## 1.6 Un deuxième théorème de Lagrange, HP

**Lemme 1.40** (Partition par les classes à gauche modulo $H$)**.** *Soit $G$ un groupe fini et $H$ un sous-groupe de $G$. Alors $\{aH, a \in G\}$ est une partition de $G$.*

Éléments de preuve. C'est la partition associée à la relation d'équivalence définie sur $G$ par

$$x \equiv y[H] \iff x^{-1}y \in H.$$

Cette relation est appelée relation de congruence à gauche modulo $H$. □

**Remarque 1.41.** *Lorsque $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ (et en revenant aux notations additives), la congruence modulo $H$ correspond à la congruence modulo $n$ bien connue.*

**Lemme 1.42** (Cardinal des classes à gauche modulo $H$)**.** *Pour tout $a \in G$, $|aH| = |H|$.*

Éléments de preuve. L'application $h \mapsto ah$ est une bijection de $H$ dans $aH$. □

**Théorème 1.43** (Lagrange pour les sous-groupes)**.** *Soit $G$ un groupe fini et $H$ un sous-groupe de $G$. Alors l'ordre de $H$ divise l'ordre de $G$.*

Éléments de preuve. On a partitionné $G$ avec des parts qui ont toutes le même cardinal que $H$. □

**Remarque 1.44** (Groupes quotients)**.**

1. *On aurait pu faire la même chose avec les classes à droite $Ha$.*
2. *Quand $G$ n'est pas abélien, la partition des classes à gauche n'est en général par la même que la partition des classes à droite.*
3. *Cela peut néanmoins arriver. Cela se produit lorsque pour tout $a \in G$, $aH = Ha$, c'est-à-dire $aHa^{-1} = H$. On dit dans ce cas que $H$ est un sous-groupe normal de $G$ (terminologie anglaise) ou un sous-groupe distingué de $G$ (terminologie française).*
4. *Dans ce cas, on peut montrer que la loi de $G$ passe sur les classes, dans le sens où la classe (à droite ou gauche) de $xy$ ne dépend pas du choix de $x$ et $y$ dans leur classe respective. Cela permet de définir une loi sur l'ensemble des classes modulo $H$, qui en fait un groupe. C'est ce qu'on appelle le groupe quotient $G/H$.*
5. *Cette situation se produit systématiquement lorsque $G$ est abélien, puisque dans ce cas, les classes à gauche et à droite sont clairement confondues. Ainsi, on peut toujours définir le groupe quotient $G/H$ dans cette situation.*
6. *Un cas particulier est le cas du sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$ : en formant le groupe quotient, on retrouve le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ déjà étudié.*

**Exercise 1.45.** *Soit $G$ un groupe non réduit à son élément neutre. Montrer que $G$ n'admet aucun sous-groupe propre (i.e. distinct de $\{e\}$ et de $G$) si et seulement si $G$ est cyclique d'ordre $p$ premier.*

# 2. Anneaux et idéaux

## 2.1 Rappels

**Définition 2.1** (Anneau). $(A, +, \times)$ *(ou plus simplement $A$) est un anneau si :*

*(i)* $(A, +)$ *est un groupe abélien ; le neutre est noté* $0_A$ *ou* $0$*;*

*(ii)* $\times$ *est associative, et admet un neutre* $1_A$*;*

*(iii)* $\times$ *est distributive sur* $+$*.*

*On dit que $A$ est un anneau commutatif si de plus $\times$ est commutative.*

**Définition 2.2** (Corps). $(K, +, \times)$ *est un corps si c'est un anneau commutatif, tel que tout $x \neq 0$ de $K$ admet un inverse pour $\times$.*

**Exemple 2.3.**
1. *$\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ et $\mathbb{C}$ munis des opérations usuelles sont des anneaux. $\mathbb{R}, \mathbb{Q}$ et $\mathbb{C}$ sont même des corps.*
2. *Pour tout $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.*
3. *L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans un corps $\mathbb{K}$ est un anneau commutatif.*
4. *L'ensemble $M_n(\mathbb{R})$ des matrices carrées est un anneau non commutatif.*

**Exercise 2.4.** *Soit $\mathbb{K}$ un corps fini. On admet que tout polynôme non nul à coefficients dans $\mathbb{K}$, de degré $n \geq 0$, admet au plus $n$ racines. Soit $n = |\mathbb{K}| - 1$.*

1. *Montrer que tout élément de $\mathbb{K}^*$ est racine de $X^n - 1$.*
2. *Montrer que s'il n'existe pas un élément de $\mathbb{K}^*$ dont l'ordre est $n$, il existe $p < n$ tel que tout élément de $\mathbb{K}^*$ soit racine de $X^p - 1$.*
3. *En déduire que $(\mathbb{K}^*, \times)$ est un groupe cyclique.*

**Théorème 2.5** (Groupe des inversibles d'un anneau). *Soit $A$ un anneau. Alors l'ensemble des éléments inversibles de $A$, généralement noté $A^\times$ ou $U(A)$, est stable pour la loi $\times$, et la loi induite munit $A^\times$ d'une structure de groupe multiplicatif.*

**Définition 2.6** (Régularité et diviseurs de 0). *Soit $A$ un anneau commutatif. Un élément $a \in A$ est appelé :*

- *élément régulier s'il est simplifiable : $ax = ay$ implique $x = y$;*
- *diviseur de 0 s'il est non nul, et qu'il existe $b \neq 0$ tel que $ab = 0$.*

**Proposition 2.7** (Description des éléments réguliers). *Soit $A$ un anneau commutatif et $a \in A\backslash\{0\}$. Les propositions suivantes sont équivalentes:*

*(i)* $a$ *est régulier.*

*(ii)* $a$ *n'est pas diviseur de 0.*

**Définition 2.8** (Anneau intègre). *Un anneau $A$ est intègre si :*