ACCQ 201 - Structures algébriques finies

1 Groupes

Relations d'équivalence et structures quotient

Def. Une **relation** $\mathcal{R}$ sur un ensemble E est la donnée d'une partie $\mathcal{R} \subset E \times E$. On écrit $x\mathcal{R}y$ si $(x, y) \in \mathcal{R}$.

Def. Une relation $\mathcal{R}$ sur E est dite :

- réflexive si $\forall x \in E, x\mathcal{R}x$,
- symétrique si $\forall x, y \in E, (x\mathcal{R}y) \implies (y\mathcal{R}x)$,
- transitive si $\forall x, y, z \in E, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \implies x\mathcal{R}z$

et on dit que c'est une relation d'équivalence si ces trois conditions sont vérifiées. Dans ce cas on note aussi $x \sim_{\mathcal{R}} y$ ou encore $x \equiv y \mod \mathcal{R}$.

Def. Soit $\sim$ une relation d'équivalence sur E et $A \subset E$. On dit que A est une classe d'équivalence pour la relation $\sim$ si A est non vide, $\forall x, y \in A, x \sim y$ et $\forall x \in A, \forall y \notin A, x \not\sim y$.

Not. On note $E/\sim$ l'ensemble des classes d'équivalences pour $\sim$, appelé **ensemble quotient** de E par $\sim$.

Prop. *Les classes d'équivalence forment une partition de E.*

Cor. *On a $|E| = \sum_{A \in E/\sim} |A|$.*

On dispose de la projection canonique de E sur $E/\sim$, $\pi : x \mapsto \bar{x} = \{y \in E \mid x \sim y\}$, où x est un représentant de $\bar{x}$. On dit que $\mathcal{S} \subset E$ est un **système de représentants** si $\pi_{|\mathcal{S}} : \mathcal{S} \xrightarrow{\sim} E/\sim$.

Th. *Soit $f : E \to F$ une application. On a équivalence entre les deux assertions suivantes :*

1. *f est compatible à $\sim$, i.e. $\forall x, y \in E, x \sim y \implies f(x) = f(y)$*
2. *$\exists g : E/\sim \to F, f = g \circ \pi$.*

Si ces conditions sont vérifiées, cette application g est unique. On dit qu'elle est l'application déduite de f par passage au quotient par $\sim$.

Def. Un **groupe** $(G, *, e)$ est la donnée de G non vide, $*$ une loi de composition interne et $e \in G$ tels que $*$ est associative, e est neutre et tout élement est inversible. On dit que ce groupe est **abélien** si $*$ est commutative.

Def. Un sous-ensemble H du groupe G est appelé **sous groupe** si : $e \in H$, il est stable par inversion et par composition.

Prop. *Une intersection quelconque de sous-groupes de G est encore un sous-groupe de G.*

Prop. *Soit G un groupe et $S \subset G$. Notons $\langle S \rangle \subset G$ l'intersection de tous les sous-groupes de G qui contiennent S. Alors $\langle S \rangle$ est un sous-groupe de G contenant S et c'est le plus petit d'entre eux. On l'appelle **sous-groupe** engendré par S dans G.*

Prop. *On a aussi $S = \{s_1^{m_1} * \cdots * s_r^{m_r} \mid r \in \mathbf{N}, s_i \in S, m_i \in \mathbf{Z}\}$.*

Prop. *Soit H un sous-groupe de G. On définit $x \sim y \iff x^{-1}y \in H$. Alors $\sim$ est une relation d'équivalence et $G/\sim$ est noté G/H $(x \mod H) = xH$.*

Def. Soit H un sous-groupe de G. On définit l'**indice** de H dans G par $[G : H] = |G/H|$ (éventuellement infini).

Prop. *Soit G un groupe fini. Alors tout sous-groupe H de G est fini, d'indice fini et on a $|G| = |H| \cdot [G : H]$.*

Action d'un groupe sur un ensemble

Def. Une action de $(G, *, e)$ sur un ensemble X est la donnée d'une application $\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & g \cdot x \end{array}$ telle que $\forall x \in X, e \cdot x = x$ et $\forall g, g' \in G, \forall x \in X, g \cdot (g' \cdot x) = (g * g') \cdot x$.

Def. Soit G agissant sur X. Pour tout élément $x \in X$, on définit son stabilisateur $G_x = \{g \in G \mid g \cdot x = x\}$ et son orbite $O_x = G \cdot x = \{g \cdot x \mid g \in G\}$.

Prop. *Le stabilisateur G_x est un sous-groupe de G.*

Prop. *La relation $\sim$ définie par $(x \sim x') \iff (\exists g \in G, x' = g \cdot x)$ est une relation d'équivalence. Les orbites de l'action sont alors précisément le classes d'équivalences pour $\sim$.*

Ex. Des actions classiques de H sur G, avec H sous-groupe de G, sont :

1. translation à gauche, $(h, x) \mapsto xh^{-1}$,
2. translation à droite, $(h, x) \mapsto hx$,
3. conjugaison, $(h, x) \mapsto hxh^{-1}$.

Prop. *Soit G agissant sur X. Alors $\forall x \in X$, $g \mapsto g \cdot x$ induit par passage au quotient une bijection $G/G_x \xrightarrow{\sim} O_x$ et en particulier $|O_x| = [G : G_x]$.*

Th (Formule de Burnside). *Soit G un groupe fini agissant sur X fini. Alors*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|\{x\in X \mid g\cdot x = x\}|$$

autrement dit le nombre d'orbites de l'action est égal à l'espérance du nombre de points fixes d'un élément aléatoire de G.

Morphismes

Def. Un **(homo)morphisme** de $(G,*,e)$ dans $(G',*',e')$ est une application $f\colon G\to G'$ telle que : $f(e)=e'$, $\forall x\in G, f(x^{-1})=f(x)^{-1}$, $\forall x,y\in G, f(x*y)=f(x)*'f(y)$. Pour $G=G'$ c'est un **endomorphisme**, si f est bijective c'est un **isomorphisme** et pour les deux à la fois c'est un **automorphisme**.

Prop. *Les images directes et réciproques de sous-groupes par un morphisme de groupes sont des sous-groupes.*

Def. Soit $f\colon G\to G'$ un morphisme de groupes. Alors

1. $\mathrm{Ker}(f)=f^{-1}(e')$ est un sous-groupe de G appelé **noyau** de f,
2. $\mathrm{Im}(f)=f(G)$ est un sous-groupe de G' appelé **image** de f.

Prop. *Un morphisme $f\colon G\to G'$ est injectif si et seulement si* $\mathrm{Ker}(f)=\{e\}$.

Groupe quotient d'un groupe abélien par un sous-groupe

Soit H s-g de $(G,+,0)$ abélien.

Lem. *On munit G/H d'une structure de groupe abélien avec la loi $+$ telle que $\bar{a}+\bar{b}=(a+H)+(b+H)=(a+b)+H=\overline{a+b}$. L'ensemble quotient muni de cette loi est appelé **groupe quotient** de G par H.*

Prop. *La projection canonique $\pi\colon G\to G/H$ est un morphisme de groupes, surjectif, de noyau H.*

Th. *Les sous-groupes de G/H sont en bijection avec les sous-groupes de G contenant H.*

Morphisme défini par passage au quotient

Th (de factorisation). *Soient $f\colon G\to G'$ un morphisme de groupes abéliens, H un s-g de G et $\pi\colon G\to G/H$ la projection canonique. Alors*

$$(H\subset\mathrm{Ker}(f)) \iff (\exists! g\colon G/H\to G', f=g\circ\pi)$$

et on dit que g se déduit de f par passage au quotient par H. De plus, on a alors $\mathrm{Im}(g)=\mathrm{Im}(f)$ *et* $\mathrm{Ker}(g)=\mathrm{Ker}(f)/H$.

Cor. *Si $f\colon G\to G'$ est un morphisme de groupes abéliens, f induit par passage au quotient un isomorphisme*

$$G/\mathrm{Ker}(f)\xrightarrow{\sim}\mathrm{Im}(f)\ .$$

En particulier, si G est fini on a $|G|=|\mathrm{Ker}(f)|\cdot|\mathrm{Im}(f)|$.

Sous-groupes monogènes, ordre d'un élément

Def. Si $x\in G$, on définit l'**ordre** de x, noté $\omega_G(x)$ comme le plus petit $n\in\mathbf{N}^*$ tel que $x^n=e$ s'il existe, et $+\infty$ sinon.

Lem. *Soit $f\colon G\to G'$ un morphisme de groupes injectif. Alors $\forall x\in G, \omega(f(x))=\omega(x)$.*

Lem. *Pour tout diviseur d de $\omega(x)$ on a $\omega(x^d)=\frac{w(x)}{d}$.*

Lem. *Soit G un groupe. Pour tout $x\in G$, il existe un unique morphisme de groupes $f_x\colon\mathbf{Z}\to G$ envoyant 1 sur x, c'est $k\mapsto x^k$ et son image est $\langle x\rangle$.*

Lem. *Tout s-g non nul H de $(\mathbf{Z},+,0)$ est de la forme $H=N\mathbf{Z}$ où $N=[\mathbf{Z}:H]=\min(H\cap\mathbf{N}^*)$.*

Prop. *Soit G un groupe et $x\in G$.*

1. *Si $\omega(x)=\infty$, $f_x\colon\mathbf{Z}\xrightarrow{\sim}\langle x\rangle$.*
2. *Si $\omega(x)<\infty$, $\mathrm{Ker}(f_x)=\omega(x)\mathbf{Z}$, f_x induit par passage au quotient un isomorphisme entre $\mathbf{Z}/\omega(x)\mathbf{Z}$ et $\langle x\rangle$ et $\langle x\rangle=\{e,x,x^2,\dots,x^{\omega(x)-1}\}$.*

Dans les deux cas $|\langle x\rangle|=\omega(x)$.

Cor. *Soit x d'ordre fini. Alors $\forall n\in\mathbf{Z}, (x^n=e) \iff (\omega(x)\mid n)$.*

Th (**Lagrange**). *Soit G un groupe fini. Alors, pour tout $x\in G$, $x^{|G|}=e$ et $\omega(x)|G$.*

Groupes cycliques

Prop. *Soit $(G,*,e)$ un groupe fini, $N=|G|$ son ordre et $g_0\in G$. Les assertions suivantes sont équivalentes :*

(i) *g_0 est d'ordre N,*

(ii) *$G=\langle g_0\rangle$,*

(iii) *il existe un isomorphisme $\varphi\colon\mathbf{Z}/N\mathbf{Z}\xrightarrow{\sim}G$ qui envoie $\bar{1}$ sur g_0,*

(iv) *tout élément $g\in G$ peut s'écrire $g=g_0^n$ pour un certain $n\in\mathbf{N}$.*

Def. Un groupe fini vérifiant les assertions précédentes est appelé **groupe cyclique**. On dit que g_0 est un **générateur** de G.

Prop. *Soit $N \in \mathbf{N}^*$.*

1. *Si $d \mid n$, $d\mathbf{Z}/N\mathbf{Z} = \left\{\bar{0}, \bar{d}, \ldots, \overline{\left(\frac{N}{d}-1\right)d}\right\}$ est un sous groupe de $\mathbf{Z}/N\mathbf{Z}$. Inversement, tout s-g de $\mathbf{Z}/N\mathbf{Z}$ est de cette forme pour un entier d divisant N uniquement déterminé, mettant en bijection les s-g de $\mathbf{Z}/N\mathbf{Z}$ et les diviseurs de N.*
2. *Si d_1 et d_2 divisent N, on a $(d_2\mathbf{Z}/N\mathbf{Z} \subset d_1\mathbf{Z}/N\mathbf{Z}) \iff (d_1 \mid d_2)$.*
3. *Le sous-groupe $d\mathbf{Z}/N\mathbf{Z}$ est cyclique, d'ordre $\frac{N}{d}$ et d'indice $[\mathbf{Z}/N\mathbf{Z} : d\mathbf{Z}/N\mathbf{Z}] = d$.*
4. *Les éléments de $d\mathbf{Z}/N\mathbf{Z}$ sont les éléments de $\mathbf{Z}/N\mathbf{Z}$ (additif) dont l'ordre divise $\frac{N}{d}$.*
5. *Soit $x \in \mathbf{Z}$. On a $\langle \bar{x} \rangle = d\mathbf{Z}/N\mathbf{Z}$ où $d = \operatorname{pgcd}(x, N)$. Alors x est d'ordre $\frac{N}{d}$ (additif). En particulier, $\bar{x}$ est générateur de $\mathbf{Z}/N\mathbf{Z}$ si et seulement si x est premier avec N.*

Cor (Bézout). *Soit $a, b \in \mathbf{Z}$ non tous les deux nuls. Alors $\exists m, n \in \mathbf{Z}, ma + nb = \operatorname{pgcd}(a, b)$.*

Cor. *Soit $(G, *, e)$ groupe cyclique d'ordre N. Alors pour tout $y \in G$ et $d \mid N$ on a $(\exists x \in G, y = x^d) \iff \left(y^{\frac{N}{d}} = e\right)$. Pour $k \in \mathbf{N}^*$ on a $(\exists x \in G, y = x^d) \iff \left(y^{\frac{N}{\operatorname{pgcd}(N,k)}} = e\right)$. En particulier, si k est premier avec N, tout élément de G est une puissance k-ième.*