Université Paris 13, Institut Galilée
Département de Mathématiques
Licence 2ème année Informatique
2013-2014

Cours de Mathématiques pour l'Informatique
Des nombres aux structures
Sylviane R. Schwer

Leçon du 18 mars 2014 : Structures algébriques : Etude des groupes finis $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{0})$ et $((\mathbb{Z}/n\mathbb{Z})^*, \dot{\times}, \dot{1})$

1 Groupes finis

Rappelons qu'un groupe $(G, *, e)$ est une structure telle que $*$ est une opération partout définie, associative, dont e est élément neutre et pour laquelle tout élément de G possède un inverse. $(G, *, e)$ est un groupe commutatif ou abélien si $*$ est commutative. On a démontré le résultat suivant :

$$\forall n \in \mathbb{N}, n \geq 2, (\mathbb{Z}/n\mathbb{Z}, +) \text{ est un groupe commutatif.}$$

Définition 1.1 (sous-groupe) *Une partie F de $(G, *, e)$ est un sous groupe de $(G, *, e)$ ssi $(F, *, e)$ est un groupe.*
F est un sous-groupe propre ssi $F \neq G$ et $F \neg \{e\}$.

Proposition 1.1 *Dans un groupe $(G, *, e)$, une partie F non vide est un sous-groupe ssi*

$$\forall x, y \in F, x * y^{-1} \in F$$

Preuve :
• Supposons que $(F, *, e)$ soit un groupe, Soit $x, y \in F$, $y^{-1} \in F$ et $x.y^{-1} \in F$
• Supposons que $\forall x, y \in F, x * y^{-1} \in F$, en particulier, $e = x * x^{-1} \in F$. F hérite naturellement de l'associativité et e est élément neutre. Soit $x \in F$, $x^{-1} = e * x^{-1} \in F$ par hypothèse. □

Définition 1.2 *Un groupe $(G, *, e)$ est* fini *si le nombre de ses éléments, appelé alors* ordre *du groupe, est fini.*

$(Z, +)$ n'est pas un groupe fini. $\forall n \geq 2, (\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe fini d'ordre n.
$\forall n \geq 2, (\mathbb{Z}/n\mathbb{Z}, .)*$ est un groupe fini d'ordre $\varphi(n)$.

Proposition 1.2 (Lagrange) *Dans un groupe fini $(G, *, e)$ d'ordre n, si k est l'ordre d'un sous-groupe $(F, *, e)$, alors $k|n$.*

Preuve :
Soit la relation $\mathcal{R}$ définie sur $(G, *, e)$ par $a\mathcal{R}b$ ssi $a * b^{-1} \in F$. F étant un groupe, $\mathcal{R}$ est une relation d'équivalence dont les classes sont en nombre fini. Tout élément étant régulier, il y a exactement $\#F$ éléments par classe. □

Corollaire 1.1 $(\mathbb{Z}/n\mathbb{Z}, +, [0]_n)$ *possèdent des sous-groupes propres ssi* $n \notin \mathbb{P}$.

$(\mathbb{Z}/6\mathbb{Z}, +, [0]_6)$ possèdent des sous-groupes propre d'ordre 2 et 3.

Proposition 1.3 (Quotient d'un groupe commutatif par un sous-groupe) *Soit* $(G, *, e)$ *un groupe commutatif, et* H *un sous-groupe de* G*, alors la relation* $\mathcal{R}$ *définie sur* $(G, *, e)$ *par* $a\mathcal{R}b$ *ssi* $a * b^{-1} \in F$ *est compatible avec* $*$*, et permet de construire le groupe quotient* $(G/\mathcal{R}, *, F)$

Preuve :
• La compatibilité de $\mathcal{R}$ avec $*$ est assurée par la commutativité : Supposons $a\mathcal{R}b$ et $a'\mathcal{R}b'$. Montrons que $a * a'\mathcal{R}b * b'$. Or $(a * a') * (b * b')^{-1} =_{def} a * a' * b'^{-1} * b^{-1} =$ par commutativité$= (a * b^{-1}) * (a' * b'^{-1}) \in F$ car F est un sous-groupe.
• La classe de e est F. □

Exemple : $n\mathbb{Z}$ est un sous groupe additif de $(\mathbb{Z}, +, 0)$, $a \equiv_n b$ est la relation définie dans la proposition 1.3, $\mathbb{Z}/n\mathbb{Z}$ est un groupe quotient.

Définition 1.3 (sous-groupe engendré par une partie finie A) *Dans un groupe de* $(G, *, e)$ *soit* A *une partie finie de* G*. On dit qu'un sous-groupe* F *est* engendré par A *si tout élément de* F *s'exprime comme un composé par l'opération* $*$ *d'éléments de* A *.*

Si A *est un singleton* $\{a\}$*, on dit que* F un sous-groupe monogène engendré par a*.* F *est alors l'ensemble des puissances positives et négatives de* a *pour la moi* $*$*.*

Si F *est fini et monogène, on dit qu'il est* cyclique*.*

Remarques :
• si $*$ est la loi additive, on parle plutôt de multiples, si c'est la loi multiplicative de puissance.
•Tout sous-groupe cyclique est commutatif.
• $(\mathbb{Z}, +, 0)$ est un groupe monogène non cyclique engendré par 1.
• $\forall n \geq 2, (\mathbb{Z}/n\mathbb{Z}, +, 0)$ est un groupe cyclique engendré par la classe de 1.

Lemme 1.1 $\forall n \geq 2, (\mathbb{Z}/n\mathbb{Z}, +, 0)$ *,l'ordre d'un élément* $[a]_n$ *est égal à* $\dfrac{n}{n \wedge a}$.

Preuve : $ka \equiv_n 0 \Longleftrightarrow n|ka$. □

2 Morphismes de groupes

2.1 Rappels sur les fonctions

Les ensembles produits $E \times F = \{(x, y), x \in E, y \in F\}$ peuvent être considérés comme des types d'objets particuliers, les relations, que l'on étudie en propre (cf. TD n° 8). Nous nous intéressons dans ce paragraphe à des relations particulières, les fonctions.

Définition 2.1 *Soit E et F deux ensembles, Les parties de $E \times F$ sont appelées* relations. *Soit f une relation de $E \times F$. On appelle image $x \in E$ par f, et l'on note $f(x)$ l'ensemble*

$$f(x) = \{y \in F, y = f(x)\}$$

On appelle restriction de f à $A \subset E$ et $B \subset F$, la relation $\{(x, y) \in A \times B, (x, y) \in f\}$
On appelle image d'une partie A de E par f, et l'on note $f(A)$ l'ensemble

$$f(A) = \{y \in F, \exists x \in A, y = f(x)\} = \bigcup_{x \in A} f(x)$$

On appelle image réciproque - ou ensemble des antécédents *- d'un élément $y \in F$, l'ensemble*

$$f^{-1}(y) = \{x \in E, y = f(x)\}$$

On appelle image réciproque d'une partie $K \subseteq F$, l'ensemble

$$f^{-1}(K) = \{x \in E, \exists y \in F, y = f(x)\} = \bigcup_{y \in K} f^{-1}(y)$$

On appelle domaine de définition *de f, l'ensemble $D_f = f{-}1(F)$*
On appelle image ou codomaine *de f, l'ensemble $f(E)$*

- *f est une* fonction *ssi* $\forall x \in E, \#f(x) \leq 1$.
- *f est* surjective *ssi* $f(E) = F$.
- *f est* totale *(ou une* application*) ssi* $f^{-1}(F) = E$.
- *f est* injective *ssi* $\forall y \in F, \#f^{-1}(y) \leq 1$.
- *f est une* bijection *ssi f est une application injective et surjective.*

Une fonction f établie une correspondance "$\rightarrow$"entre deux ensembles. elle est donc composée d'un domaine E, d'un ensemble image (ou codomaine) F et d'une procédure "$\longmapsto$" qui à chaque élément x de E établit cette correspondance avec $f(x)$ dans F. Un correspondant est une sorte de "représentant de son antécédent. On note $f \left| \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} \right.$. Etre injective signifie que chaque correspondant n'a qu'un correspondant, ou que la réciproque de la fonction est aussi une fonction.

Si f est injective, alors sa restriction $\left| \begin{array}{ccc} D_f & \longrightarrow & f(E) \\ x & \longmapsto & f(x) \end{array} \right.$ est une bijection.

2.2 Morphismes de groupes

La notion de morphisme est fondamentale puisqu'elle permet de définir des correspondances entre les structures, et ainsi permet la construction et/ou l'étude des objets nouveaux à partir d'objets connus. Nous commençons avec la structure de monoïde, et complétons par celle de groupe.

Qui dit correspondance entre les structures dit correspondance entre les éléments remarquables comme les éléments neutres, absorbants, ... pour les opérations ou minimum et maximum, ... pour les relations d'ordre, les classes pour les relations d'équivalence.

Définition 2.2 (homomorphisme de monoïde) *Soit $(M_1, *_1, e_1)$ et $(M_2, *_2, e_2)$ deux monoïdes, f est un (homo)morphisme de monoides de M_1 dans M_2 ssi f est une application compatible avec la structure de monoïdes, c'est-à-dire que*

- $f(x *_1 y) = f(x) *_2 f(y)$
- $f(e_1) = e_2$

Si de plus, f est bijective, alors f est un isomorphime.

Remarque : Si $(M_1, *_1, e_1)$ et $(M_2, *_2, e_2)$ sont deux groupes,
$e_2 = f(e_1) = f(x *_1 x^{-1_{*_1}}) = f(x) *_2 f(x^{-1_{*_1}})$, donc

$$f(x^{-1_{*_1}}) = f(x)^{-1_{*_2}}.$$

Réciproquement, si l'on a $f(x *_1 y) = f(x) *_2 f(y)$ et $f(x^{-1_{*_1}}) = f(x)^{-1_{*_2}}$, $f(e_1) = f(e_1 *_1 e_1) = f(e_1) *_2 f(e_1)$. Or dans un groupe, out élément est régulier,en particulier $f(e_1)$ donc e simplifiant, on obtient $e_2 = f(e_1)$.
On peut vérifier l'homomorphisme de groupes de f en vérifiant l'unique égalié
$f(x *_1 y^{-1_{*_1}}) = f(x) *_2 [f(y)]^{-1_{*_2}}$

Notations : $Hom(G_1, G_2)$ est l'ensemble des homomorphimes de G_1 dans G_2.
$Iso(G_1, G_2)$ est l'ensemble des isomorphimes de G_1 dans G_2.

Exemple : $f \left| \begin{array}{ccc} (A^*, ., \varepsilon) & \longrightarrow & (\mathbb{N}, +, 0) \\ w & \longmapsto & |w| \end{array} \right.$ est un morphisme de monoïdes.

Proposition 2.1 (Image d'un morphisme) *Soit f un morphisme de monoïdes [resp. de groupes] entre $(M_1, *_1, e_1)$ et $(M_2, *_2, e_2)$, $f(E)$ est un sous-monoïde [resp. sous-groupe] de $(M_2, *_2, e_2)$.*

Preuve :
• f(E) n'est pas vide car contient e_2.
• Montrons sa stabilité par $*_2$: soit $y, y' \in F$, $\exists x,\ x' \in E, y = f(x), y' = f(x')$. $y + y' = f(x) + f(x')$ =f est un morphisme= $f(x + x')$, or $x + x' \in E$, donc $y + y' \in f(E)$. $f(E)$ est donc un sous-monoïde de M_2.
• Supposons maintenant que f est un morphisme de groupe. Si $y = f(x)$, comme $f(x^{-1_{*_1}}) = f(x)^{-1_{*_2}}$, $y^{-1_{*_2}} \in f(E)$, donc $f(E)$ est un sous-groupe de F. □

Définition 2.3 (noyau d'un morphisme) *Soit f un morphisme de monoïdes [resp. de groupes] entre $(M_1, *_1, e_1)$ et $(M_2, *_2, e_2)$, le noyau de f est l'ensemble $Ker(f) = f^{-1}(e_2)$.*

Remarque : Le noyau d'un morphisme de monoïde [resp. groupe] n'est pas vide car il contient e_1. Mieux encore,

Proposition 2.2 *Soit f un morphisme de monoïdes [resp. de groupes] entre $(M_1, *_1, e_1)$ et $(M_2, *_2, e_2)$, $Ker(f)$ est un sous-monoïde [resp. sous-groupe] de $(M_1, *_1, e_1)$*

Preuve :
• Pour établir la structure de sous-monoïde de $Ker(f)$, il suffit de prouver sa stabilité par $*_1$: soit $x, x' \in Ker(f)$, $f(x) = f(x') = e_2$. Donc, comme f est un homomorphisme, $f(x + x') = f(x) + f(x') = e_2$ donc $x + x' \in Ker(f)$.
• Pour établir de plus la propriété de sous-groupe (si M_1 est lui-même un groupe), il reste à établir la stabilité par l'inversion : soit $x \in Ker(f)$. $x *_1 x^{-1} = e_1$ donc $f(x) *_2 f(x^{-1}) = e_2$ soit $f(x^{-1}) = e_2$.

Proposition 2.3 *Soit f un morphisme de groupes entre $(G_1, *_1, e_1)$ et $(G_2, *_2, e_2)$, f est injective si et seulement si $Ker(f) = \{e_1\}$.*

Preuve :
• Supposons f injective, alors l'équation $f(x) = e_2$ possède au plus une solution, or $x = e_1$ est une solution donc $Ker(f) = \{e_1\}$.
• Réciproquement : supposons que $Ker(f) = \{e_1\}$. Soit x et x' deux éléments de M_1 ayant même image, $f(x) = f(x')$. Comme G_2 est un groupe et f un morphisme de groupe, $f(x) = f(x') \iff f(x)^{-1_{*_2}} *_2 f(x') = e_2 \iff f(x^{-1_{*_1}} *_1 x') = e_2 \iff x^{-1_{*_1}} *_1 x' \in Ker(f)$, par hypothèse, $\iff x^{-1_{*_1}} *_1 x' = e_1 \iff x = x' \iff f$ est injective. □

Remarque : D'après la première partie de la preuve, si un morphisme est injectif, le noyau est réduit à $\{e_1\}$. En revanche, il existe des morphismes de monoïdes non injectifs dont le noyau est réduit à $\{e_1\}$, comme $f \left| \begin{array}{ccc} (A^*, ., \varepsilon) & \longrightarrow & (\mathbb{N}, +, 0) \\ w & \longmapsto & |w| \end{array} \right.$, dès que $\#A \geq 2$.

Proposition 2.4 *Soit f est un morphisme de groupes de $(G_1, *_1, e_1)$ et $(G_2, *_2, e_2)$, la relation $x \equiv_f x'$ ssi $f(x) = f(x')$ est une relation de congruence qui confère à $(G_1/\equiv_f, [*_1]_{\equiv_f}, [e_1]_{\equiv_f})$ une structure de groupe.*

Preuve :
• $x \equiv_f x'$ est une relation d'équivalence pour toute fonction.
• Il suffit donc de prouver la compatibilité avec $*_1$: Supposons $a \equiv_f a', b \equiv_f b'$, soit $f(a) = f(a')$ et $f(b) = f(b')$. Alors $f(a *_1 b) =$f morphisme$= f(a) *_2 f(b) =$hypothèse$=$ $f(a') *_2 f(b') =$f morphisme$= f(a' *_1 b'$, soit $a + a' \equiv_f b + b')$.
• Sur l'ensemble des classes $(G_1/\equiv_f, [*_1]_{\equiv_f}$, $[*_1]_{\equiv_f}$ est une opération parfaitement définie par $[a]_{\equiv_f}[*_1]_{\equiv_f}[b]_{\equiv_f} = [a *_1 b]_{\equiv_f}$ qui est
— associative car $([a]_{\equiv_f}[*_1]_{\equiv_f}[b]_{\equiv_f})[*_1]_{\equiv_f}[c]_{\equiv_f}$ =def= $[a *_1 b]_{\equiv_f}[*_1]_{\equiv_f}[c]_{\equiv_f}$ =def= $[(a *_1$

$b) * 1c]_{\equiv_f}$ =associativité dans G_1= $[a *_1 (b *_1 c)]_{\equiv_f}$ =def= $[a]_{\equiv_f}[*_1]_{\equiv_f}[b *_1 c]_{\equiv_f}$ =def= $[a]_{\equiv_f}[*_1]_{\equiv_f}([b]_{\equiv_f}[*_1]_{\equiv_f}[c]_{\equiv_f})$
— $Ker(f)$ est l'élément neutre, c'est la classe de e_1 : $[e_1]_{\equiv_f}[*_1]_{\equiv_f}[a]_{\equiv_f}$ =def= $[e_1 *_1 a]_{\equiv_f}$ $=e_1$ élément neutre dans G_1=$[a]_{\equiv_f}$ et de même à droite.
— $[a^{-1}]_{\equiv_f}$ est l'inverse de $[a]_{\equiv_f}$ pout $[*_1]_{\equiv_f}$.
□

Théorème 2.5 *Soit f est un morphisme de groupes de $(G_1, *_1, e_1)$ et $(G_2, *_2, e_2)$,*

- *l'application* $s_f \left| \begin{array}{ccc} (G_1, *_1, e_1) & \longrightarrow & (G_1/\equiv_f, [*_1]_{\equiv_f}, [e_1]_{\equiv_f}) \\ x & \longmapsto & [x]_{\equiv_f} \end{array} \right.$ *est un morphisme surjectif*
- *la fonction* $i_f \left| \begin{array}{ccc} (f(G_1), *_2, e_2) & \longrightarrow & (G_2, *_2, e_2) \\ y & \longmapsto & y \end{array} \right.$ *est un morphisme injectif.*

Ces fonctions définissent l'isomorphisme de groupe $\bar{f}$ de $(G_1/\equiv_f, [*_1]_{\equiv_f}, [e_1]_{\equiv_f})$ dans $(f(G_1), *_2, e_2)$ par la relation

$$f = i_f \circ \bar{f} \circ s_f$$

représentée par le diagramme carré commutatif suivant :

$$\begin{array}{ccc} (G_1, *_1, e_1) & \xrightarrow{\quad f \quad} & (G_2, *_2, e_2) \\ \downarrow{\scriptstyle s_f} & & \uparrow{\scriptstyle i_f} \\ (G_1/\equiv_f, [*_1]_{\equiv_f}, [e_1]_{\equiv_f}) & \xrightarrow{\bar{f}} & (f(G_1), *_2, e_2) \end{array}$$

Preuve :
• s_f est un morphisme surjectif car $\equiv_f$ est une congruence, donc partitionne G_1 de façon compatible à f
• i_f est l'injection naturelle à l'inclusion ensembliste, sa réciproque est une fonction partielle (si f n'est pas surjective) injective et surjective.
• $\bar{f}$ est une application car f l'est. Elle est injective et surjective par construction : $\bar{f}([a]_{\equiv_f}) = \bar{f}[b]_{\equiv_f} \Longleftrightarrow f(a) = f(b) \Longleftrightarrow a \equiv_f b$.
• $\bar{f}$ est un isomorphisme de groupe car $\bar{f}([a]_{\equiv_f}[*_1]_{\equiv_f}[b]_{\equiv_f}) = \bar{f}([a *_1 b]_{\equiv_f} = i_f^{-1} \circ f(a *_1 b) = i_f^{-1}[f(a) *_2 f(b)] = i_f^{-1}[f(a)] *_2 i_f[f(b)] = \bar{f}[s_f(a)] *_2 \bar{f}[s_f(b)] = \bar{f}([a]_{\equiv_f}) *_2 \bar{f}([b]_{\equiv_f})$

Corollaire 2.1 *Soit $n, a, b \in \mathbb{N}, n \geq 4, n = a.b$, l'application* $\gamma \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times Z/b\mathbb{Z} \\ [x]_n & \longmapsto & ([x]_a, [x]_b) \end{array} \right.$
est un isomorphisme de groupe additif si et seulement si $a \wedge b = 1$

Preuve : La fonction γ est $\bar{f}$ de la fonction $f \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times Z/b\mathbb{Z} \\ x & \longmapsto & ([x]_a, [x]_b) \end{array} \right.$ qui est un morphisme de groupe. On a le carré

$$\begin{array}{ccc} (\mathbb{Z}, +, 0) & \xrightarrow{\quad f \quad} & (\mathbb{Z}/a\mathbb{Z} \times Z/b\mathbb{Z}, (\dot{+}_a, \dot{+}_b), ([0]_a, [0]_b)) \\ \downarrow{\scriptstyle s_f} & & \uparrow{\scriptstyle i_f} \\ (\mathbb{Z}/\equiv_f, [+]_{\equiv_f}, [0]_{\equiv_f}) & \xrightarrow{\bar{f}} & (f(\mathbb{Z}), (\dot{+}_a, \dot{+}_b), ([0]_a, [0]_b)) \end{array}$$

$Ker(f) = a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

Donc $\mathbb{Z}/(a \vee b)\mathbb{Z}$ est isomorphe à $f(\mathbb{Z}/(a \vee b)\mathbb{Z})$ qui est un sous-groupe de $\mathbb{Z}/a\mathbb{Z} \times Z/b\mathbb{Z}$. Or $\#\mathbb{Z}/(a \vee b)\mathbb{Z} = a \vee b = \dfrac{n}{a \wedge b}$. Donc $a \wedge b = 1 \iff$ f bijective.

Exemple : Construire γ pour $n = 12$, $a = 6$ et $b = 4$. On peut donc observer que le

Table 1: default

x	$[0]_{12}$	$[1]_{12}$	$[2]_{12}$	$[3]_{12}$	$[4]_{12}$	$[5]_{12}$
$\gamma(x)$	$([0]_6, [0]_4)$	$([1]_6, [1]_4)$	$([2]_6, [2]_4)$	$([3]_6, [3]_4)$	$([4]_6, [0]_4)$	$([5]_6, [1]_4)$
x	$[6]_{12}$	$[7]_{12}$	$[8]_{12}$	$[9]_{12}$	$[10]_{12}$	$[11]_{12}$
$\gamma(x)$	$([0]_6, [2]_4)$	$([1]_6, [3]_4)$	$([2]_6, [0]_4)$	$([3]_6, [1]_4)$	$([4]_6, [2]_4)$	$([5]_6, [3]_4)$

système suivant n'a pas de solution dans $\mathbb{Z}/12\mathbb{Z}$, donc pas de solution. γ est une injection, mais pas une bijection de $\mathbb{Z}/12\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

$$\begin{cases} x \equiv 1 \quad (6) \\ x \equiv 2 \quad (4) \end{cases}$$

Pour qu'un système

$$\begin{cases} x \equiv a \quad (6) \\ x \equiv b \quad (4) \end{cases}$$

possède une solution, il faut et il suffit que $a \equiv_{6\wedge 4} b$, c'est-à-dire de même parité.

Exemple : Construire γ pour $n = 12$, $a = 3$ et $b = 4$.

Table 2: default

x	$[0]_{12}$	$[1]_{12}$	$[2]_{12}$	$[3]_{12}$	$[4]_{12}$	$[5]_{12}$
$\gamma(x)$	$([0]_3, [0]_4)$	$([1]_3, [1]_4)$	$([2]_3, [2]_4)$	$([0]_3, [3]_4)$	$([1]_3, [0]_4)$	$([2]_3, [1]_4)$
x	$[6]_{12}$	$[7]_{12}$	$[8]_{12}$	$[9]_{12}$	$[10]_{12}$	$[11]_{12}$
$\gamma(x)$	$([0]_3, [2]_4)$	$([1]_3, [3]_4)$	$([2]_3, [0]_4)$	$([0]_3, [1]_4)$	$([1]_3, [2]_4)$	$([2]_3, [3]_4)$

On peut donc observer que γ est bien une bijection et que le système

$$\begin{cases} x \equiv 1 \quad (3) \\ x \equiv 2 \quad (4) \end{cases}$$

est équivalent à l'équation

$$x \equiv 10 \quad (12)$$

.