Définition 1.32 - *sous-groupe engendré par une partie*

Soit $(G, \star)$, un groupe, L'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G, appelé *sous-groupe engendré par A* et noté $\langle A \rangle$.

$$\langle A \rangle = \bigcap_{\substack{H \text{ sg de } G \\ A \subset H}} H$$

Proposition 1.33 - *caractérisation du sous-groupe engendré par A*

Soit $(G, \star)$ un groupe et A une partie de G. Alors $\langle A \rangle$ est, au sens de l'inclusion, le plus petit sous-groupe de G contenant A.

Définition 1.35 - *groupe monogène*

Un groupe $(G, \star)$ est *monogène* lorsqu'il est engendré par un seul de ses éléments. En d'autres termes, s'il existe $g \in G$ tel que $G = \langle \{g\} \rangle$ (ou $\langle g \rangle$).
Dans ce cas tout élément $g \in G$ tel que $G = \langle g \rangle$ est appelé *générateur* de G.

Définition 1.35 bis - *groupe cyclique*

Un groupe est dit cyclique s'il est fini et monogène.

Définition 1.59 - *classe d'équivalence, représentant*

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. On appelle *classe d'équivalence d'un élément* l'ensemble des éléments qui sont en relation avec lui :

$$\mathrm{cl}(x) = \overline{x} = \{y \in E,\, x\mathcal{R}y\}$$

On appelle *représentant* de la classe $\mathrm{cl}(x)$ tout élément y tel que $y \in \mathrm{cl}(x)$.

Théorème 1.61 - *partition d'un ensemble par les classes d'équivalence*

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Les classes d'équivalence de $\mathcal{R}$ forment une partition de E :

1. Aucune classe n'est vide : pour tout $x \in E$, $\mathrm{cl}(x) \neq \varnothing$.
2. Deux classes distinctes sont disjointes : si $\mathrm{cl}(x) \neq \mathrm{cl}(y)$ alors $\mathrm{cl}(x) \cap \mathrm{cl}(y) = \varnothing$.
3. La réunion de toutes les classes est égale à E.

Théorème 1.62 - *de Lagrange*

Dans un groupe fini, le cardinal d'un sous-groupe divise le cardinal du groupe.

Définition 1.65 - *l'ensemble* $\mathbb{Z}/n\mathbb{Z}$

L'ensemble des classes d'équivalence pour la congruence modulo $n \in \mathbb{Z}$ est par définition :

$$\mathbb{Z}/n\mathbb{Z} = \{\mathrm{cl}(0), \ldots, \mathrm{cl}(n-1)\}$$

Théorème 1.67 - *groupe quotient* $(\mathbb{Z}/n\mathbb{Z}, +)$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien pour la loi $+$ définie par $\mathrm{cl}(a+b) = \mathrm{cl}(a) + \mathrm{cl}(b)$, appelé groupe quotient.

Théorème 1.70 - *générateurs de* $(\mathbb{Z}/n\mathbb{Z}, +)$

Soit $k \in \mathbb{Z}$. la classe $\mathrm{cl}(k)$ génère $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $k \wedge n = 1$.

Théorème 1.71 - *produits de groupes quotients*

Soit $(n, p) \in \mathbb{N}^2$ premiers entre eux. Les groupes $\mathbb{Z}/np\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ sont isomorphes.

Proposition 1.75 - *description des groupes monogènes*

Soit $n \in \mathbb{Z}$.

1. Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.
2. Tout groupe monogène fini (ou cyclique) d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

Définition 1.76 - *ordre d'un groupe fini, ordre d'un élément d'un groupe*

On appelle ordre d'un groupe fini son cardinal, qui est dit infini pour un groupe infini.
On appelle ordre d'un élément a d'un groupe l'ordre du sous-groupe engendré par a.

Théorème 1.79 - *ordre d'un élément d'un groupe fini*

L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.