Université Saclay-Paris-Sud Feuille de TD 2 M303

Exercice 1. 1. Quel est l'ordre de 2 modulo 19 dans le groupe multiplicatif $(\mathbb{Z}/19\mathbb{Z})^\times$?

2. Montrer que pour tout entier $k \geq 0$, on a $2^{6k+2} = 4 \mod 9$.

3. Utiliser ceci pour montrer que $2^{2^{6k+2}} + 3 = 0 \mod 19$.

Exercice 2. 1. Soit g un entier ≥ 1. Montrer qu'un entier a qui s'écrit $a_r a_{r-1} \dots a_0$ en base g est congru à $a_0 + \dots + a_r$ modulo $g - 1$.

2. Énoncer en base g une *preuve* étendant la *preuve par* 9 en base 10.

3. Montrer que modulo $g + 1$, a est congru à $a_0 - a_1 + a_2 \dots + (-1)^r a_r$; en déduire un analogue de la *preuve par* 11.

Exercice 3. 1. Montrer que tout groupe de cardinal premier est cyclique.

2. Montrer qu'un groupe G dont tous les éléments x vérifient $x^2 = 1_G$ est abélien. En déduire qu'un groupe de cardinal 4 est abélien.

3. Trouver, à isomorphisme près, tous les groupes de cardinal au plus 5 et tous les groupes abéliens de cardinal 6. Connaissez-vous un groupe non abélien de cardinal 6 ?

Exercice 4. Soit G l'ensemble des applications $f_i : \mathbb{R}-\{0,1\} \to \mathbb{R}-\{0,1\}$, pour $i \in \{0, \dots, 5\}$, données par

$$f_0(x) = x,\ f_1(x) = \frac{1}{1-x},\ f_2(x) = \frac{x-1}{x},\ f_3(x) = \frac{1}{x},\ f_4(x) = \frac{x}{x-1},\ f_5(x) = 1 - x.$$

1. $(G, \circ)$ est-il un groupe (avec $\circ$ la composition des applications) ?

2. Trouver les sous-groupes d'ordre 2.

3. Trouver les sous-groupes d'ordre 3 et les sous-groupes d'ordre 4.

Exercice 5. Soit le groupe $G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/7^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Combien G a-t-il d'éléments d'ordre 7^2 ? d'ordre 7^3 ? Justifier.

Exercice 6. Soit G le group $G := \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Combien G a-t-il de sous-groupes d'ordre 4 ? On indiquera précisément la méthode pour les trouver.

Exercice 7. Parmi les assertions suivantes, dire celles qui sont vraies. Si elles sont fausses, donner un contre-exemple concret. Si elles sont vraies, donner une justification. Les lettres G et G' désignent des groupes finis et $f : G \to G'$ un morphisme de groupes.

1. Si x est un élément de G d'ordre fini n, alors $f(x)$ est d'ordre un multiple de n.

2. Si x est un élement de G d'ordre fini n, alors $f(x)$ est d'ordre un diviseur de n.

3. Si f est surjectif et si x est un élément de G d'ordre fini n, alors $f(x)$ est d'ordre n.

4. Si d est un diviseur de l'ordre de G, il existe dans G un élément d'ordre d.

On suppose maintenant que G est de plus abélien.

1. Si l'ordre de G et son exposant sont égaux, alors G est cyclique.
2. Si G est d'ordre $3 \times 5 \times 20$, il existe dans G un élément d'ordre 5^2.
3. Si G est d'ordre $3 \times 5 \times 20$, les diviseurs premiers de l'exposant de G sont 3 et 5.

Exercice 8. Soit $\phi : G \to H$ un morphisme de groupes bijectif ie un isomorphisme de groupes.

1. Montrer que l'application qui à tout sous-groupe G' de G associe $\phi(G')$ est une bijection de l'ensemble des sous-groupes de G sur l'ensemble des sous-groupes de H.
2. Montrer que pour tout $g \in G$, g et $\phi(g)$ ont même ordre.
3. Montrer que g est un générateur de G si et seulement si $\phi(g)$ engendre H .
4. Plus généralement, montrer que pour toute partie S de G, l'image du sous-groupe engendré par S est le sous-groupe de H engendré par $\phi(S)$.

Exercice 9 (Les endomorphismes de $(\mathbb{Z}, +)$)**.** Soit f un morphisme de groupes de $(\mathbb{Z}, +)$ dans lui-même : on dira que f est un *endomorphisme* du groupe $(\mathbb{Z}, +)$.

1. Montrer que $\forall a \in \mathbb{N},\ \forall b \in \mathbb{N},\ f(ab) = af(b)$, puis en déduire la même assertion pour $a, b \in \mathbb{Z}$.
2. En déduire que $\forall a \in \mathbb{Z},\ f(a) = af(1)$.
3. À quelle condition nécessaire et suffisante (portant sur $f(1)$) le morphisme f est-il injectif ?
4. Montrer que f est surjectif si et seulement si $f(1) = \pm 1$.
5. À quelle condition nécessaire et suffisante (portant sur $f(1)$) le morphisme f est-il un isomorphisme ? Quelle est son application réciproque ?

Exercice 10 (L'équation $ax^2 + by^2 = 1$)**.** Étant donné un nombre premier p on note $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, *)$ le corps à p éléments.

1. Montrer que pour p impair, l'équation $x^2 = 1$ a exactement deux solutions distinctes dans $\mathbb{F}_p$. Qu'en est-il pour $p = 2$?
2. Dans cette question et toutes les questions suivantes, p est un nombre premier impair. On note $\chi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times,\ x \mapsto x^2$. Montrer que χ est un morphisme de groupes.
3. Déterminer le noyau de χ et donner son cardinal.
4. Donner le cardinal de l'image de χ. En déduire que l'ensemble C des carrés de $\mathbb{F}_p$ ie $C := \{x \in \mathbb{F}_p \mid \exists y \in \mathbb{F}_p,\ x = y^2\}$ possède $\frac{p+1}{2}$ éléments.
5. Soit $(a, b) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times$ un couple d'éléments. On note
$$A := \{x \in \mathbb{F}_p \mid \exists y \in \mathbb{F}_p,\ x = ay^2\} \text{ et } B := \{x \in \mathbb{F}_p \mid \exists y \in \mathbb{F}_p\ x = 1 - by^2\}.$$
Quel est le cardinal de A (resp. B) ?
6. En déduire que $A \cap B \neq \emptyset$.
7. Conclure finalement que pour tout couple (a, b) d'éléments non nuls de $\mathbb{F}_p$, l'équation $ax^2 + by^2 = 1$ possède toujours un couple solution dans $\mathbb{F}_p \times \mathbb{F}_p$.