléments de G, on notera $f \circ g$ la composée de g par f.

1. Montrer que $(G, \circ)$ est un groupe.
2. Soit F un sous-ensemble fini de E. Soit $H = \{f \in G / \ \forall x \in F, f(x) \in F\}$. Montrer que H est un sous-groupe de G.

1.8

Soit $(G, *)$ un groupe tel que G est un ensemble de 4 éléments. On note e l'élément neutre de G.

1. Montrer qu'il existe un élément de G qui est son propre inverse. On note cet élément a et on note b et c les deux éléments restants.
2. Quelles sont les tables de multiplication possibles pour le groupe $(G, *)$? On pourra étudier deux cas, suivant que b et c sont leurs propres inverses ou non.
3. Dans quel(s) cas G est-il commutatif ?

1.9

Soit $(G, \cdot)$ un groupe. On note $C(G) = \{x \in G / \forall y \in G, xy = yx\}$. Montrer que $C(G)$ est un sous-groupe de G (appelé *centre* de G). Quel est le centre de G si G est commutatif ?

1.10

Soient X un ensemble non vide et $(G, *)$ un groupe. On note $\mathcal{A}$ l'ensemble des applications de X dans G. On définit une application $\square : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$ par :

$$f \square g(x) = f(x) * g(x) \quad (f \in \mathcal{A},\ g \in \mathcal{A},\ x \in X).$$

Montrer que $(\mathcal{A}, \square)$ est un groupe.

1.11 Etude des sous-groupes de $\mathbb{R}$

1. Soit $\alpha \in \mathbb{R}$. Posons $\alpha\mathbb{Z} = \{\alpha n \in \mathbb{R} / n \in \mathbb{Z}\}$. Montrer que $\alpha\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$.
2. Soit G un sous-groupe de $\mathbb{R}$ non réduit à $\{0\}$ et $\alpha = \inf\{x \in G, x > 0\}$.

   a) Montrer que α est non nul si et seulement si $G = \alpha\mathbb{Z}$.
   Indication : Supposons $\alpha \neq 0$.
   • Montrer par l'absurde que $\alpha \in G$.
   • Soit $x \in G$. Soit n la partie entière de $\frac{x}{\alpha}$. Montrer que $x = n\alpha$. En déduire que $G \subset \alpha\mathbb{Z}$.
   • En déduire que $G = \alpha\mathbb{Z}$.
   b) Montrer que si α est nul, alors tout intervalle de $\mathbb{R}$ non réduit à un point contient au moins un élément de G.
   Indication : Considérons l'intervalle $I =]a - \frac{\varepsilon}{2}, a + \frac{\varepsilon}{2}[$. Il existe $x \in G$ tel que $0 < x < \frac{\varepsilon}{2}$. Montrer que $nx \in I$ où n est la partie entière de $\frac{a}{x}$.

   On dit que G est un sous-groupe discret de $\mathbb{R}$ dans la cas a) et un sous-groupe dense dans le cas b).
3. Montrer que $G = \{x + y\sqrt{2}, x \in \mathbb{Z}, y \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{R}$. Est-ce un sous-groupe discret de $\mathbb{R}$?
   Indication : Si G est du type $\alpha\mathbb{Z}$, montrer que 1 et $\sqrt{2}$ sont des multiples de α. Montrer que c'est impossible en utilisant l'irrationnalité de $\sqrt{2}$.

1.12

Soient $n \in \mathbb{N} - \{0,1\}, a = n^2 + 3n + 1$ et $b = n - 1$.

1. Effectuer la division euclidienne de a par b (discuter suivant les valeurs de n).
2. Déterminer tous les entiers n pour lesquels b divise a.
3. Calculer le quotient et le reste de la division euclidienne pour : $n = 2^{2002}$.

1.13

Soient $n \in \mathbb{N}^*$ et $p \in \mathbb{N} - \{0,1\}$.
Calculer le PGCD de p et $p^n + 1$.
Calculer le PGCD de $p^n + 1$ et $\sum_{i=0}^{n-1} p^i$.

1.14 Nombres de Mersenne

1. Soit a un entier, $a > 2$. Montrer que pour $n > 1$, $a^n - 1$ n'est pas premier.
2. Montrer que si $2^n - 1$ est premier, alors n est premier.

1.15 Nombres de Fermat

On définit pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$.

1. Montrer que si $2^n + 1$ est un nombre premier, n est une puissance de 2.
2. Montrer que $5 \times 2^7 + 1$ divise $5^4 \times 2^{28} - 1$ et que $5^4 + 2^4$ divise $5^4 \times 2^{28} + 2^{32}$. En déduire que 641 divise F_5.
3. Montrer que pour tout couple (m, n) d'entiers distincts F_n et F_m sont premiers entre eux. (On pourra supposer que $n > m$ et utiliser l'identité $2^{2^n} + 1 = (2^{2^m})^{2^{n-m}} - (-1)^{2^{n-m}} + 2$.)

1.16

Montrer qu'il existe une infinité de nombres premiers.
Indication : Supposer qu'il y a une liste finie de nombres premiers $p_1, p_2, \cdots, p_n$. Considérer le nombre $N = \prod_{i=1}^{n} p_i + 1$ et un diviseur premier q de N. Montrer alors que q n'appartient pas à $\{p_1, p_2, \cdots, p_n\}$.