À SAVOIR

Théorème. *Soit $(G,*)$ une groupe et H une partie non vide de G. $(H,*)$ est un sous groupe de $(G,*)$ si et seulement si*

(1) pour tout $(a,b) \in G^2$ l'élément $a*b$ appartient à H

(2) pour tout $a \in H$, si a^{-1} désigne le symétrique de a dans G, alors $a^{-1} \in H$.

Théorème. *L'intersection d'une famille non vide de sous-groupes de $(G,*)$ est un sous-groupe de $(G,*)$.*

Théorème. *Soient $(G,*)$ et (G',T) deux groupes et f un morphisme de $(G,*)$ dans (G',T). On note e l'élément neutre de G. Alors*

$$f \text{ injective} \quad \Leftrightarrow \quad \ker f = \{e\}.$$

Théorème. *Soit H un sous-groupe de $(\mathbb{Z},+)$. Alors il existe $a \in \mathbb{N}$ tel que $H = a\mathbb{Z}$.*

Proposition. *Soient σ et τ deux permutations de $\mathscr{S}_n$. Si σ et τ sont à supports disjoints alors elles commutent et* $\operatorname{supp}(\sigma \circ \tau) = \operatorname{supp}(\sigma) \cup \operatorname{supp}(\tau)$.

Proposition. *Soit $f : A \mapsto B$ un morphisme d'anneau unitaire et soit J un idéal de B. Alors $f^{-1}(J)$ est un idéal de A.*

Lemme. *Lemme de Gauss dans $\mathbb{Z}$.*

Proposition. *Les polynômes de degré 1 sont irréductibles.*

Théorème. *L'élément a est racine de P si seulement si $(X-a)$ divise P.*

Proposition. *Montrer que si α est racine d'ordre k, avec $k \geq 2$, du polynôme P alors α est racine d'ordre $k-1$ de P'. Donner un exemple où la quantité 0 est racine double de P' sans être racine de P.*