Chapitre 9

Groupes et congruences

9.1 Groupes

9.1.1 Structure de groupe

Définition 9.1 *Une loi interne sur un ensemble E est une application de $E \times E$ vers E.*

Notation : une loi interne est notée usuellement de manière infixe (exemple : $3+5$) plutôt que préfixe (exemple $+(3,5)$). Mais il ne faut pas oublier l'interprétation préfixe, surtout avec les logiciels de calcul formel (Maple, Mathematica) : `op(0,a+b)` renvoie `+` comme `op(0,f(a,b))` renvoie `f`.

Définition 9.2 *Un groupe $(G,*)$ est un couple formé d'un ensemble et d'une loi interne sur cet ensemble, vérifiant les hypothèses :*

- *La loi $*$ est associative :*
$$\forall (x,y,z) \in G^3 \quad (x*y)*z = x*(y*z).$$
- *La loi possède un élément neutre*
$$\exists e \in G \quad \forall x \in G \quad e*x = x*e = x.$$
- *Tout élément possède un symétrique*
$$\forall x \in G \quad \exists x' \in G \quad x*x' = x'*x = e.$$

Abus : on dira souvent que G est un groupe, en sous-entendant la loi.

Vocabulaire : Un groupe $(G,*)$ est dit commutatif ou abélien [1] si la loi $*$ est commutative, c'est-à-dire si

$$\forall (x,y) \in G^2 \quad x*y = y*x.$$

Il est de tradition de noter une loi commutative avec le symbole $+$, l'élément neutre se note 0, le symétrique d'un élément x étant noté $-x$. Si la loi n'est pas commutative (elle peut quand même l'être) on la note multiplicativement (sans symbole) xy au lieu de $x*y$. L'élément neutre se note souvent(mais pas toujours) 1, et le symétrique de x se note x^{-1}.

Remarque : la troisième partie de la définition est justifiée par le fait que s'il existe un élément neutre alors il est unique. on peut aussi montrer que si la loi est associative et s'il existe un élément neutre alors le symétrique d'un élément,s'il existe, est unique.

Définition 9.3 *Soit E un ensemble muni d'une loi interne $*$ on dit qu'un élément x de E est régulier à gauche si et seulement si*

$$\forall (y,z) \in E^2 \quad x*y = x*z \Rightarrow y = z.$$

On définit de même la notion d'élément régulier à droite. Un élément régulier à droite et à gauche est simplement dit régulier.

Exemple : Une matrice carrée régulière à droite ou à gauche pour la multiplication des matrices est inversible. C'est pourquoi certains utilisent le terme régulière au lieu d'inversible.

Proposition 9.1 *Dans un groupe tout élément est régulier.*

1. ABEL Niels Henrik, norvégien, Finnoy 1802-Arendal 1829

Remarque : la réciproque est fausse. Dans $(\mathbb{N}, +)$ tout élément est régulier.

Théorème 9.1 *(Théorème de Cayley) Si G est un groupe et a un élément de G l'application*

$$\begin{array}{rccc} s_a & : & G & \to & G \\ & & x & \mapsto & ax \end{array}$$

est une bijection.

Si n appartient à $\mathbb{Z}$ on définit dans tout groupe G et pour tout élément x de G l'élément x^n par
- $x^0 = e$
- $x^{n+1} = x^n x$ si $n \geq 0$
- $x^n = (x^{-1})^{-n}$ si $n < 0$

Proposition 9.2 *Si G est un groupe dont la loi est notée multiplicativement*

$$\forall x \in G \ \forall (m,n) \in \mathbb{Z}^2 \quad x^{m+n} = x^m x^n.$$

9.1.2 Sous-groupes

Définition 9.4 *Une partie H d'un groupe G est un sous-groupe de G, muni de la même loi si et seulement si*
- *H est stable pour la loi interne,*
- *H est un groupe pour la loi induite.*

Proposition 9.3 *Une partie H de G, groupe pour la loi $*$, est un sous-groupe si et seulement si :*
- *e appartient à H.*
- *$\forall (x,y) \in H^2 \ x * y^{-1} \in H$.*

Proposition 9.4 *Une partie H de G, groupe pour la loi $*$, est un sous-groupe si et seulement si :*
- *e appartient à H.*
- *$\forall (x,y) \in H^2 \ x * y \in H$,*
- *$\forall y \in H^2 \ y^{-1} \in H$.*

Proposition 9.5 *Toute intersection de sous-groupes de G est un sous-groupe de G.*

9.1.3 Morphismes

Définition 9.5 *Un morphisme du groupe $(G, *)$ dans le groupe $(G', \perp)$ est une application f de G vers G' telle que*

$$\forall (x,y) \in G^2 \qquad f(x * y) = f(x) \perp f(y).$$

Proposition 9.6 *Si $f : (G, *) \to (G', \perp)$ est un morphisme de groupes alors :*
- *$f(e) = e'$,*
- *$\text{Ker } f = \{x \in G; f(x) = e'\}$ est un sous-groupe de G, on l'appelle le noyau de f,*
- *$\text{Im } f = \{f(x); x \in G\}$ est un sous-groupe de G', on l'appelle l'image de f.*
- *Plus précisément l'imge de tout sous-groupe de G est un sous-groupe de G' et l'image réciproque de tout sous-groupe de G' est un sous-groupe de G.*

9.1.4 Groupes déduits d'autres groupes

Proposition 9.7 *Si $(G, *)$ et $(G', \perp)$ dont deux groupes on peut munir $G \times G'$ d'une structure de groupe en posant $(g, g').(h, h') = (g * h, g' \perp h')$. Le groupe ainsi obtenu s'appelle le groupe produit de G et G'*

Proposition 9.8 *Si G est un groupe et X un ensemble on peut munir $\mathcal{A}(X, G)$ d'une structure de groupe en posant $(f * g)(x) = f(x) * g(x)$.*

On remarquera qu'on emploie la même notation pour la loi dans $\mathcal{A}(X, G)$ et dans G.

9.1.5 Partie génératrice d'un groupe

Définition 9.6 *Soit S une partie d'un groupe G on appelle sous-groupe engendré par S, noté $< S >$, le plus petit sous-groupe de G contenant S. C'est l'intersection de tous les sous-groupes de G contenant S.*

Cette définition est justifiée par le fait que toute intersection de sous-groupes de G est un sous-groupe de G.

Exemples :

- Le groupe $(\mathbb{Z}, +)$ est engendré par 1.
- Le groupe symétrique S_n est engendré par toutes les transpositions.
- Le groupe symetrique S_n est engendré par la transposition $(1, 2)$ et le cycle $(1, 2, \cdots, n)$.
- Le groupe $O(2)$ est engendré par les symétries.
- Le groupe $O(3)$ est engendré par les réflexions.
- Le groupe $SL_2(\mathbb{Z})$ est engendré par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Définition 9.7 *S'il existe un élément a tel que $< a >= G$ alors G est dit monogène et a s'appelle un générateur de G.*

Définition 9.8 *Si G est fini et monogène on dit que G est un groupe cyclique.*

Définition 9.9 *Soit a un élément d'un groupe G. Si le groupe engendré par a est fini on dit que a est d'ordre fini. L'ordre de a est alors le plus petit entier m non nul tel que $a^m = e$.*

Proposition 9.9 *Si a est un élément du groupe G d'ordre fini m, alors le sous-groupe engendré par a est l'ensemble des éléments $e, a \ldots, a^{m-1}$. En particulier l'ordre de a est le cardinal du sous-groupe engendré par a. De plus si p est un élément de $\mathbb{Z}$, $a^p = e$ si et seulement si m divise p.*

Proposition 9.10 *Si G est un groupe d'orde fini, tout élément de G est d'ordre fini et l'ordre d'un élément de G divise le cardinal de G*

Première démonstration C'est la démonstration officiellement au programme. On suppose G commutatif. Si a est dans G l'application $g \mapsto ag$ est bijective donc $\prod_{g\in G} ag = \prod_{g\in G} g$, $a^{\operatorname{Card} G} \prod_{g\in G} g = \prod_{g\in G} g$ et dans un groupe tout élément est simplifiable, donc $a^{\operatorname{Card} G} = e$.

Deuxième démonstration On utilise le théorème de Lagrange : l'ordre de tout sous-groupe divise l'ordre du groupe.

9.2 Congruences

9.2.1 Sous-groupes de $\mathbb{Z}$

Théorème 9.2 *Les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles $a\mathbb{Z} = \{ax; x \in \mathbb{Z}\}$ où a est entier.*

9.2.2 $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Définition 9.10 *Soit n un entier strictement positif. Soient a et b deux entiers relatifs, a et b ont même reste dans la division enclidienne par n si et seulement si n divise $b - a$. On dit alors que a et b sont congrus modulo n. On écrit $a \equiv b$ modulo n.*

Proposition 9.11 *Si n est un entier strictement positif la relation de congruence modulo n est une relation d'équivalence.*

Définition 9.11 *Si n est un entier strictement positif l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n s'appelle l'ensemble des entiers modulo n et se note $\frac{\mathbb{Z}}{n\mathbb{Z}}$.*

On notera $\overline{x}$ la classe d'équivalence de l'entier relatif x, le module n étant sous-entendu par le contexte.

Proposition 9.12 *Si n est un entier strictement positif $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un ensemble fini de cardinal n.*

Proposition 9.13 *L'addition est compatible avec la relation de congruence. On peut donc par passage au quotient munir $\frac{\mathbb{Z}}{n\mathbb{Z}}$ d'une loi interne qui en fait un groupe commutatif. De plus la surjection canonique*

$$\begin{array}{rccc} p & : & \mathbb{Z} & \to & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ & & x & \mapsto & \overline{x} \end{array}$$

est un morphisme de groupe dont le noyau est $n\mathbb{Z}$.

9.2.3 Groupes cycliques

Théorème 9.3 *$\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un groupet cyclique, de plus $\overline{a}$ est générateur si et seulement si a est premier avec n.*

Culture : indicatrice d'Euler. C'est la fonction ϕ telle que $\phi(n)$ est le nombre d'entiers de $[0, n-1]$ premiers avec n. C'est aussi le nombre de générateurs de $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Proposition 9.14 *Soit a un élement d'un groupe G, alors l'application*

$$\begin{array}{rccc} \phi & : & \mathbb{Z} & \to & G \\ & & k & \mapsto & a^k \end{array}$$

est un morphisme de groupes dont l'image est le sous-groupe engendré par a. Le noyau de ϕ est de la forme $n\mathbb{Z}$. Si $n = 0$ alors $< a >$ est isomorphe à $\mathbb{Z}$. Sinon $< a >$ est un groupe cyclique isomorphe à $\frac{\mathbb{Z}}{n\mathbb{Z}}$. En particulier tout groupe cyclique est de la forme $\frac{\mathbb{Z}}{n\mathbb{Z}}$, pour un certain n.

Proposition 9.15 *Le groupe U_n des racines n-ième de l'unité est isomorphe à $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Les générateurs de U_n s'appellent les racines primitives n-ièmes de l'unité, ce sont les éléments de la forme $\exp(\frac{2ik\pi}{n})$ où k est premier avec n.*

Il y a donc $\phi(n)$ racine primitives n-ième de l'unité.