

François Liret

Arithmétique

DUNOD

Couverture: underworld 111 © istockphoto.com

© Dunod, 2011
2019 pour la nouvelle présentation
11 rue Paul Bert, 92240 Malakoff
ISBN 978-2-10-080656-0
www.dunod.com

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

TABLE DES MATIÈRES

Chapitre 1 • Relation d'équivalence et ensemble quotient

1.1	Partition et relation d'équivalence	1
1.2	Ensemble quotient	4
1.3	Passage au quotient d'une application	5
	Exercices	7
	Solutions	8

Chapitre 2 • Divisibilité dans $\mathbb{Z}$

2.1	Multiple et diviseur	11
2.2	Division euclidienne	13
2.3	PGCD	14
2.4	Équation $ax + by = c$, $(x, y) \in \mathbb{Z} \times \mathbb{Z}$	18
2.5	PPCM	19
2.6	Décomposition en facteurs premiers	20
	Exercices	22
	Solutions	24

Chapitre 3 • Congruence

3.1	Relation de congruence	29
3.2	Règles de calcul	31
3.3	Résolution d'équations	33
3.4	Triplets pythagoriciens	35
	Exercices	36
	Solutions	37

Chapitre 4 • Groupes

4.1	Notion de groupe	43
4.2	Sous-groupe	46
4.3	Morphisme de groupe	48
4.4	Sous-groupe engendré par un élément	51
4.5	Ordre d'un élément	52
4.6	Classes modulo un sous-groupe	54

Table des matières

4.7	Sous-groupe distingué	58
	Exercices	63
	Solutions	64

Chapitre 5 • Groupes cycliques

5.1	Définition et premières propriétés	69
5.2	Sous-groupes d'un groupe cyclique	72
5.3	Morphismes	73
	Exercices	75
	Solutions	77

Chapitre 6 • Anneaux et corps

6.1	Notions générales	83
6.2	Anneau quotient	89
6.3	Anneau $\mathbb{Z}/n\mathbb{Z}$	91
6.4	Le corps $\mathbb{F}_p$	96
	Exercices	97
	Solutions	98

Chapitre 7 • Polynômes

7.1	Polynômes à coefficients dans un anneau	103
7.2	Anneau $K[X]$	108
7.3	Polynômes à coefficients dans $\mathbb{F}_p$	110
7.4	Calcul des coefficients binomiaux modulo p	113
	Exercices	115
	Solutions	116

Chapitre 8 • Le corps $\mathbb{F}_p$

8.1	Les carrés dans $\mathbb{F}_p$	119
8.2	Le groupe $\mathbb{F}_p^*$	124
8.3	Le calcul des puissances modulo	126
8.4	Applications à la cryptographie	126
	Exercices	128
	Solutions	130

Chapitre 9 • Anneaux principaux, anneaux euclidiens

9.1	Anneau principal	135
9.2	Polynômes irréductibles de $K[X]$	140
9.3	Anneau euclidien	145
9.4	Des anneaux pour l'arithmétique	146

Exercices	151
Solutions	152
 Chapitre 10 • Deux problèmes classiques	
10.1 Entiers somme de deux carrés	157
10.2 L'équation de Pell-Fermat	160
Exercices	165
Solutions	167
 Chapitre 11 • Construction de corps	
11.1 Caractéristique d'un corps	173
11.2 Sous-corps	174
11.3 Quotient d'un anneau de polynômes	177
11.4 Extension de corps	181
Exercices	185
Solutions	187
 Chapitre 12 • Corps finis	
12.1 Structure des corps finis	195
12.2 L'automorphisme de Frobenius	199
12.3 Sous-corps	200
12.4 Polynômes irréductibles et corps finis	202
12.5 Polynômes irréductibles de $\mathbb{F}_p[X]$	205
12.6 Applications à la cryptographie	207
Exercices	208
Solutions	210
 Chapitre 13 • Réciprocité quadratique	
13.1 Symbole de Legendre	215
13.2 La loi de réciprocité quadratique	217
Exercices	221
Solutions	222
 Principales notations	 227
 Index	 229

RELATION D'ÉQUIVALENCE ET ENSEMBLE QUOTIENT

1

PLAN

- 1.1 Partition et relation d'équivalence
- 1.2 Ensemble quotient
- 1.3 Passage au quotient d'une application

OBJECTIF

On est souvent amené à partager les éléments d'un ensemble en différentes classes, c'est-à-dire à définir une partition de cet ensemble. Il devient alors possible de raisonner et de calculer sur les classes : c'est un puissant procédé algébrique.

1.1 PARTITION ET RELATION D'ÉQUIVALENCE

Définition

Soit E un ensemble. Une *partition* de E est la donnée de parties C_i de E , non vides, deux à deux disjointes et dont la réunion est E . On dit que les parties C_i sont des *classes*.

Exemple

Notons C_0 l'ensemble des entiers impairs, C_1 l'ensemble des entiers multiples de 2 mais pas de 4 et plus généralement, pour tout entier $n \geq 0$, notons

C_n l'ensemble des entiers multiples de 2^n mais pas de 2^{n+1} .

Les parties $(C_n)_{n \in \mathbb{N}}$ forment une partition de $\mathbb{Z}$.

1.1.1 Comment définir une partition d'un ensemble E ?

Il y a essentiellement deux procédés.

1. Au moyen d'une application définie sur E

Soit $f : E \longrightarrow F$ une application surjective.

Rappelons que pour tout élément $b \in F$, la partie de E définie par

$$f^{-1}(b) = \{x \in E \mid f(x) = b\}$$

s'appelle *l'image réciproque de b par f* . Puisque f est surjective, $f^{-1}(b)$ est non vide.

Les parties $C_b = f^{-1}(b)$ sont deux à deux disjointes, car s'il existe x commun à C_b et $C_{b'}$, alors $b = f(x) = b'$; leur réunion est E , car pour tout $x \in E$, on a $x \in f^{-1}(f(x))$, donc $x \in C_{f(x)}$. Les parties C_b forment donc une partition de E .

Exemple

Soit $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ l'application définie par $f(x, y) = 2x + 3y$. L'application f est surjective car pour tout entier $k \in \mathbb{Z}$, on a $f(-k, k) = -2k + 3k = k$. Ainsi par exemple, les parties

$$C_0 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 2x + 3y = 0\} \quad \text{et} \quad C_5 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 2x + 3y = 5\}$$

sont des classes de la partition de $\mathbb{Z} \times \mathbb{Z}$ définie par f .

2. Au moyen d'une relation d'équivalence sur E

Définition

Une relation $\sim$ sur un ensemble E est une *relation d'équivalence* si elle est

- (i) réflexive : $\forall a \in E, a \sim a$
- (ii) symétrique : $\forall a, b \in E, (a \sim b) \implies (b \sim a)$
- (iii) transitive : $\forall a, b, c \in E, (a \sim b \text{ et } b \sim c) \implies (a \sim c)$

Pour tout $a \in E$, l'ensemble $\text{cl}(a) = \{x \in E \mid x \sim a\}$ s'appelle *la classe (d'équivalence) de a* .

Proposition

Soit $\sim$ une relation d'équivalence sur E .

- Pour tout $a \in E, a \in \text{cl}(a)$.
- Pour tous $a, b \in E$, on a l'équivalence : $a \sim b \iff \text{cl}(a) = \text{cl}(b)$.
- Pour tous $a, b \in E$, si $\text{cl}(a) \neq \text{cl}(b)$, alors $\text{cl}(a) \cap \text{cl}(b) = \emptyset$.

DÉMONSTRATION. Soient $a, b \in E$.

Puisque $a \sim a$ d'après (i), on a $a \in \text{cl}(a)$.

Supposons $a \sim b$. Alors pour tout $z \in \text{cl}(a)$, on a $z \sim a$ et puisque $a \sim b$, il s'ensuit (transitivité) $z \sim b$, donc $z \in \text{cl}(b)$. Cela montre que $\text{cl}(a) \subset \text{cl}(b)$; mais

comme on a aussi $b \sim a$ (symétrie), il vient $\text{cl}(b) \subset \text{cl}(a)$, donc $\text{cl}(a) = \text{cl}(b)$. Réciproquement, si $\text{cl}(a) = \text{cl}(b)$, alors $a \in \text{cl}(b)$, donc $a \sim b$.

Montrons la dernière propriété en raisonnant par contraposée.

Supposons $\text{cl}(a) \cap \text{cl}(b) \neq \emptyset$. Alors il existe $z \in \text{cl}(a) \cap \text{cl}(b)$ et l'on a $a \sim z$ et $z \sim b$, donc $a \sim b$, donc $\text{cl}(a) = \text{cl}(b)$. $\square$

Remarquons que E est la réunion des classes d'équivalence, car tout élément $a \in E$ est dans $\text{cl}(a)$. On en déduit la proposition suivante.

Proposition

Etant donnée une relation d'équivalence sur E , les classes d'équivalence forment une partition de E .

Réciproquement, si l'on se donne une partition $(C_i)_{i \in I}$ de E , alors la relation définie par : $a \sim b \iff (\exists i \in I \text{ tel que } a, b \in C_i)$ est une relation d'équivalence dont les classes sont les C_i .

Exemple

Soit $\vec{u} \in \mathbb{R}^2$, $\vec{u} \neq \vec{0}$. Dans le plan affine, la relation :

$$(M \sim M') \iff (\overrightarrow{MM'} \text{ est colinéaire à } \vec{u})$$

est une relation d'équivalence. La classe d'un point A est la droite affine passant par A et de vecteur directeur $\vec{u}$.

1.1.2 Relation d'équivalence définie par une application

Soit $f : E \longrightarrow F$ une application. Définissons une relation $\sim_f$ sur E en posant

$$\forall x, y \in E, x \sim_f y \iff f(x) = f(y)$$

Cette relation est réflexive, symétrique et transitive.

Définition

Soit $f : E \rightarrow F$ une application. La relation d'équivalence $\sim_f$ définie par

$$\forall x, y \in E, x \sim_f y \iff f(x) = f(y)$$

s'appelle la relation d'équivalence définie par f .

Pour tout $a \in E$, la classe de a est $\text{cl}(a) = \{x \in E \mid f(x) = f(a)\} = f^{-1}(f(a))$.

Exemple

Soit O un point du plan euclidien E et soit $f : E \longrightarrow \mathbb{R}$ la fonction $M \mapsto OM$. La relation d'équivalence associée à f est

$$\forall M, M' \in E, M \sim_f M' \iff OM = OM'$$

La classe d'équivalence d'un point $A \in E$ est formée des points M qui sont à la même distance de O que A : si $A \neq O$, la classe de A est le cercle de centre O passant par A ; la classe de O est $\{O\}$.

1.2 ENSEMBLE QUOTIENT

Définitions

Soit $\sim$ une relation d'équivalence sur un ensemble E .

- L'ensemble des classes d'équivalence s'appelle *l'ensemble quotient de E par $\sim$* et se note $E/\sim$.
- L'application $p : E \longrightarrow E/\sim$ définie par $p(x) = \text{cl}(x)$ s'appelle la *projection canonique*.
- Etant donnée une classe d'équivalence $\text{cl}(a)$, tout élément $x \in \text{cl}(a)$ s'appelle *un représentant* de cette classe.

Propriétés de la projection canonique

- L'application p est surjective : $\forall \alpha \in E/\sim, \exists a \in E, \alpha = p(a)$.
- La relation $\sim$ est la relation d'équivalence définie par p :

$$\forall x, y \in E, p(x) = p(y) \iff x \sim y$$

DÉMONSTRATION. Toute classe $\alpha \in E/\sim$ est la classe d'au moins un élément $a \in E$: $\alpha = \text{cl}(a)$, donc $\alpha = p(a)$.

Pour tous $x, y \in E$, on a $x \sim y \iff \text{cl}(x) = \text{cl}(y) \iff p(x) = p(y)$, donc $\sim$ est la relation d'équivalence définie par l'application p . $\square$

Toute relation d'équivalence sur E est donc définie par une application : la projection canonique $E \longrightarrow E/\sim$.

Exemple

Définissons une relation dans $\mathbb{R}^*$ en posant : $x \sim y \iff xy > 0$.

C'est une relation d'équivalence, car $x \sim y$ si et seulement si x et y ont le même signe.

La relation $\sim$ est la relation d'équivalence définie par l'application $\text{sgn} : \mathbb{R}^* \longrightarrow \{+1, -1\}$ qui à tout $x \in \mathbb{R}^*$ associe son signe.

Il y a deux classes : $\text{cl}(1) = \mathbb{R}^{*+}$ et $\text{cl}(-1) = \mathbb{R}^{*-}$. L'ensemble quotient $\mathbb{R}^*/\sim$ a donc deux éléments.

1.3 PASSAGE AU QUOTIENT D'UNE APPLICATION

Le théorème suivant permet de définir des applications sur un ensemble quotient. C'est un résultat constamment utilisé en mathématique.

Théorème de passage au quotient

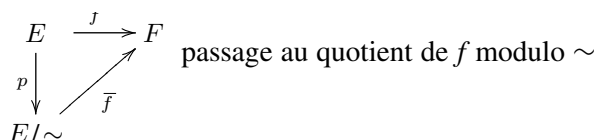
Soit $\sim$ une relation d'équivalence sur un ensemble E et $p : E \rightarrow E/\sim$ la projection canonique. Soit $f : E \rightarrow F$.

Pour qu'il existe une application $\bar{f} : E/\sim \rightarrow F$ telle que $\bar{f} \circ p = f$, il faut et il suffit que $\forall x, y \in E, x \sim y \implies f(x) = f(y)$.

Dans ce cas,

- $\bar{f}$ est unique et pour toute classe $\alpha \in E/\sim$, on a $\bar{f}(\alpha) = f(a)$ pour tout représentant a de α ;
- $\bar{f}$ est injective si et seulement si $\forall x, y \in E, x \sim y \iff f(x) = f(y)$;
- Les applications f et $\bar{f}$ ont la même image.

Si l'application $\bar{f}$ existe, on dit que f passe au quotient modulo $\sim$ et $\bar{f}$ s'appelle la factorisation de f par $E/\sim$.



DÉMONSTRATION

- Supposons qu'il existe $\bar{f} : E/\sim \rightarrow F$ telle que $f = \bar{f} \circ p$. Si $x, y \in E$ sont tels que $x \sim y$, alors $p(x) = p(y)$, donc $f(x) = \bar{f}(p(x)) = \bar{f}(p(y)) = f(y)$. Réciproquement, supposons $\forall x, y \in E, x \sim y \implies f(x) = f(y)$. Si $\alpha \in E/\sim$, alors pour tous représentants a, a' de α , on a $a' \sim a$ donc $f(a) = f(a')$: l'application f prend la même valeur sur tous les représentants de α . On peut donc poser $\bar{f}(\alpha) = f(a)$, où a est un représentant quelconque de α . On définit ainsi une application $\bar{f} : E/\sim \rightarrow F$ telle que $\bar{f}(p(a)) = f(a)$ quel que soit $a \in E$.
- Supposons $\bar{f}$ injective et soient $x, y \in E$ tels que $f(x) = f(y)$. Alors $\bar{f}(p(x)) = \bar{f}(p(y))$, donc $p(x) = p(y)$ et par suite $x \sim y$. Réciproquement, supposons $\forall x, y \in E, x \sim y \iff f(x) = f(y)$. Soient $\alpha = p(a)$ et $\beta = p(b)$ des éléments de $E/\sim$ tels que $\bar{f}(\alpha) = \bar{f}(\beta)$. Alors $f(a) = \bar{f}(\alpha) = \bar{f}(\beta) = f(b)$, donc $a \sim b$ et $\alpha = \beta$: l'application $\bar{f}$ est donc injective.
- Puisque $f = \bar{f} \circ p$, on a $f(E) = \bar{f}(p(E)) = \bar{f}(E/\sim)$ car p est surjective. $\square$

En appliquant le théorème à la relation $\sim_f$ définie par f , on obtient le corollaire très utile suivant.