

Introduction à la Cryptologie

Chapitre 7 : Groupes

Michael Eisermann (Institut Fourier, UJF Grenoble)

Année 2008-2009
IF / IMAG, Master 1, S1-S2

document mis à jour le 7 juillet 2009



UNIVERSITE JOSEPH FOURIER
SCIENCES. TECHNOLOGIE. SANTÉ



www-fourier.ujf-grenoble.fr/~eiserm/cours#crypto

- 1 Groupes
- 2 Applications en cryptographie
- 3 Le théorème de Lagrange et applications
- 4 Groupes quotients dans le cas commutatif
- 5 Exercices

- 1 Groupes
 - Groupes et morphismes
 - Sous-groupes
 - Groupes cycliques
- 2 Applications en cryptographie
- 3 Le théorème de Lagrange et applications
- 4 Groupes quotients dans le cas commutatif
- 5 Exercices

Définition

Un *groupe* (G, \bullet) est un ensemble G muni d'une application $\bullet: G \times G \rightarrow G$, notée $(a, b) \mapsto a \bullet b$, vérifiant les axiomes suivants :

Définition

Un *groupe* (G, \bullet) est un ensemble G muni d'une application $\bullet: G \times G \rightarrow G$, notée $(a, b) \mapsto a \bullet b$, vérifiant les axiomes suivants :

(G1 : associativité)

$$\forall a, b, c \in G : (a \bullet b) \bullet c = a \bullet (b \bullet c)$$

Définition

Un *groupe* (G, \bullet) est un ensemble G muni d'une application $\bullet: G \times G \rightarrow G$, notée $(a, b) \mapsto a \bullet b$, vérifiant les axiomes suivants :

$$\text{(G1 : associativité)} \quad \forall a, b, c \in G : (a \bullet b) \bullet c = a \bullet (b \bullet c)$$

$$\text{(G2 : élément neutre)} \quad \exists e \in G \quad \forall a \in G : a \bullet e = e \bullet a = a$$

Définition

Un *groupe* (G, \bullet) est un ensemble G muni d'une application $\bullet: G \times G \rightarrow G$, notée $(a, b) \mapsto a \bullet b$, vérifiant les axiomes suivants :

- | | | |
|--------------------------|---|---|
| (G1 : associativité) | $\forall a, b, c \in G :$ | $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ |
| (G2 : élément neutre) | $\exists e \in G \quad \forall a \in G :$ | $a \bullet e = e \bullet a = a$ |
| (G3 : éléments inverses) | $\forall a \in G \quad \exists b \in G :$ | $a \bullet b = b \bullet a = e$ |

Définition

Un *groupe* (G, \bullet) est un ensemble G muni d'une application $\bullet : G \times G \rightarrow G$, notée $(a, b) \mapsto a \bullet b$, vérifiant les axiomes suivants :

$$(G1 : \text{associativité}) \quad \forall a, b, c \in G : (a \bullet b) \bullet c = a \bullet (b \bullet c)$$

$$(G2 : \text{élément neutre}) \quad \exists e \in G \quad \forall a \in G : a \bullet e = e \bullet a = a$$

$$(G3 : \text{éléments inverses}) \quad \forall a \in G \quad \exists b \in G : a \bullet b = b \bullet a = e$$

Un groupe (G, \bullet) est dit *commutatif* (ou *abélien*) s'il satisfait

$$(GA : \text{commutativité}) \quad \forall a, b \in G : a \bullet b = b \bullet a.$$

Définition

Un *groupe* (G, \bullet) est un ensemble G muni d'une application $\bullet: G \times G \rightarrow G$, notée $(a, b) \mapsto a \bullet b$, vérifiant les axiomes suivants :

$$\text{(G1 : associativité)} \quad \forall a, b, c \in G : (a \bullet b) \bullet c = a \bullet (b \bullet c)$$

$$\text{(G2 : élément neutre)} \quad \exists e \in G \quad \forall a \in G : a \bullet e = e \bullet a = a$$

$$\text{(G3 : éléments inverses)} \quad \forall a \in G \quad \exists b \in G : a \bullet b = b \bullet a = e$$

Un groupe (G, \bullet) est dit *commutatif* (ou *abélien*) s'il satisfait

$$\text{(GA : commutativité)} \quad \forall a, b \in G : a \bullet b = b \bullet a.$$

Proposition

L'élément neutre de G est unique ; l'élément inverse de a dans G est unique.

Définition

Un *groupe* (G, \bullet) est un ensemble G muni d'une application $\bullet : G \times G \rightarrow G$, notée $(a, b) \mapsto a \bullet b$, vérifiant les axiomes suivants :

$$(G1 : \text{associativité}) \quad \forall a, b, c \in G : (a \bullet b) \bullet c = a \bullet (b \bullet c)$$

$$(G2 : \text{élément neutre}) \quad \exists e \in G \quad \forall a \in G : a \bullet e = e \bullet a = a$$

$$(G3 : \text{éléments inverses}) \quad \forall a \in G \quad \exists b \in G : a \bullet b = b \bullet a = e$$

Un groupe (G, \bullet) est dit *commutatif* (ou *abélien*) s'il satisfait

$$(GA : \text{commutativité}) \quad \forall a, b \in G : a \bullet b = b \bullet a.$$

Proposition

L'élément neutre de G est unique ; l'élément inverse de a dans G est unique.

Remarque

Pour un *monoïde* (M, \bullet) on n'exige que les axiomes (G1) et (G2).

Définition

Un *groupe* (G, \bullet) est un ensemble G muni d'une application $\bullet : G \times G \rightarrow G$, notée $(a, b) \mapsto a \bullet b$, vérifiant les axiomes suivants :

$$(G1 : \text{associativité}) \quad \forall a, b, c \in G : (a \bullet b) \bullet c = a \bullet (b \bullet c)$$

$$(G2 : \text{élément neutre}) \quad \exists e \in G \quad \forall a \in G : a \bullet e = e \bullet a = a$$

$$(G3 : \text{éléments inverses}) \quad \forall a \in G \quad \exists b \in G : a \bullet b = b \bullet a = e$$

Un groupe (G, \bullet) est dit *commutatif* (ou *abélien*) s'il satisfait

$$(GA : \text{commutativité}) \quad \forall a, b \in G : a \bullet b = b \bullet a.$$

Proposition

L'élément neutre de G est unique ; l'élément inverse de a dans G est unique.

Remarque

Pour un *monoïde* (M, \bullet) on n'exige que les axiomes (G1) et (G2).
Par exemple $(\mathbb{Z}, +)$ est un groupe, alors que $(\mathbb{N}, +)$ n'est qu'un monoïde.

Exemples

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/m, +)$

sont des groupes abéliens.

Exemples

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/m, +)$

$(\mathbb{Z}^\times, \cdot)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(\mathbb{Z}/m^\times, \cdot)$

sont des groupes abéliens.

sont des groupes abéliens.

Exemples de groupes

Exemples

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/m, +)$

$(\mathbb{Z}^\times, \cdot)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(\mathbb{Z}/m^\times, \cdot)$

$(\text{Sym}(3), \circ)$ et $(\text{GL}(2, \mathbb{R}), \cdot)$

sont des groupes abéliens.

sont des groupes abéliens.

sont des groupes non abéliens.

Exemples de groupes

Exemples

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/m, +)$

$(\mathbb{Z}^\times, \cdot)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(\mathbb{Z}/m^\times, \cdot)$

$(\text{Sym}(3), \circ)$ et $(\text{GL}(2, \mathbb{R}), \cdot)$

sont des groupes abéliens.

sont des groupes abéliens.

sont des groupes non abéliens.

Notation

Dans un groupe (G, \cdot) noté multiplicativement on écrit ab au lieu de $a \cdot b$.

Exemples de groupes

Exemples

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/m, +)$

$(\mathbb{Z}^\times, \cdot)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(\mathbb{Z}/m^\times, \cdot)$

$(\text{Sym}(3), \circ)$ et $(\text{GL}(2, \mathbb{R}), \cdot)$

sont des groupes abéliens.

sont des groupes abéliens.

sont des groupes non abéliens.

Notation

Dans un groupe (G, \cdot) noté multiplicativement on écrit ab au lieu de $a \cdot b$.

L'élément neutre est noté 1, et l'élément inverse de a est noté a^{-1} .

Exemples de groupes

Exemples

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/m, +)$ sont des groupes abéliens.
 $(\mathbb{Z}^\times, \cdot)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(\mathbb{Z}/m^\times, \cdot)$ sont des groupes abéliens.
 $(\text{Sym}(3), \circ)$ et $(\text{GL}(2, \mathbb{R}), \cdot)$ sont des groupes non abéliens.

Notation

Dans un groupe (G, \cdot) noté multiplicativement on écrit ab au lieu de $a \cdot b$.
L'élément neutre est noté 1 , et l'élément inverse de a est noté a^{-1} .

Dans un groupe $(G, +)$ noté additivement, par contre,
l'élément neutre est noté 0 , et l'élément inverse de a est noté $-a$.

Exemples de groupes

Exemples

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/m, +)$ sont des groupes abéliens.
 $(\mathbb{Z}^\times, \cdot)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(\mathbb{Z}/m^\times, \cdot)$ sont des groupes abéliens.
 $(\text{Sym}(3), \circ)$ et $(\text{GL}(2, \mathbb{R}), \cdot)$ sont des groupes non abéliens.

Notation

Dans un groupe (G, \cdot) noté multiplicativement on écrit ab au lieu de $a \cdot b$.
L'élément neutre est noté 1, et l'élément inverse de a est noté a^{-1} .

Dans un groupe $(G, +)$ noté additivement, par contre,
l'élément neutre est noté 0, et l'élément inverse de a est noté $-a$.

Proposition

Si $(G_1, \cdot), \dots, (G_n, \cdot)$ sont des groupes, alors le produit $G = G_1 \times \dots \times G_n$ est un groupe pour la loi $(g_1, \dots, g_n) \cdot (h_1, \dots, h_n) := (g_1 h_1, \dots, g_n h_n)$.

Exemples de groupes

Exemples

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/m, +)$ sont des groupes abéliens.
 $(\mathbb{Z}^\times, \cdot)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(\mathbb{Z}/m^\times, \cdot)$ sont des groupes abéliens.
 $(\text{Sym}(3), \circ)$ et $(\text{GL}(2, \mathbb{R}), \cdot)$ sont des groupes non abéliens.

Notation

Dans un groupe (G, \cdot) noté multiplicativement on écrit ab au lieu de $a \cdot b$.
L'élément neutre est noté 1, et l'élément inverse de a est noté a^{-1} .

Dans un groupe $(G, +)$ noté additivement, par contre,
l'élément neutre est noté 0, et l'élément inverse de a est noté $-a$.

Proposition

Si $(G_1, \cdot), \dots, (G_n, \cdot)$ sont des groupes, alors le produit $G = G_1 \times \dots \times G_n$ est un groupe pour la loi $(g_1, \dots, g_n) \cdot (h_1, \dots, h_n) := (g_1 h_1, \dots, g_n h_n)$.

L'élément neutre de G est $e = (e_1, \dots, e_n)$.

Exemples de groupes

Exemples

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}/m, +)$ sont des groupes abéliens.
 $(\mathbb{Z}^\times, \cdot)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(\mathbb{Z}/m^\times, \cdot)$ sont des groupes abéliens.
 $(\text{Sym}(3), \circ)$ et $(\text{GL}(2, \mathbb{R}), \cdot)$ sont des groupes non abéliens.

Notation

Dans un groupe (G, \cdot) noté multiplicativement on écrit ab au lieu de $a \cdot b$.
L'élément neutre est noté 1, et l'élément inverse de a est noté a^{-1} .

Dans un groupe $(G, +)$ noté additivement, par contre,
l'élément neutre est noté 0, et l'élément inverse de a est noté $-a$.

Proposition

Si $(G_1, \cdot), \dots, (G_n, \cdot)$ sont des groupes, alors le produit $G = G_1 \times \dots \times G_n$ est un groupe pour la loi $(g_1, \dots, g_n) \cdot (h_1, \dots, h_n) := (g_1 h_1, \dots, g_n h_n)$.

L'élément neutre de G est $e = (e_1, \dots, e_n)$.

L'inverse de (g_1, \dots, g_n) est $(g_1, \dots, g_n)^{-1} = (g_1^{-1}, \dots, g_n^{-1})$. □

Définition

Soient (G, \circ) et (H, \bullet) des groupes.

Définition

Soient (G, \circ) et (H, \bullet) des groupes. Une application $\phi: G \rightarrow H$ est un *morphisme de groupes* si $\phi(a \circ b) = \phi(a) \bullet \phi(b)$ pour tout $a, b \in G$.

Définition

Soient (G, \circ) et (H, \bullet) des groupes. Une application $\phi: G \rightarrow H$ est un *morphisme de groupes* si $\phi(a \circ b) = \phi(a) \bullet \phi(b)$ pour tout $a, b \in G$.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un morphisme de groupes.

Définition

Soient (G, \circ) et (H, \bullet) des groupes. Une application $\phi: G \rightarrow H$ est un *morphisme de groupes* si $\phi(a \circ b) = \phi(a) \bullet \phi(b)$ pour tout $a, b \in G$.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un morphisme de groupes.

L'application quotient $\pi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m, +)$ est un morphisme de groupes.

Définition

Soient (G, \circ) et (H, \bullet) des groupes. Une application $\phi: G \rightarrow H$ est un *morphisme de groupes* si $\phi(a \circ b) = \phi(a) \bullet \phi(b)$ pour tout $a, b \in G$.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un morphisme de groupes.

L'application quotient $\pi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m, +)$ est un morphisme de groupes.

Exemples

L'exponentielle $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$ est un morphisme de groupes.

Définition

Soient (G, \circ) et (H, \bullet) des groupes. Une application $\phi: G \rightarrow H$ est un *morphisme de groupes* si $\phi(a \circ b) = \phi(a) \bullet \phi(b)$ pour tout $a, b \in G$.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un morphisme de groupes.

L'application quotient $\pi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m, +)$ est un morphisme de groupes.

Exemples

L'exponentielle $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$ est un morphisme de groupes.

Le logarithme $\log: (\mathbb{R}_{>0}, \cdot) \rightarrow (\mathbb{R}, +)$ est un morphisme de groupes.

Définition

Soient (G, \circ) et (H, \bullet) des groupes. Une application $\phi: G \rightarrow H$ est un *morphisme de groupes* si $\phi(a \circ b) = \phi(a) \bullet \phi(b)$ pour tout $a, b \in G$.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un morphisme de groupes.

L'application quotient $\pi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m, +)$ est un morphisme de groupes.

Exemples

L'exponentielle $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$ est un morphisme de groupes.

Le logarithme $\log: (\mathbb{R}_{>0}, \cdot) \rightarrow (\mathbb{R}, +)$ est un morphisme de groupes.

Proposition

Si ϕ est un morphisme de groupes, alors $\phi(e_G) = e_H$ et $\phi(a^{-1}) = \phi(a)^{-1}$.

Définition

Soient (G, \circ) et (H, \bullet) des groupes. Une application $\phi: G \rightarrow H$ est un *morphisme de groupes* si $\phi(a \circ b) = \phi(a) \bullet \phi(b)$ pour tout $a, b \in G$.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un morphisme de groupes.

L'application quotient $\pi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m, +)$ est un morphisme de groupes.

Exemples

L'exponentielle $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$ est un morphisme de groupes.

Le logarithme $\log: (\mathbb{R}_{>0}, \cdot) \rightarrow (\mathbb{R}, +)$ est un morphisme de groupes.

Proposition

Si ϕ est un morphisme de groupes, alors $\phi(e_G) = e_H$ et $\phi(a^{-1}) = \phi(a)^{-1}$.

Notation

Soit (G, \cdot) un groupe noté multiplicativement et soit $g \in G$ un élément.

Notation

Soit (G, \cdot) un groupe noté multiplicativement et soit $g \in G$ un élément.
Pour $n \in \mathbb{N}$ on définit g^n par $g^0 := 1_G$, puis $g^{n+1} := g^n \cdot g$.

Notation

Soit (G, \cdot) un groupe noté multiplicativement et soit $g \in G$ un élément.

Pour $n \in \mathbb{N}$ on définit g^n par $g^0 := 1_G$, puis $g^{n+1} := g^n \cdot g$.

Pour les exposants négatifs on pose $g^{-n} := (g^n)^{-1}$.

Notation

Soit (G, \cdot) un groupe noté multiplicativement et soit $g \in G$ un élément.

Pour $n \in \mathbb{N}$ on définit g^n par $g^0 := 1_G$, puis $g^{n+1} := g^n \cdot g$.

Pour les exposants négatifs on pose $g^{-n} := (g^n)^{-1}$.

Proposition

Pour tout $m, n \in \mathbb{Z}$ on a $g^{m+n} = g^m \cdot g^n$.

Notation

Soit (G, \cdot) un groupe noté multiplicativement et soit $g \in G$ un élément.

Pour $n \in \mathbb{N}$ on définit g^n par $g^0 := 1_G$, puis $g^{n+1} := g^n \cdot g$.

Pour les exposants négatifs on pose $g^{-n} := (g^n)^{-1}$.

Proposition

Pour tout $m, n \in \mathbb{Z}$ on a $g^{m+n} = g^m \cdot g^n$. L'application $\exp_g : \mathbb{Z} \rightarrow G$ définie par $\exp_g(k) = g^k$ est un morphisme du groupe $(\mathbb{Z}, +)$ dans le groupe (G, \cdot) .

Notation

Soit (G, \cdot) un groupe noté multiplicativement et soit $g \in G$ un élément.

Pour $n \in \mathbb{N}$ on définit g^n par $g^0 := 1_G$, puis $g^{n+1} := g^n \cdot g$.

Pour les exposants négatifs on pose $g^{-n} := (g^n)^{-1}$.

Proposition

Pour tout $m, n \in \mathbb{Z}$ on a $g^{m+n} = g^m \cdot g^n$. L'application $\exp_g : \mathbb{Z} \rightarrow G$ définie par $\exp_g(k) = g^k$ est un morphisme du groupe $(\mathbb{Z}, +)$ dans le groupe (G, \cdot) .

Remarque

L'algorithme de puissance rapide s'applique au calcul de g^n dans un groupe !

Notation

Soit (G, \cdot) un groupe noté multiplicativement et soit $g \in G$ un élément.
Pour $n \in \mathbb{N}$ on définit g^n par $g^0 := 1_G$, puis $g^{n+1} := g^n \cdot g$.
Pour les exposants négatifs on pose $g^{-n} := (g^n)^{-1}$.

Proposition

Pour tout $m, n \in \mathbb{Z}$ on a $g^{m+n} = g^m \cdot g^n$. L'application $\exp_g : \mathbb{Z} \rightarrow G$ définie par $\exp_g(k) = g^k$ est un morphisme du groupe $(\mathbb{Z}, +)$ dans le groupe (G, \cdot) .

Remarque

L'algorithme de puissance rapide s'applique au calcul de g^n dans un groupe !

Notation

Soit $(G, +)$ un groupe noté additivement et soit $g \in G$ un élément.

Notation

Soit (G, \cdot) un groupe noté multiplicativement et soit $g \in G$ un élément.
Pour $n \in \mathbb{N}$ on définit g^n par $g^0 := 1_G$, puis $g^{n+1} := g^n \cdot g$.
Pour les exposants négatifs on pose $g^{-n} := (g^n)^{-1}$.

Proposition

Pour tout $m, n \in \mathbb{Z}$ on a $g^{m+n} = g^m \cdot g^n$. L'application $\exp_g : \mathbb{Z} \rightarrow G$ définie par $\exp_g(k) = g^k$ est un morphisme du groupe $(\mathbb{Z}, +)$ dans le groupe (G, \cdot) .

Remarque

L'algorithme de puissance rapide s'applique au calcul de g^n dans un groupe !

Notation

Soit $(G, +)$ un groupe noté additivement et soit $g \in G$ un élément.
Pour $n \in \mathbb{N}$ on définit ng par $0g := 0_G$ puis $(n+1)g := ng + g$.

Notation

Soit (G, \cdot) un groupe noté multiplicativement et soit $g \in G$ un élément.
Pour $n \in \mathbb{N}$ on définit g^n par $g^0 := 1_G$, puis $g^{n+1} := g^n \cdot g$.
Pour les exposants négatifs on pose $g^{-n} := (g^n)^{-1}$.

Proposition

Pour tout $m, n \in \mathbb{Z}$ on a $g^{m+n} = g^m \cdot g^n$. L'application $\exp_g : \mathbb{Z} \rightarrow G$ définie par $\exp_g(k) = g^k$ est un morphisme du groupe $(\mathbb{Z}, +)$ dans le groupe (G, \cdot) .

Remarque

L'algorithme de puissance rapide s'applique au calcul de g^n dans un groupe !

Notation

Soit $(G, +)$ un groupe noté additivement et soit $g \in G$ un élément.
Pour $n \in \mathbb{N}$ on définit ng par $0g := 0_G$ puis $(n+1)g := ng + g$.
Pour les facteurs négatifs on pose $(-n)g := -(ng)$.

Définition

Un morphisme de groupes $\phi: G \rightarrow H$ est appelé

Définition

Un morphisme de groupes $\phi: G \rightarrow H$ est appelé

- *monomorphisme* si ϕ est injectif,

Définition

Un morphisme de groupes $\phi: G \rightarrow H$ est appelé

- *monomorphisme* si ϕ est injectif,
- *épimorphisme* si ϕ est surjectif,

Définition

Un morphisme de groupes $\phi: G \rightarrow H$ est appelé

- *monomorphisme* si ϕ est injectif,
- *épimorphisme* si ϕ est surjectif,
- *isomorphisme* si ϕ est bijectif.

Définition

Un morphisme de groupes $\phi: G \rightarrow H$ est appelé

- *monomorphisme* si ϕ est injectif,
- *épimorphisme* si ϕ est surjectif,
- *isomorphisme* si ϕ est bijectif.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un monomorphisme.

Définition

Un morphisme de groupes $\phi: G \rightarrow H$ est appelé

- *monomorphisme* si ϕ est injectif,
- *épimorphisme* si ϕ est surjectif,
- *isomorphisme* si ϕ est bijectif.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un monomorphisme.

L'application quotient $\pi_m: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m, +)$ est un épimorphisme.

Définition

Un morphisme de groupes $\phi: G \rightarrow H$ est appelé

- *monomorphisme* si ϕ est injectif,
- *épimorphisme* si ϕ est surjectif,
- *isomorphisme* si ϕ est bijectif.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un monomorphisme.

L'application quotient $\pi_m: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m, +)$ est un épimorphisme.

Exemple

L'exponentielle $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$ est un isomorphisme.

Définition

Un morphisme de groupes $\phi: G \rightarrow H$ est appelé

- *monomorphisme* si ϕ est injectif,
- *épimorphisme* si ϕ est surjectif,
- *isomorphisme* si ϕ est bijectif.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un monomorphisme.

L'application quotient $\pi_m: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m, +)$ est un épimorphisme.

Exemple

L'exponentielle $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$ est un isomorphisme.

Le logarithme $\log: (\mathbb{R}_{>0}, \cdot) \rightarrow (\mathbb{R}, +)$ est l'isomorphisme inverse.

Définition

Un morphisme de groupes $\phi: G \rightarrow H$ est appelé

- *monomorphisme* si ϕ est injectif,
- *épimorphisme* si ϕ est surjectif,
- *isomorphisme* si ϕ est bijectif.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un monomorphisme.

L'application quotient $\pi_m: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m, +)$ est un épimorphisme.

Exemple

L'exponentielle $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$ est un isomorphisme.

Le logarithme $\log: (\mathbb{R}_{>0}, \cdot) \rightarrow (\mathbb{R}, +)$ est l'isomorphisme inverse.

Exemple

Pour tout $m, n \in \mathbb{Z}$ on a un morphisme $\Phi: \mathbb{Z}/mn \rightarrow \mathbb{Z}/m \times \mathbb{Z}/n$ donné par $\Phi(\pi_{mn}(a)) = (\pi_m(a), \pi_n(a))$.

Définition

Un morphisme de groupes $\phi: G \rightarrow H$ est appelé

- *monomorphisme* si ϕ est injectif,
- *épimorphisme* si ϕ est surjectif,
- *isomorphisme* si ϕ est bijectif.

Exemples

L'inclusion $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ est un monomorphisme.

L'application quotient $\pi_m: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m, +)$ est un épimorphisme.

Exemple

L'exponentielle $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$ est un isomorphisme.

Le logarithme $\log: (\mathbb{R}_{>0}, \cdot) \rightarrow (\mathbb{R}, +)$ est l'isomorphisme inverse.

Exemple

Pour tout $m, n \in \mathbb{Z}$ on a un morphisme $\Phi: \mathbb{Z}/mn \rightarrow \mathbb{Z}/m \times \mathbb{Z}/n$ donné par $\Phi(\pi_{mn}(a)) = (\pi_m(a), \pi_n(a))$. C'est un isomorphisme ssi $\text{pgcd}(m, n) = 1$.

Définition & proposition

Un *sous-groupe* d'un groupe (G, \cdot) est un sous-ensemble $H \subset G$ tel que

$$(SG1) \quad e_G \in H$$

$$(SG2) \quad \forall a \in H : a^{-1} \in H$$

$$(SG3) \quad \forall a, b \in H : ab \in H$$

Définition & proposition

Un *sous-groupe* d'un groupe (G, \cdot) est un sous-ensemble $H \subset G$ tel que

$$(SG1) \quad e_G \in H$$

$$(SG2) \quad \forall a \in H : a^{-1} \in H$$

$$(SG3) \quad \forall a, b \in H : ab \in H$$

L'ensemble H avec l'opération restreinte $\cdot : H \times H \rightarrow H$ est alors un groupe,

Définition & proposition

Un *sous-groupe* d'un groupe (G, \cdot) est un sous-ensemble $H \subset G$ tel que

$$(SG1) \quad e_G \in H$$

$$(SG2) \quad \forall a \in H : a^{-1} \in H$$

$$(SG3) \quad \forall a, b \in H : ab \in H$$

L'ensemble H avec l'opération restreinte $\cdot : H \times H \rightarrow H$ est alors un groupe, et l'inclusion $\iota : H \hookrightarrow G$ est un monomorphisme de groupes.

Définition & proposition

Un *sous-groupe* d'un groupe (G, \cdot) est un sous-ensemble $H \subset G$ tel que

$$(SG1) \quad e_G \in H$$

$$(SG2) \quad \forall a \in H : a^{-1} \in H$$

$$(SG3) \quad \forall a, b \in H : ab \in H$$

L'ensemble H avec l'opération restreinte $\cdot : H \times H \rightarrow H$ est alors un groupe, et l'inclusion $\iota : H \hookrightarrow G$ est un monomorphisme de groupes.

Exemples

Tout groupe G admet $\{e_G\}$ et G comme sous-groupes.

Définition & proposition

Un *sous-groupe* d'un groupe (G, \cdot) est un sous-ensemble $H \subset G$ tel que

$$(SG1) \quad e_G \in H$$

$$(SG2) \quad \forall a \in H : a^{-1} \in H$$

$$(SG3) \quad \forall a, b \in H : ab \in H$$

L'ensemble H avec l'opération restreinte $\cdot : H \times H \rightarrow H$ est alors un groupe, et l'inclusion $\iota : H \hookrightarrow G$ est un monomorphisme de groupes.

Exemples

Tout groupe G admet $\{e_G\}$ et G comme sous-groupes.

\mathbb{Z} est un sous-groupe de $(\mathbb{Q}, +)$, et \mathbb{Q} est un sous-groupe de $(\mathbb{R}, +)$.

Définition & proposition

Un *sous-groupe* d'un groupe (G, \cdot) est un sous-ensemble $H \subset G$ tel que

$$(SG1) \quad e_G \in H$$

$$(SG2) \quad \forall a \in H : a^{-1} \in H$$

$$(SG3) \quad \forall a, b \in H : ab \in H$$

L'ensemble H avec l'opération restreinte $\cdot : H \times H \rightarrow H$ est alors un groupe, et l'inclusion $\iota : H \hookrightarrow G$ est un monomorphisme de groupes.

Exemples

Tout groupe G admet $\{e_G\}$ et G comme sous-groupes.

\mathbb{Z} est un sous-groupe de $(\mathbb{Q}, +)$, et \mathbb{Q} est un sous-groupe de $(\mathbb{R}, +)$.

\mathbb{N} n'est pas un sous-groupe de $(\mathbb{Z}, +)$ car (SG2) n'est pas vérifié.

Proposition

Pour tout $m \in \mathbb{Z}$ l'ensemble $m\mathbb{Z} = \{mq \mid q \in \mathbb{Z}\}$ est un sous-groupe de \mathbb{Z} .

Proposition

*Pour tout $m \in \mathbb{Z}$ l'ensemble $m\mathbb{Z} = \{mq \mid q \in \mathbb{Z}\}$ est un sous-groupe de \mathbb{Z} .
Réciproquement, tout sous-groupe de \mathbb{Z} est de la forme $m\mathbb{Z}$ pour un $m \in \mathbb{Z}$.*

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Corollaire

L'image $\text{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ est un sous-groupe de H .

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Corollaire

L'image $\text{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ est un sous-groupe de H .

Le noyau $\text{ker}(\phi) = \phi^{-1}(e_H) = \{g \in G \mid \phi(g) = e_H\}$ est un sous-groupe de G .

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Corollaire

L'image $\text{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ est un sous-groupe de H .

Le noyau $\text{ker}(\phi) = \phi^{-1}(e_H) = \{g \in G \mid \phi(g) = e_H\}$ est un sous-groupe de G .

Un morphisme de groupes $\phi: G \rightarrow H$ est surjectif ssi $\text{im}(\phi) = H$.

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Corollaire

L'image $\text{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ est un sous-groupe de H .

Le noyau $\text{ker}(\phi) = \phi^{-1}(e_H) = \{g \in G \mid \phi(g) = e_H\}$ est un sous-groupe de G .

Un morphisme de groupes $\phi: G \rightarrow H$ est surjectif ssi $\text{im}(\phi) = H$.

Pour l'injectivité nous avons le critère suivant :

Proposition

Un morphisme de groupes $\phi: G \rightarrow H$ est injectif ssi $\text{ker}(\phi) = \{e_G\}$.

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Corollaire

L'image $\text{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ est un sous-groupe de H .

Le noyau $\ker(\phi) = \phi^{-1}(e_H) = \{g \in G \mid \phi(g) = e_H\}$ est un sous-groupe de G .

Un morphisme de groupes $\phi: G \rightarrow H$ est surjectif ssi $\text{im}(\phi) = H$.

Pour l'injectivité nous avons le critère suivant :

Proposition

Un morphisme de groupes $\phi: G \rightarrow H$ est injectif ssi $\ker(\phi) = \{e_G\}$.

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Corollaire

L'image $\text{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ est un sous-groupe de H .

Le noyau $\text{ker}(\phi) = \phi^{-1}(e_H) = \{g \in G \mid \phi(g) = e_H\}$ est un sous-groupe de G .

Un morphisme de groupes $\phi: G \rightarrow H$ est surjectif ssi $\text{im}(\phi) = H$.

Pour l'injectivité nous avons le critère suivant :

Proposition

Un morphisme de groupes $\phi: G \rightarrow H$ est injectif ssi $\text{ker}(\phi) = \{e_G\}$.

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Corollaire

L'image $\text{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ est un sous-groupe de H .

Le noyau $\text{ker}(\phi) = \phi^{-1}(e_H) = \{g \in G \mid \phi(g) = e_H\}$ est un sous-groupe de G .

Un morphisme de groupes $\phi: G \rightarrow H$ est surjectif ssi $\text{im}(\phi) = H$.

Pour l'injectivité nous avons le critère suivant :

Proposition

Un morphisme de groupes $\phi: G \rightarrow H$ est injectif ssi $\text{ker}(\phi) = \{e_G\}$.

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Corollaire

L'image $\text{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ est un sous-groupe de H .

Le noyau $\text{ker}(\phi) = \phi^{-1}(e_H) = \{g \in G \mid \phi(g) = e_H\}$ est un sous-groupe de G .

Un morphisme de groupes $\phi: G \rightarrow H$ est surjectif ssi $\text{im}(\phi) = H$.

Pour l'injectivité nous avons le critère suivant :

Proposition

Un morphisme de groupes $\phi: G \rightarrow H$ est injectif ssi $\text{ker}(\phi) = \{e_G\}$.

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Corollaire

L'image $\text{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ est un sous-groupe de H .

Le noyau $\text{ker}(\phi) = \phi^{-1}(e_H) = \{g \in G \mid \phi(g) = e_H\}$ est un sous-groupe de G .

Un morphisme de groupes $\phi: G \rightarrow H$ est surjectif ssi $\text{im}(\phi) = H$.

Pour l'injectivité nous avons le critère suivant :

Proposition

Un morphisme de groupes $\phi: G \rightarrow H$ est injectif ssi $\text{ker}(\phi) = \{e_G\}$.

Proposition

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Si $G' \subset G$ est un sous-groupe, alors $\phi(G') \subset H$ est un sous-groupe.

Si $H' \subset H$ est un sous-groupe, alors $\phi^{-1}(H') \subset G$ est un sous-groupe.

Corollaire

L'image $\text{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ est un sous-groupe de H .

Le noyau $\text{ker}(\phi) = \phi^{-1}(e_H) = \{g \in G \mid \phi(g) = e_H\}$ est un sous-groupe de G .

Un morphisme de groupes $\phi: G \rightarrow H$ est surjectif ssi $\text{im}(\phi) = H$.

Pour l'injectivité nous avons le critère suivant :

Proposition

Un morphisme de groupes $\phi: G \rightarrow H$ est injectif ssi $\text{ker}(\phi) = \{e_G\}$.

Exercice

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Exercice

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Soit \mathcal{X} l'ensemble des sous-groupes $F \subset G$ contenant $\ker(\phi)$.

Exercice

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Soit \mathcal{X} l'ensemble des sous-groupes $F \subset G$ contenant $\ker(\phi)$.

Soit \mathcal{Y} l'ensemble des sous-groupes $K \subset H$ contenus dans $\text{im}(\phi)$.

Exercice

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Soit \mathcal{X} l'ensemble des sous-groupes $F \subset G$ contenant $\ker(\phi)$.

Soit \mathcal{Y} l'ensemble des sous-groupes $K \subset H$ contenus dans $\text{im}(\phi)$.

Pour tout $F \in \mathcal{X}$ on a $\phi(F) \in \mathcal{Y}$, et pour tout $K \in \mathcal{Y}$ on a $\phi^{-1}(K) \in \mathcal{X}$.

Exercice

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Soit \mathcal{X} l'ensemble des sous-groupes $F \subset G$ contenant $\ker(\phi)$.

Soit \mathcal{Y} l'ensemble des sous-groupes $K \subset H$ contenus dans $\text{im}(\phi)$.

Pour tout $F \in \mathcal{X}$ on a $\phi(F) \in \mathcal{Y}$, et pour tout $K \in \mathcal{Y}$ on a $\phi^{-1}(K) \in \mathcal{X}$.

Les applications

$$\Phi: \mathcal{X} \rightarrow \mathcal{Y}, F \mapsto \phi(F), \quad \text{et} \quad \Psi: \mathcal{Y} \rightarrow \mathcal{X}, K \mapsto \phi^{-1}(K),$$

sont des bijections mutuellement inverses.

Exercice

Soit $\phi: G \rightarrow H$ un morphisme de groupes.

Soit \mathcal{X} l'ensemble des sous-groupes $F \subset G$ contenant $\ker(\phi)$.

Soit \mathcal{Y} l'ensemble des sous-groupes $K \subset H$ contenus dans $\text{im}(\phi)$.

Pour tout $F \in \mathcal{X}$ on a $\phi(F) \in \mathcal{Y}$, et pour tout $K \in \mathcal{Y}$ on a $\phi^{-1}(K) \in \mathcal{X}$.

Les applications

$$\Phi: \mathcal{X} \rightarrow \mathcal{Y}, F \mapsto \phi(F), \quad \text{et} \quad \Psi: \mathcal{Y} \rightarrow \mathcal{X}, K \mapsto \phi^{-1}(K),$$

sont des bijections mutuellement inverses.

Exercice

A quelle condition sur $m, n \in \mathbb{Z}$ a-t-on l'inclusion $m\mathbb{Z} \subset n\mathbb{Z}$?

Expliciter les sous-groupes de $\mathbb{Z}/_{11}$, puis de $\mathbb{Z}/_{12}$, et leurs inclusions.

Plus généralement, décrire les sous-groupes de $\mathbb{Z}/_m$ en fonction de m .

Proposition

Si G est un groupe et $H_i \subset G$ est un sous-groupe pour tout $i \in I$,

Proposition

Si G est un groupe et $H_i \subset G$ est un sous-groupe pour tout $i \in I$, alors leur intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Proposition

Si G est un groupe et $H_i \subset G$ est un sous-groupe pour tout $i \in I$, alors leur intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition

Soit G un groupe et soit $S \subset G$ une partie quelconque.

Proposition

Si G est un groupe et $H_i \subset G$ est un sous-groupe pour tout $i \in I$, alors leur intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition

Soit G un groupe et soit $S \subset G$ une partie quelconque.

On note $\langle S \rangle$ l'intersection des sous-groupes $H \subset G$ contenant S :

Proposition

Si G est un groupe et $H_i \subset G$ est un sous-groupe pour tout $i \in I$, alors leur intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition

Soit G un groupe et soit $S \subset G$ une partie quelconque.

On note $\langle S \rangle$ l'intersection des sous-groupes $H \subset G$ contenant S : c'est le plus petit sous-groupe contenant S , appelé *sous-groupe engendré* par S .

Proposition

Si G est un groupe et $H_i \subset G$ est un sous-groupe pour tout $i \in I$, alors leur intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition

Soit G un groupe et soit $S \subset G$ une partie quelconque. On note $\langle S \rangle$ l'intersection des sous-groupes $H \subset G$ contenant S : c'est le plus petit sous-groupe contenant S , appelé *sous-groupe engendré* par S .

Proposition

On a $\langle S \rangle = \{s_1^{k_1} \cdots s_\ell^{k_\ell} \mid \ell \geq 0; s_1, \dots, s_\ell \in S; k_1, \dots, k_\ell \in \mathbb{Z}\}$.

Proposition

Si G est un groupe et $H_i \subset G$ est un sous-groupe pour tout $i \in I$, alors leur intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition

Soit G un groupe et soit $S \subset G$ une partie quelconque. On note $\langle S \rangle$ l'intersection des sous-groupes $H \subset G$ contenant S : c'est le plus petit sous-groupe contenant S , appelé *sous-groupe engendré* par S .

Proposition

On a $\langle S \rangle = \{s_1^{k_1} \cdots s_\ell^{k_\ell} \mid \ell \geq 0; s_1, \dots, s_\ell \in S; k_1, \dots, k_\ell \in \mathbb{Z}\}$.

Démonstration.

On a « \supset » car tout sous-groupe contenant S contient aussi $s_1^{k_1} \cdots s_\ell^{k_\ell}$.

Proposition

Si G est un groupe et $H_i \subset G$ est un sous-groupe pour tout $i \in I$, alors leur intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition

Soit G un groupe et soit $S \subset G$ une partie quelconque. On note $\langle S \rangle$ l'intersection des sous-groupes $H \subset G$ contenant S : c'est le plus petit sous-groupe contenant S , appelé *sous-groupe engendré* par S .

Proposition

On a $\langle S \rangle = \{s_1^{k_1} \cdots s_\ell^{k_\ell} \mid \ell \geq 0; s_1, \dots, s_\ell \in S; k_1, \dots, k_\ell \in \mathbb{Z}\}$.

Démonstration.

On a « \supset » car tout sous-groupe contenant S contient aussi $s_1^{k_1} \cdots s_\ell^{k_\ell}$.

On a « \subset » car l'ensemble à droite est un sous-groupe de G contenant S . \square

Sous-groupes engendrés

Proposition

Si G est un groupe et $H_i \subset G$ est un sous-groupe pour tout $i \in I$, alors leur intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition

Soit G un groupe et soit $S \subset G$ une partie quelconque. On note $\langle S \rangle$ l'intersection des sous-groupes $H \subset G$ contenant S : c'est le plus petit sous-groupe contenant S , appelé *sous-groupe engendré* par S .

Proposition

On a $\langle S \rangle = \{s_1^{k_1} \cdots s_\ell^{k_\ell} \mid \ell \geq 0; s_1, \dots, s_\ell \in S; k_1, \dots, k_\ell \in \mathbb{Z}\}$.

Démonstration.

On a « \supset » car tout sous-groupe contenant S contient aussi $s_1^{k_1} \cdots s_\ell^{k_\ell}$.

On a « \subset » car l'ensemble à droite est un sous-groupe de G contenant S . \square

Notation

Si $S = \{g_1, \dots, g_n\}$, alors on note $\langle S \rangle$ par $\langle g_1, \dots, g_n \rangle$.

Sous-groupes engendrés

Proposition

Si G est un groupe et $H_i \subset G$ est un sous-groupe pour tout $i \in I$, alors leur intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de G .

Définition

Soit G un groupe et soit $S \subset G$ une partie quelconque. On note $\langle S \rangle$ l'intersection des sous-groupes $H \subset G$ contenant S : c'est le plus petit sous-groupe contenant S , appelé *sous-groupe engendré* par S .

Proposition

On a $\langle S \rangle = \{s_1^{k_1} \cdots s_\ell^{k_\ell} \mid \ell \geq 0; s_1, \dots, s_\ell \in S; k_1, \dots, k_\ell \in \mathbb{Z}\}$.

Démonstration.

On a « \supset » car tout sous-groupe contenant S contient aussi $s_1^{k_1} \cdots s_\ell^{k_\ell}$.

On a « \subset » car l'ensemble à droite est un sous-groupe de G contenant S . \square

Notation

Si $S = \{g_1, \dots, g_n\}$, alors on note $\langle S \rangle$ par $\langle g_1, \dots, g_n \rangle$.

En particulier, si $S = \{g\}$, alors $\langle S \rangle = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.

Définition

Si $G = \langle S \rangle$, on dit que S est une *partie génératrice* de G .

Définition

Si $G = \langle S \rangle$, on dit que S est une *partie génératrice* de G .

Un groupe est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Définition

Si $G = \langle S \rangle$, on dit que S est une *partie génératrice* de G .

Un groupe est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Dans ce cas on appelle g un *générateur* de G .

Définition

Si $G = \langle S \rangle$, on dit que S est une *partie génératrice* de G .

Un groupe est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Dans ce cas on appelle g un *générateur* de G .

Un groupe monogène fini est dit *cyclique*.

Définition

Si $G = \langle S \rangle$, on dit que S est une *partie génératrice* de G .

Un groupe est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Dans ce cas on appelle g un *générateur* de G .

Un groupe monogène fini est dit *cyclique*.

Exemples

Le groupe $(\mathbb{Z}, +)$ est monogène, engendré par 1, et aussi par -1 .

Définition

Si $G = \langle S \rangle$, on dit que S est une *partie génératrice* de G .

Un groupe est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Dans ce cas on appelle g un *générateur* de G .

Un groupe monogène fini est dit *cyclique*.

Exemples

Le groupe $(\mathbb{Z}, +)$ est monogène, engendré par 1, et aussi par -1 .

Le groupe $(\mathbb{Z}/m, +)$ est monogène, engendré par $\bar{1}$, et cyclique ssi $m \neq 0$.

Définition

Si $G = \langle S \rangle$, on dit que S est une *partie génératrice* de G .

Un groupe est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Dans ce cas on appelle g un *générateur* de G .

Un groupe monogène fini est dit *cyclique*.

Exemples

Le groupe $(\mathbb{Z}, +)$ est monogène, engendré par 1, et aussi par -1 .

Le groupe $(\mathbb{Z}/m, +)$ est monogène, engendré par $\bar{1}$, et cyclique ssi $m \neq 0$.

Exercice

Dans \mathbb{Z} expliciter $\langle 7, 20 \rangle$ sous forme $m\mathbb{Z}$. Même question pour $\langle 9, 15 \rangle$.

Définition

Si $G = \langle S \rangle$, on dit que S est une *partie génératrice* de G .

Un groupe est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Dans ce cas on appelle g un *générateur* de G .

Un groupe monogène fini est dit *cyclique*.

Exemples

Le groupe $(\mathbb{Z}, +)$ est monogène, engendré par 1, et aussi par -1 .

Le groupe $(\mathbb{Z}/m, +)$ est monogène, engendré par $\bar{1}$, et cyclique ssi $m \neq 0$.

Exercice

Dans \mathbb{Z} expliciter $\langle 7, 20 \rangle$ sous forme $m\mathbb{Z}$. Même question pour $\langle 9, 15 \rangle$.

Pour $m_1, \dots, m_k \in \mathbb{Z}$ déterminer $m \in \mathbb{Z}$ tel que $\langle m_1, \dots, m_k \rangle = m\mathbb{Z}$.

Définition

Si $G = \langle S \rangle$, on dit que S est une *partie génératrice* de G .

Un groupe est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Dans ce cas on appelle g un *générateur* de G .

Un groupe monogène fini est dit *cyclique*.

Exemples

Le groupe $(\mathbb{Z}, +)$ est monogène, engendré par 1, et aussi par -1 .

Le groupe $(\mathbb{Z}/m, +)$ est monogène, engendré par $\bar{1}$, et cyclique ssi $m \neq 0$.

Exercice

Dans \mathbb{Z} expliciter $\langle 7, 20 \rangle$ sous forme $m\mathbb{Z}$. Même question pour $\langle 9, 15 \rangle$.

Pour $m_1, \dots, m_k \in \mathbb{Z}$ déterminer $m \in \mathbb{Z}$ tel que $\langle m_1, \dots, m_k \rangle = m\mathbb{Z}$.

Exercice

Identifier les générateurs de $\mathbb{Z}/_{12}$, puis de $\mathbb{Z}/_m$ pour $m \geq 1$.

Définition

Si $G = \langle S \rangle$, on dit que S est une *partie génératrice* de G .

Un groupe est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$.

Dans ce cas on appelle g un *générateur* de G .

Un groupe monogène fini est dit *cyclique*.

Exemples

Le groupe $(\mathbb{Z}, +)$ est monogène, engendré par 1, et aussi par -1 .

Le groupe $(\mathbb{Z}/m, +)$ est monogène, engendré par $\bar{1}$, et cyclique ssi $m \neq 0$.

Exercice

Dans \mathbb{Z} expliciter $\langle 7, 20 \rangle$ sous forme $m\mathbb{Z}$. Même question pour $\langle 9, 15 \rangle$.

Pour $m_1, \dots, m_k \in \mathbb{Z}$ déterminer $m \in \mathbb{Z}$ tel que $\langle m_1, \dots, m_k \rangle = m\mathbb{Z}$.

Exercice

Identifier les générateurs de $\mathbb{Z}/12$, puis de \mathbb{Z}/m pour $m \geq 1$.

Est-ce que $\mathbb{Z}/2 \times \mathbb{Z}/2$ est cyclique ? et $\mathbb{Z}/2 \times \mathbb{Z}/3$?

Définition

L'ordre d'un groupe G est le cardinal $|G| = \text{ord}(G) = \text{card}(G) = \#G$.

Définition

L'ordre d'un groupe G est le cardinal $|G| = \text{ord}(G) = \text{card}(G) = \#G$.

L'ordre d'un élément $g \in G$ est l'ordre du groupe engendré $\langle g \rangle$.

Définition

L'ordre d'un groupe G est le cardinal $|G| = \text{ord}(G) = \text{card}(G) = \#G$.

L'ordre d'un élément $g \in G$ est l'ordre du groupe engendré $\langle g \rangle$.

Proposition

Pour tout $g \in G$ le morphisme $\phi: \mathbb{Z} \rightarrow \langle g \rangle$ donné par $k \mapsto g^k$ est surjectif.

Définition

L'ordre d'un groupe G est le cardinal $|G| = \text{ord}(G) = \text{card}(G) = \#G$.

L'ordre d'un élément $g \in G$ est l'ordre du groupe engendré $\langle g \rangle$.

Proposition

Pour tout $g \in G$ le morphisme $\phi: \mathbb{Z} \rightarrow \langle g \rangle$ donné par $k \mapsto g^k$ est surjectif.

Nous avons $\ker(\phi) = m\mathbb{Z}$ et ϕ induit un isomorphisme $\bar{\phi}: \mathbb{Z}/m \xrightarrow{\sim} \langle g \rangle$.

Définition

L'ordre d'un groupe G est le cardinal $|G| = \text{ord}(G) = \text{card}(G) = \#G$.

L'ordre d'un élément $g \in G$ est l'ordre du groupe engendré $\langle g \rangle$.

Proposition

Pour tout $g \in G$ le morphisme $\phi: \mathbb{Z} \rightarrow \langle g \rangle$ donné par $k \mapsto g^k$ est surjectif.

Nous avons $\ker(\phi) = m\mathbb{Z}$ et ϕ induit un isomorphisme $\bar{\phi}: \mathbb{Z}/m \xrightarrow{\sim} \langle g \rangle$.

- Si $\ker(\phi) = \{0\}$, alors $\phi: \mathbb{Z} \xrightarrow{\sim} \langle g \rangle$ et $\text{ord}(g) = \infty$.

Définition

L'ordre d'un groupe G est le cardinal $|G| = \text{ord}(G) = \text{card}(G) = \#G$.

L'ordre d'un élément $g \in G$ est l'ordre du groupe engendré $\langle g \rangle$.

Proposition

Pour tout $g \in G$ le morphisme $\phi: \mathbb{Z} \rightarrow \langle g \rangle$ donné par $k \mapsto g^k$ est surjectif.

Nous avons $\ker(\phi) = m\mathbb{Z}$ et ϕ induit un isomorphisme $\bar{\phi}: \mathbb{Z}/m \xrightarrow{\sim} \langle g \rangle$.

- Si $\ker(\phi) = \{0\}$, alors $\phi: \mathbb{Z} \xrightarrow{\sim} \langle g \rangle$ et $\text{ord}(g) = \infty$.
- Si $\ker(\phi) = m\mathbb{Z}$ où $m \geq 1$, alors $\bar{\phi}: \mathbb{Z}/m \xrightarrow{\sim} \langle g \rangle$ et $\text{ord}(g) = m$.
Ainsi, pour tout $k \in \mathbb{Z}$, on a $g^k = e$ si et seulement si $\text{ord}(g) \mid k$.

Exercice

Prouver un critère nécessaire et suffisant pour que $\mathbb{Z}/m \times \mathbb{Z}/n$ soit monogène.

Exemples de groupes cycliques

Exercice

Prouver un critère nécessaire et suffisant pour que $\mathbb{Z}/m \times \mathbb{Z}/n$ soit monogène.

Exercice

Expliciter les groupes $\mathbb{Z}/2^\times, \mathbb{Z}/3^\times, \mathbb{Z}/4^\times, \dots, \mathbb{Z}/16^\times$. Lesquels sont cycliques ?

Exemples de groupes cycliques

Exercice

Prouver un critère nécessaire et suffisant pour que $\mathbb{Z}/m \times \mathbb{Z}/n$ soit monogène.

Exercice

Expliciter les groupes $\mathbb{Z}/2^\times, \mathbb{Z}/3^\times, \mathbb{Z}/4^\times, \dots, \mathbb{Z}/16^\times$. Lesquels sont cycliques ?

Théorème (structure du groupe multiplicatif \mathbb{Z}/n^\times)

Si $p \in \mathbb{N}$ est premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$.

Exercice

Prouver un critère nécessaire et suffisant pour que $\mathbb{Z}/m \times \mathbb{Z}/n$ soit monogène.

Exercice

Expliciter les groupes $\mathbb{Z}/2^\times, \mathbb{Z}/3^\times, \mathbb{Z}/4^\times, \dots, \mathbb{Z}/16^\times$. Lesquels sont cycliques ?

Théorème (structure du groupe multiplicatif \mathbb{Z}/n^\times)

Si $p \in \mathbb{N}$ est premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$.

Si $p \in \mathbb{N}$ est premier impair, alors $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique d'ordre $(p - 1)p^{k-1}$.

Exercice

Prouver un critère nécessaire et suffisant pour que $\mathbb{Z}/m \times \mathbb{Z}/n$ soit monogène.

Exercice

Expliciter les groupes $\mathbb{Z}/2^\times, \mathbb{Z}/3^\times, \mathbb{Z}/4^\times, \dots, \mathbb{Z}/16^\times$. Lesquels sont cycliques ?

Théorème (structure du groupe multiplicatif \mathbb{Z}/n^\times)

Si $p \in \mathbb{N}$ est premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$.

Si $p \in \mathbb{N}$ est premier impair, alors $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique d'ordre $(p - 1)p^{k-1}$.

Le nombre premier 2 est particulier :

Exercice

Prouver un critère nécessaire et suffisant pour que $\mathbb{Z}/m \times \mathbb{Z}/n$ soit monogène.

Exercice

Expliciter les groupes $\mathbb{Z}/2^\times, \mathbb{Z}/3^\times, \mathbb{Z}/4^\times, \dots, \mathbb{Z}/16^\times$. Lesquels sont cycliques ?

Théorème (structure du groupe multiplicatif \mathbb{Z}/n^\times)

Si $p \in \mathbb{N}$ est premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$.

Si $p \in \mathbb{N}$ est premier impair, alors $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique d'ordre $(p - 1)p^{k-1}$.

Le nombre premier 2 est particulier :

- *Le groupe $(\mathbb{Z}/2\mathbb{Z})^\times$ est trivial.*

Exemples de groupes cycliques

Exercice

Prouver un critère nécessaire et suffisant pour que $\mathbb{Z}/m \times \mathbb{Z}/n$ soit monogène.

Exercice

Expliciter les groupes $\mathbb{Z}/2^\times, \mathbb{Z}/3^\times, \mathbb{Z}/4^\times, \dots, \mathbb{Z}/16^\times$. Lesquels sont cycliques ?

Théorème (structure du groupe multiplicatif \mathbb{Z}/n^\times)

Si $p \in \mathbb{N}$ est premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$.

Si $p \in \mathbb{N}$ est premier impair, alors $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique d'ordre $(p - 1)p^{k-1}$.

Le nombre premier 2 est particulier :

- *Le groupe $(\mathbb{Z}/2\mathbb{Z})^\times$ est trivial.*
- *Le groupe $(\mathbb{Z}/4\mathbb{Z})^\times$ est cyclique d'ordre 2.*

Exemples de groupes cycliques

Exercice

Prouver un critère nécessaire et suffisant pour que $\mathbb{Z}/m \times \mathbb{Z}/n$ soit monogène.

Exercice

Expliciter les groupes $\mathbb{Z}/2^\times, \mathbb{Z}/3^\times, \mathbb{Z}/4^\times, \dots, \mathbb{Z}/16^\times$. Lesquels sont cycliques ?

Théorème (structure du groupe multiplicatif \mathbb{Z}/n^\times)

Si $p \in \mathbb{N}$ est premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$.

Si $p \in \mathbb{N}$ est premier impair, alors $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique d'ordre $(p - 1)p^{k-1}$.

Le nombre premier 2 est particulier :

- *Le groupe $(\mathbb{Z}/2\mathbb{Z})^\times$ est trivial.*
- *Le groupe $(\mathbb{Z}/4\mathbb{Z})^\times$ est cyclique d'ordre 2.*
- *Pour $k \geq 3$ le groupe $(\mathbb{Z}/2^k\mathbb{Z})^\times = \langle -\bar{1} \rangle \times \langle \bar{5} \rangle$ est le produit direct d'un groupe d'ordre 2 et d'un groupe d'ordre 2^{k-2} et donc pas cyclique.*

Exemples de groupes cycliques

Exercice

Prouver un critère nécessaire et suffisant pour que $\mathbb{Z}/m \times \mathbb{Z}/n$ soit monogène.

Exercice

Expliciter les groupes $\mathbb{Z}/2^\times, \mathbb{Z}/3^\times, \mathbb{Z}/4^\times, \dots, \mathbb{Z}/16^\times$. Lesquels sont cycliques ?

Théorème (structure du groupe multiplicatif \mathbb{Z}/n^\times)

Si $p \in \mathbb{N}$ est premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p - 1$.

Si $p \in \mathbb{N}$ est premier impair, alors $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique d'ordre $(p - 1)p^{k-1}$.

Le nombre premier 2 est particulier :

- *Le groupe $(\mathbb{Z}/2\mathbb{Z})^\times$ est trivial.*
- *Le groupe $(\mathbb{Z}/4\mathbb{Z})^\times$ est cyclique d'ordre 2.*
- *Pour $k \geq 3$ le groupe $(\mathbb{Z}/2^k\mathbb{Z})^\times = \langle -\bar{1} \rangle \times \langle \bar{5} \rangle$ est le produit direct d'un groupe d'ordre 2 et d'un groupe d'ordre 2^{k-2} et donc pas cyclique.*

Démonstration. Plus tard. Elle n'est pas constructive !



Application : un certificat de primalité

On considère $p = 2^{32} \cdot 3^{32} \cdot 5^{32} + 1$ et l'élément $g = \bar{2}$ dans \mathbb{Z}/p .

Application : un certificat de primalité

On considère $p = 2^{32} \cdot 3^{32} \cdot 5^{32} + 1$ et l'élément $g = \bar{2}$ dans \mathbb{Z}/p .

On pose $n = p - 1$ puis on effectue / vérifie les calculs suivants :

$$g^n = \bar{1}, \quad g^{n/2} \neq \bar{1}, \quad g^{n/3} \neq \bar{1}, \quad g^{n/5} \neq \bar{1}.$$

Application : un certificat de primalité

On considère $p = 2^{32} \cdot 3^{32} \cdot 5^{32} + 1$ et l'élément $g = \bar{2}$ dans \mathbb{Z}/p .

On pose $n = p - 1$ puis on effectue / vérifie les calculs suivants :

$$g^n = \bar{1}, \quad g^{n/2} \neq \bar{1}, \quad g^{n/3} \neq \bar{1}, \quad g^{n/5} \neq \bar{1}.$$

Exercice

Le nombre p est-il premier ? L'élément g est-il générateur de \mathbb{Z}/p^\times ?

Application : un certificat de primalité

On considère $p = 2^{32} \cdot 3^{32} \cdot 5^{32} + 1$ et l'élément $g = \bar{2}$ dans \mathbb{Z}/p .
On pose $n = p - 1$ puis on effectue / vérifie les calculs suivants :

$$g^n = \bar{1}, \quad g^{n/2} \neq \bar{1}, \quad g^{n/3} \neq \bar{1}, \quad g^{n/5} \neq \bar{1}.$$

Exercice

Le nombre p est-il premier ? L'élément g est-il générateur de \mathbb{Z}/p^\times ?

À noter que $10^{47} < p < 10^{48}$. Comment prouver sa primalité ?

Application : un certificat de primalité

On considère $p = 2^{32} \cdot 3^{32} \cdot 5^{32} + 1$ et l'élément $g = \bar{2}$ dans \mathbb{Z}/p .
On pose $n = p - 1$ puis on effectue / vérifie les calculs suivants :

$$g^n = \bar{1}, \quad g^{n/2} \neq \bar{1}, \quad g^{n/3} \neq \bar{1}, \quad g^{n/5} \neq \bar{1}.$$

Exercice

Le nombre p est-il premier ? L'élément g est-il générateur de \mathbb{Z}/p^\times ?

À noter que $10^{47} < p < 10^{48}$. Comment prouver sa primalité ?
Des tests exhaustifs pour $d = 2, \dots, \sqrt{p}$ sont hors de question !

Définition

Un *certificat de primalité* pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \dots, p_\ell, e_\ell; g)$ tels que

Définition

Un *certificat de primalité* pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \dots, p_\ell, e_\ell; g)$ tels que

- On a la factorisation $p - 1 = p_1^{e_1} \cdots p_\ell^{e_\ell}$.

Définition

Un *certificat de primalité* pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \dots, p_\ell, e_\ell; g)$ tels que

- On a la factorisation $p - 1 = p_1^{e_1} \cdots p_\ell^{e_\ell}$.
- Les $p_1 < \cdots < p_\ell$ sont premiers (certifiés à leur tour).

Définition

Un *certificat de primalité* pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \dots, p_\ell, e_\ell; g)$ tels que

- On a la factorisation $p - 1 = p_1^{e_1} \cdots p_\ell^{e_\ell}$.
- Les $p_1 < \cdots < p_\ell$ sont premiers (certifiés à leur tour).
- L'élément \bar{g} est d'ordre $p - 1$ dans \mathbb{Z}/p^\times ,

Définition

Un *certificat de primalité* pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \dots, p_\ell, e_\ell; g)$ tels que

- On a la factorisation $p - 1 = p_1^{e_1} \cdots p_\ell^{e_\ell}$.
- Les $p_1 < \cdots < p_\ell$ sont premiers (certifiés à leur tour).
- L'élément \bar{g} est d'ordre $p - 1$ dans \mathbb{Z}/p^\times , c'est-à-dire :
on a $\bar{g}^{p-1} = \bar{1}$ mais $\bar{g}^{(p-1)/p_k} \neq \bar{1}$ pour tout $k = 1, \dots, \ell$

Définition

Un *certificat de primalité* pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \dots, p_\ell, e_\ell; g)$ tels que

- On a la factorisation $p - 1 = p_1^{e_1} \cdots p_\ell^{e_\ell}$.
- Les $p_1 < \cdots < p_\ell$ sont premiers (certifiés à leur tour).
- L'élément \bar{g} est d'ordre $p - 1$ dans \mathbb{Z}/p^\times , c'est-à-dire :
on a $\bar{g}^{p-1} = \bar{1}$ mais $\bar{g}^{(p-1)/p_k} \neq \bar{1}$ pour tout $k = 1, \dots, \ell$

Proposition

Un nombre p est premier si et seulement s'il admet de tels certificats.

Définition

Un *certificat de primalité* pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \dots, p_\ell, e_\ell; g)$ tels que

- On a la factorisation $p - 1 = p_1^{e_1} \cdots p_\ell^{e_\ell}$.
- Les $p_1 < \cdots < p_\ell$ sont premiers (certifiés à leur tour).
- L'élément \bar{g} est d'ordre $p - 1$ dans \mathbb{Z}/p^\times , c'est-à-dire :
on a $\bar{g}^{p-1} = \bar{1}$ mais $\bar{g}^{(p-1)/p_k} \neq \bar{1}$ pour tout $k = 1, \dots, \ell$

Proposition

Un nombre p est premier si et seulement s'il admet de tels certificats.

La *vérification* d'un certificat est facile — avec la puissance modulaire rapide !

Définition

Un *certificat de primalité* pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \dots, p_\ell, e_\ell; g)$ tels que

- On a la factorisation $p - 1 = p_1^{e_1} \cdots p_\ell^{e_\ell}$.
- Les $p_1 < \cdots < p_\ell$ sont premiers (certifiés à leur tour).
- L'élément \bar{g} est d'ordre $p - 1$ dans \mathbb{Z}/p^\times , c'est-à-dire :
on a $\bar{g}^{p-1} = \bar{1}$ mais $\bar{g}^{(p-1)/p_k} \neq \bar{1}$ pour tout $k = 1, \dots, \ell$

Proposition

Un nombre p est premier si et seulement s'il admet de tels certificats.

La *vérification* d'un certificat est facile — avec la puissance modulaire rapide !

La *construction* d'un certificat est moins facile — cela dépend de p :

Définition

Un *certificat de primalité* pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \dots, p_\ell, e_\ell; g)$ tels que

- On a la factorisation $p - 1 = p_1^{e_1} \cdots p_\ell^{e_\ell}$.
- Les $p_1 < \cdots < p_\ell$ sont premiers (certifiés à leur tour).
- L'élément \bar{g} est d'ordre $p - 1$ dans \mathbb{Z}/p^\times , c'est-à-dire :
on a $\bar{g}^{p-1} = \bar{1}$ mais $\bar{g}^{(p-1)/p_k} \neq \bar{1}$ pour tout $k = 1, \dots, \ell$

Proposition

Un nombre p est premier si et seulement s'il admet de tels certificats.

La *vérification* d'un certificat est facile — avec la puissance modulaire rapide !

La *construction* d'un certificat est moins facile — cela dépend de p :

- Il faut factoriser $p - 1$: c'est faisable quand on *construit* p au choix.

Définition

Un *certificat de primalité* pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \dots, p_\ell, e_\ell; g)$ tels que

- On a la factorisation $p - 1 = p_1^{e_1} \cdots p_\ell^{e_\ell}$.
- Les $p_1 < \cdots < p_\ell$ sont premiers (certifiés à leur tour).
- L'élément \bar{g} est d'ordre $p - 1$ dans \mathbb{Z}/p^\times , c'est-à-dire :
on a $\bar{g}^{p-1} = \bar{1}$ mais $\bar{g}^{(p-1)/p_k} \neq \bar{1}$ pour tout $k = 1, \dots, \ell$

Proposition

Un nombre p est premier si et seulement s'il admet de tels certificats.

La *vérification* d'un certificat est facile — avec la puissance modulaire rapide !

La *construction* d'un certificat est moins facile — cela dépend de p :

- Il faut factoriser $p - 1$: c'est faisable quand on *construit* p au choix.
- Il faut trouver un générateur $\bar{g} \in \mathbb{Z}/p$: heureusement il y en a assez.

- 1 Groupes
- 2 Applications en cryptographie**
 - Le problème du logarithme discret (DLP)
 - Le protocole Diffie–Hellman
 - Le protocole Elgamal
- 3 Le théorème de Lagrange et applications
- 4 Groupes quotients dans le cas commutatif
- 5 Exercices

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Il n'y a pas unicité : a est n'est déterminé que modulo $\text{ord}(g)$.

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Il n'y a pas unicité : a est n'est déterminé que modulo $\text{ord}(g)$.

Le logarithme discret peut être facile à calculer. —

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Il n'y a pas unicité : a est n'est déterminé que modulo $\text{ord}(g)$.

Le logarithme discret peut être facile à calculer. —

Exemple : trouver un log discret de 645 à base 1 dans $(\mathbb{Z}, +)$.

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Il n'y a pas unicité : a est n'est déterminé que modulo $\text{ord}(g)$.

Le logarithme discret peut être facile à calculer. —

Exemple : trouver un log discret de 645 à base 1 dans $(\mathbb{Z}, +)$.

Dans d'autre cas c'est moins facile. —

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Il n'y a pas unicité : a est n'est déterminé que modulo $\text{ord}(g)$.

Le logarithme discret peut être facile à calculer. —

Exemple : trouver un log discret de 645 à base 1 dans $(\mathbb{Z}, +)$.

Dans d'autre cas c'est moins facile. —

Exemple : trouver un log discret de 9 à base 2 dans $(\mathbb{Z}/_{11}^{\times}, \cdot)$.

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Il n'y a pas unicité : a est n'est déterminé que modulo $\text{ord}(g)$.

Le logarithme discret peut être facile à calculer. —

Exemple : trouver un log discret de 645 à base 1 dans $(\mathbb{Z}, +)$.

Dans d'autre cas c'est moins facile. —

Exemple : trouver un log discret de 9 à base 2 dans $(\mathbb{Z}/_{11}^{\times}, \cdot)$.

Tester si $g^k = x$ pour $k = 0, 1, 2, 3, \dots$ est trop coûteux en général.

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Il n'y a pas unicité : a est n'est déterminé que modulo $\text{ord}(g)$.

Le logarithme discret peut être facile à calculer. —

Exemple : trouver un log discret de 645 à base 1 dans $(\mathbb{Z}, +)$.

Dans d'autre cas c'est moins facile. —

Exemple : trouver un log discret de 9 à base 2 dans $(\mathbb{Z}/_{11}^{\times}, \cdot)$.

Tester si $g^k = x$ pour $k = 0, 1, 2, 3, \dots$ est trop coûteux en général.

Par contre, étant donné g et a il est facile à calculer g^a .

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Il n'y a pas unicité : a est n'est déterminé que modulo $\text{ord}(g)$.

Le logarithme discret peut être facile à calculer. —

Exemple : trouver un log discret de 645 à base 1 dans $(\mathbb{Z}, +)$.

Dans d'autre cas c'est moins facile. —

Exemple : trouver un log discret de 9 à base 2 dans $(\mathbb{Z}/_{11}^{\times}, \cdot)$.

Tester si $g^k = x$ pour $k = 0, 1, 2, 3, \dots$ est trop coûteux en général.

Par contre, étant donné g et a il est facile à calculer g^a .

Slogan

La cryptographie repose sur des fonctions $f: X \rightarrow Y$ à «sens unique» :

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Il n'y a pas unicité : a est n'est déterminé que modulo $\text{ord}(g)$.

Le logarithme discret peut être facile à calculer. —

Exemple : trouver un log discret de 645 à base 1 dans $(\mathbb{Z}, +)$.

Dans d'autre cas c'est moins facile. —

Exemple : trouver un log discret de 9 à base 2 dans $(\mathbb{Z}/_{11}^{\times}, \cdot)$.

Tester si $g^k = x$ pour $k = 0, 1, 2, 3, \dots$ est trop coûteux en général.

Par contre, étant donné g et a il est facile à calculer g^a .

Slogan

La cryptographie repose sur des fonctions $f: X \rightarrow Y$ à «sens unique» :

- 1 Étant donné $x \in X$ il est facile à calculer $y = f(x)$.

Le problème du logarithme discret (DLP)

Soit G un groupe, soit $g \in G$, et soit $x \in \langle g \rangle$.

Définition

Un *logarithme discret* de x à base g est un entier $a \in \mathbb{Z}$ tel que $g^a = x$.

Il n'y a pas unicité : a est n'est déterminé que modulo $\text{ord}(g)$.

Le logarithme discret peut être facile à calculer. —

Exemple : trouver un log discret de 645 à base 1 dans $(\mathbb{Z}, +)$.

Dans d'autre cas c'est moins facile. —

Exemple : trouver un log discret de 9 à base 2 dans $(\mathbb{Z}/_{11}^{\times}, \cdot)$.

Tester si $g^k = x$ pour $k = 0, 1, 2, 3, \dots$ est trop coûteux en général.

Par contre, étant donné g et a il est facile à calculer g^a .

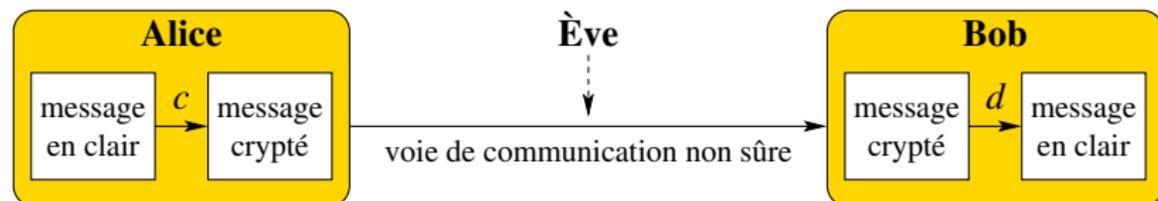
Slogan

La cryptographie repose sur des fonctions $f: X \rightarrow Y$ à «sens unique» :

- 1 Étant donné $x \in X$ il est facile à calculer $y = f(x)$.
- 2 Étant donné $y \in Y$ il est difficile à trouver $x \in X$ tel que $f(x) = y$.

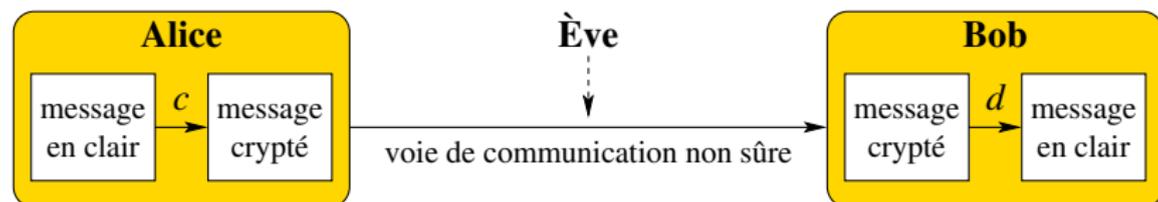
Le protocole Diffie–Hellman (1976)

Objectif : Alice et Bob veulent se mettre d'accord sur une clé commune.



Le protocole Diffie–Hellman (1976)

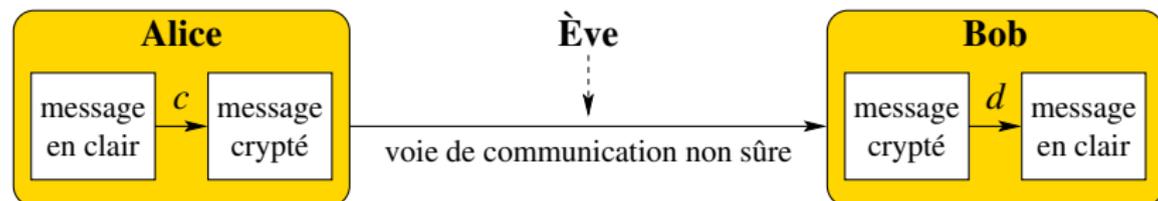
Objectif : Alice et Bob veulent se mettre d'accord sur une clé commune.



Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Le protocole Diffie–Hellman (1976)

Objectif : Alice et Bob veulent se mettre d'accord sur une clé commune.

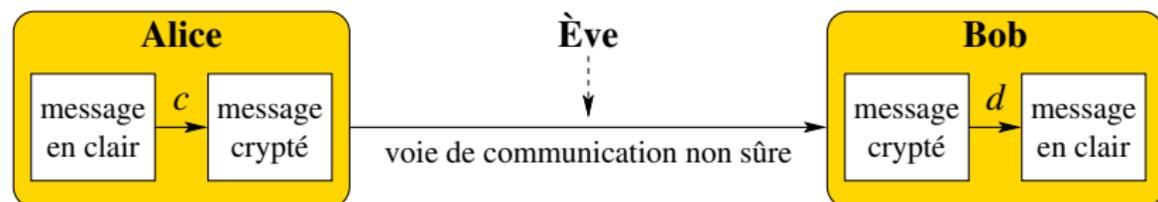


Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$ et transmet (G, g, x) à Bob.

Le protocole Diffie–Hellman (1976)

Objectif : Alice et Bob veulent se mettre d'accord sur une clé commune.

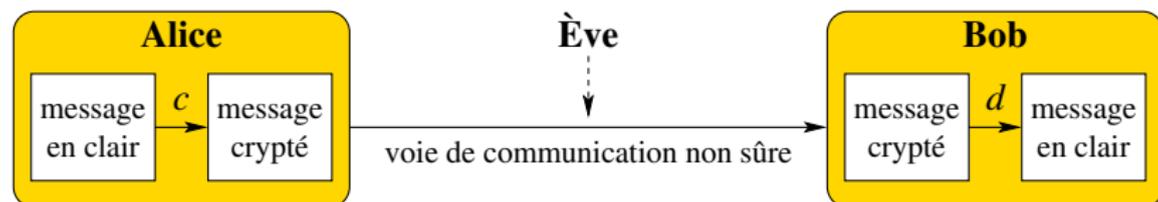


Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.
Elle calcule $x = g^a$ et transmet (G, g, x) à Bob.

Bob récupère (G, g, x) , il choisit un entier $b \in \mathbb{Z}$ et calcule $y = g^b$.

Le protocole Diffie–Hellman (1976)

Objectif : Alice et Bob veulent se mettre d'accord sur une clé commune.

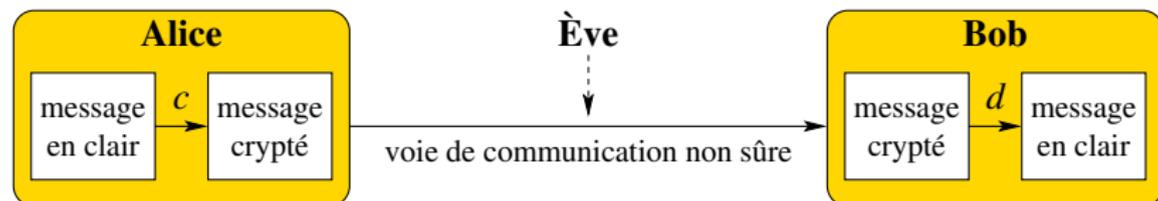


Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.
Elle calcule $x = g^a$ et transmet (G, g, x) à Bob.

Bob récupère (G, g, x) , il choisit un entier $b \in \mathbb{Z}$ et calcule $y = g^b$.
Il transmet y à Alice.

Le protocole Diffie–Hellman (1976)

Objectif : Alice et Bob veulent se mettre d'accord sur une clé commune.



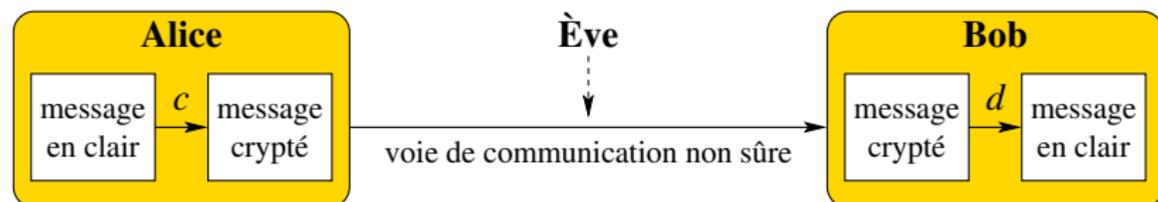
Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.
Elle calcule $x = g^a$ et transmet (G, g, x) à Bob.

Bob récupère (G, g, x) , il choisit un entier $b \in \mathbb{Z}$ et calcule $y = g^b$.
Il transmet y à Alice.

Clé commune :

Le protocole Diffie–Hellman (1976)

Objectif : Alice et Bob veulent se mettre d'accord sur une clé commune.



Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.
Elle calcule $x = g^a$ et transmet (G, g, x) à Bob.

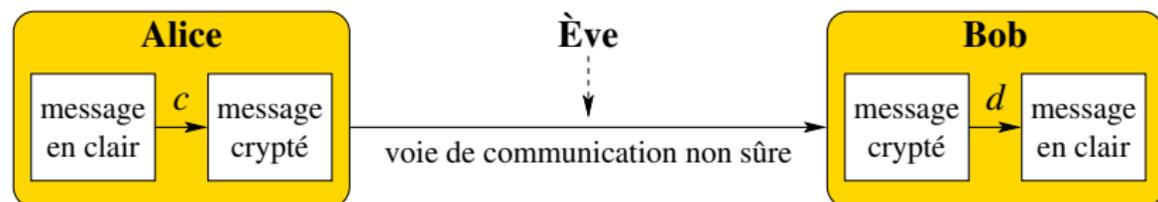
Bob récupère (G, g, x) , il choisit un entier $b \in \mathbb{Z}$ et calcule $y = g^b$.
Il transmet y à Alice.

Clé commune :

Alice connaît G, g, a, x, y et elle calcule $z = y^a = (g^b)^a = g^{ab}$.

Le protocole Diffie–Hellman (1976)

Objectif : Alice et Bob veulent se mettre d'accord sur une clé commune.



Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.
Elle calcule $x = g^a$ et transmet (G, g, x) à Bob.

Bob récupère (G, g, x) , il choisit un entier $b \in \mathbb{Z}$ et calcule $y = g^b$.
Il transmet y à Alice.

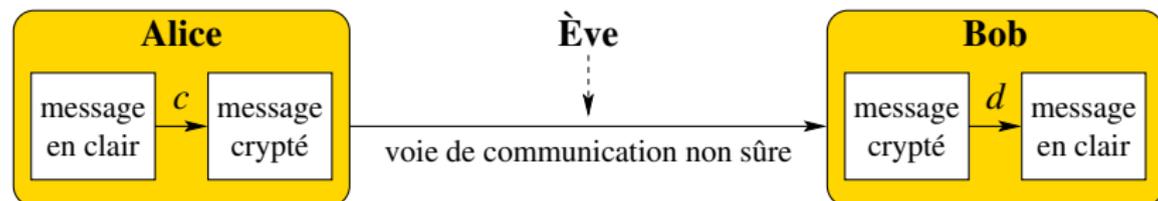
Clé commune :

Alice connaît G, g, a, x, y et elle calcule $z = y^a = (g^b)^a = g^{ab}$.

Bob connaît G, g, b, x, y et il calcule $z = x^b = (g^a)^b = g^{ab}$.

Le protocole Diffie–Hellman (1976)

Objectif : Alice et Bob veulent se mettre d'accord sur une clé commune.



Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.
Elle calcule $x = g^a$ et transmet (G, g, x) à Bob.

Bob récupère (G, g, x) , il choisit un entier $b \in \mathbb{Z}$ et calcule $y = g^b$.
Il transmet y à Alice.

Clé commune :

Alice connaît G, g, a, x, y et elle calcule $z = y^a = (g^b)^a = g^{ab}$.

Bob connaît G, g, b, x, y et il calcule $z = x^b = (g^a)^b = g^{ab}$.

La clé commune z n'a jamais transité le réseau !

La sécurité du protocole Diffie–Hellman repose sur certaines hypothèses :

La sécurité du protocole Diffie–Hellman repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .

La sécurité du protocole Diffie–Hellman repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver g^{ab} à partir de g, g^a, g^b .

La sécurité du protocole Diffie–Hellman repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver g^{ab} à partir de g, g^a, g^b .

Implémentations courantes :

La sécurité du protocole Diffie–Hellman repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver g^{ab} à partir de g, g^a, g^b .

Implémentations courantes :

- $G = (\mathbb{Z}/p^\times, \cdot)$ où p est un grand nombre premier (déjà discuté)

La sécurité du protocole Diffie–Hellman repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver g^{ab} à partir de g, g^a, g^b .

Implémentations courantes :

- $G = (\mathbb{Z}/p^\times, \cdot)$ où p est un grand nombre premier (déjà discuté)
- $G = (\mathbb{F}_q^\times, \cdot)$ où $q = p^n$ et p est un nombre premier (plus tard)

La sécurité du protocole Diffie–Hellman repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver g^{ab} à partir de g, g^a, g^b .

Implémentations courantes :

- $G = (\mathbb{Z}/p^\times, \cdot)$ où p est un grand nombre premier (déjà discuté)
- $G = (\mathbb{F}_q^\times, \cdot)$ où $q = p^n$ et p est un nombre premier (plus tard)
- $G = E(\mathbb{F}_q)$ une courbe elliptique (voir Master 2)

La sécurité du protocole Diffie–Hellman repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver g^{ab} à partir de g, g^a, g^b .

Implémentations courantes :

- $G = (\mathbb{Z}/p^\times, \cdot)$ où p est un grand nombre premier (déjà discuté)
- $G = (\mathbb{F}_q^\times, \cdot)$ où $q = p^n$ et p est un nombre premier (plus tard)
- $G = E(\mathbb{F}_q)$ une courbe elliptique (voir Master 2)

L'attaque de l'homme au milieu :

Ce protocole est vulnérable si l'attaquant est capable d'intercepter et de *modifier* tous les messages échangés entre Alice et Bob.

La sécurité du protocole Diffie–Hellman repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver g^{ab} à partir de g, g^a, g^b .

Implémentations courantes :

- $G = (\mathbb{Z}/p^\times, \cdot)$ où p est un grand nombre premier (déjà discuté)
- $G = (\mathbb{F}_q^\times, \cdot)$ où $q = p^n$ et p est un nombre premier (plus tard)
- $G = E(\mathbb{F}_q)$ une courbe elliptique (voir Master 2)

L'attaque de l'homme au milieu :

Ce protocole est vulnérable si l'attaquant est capable d'intercepter et de *modifier* tous les messages échangés entre Alice et Bob.

Alice et Bob croient ainsi avoir échangé une clé secrète entre eux, alors qu'ils ont chacun échangé une clé secrète avec l'attaquant.

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$.

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$.

Clé publique, diffusé sur le réseau : (G, g, x)

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$.

Clé publique, diffusé sur le réseau : (G, g, x)

Clé privée, gardée secrète par Alice : a

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$.

Clé publique, diffusé sur le réseau : (G, g, x)

Clé privée, gardée secrète par Alice : a

Cryptage d'un message :

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$.

Clé publique, diffusé sur le réseau : (G, g, x)

Clé privée, gardée secrète par Alice : a

Cryptage d'un message :

Bob récupère le triplet (G, g, x) et choisit un entier $b \in \mathbb{Z}$.

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$.

Clé publique, diffusé sur le réseau : (G, g, x)

Clé privée, gardée secrète par Alice : a

Cryptage d'un message :

Bob récupère le triplet (G, g, x) et choisit un entier $b \in \mathbb{Z}$.

Il code son message en un élément $m \in G$ puis calcule $y = g^b$ et $z = x^b m$.

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$.

Clé publique, diffusé sur le réseau : (G, g, x)

Clé privée, gardée secrète par Alice : a

Cryptage d'un message :

Bob récupère le triplet (G, g, x) et choisit un entier $b \in \mathbb{Z}$.

Il code son message en un élément $m \in G$ puis calcule $y = g^b$ et $z = x^b m$.

Message crypté : (y, z)

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$.

Clé publique, diffusé sur le réseau : (G, g, x)

Clé privée, gardée secrète par Alice : a

Cryptage d'un message :

Bob récupère le triplet (G, g, x) et choisit un entier $b \in \mathbb{Z}$.

Il code son message en un élément $m \in G$ puis calcule $y = g^b$ et $z = x^b m$.

Message crypté : (y, z)

Décryptage d'un message :

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$.

Clé publique, diffusé sur le réseau : (G, g, x)

Clé privée, gardée secrète par Alice : a

Cryptage d'un message :

Bob récupère le triplet (G, g, x) et choisit un entier $b \in \mathbb{Z}$.

Il code son message en un élément $m \in G$ puis calcule $y = g^b$ et $z = x^b m$.

Message crypté : (y, z)

Décryptage d'un message :

Alice reçoit le message crypté (y, z) . Elle connaît sa clé privée a .

Le protocole Elgamal (1984)

Objectif : Bob veut envoyer un message secret à Alice.

Production des clés :

Alice choisit un groupe (G, \cdot) , un élément $g \in G$ et un entier $a \in \mathbb{Z}$.

Elle calcule $x = g^a$.

Clé publique, diffusé sur le réseau : (G, g, x)

Clé privée, gardée secrète par Alice : a

Cryptage d'un message :

Bob récupère le triplet (G, g, x) et choisit un entier $b \in \mathbb{Z}$.

Il code son message en un élément $m \in G$ puis calcule $y = g^b$ et $z = x^b m$.

Message crypté : (y, z)

Décryptage d'un message :

Alice reçoit le message crypté (y, z) . Elle connaît sa clé privée a .

Elle calcule $y^{-a} z = (g^b)^{-a} x^b m = g^{-ab} g^{ab} m = m$.

La sécurité du protocole Elgamal repose sur certaines hypothèses :

La sécurité du protocole Elgamal repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .

La sécurité du protocole Elgamal repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver m à partir de $x = g^a$, $y = g^b$, $z = x^b m$.

La sécurité du protocole Elgamal repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver m à partir de $x = g^a$, $y = g^b$, $z = x^b m$.

Remarques

La sécurité du protocole Elgamal repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver m à partir de $x = g^a$, $y = g^b$, $z = x^b m$.

Remarques

- Bob choisit une deuxième clé b , ce qui peut augmenter la sécurité par rapport à une clé unique, comme dans RSA par exemple.

La sécurité du protocole Elgamal repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver m à partir de $x = g^a$, $y = g^b$, $z = x^b m$.

Remarques

- Bob choisit une deuxième clé b , ce qui peut augmenter la sécurité par rapport à une clé unique, comme dans RSA par exemple.
- Il faut une méthode pour coder le message (un entier) en un élément $m \in G$: cela dépend comment on construit / représente le groupe G .

La sécurité du protocole Elgamal repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver m à partir de $x = g^a$, $y = g^b$, $z = x^b m$.

Remarques

- Bob choisit une deuxième clé b , ce qui peut augmenter la sécurité par rapport à une clé unique, comme dans RSA par exemple.
- Il faut une méthode pour coder le message (un entier) en un élément $m \in G$: cela dépend comment on construit / représente le groupe G .

Implémentations courantes :

La sécurité du protocole Elgamal repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver m à partir de $x = g^a$, $y = g^b$, $z = x^b m$.

Remarques

- Bob choisit une deuxième clé b , ce qui peut augmenter la sécurité par rapport à une clé unique, comme dans RSA par exemple.
- Il faut une méthode pour coder le message (un entier) en un élément $m \in G$: cela dépend comment on construit / représente le groupe G .

Implémentations courantes :

- $G = (\mathbb{Z}/p^\times, \cdot)$ où p est un grand nombre premier (déjà discuté)

La sécurité du protocole Elgamal repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver m à partir de $x = g^a$, $y = g^b$, $z = x^b m$.

Remarques

- Bob choisit une deuxième clé b , ce qui peut augmenter la sécurité par rapport à une clé unique, comme dans RSA par exemple.
- Il faut une méthode pour coder le message (un entier) en un élément $m \in G$: cela dépend comment on construit / représente le groupe G .

Implémentations courantes :

- $G = (\mathbb{Z}/p^\times, \cdot)$ où p est un grand nombre premier (déjà discuté)
- $G = (\mathbb{F}_q^\times, \cdot)$ où $q = p^n$ et p est un nombre premier (plus tard)

La sécurité du protocole Elgamal repose sur certaines hypothèses :

- Il est difficile de calculer le logarithme discret de x à base g dans G .
- Il est difficile de trouver m à partir de $x = g^a$, $y = g^b$, $z = x^b m$.

Remarques

- Bob choisit une deuxième clé b , ce qui peut augmenter la sécurité par rapport à une clé unique, comme dans RSA par exemple.
- Il faut une méthode pour coder le message (un entier) en un élément $m \in G$: cela dépend comment on construit / représente le groupe G .

Implémentations courantes :

- $G = (\mathbb{Z}/p^\times, \cdot)$ où p est un grand nombre premier (déjà discuté)
- $G = (\mathbb{F}_q^\times, \cdot)$ où $q = p^n$ et p est un nombre premier (plus tard)
- $G = E(\mathbb{F}_q)$ n'est pas utilisable car on ne sait pas y coder un entier.

- 1 Groupes
- 2 Applications en cryptographie
- 3 Le théorème de Lagrange et applications**
 - Le théorème de Lagrange
 - Les théorèmes de Fermat et d'Euler
 - Calculer l'ordre d'un élément dans un groupe
- 4 Groupes quotients dans le cas commutatif
- 5 Exercices

Théorème

Si H est un sous-groupe d'un groupe fini G , alors $|H|$ divise $|G|$.

Théorème

*Si H est un sous-groupe d'un groupe fini G , alors $|H|$ divise $|G|$.
En particulier l'ordre de tout élément $g \in G$ divise l'ordre du groupe G .*

Corollaire (petit théorème de Fermat)

Soit $p \in \mathbb{N}$ premier. Alors tout élément non nul $x \in \mathbb{Z}/p^$ vérifie $x^{p-1} = \bar{1}$.*

Corollaire (petit théorème de Fermat)

Soit $p \in \mathbb{N}$ premier. Alors tout élément non nul $x \in \mathbb{Z}/p^*$ vérifie $x^{p-1} = \bar{1}$.

Démonstration. Le groupe $\mathbb{Z}/p^\times = \mathbb{Z}/p \setminus \{0\}$ est d'ordre $p - 1$.
Donc $\text{ord}(x) \mid p - 1$ et ainsi $x^{p-1} = \bar{1}$. □

Corollaire (petit théorème de Fermat)

Soit $p \in \mathbb{N}$ premier. Alors tout élément non nul $x \in \mathbb{Z}/p^*$ vérifie $x^{p-1} = \bar{1}$.

Démonstration. Le groupe $\mathbb{Z}/p^\times = \mathbb{Z}/p \setminus \{0\}$ est d'ordre $p - 1$.
Donc $\text{ord}(x) \mid p - 1$ et ainsi $x^{p-1} = \bar{1}$. □

Le petit théorème de Fermat a été généralisé par Euler comme suit :

Corollaire (petit théorème de Fermat)

Soit $p \in \mathbb{N}$ premier. Alors tout élément non nul $x \in \mathbb{Z}/_p^*$ vérifie $x^{p-1} = \bar{1}$.

Démonstration. Le groupe $\mathbb{Z}/_p^\times = \mathbb{Z}/_p \setminus \{0\}$ est d'ordre $p - 1$.
Donc $\text{ord}(x) \mid p - 1$ et ainsi $x^{p-1} = \bar{1}$. □

Le petit théorème de Fermat a été généralisé par Euler comme suit :

Corollaire (théorème d'Euler)

Soit $n \in \mathbb{N}$. Tout élément inversible $x \in \mathbb{Z}/_n^\times$ vérifie $x^{\varphi(n)} = \bar{1}$.

Corollaire (petit théorème de Fermat)

Soit $p \in \mathbb{N}$ premier. Alors tout élément non nul $x \in \mathbb{Z}/_p^*$ vérifie $x^{p-1} = \bar{1}$.

Démonstration. Le groupe $\mathbb{Z}/_p^\times = \mathbb{Z}/_p \setminus \{0\}$ est d'ordre $p - 1$.
Donc $\text{ord}(x) \mid p - 1$ et ainsi $x^{p-1} = \bar{1}$. □

Le petit théorème de Fermat a été généralisé par Euler comme suit :

Corollaire (théorème d'Euler)

Soit $n \in \mathbb{N}$. Tout élément inversible $x \in \mathbb{Z}/_n^\times$ vérifie $x^{\varphi(n)} = \bar{1}$.

Démonstration. Par définition nous avons $\varphi(n) = |\mathbb{Z}/_n^\times|$.
Donc $\text{ord}(x) \mid \varphi(n)$ et ainsi $x^{\varphi(n)} = \bar{1}$. □

Corollaire (petit théorème de Fermat)

Soit $p \in \mathbb{N}$ premier. Alors tout élément non nul $x \in \mathbb{Z}/p^*$ vérifie $x^{p-1} = \bar{1}$.

Démonstration. Le groupe $\mathbb{Z}/p^\times = \mathbb{Z}/p \setminus \{0\}$ est d'ordre $p - 1$.
Donc $\text{ord}(x) \mid p - 1$ et ainsi $x^{p-1} = \bar{1}$. □

Le petit théorème de Fermat a été généralisé par Euler comme suit :

Corollaire (théorème d'Euler)

Soit $n \in \mathbb{N}$. Tout élément inversible $x \in \mathbb{Z}/n^\times$ vérifie $x^{\varphi(n)} = \bar{1}$.

Démonstration. Par définition nous avons $\varphi(n) = |\mathbb{Z}/n^\times|$.
Donc $\text{ord}(x) \mid \varphi(n)$ et ainsi $x^{\varphi(n)} = \bar{1}$. □

Pour $n = pq$ nous avons utilisé cette propriété dans le cryptosystème RSA.

Calculer l'ordre d'un élément dans un groupe

Algorithme 7.1 calculer l'ordre d'un élément x dans un groupe G

Entrée: un élément x dans un groupe G et la factorisation $|G| = p_1^{e_1} \cdots p_\ell^{e_\ell}$

Sortie: l'ordre de x dans G , c'est-à-dire le plus petit entier $n \geq 1$ tel que $x^n = 1$

```
 $n \leftarrow |G|$   
pour  $i$  de 1 à  $\ell$  faire  
   $n \leftarrow n/p_i^{e_i}$   
   $y \leftarrow x^n$   
  tant que  $y \neq 1$  faire  
     $n \leftarrow np_i$   
     $y \leftarrow y^{p_i}$   
  fin tant que  
fin pour  
retourner  $n$ 
```

Calculer l'ordre d'un élément dans un groupe

Algorithme 7.2 calculer l'ordre d'un élément x dans un groupe G

Entrée: un élément x dans un groupe G et la factorisation $|G| = p_1^{e_1} \cdots p_\ell^{e_\ell}$

Sortie: l'ordre de x dans G , c'est-à-dire le plus petit entier $n \geq 1$ tel que $x^n = 1$

```
 $n \leftarrow |G|$   
pour  $i$  de 1 à  $\ell$  faire  
   $n \leftarrow n/p_i^{e_i}$   
   $y \leftarrow x^n$   
  tant que  $y \neq 1$  faire  
     $n \leftarrow np_i$   
     $y \leftarrow y^{p_i}$   
  fin tant que  
fin pour  
retourner  $n$ 
```

Exemple

Appliquer l'algorithme à l'exemple $x = \bar{3}$ dans \mathbb{Z}/p^\times où $p = 2^{32} \cdot 3^{32} \cdot 5^{32} + 1$.

Calculer l'ordre d'un élément dans un groupe

Algorithme 7.3 calculer l'ordre d'un élément x dans un groupe G

Entrée: un élément x dans un groupe G et la factorisation $|G| = p_1^{e_1} \cdots p_\ell^{e_\ell}$

Sortie: l'ordre de x dans G , c'est-à-dire le plus petit entier $n \geq 1$ tel que $x^n = 1$

```
 $n \leftarrow |G|$   
pour  $i$  de 1 à  $\ell$  faire  
   $n \leftarrow n/p_i^{e_i}$   
   $y \leftarrow x^n$   
  tant que  $y \neq 1$  faire  
     $n \leftarrow np_i$   
     $y \leftarrow y^{p_i}$   
  fin tant que  
fin pour  
retourner  $n$ 
```

Exemple

Appliquer l'algorithme à l'exemple $x = \bar{3}$ dans \mathbb{Z}/p^\times où $p = 2^{32} \cdot 3^{32} \cdot 5^{32} + 1$.

Exercice

Prouver que cet algorithme est correct. Discuter sa complexité.

- 1 Groupes
- 2 Applications en cryptographie
- 3 Le théorème de Lagrange et applications
- 4 Groupes quotients dans le cas commutatif**
 - Construction du groupe quotient
 - Passage au groupe quotient
 - Classification des groupes abéliens finis
- 5 Exercices

Définition

Soit $(G, +)$ un groupe abélien et soit $H \subset G$ un sous-groupe.

Définition

Soit $(G, +)$ un groupe abélien et soit $H \subset G$ un sous-groupe.
On définit une relation d'équivalence $a \sim b$ par $b - a \in H$.

Définition

Soit $(G, +)$ un groupe abélien et soit $H \subset G$ un sous-groupe.

On définit une relation d'équivalence $a \sim b$ par $b - a \in H$.

La classe de $a \in G$ est $\text{cl}(a) = a + H = \{a + h \mid h \in H\}$.

Définition

Soit $(G, +)$ un groupe abélien et soit $H \subset G$ un sous-groupe.

On définit une relation d'équivalence $a \sim b$ par $b - a \in H$.

La classe de $a \in G$ est $\text{cl}(a) = a + H = \{a + h \mid h \in H\}$.

On note $\pi: G \rightarrow G/H, a \mapsto \text{cl}(a)$, l'application quotient.

Définition

Soit $(G, +)$ un groupe abélien et soit $H \subset G$ un sous-groupe.

On définit une relation d'équivalence $a \sim b$ par $b - a \in H$.

La classe de $a \in G$ est $\text{cl}(a) = a + H = \{a + h \mid h \in H\}$.

On note $\pi: G \rightarrow G/H, a \mapsto \text{cl}(a)$, l'application quotient.

Proposition

Il existe sur l'ensemble quotient G/H une unique structure de groupe

$$+: G/H \times G/H \rightarrow G/H$$

telle que $\pi: G \rightarrow G/H$ soit un morphisme de groupes.

Définition

Soit $(G, +)$ un groupe abélien et soit $H \subset G$ un sous-groupe.

On définit une relation d'équivalence $a \sim b$ par $b - a \in H$.

La classe de $a \in G$ est $\text{cl}(a) = a + H = \{a + h \mid h \in H\}$.

On note $\pi: G \rightarrow G/H, a \mapsto \text{cl}(a)$, l'application quotient.

Proposition

Il existe sur l'ensemble quotient G/H une unique structure de groupe

$$+: G/H \times G/H \rightarrow G/H$$

telle que $\pi: G \rightarrow G/H$ soit un morphisme de groupes.

Exemples

- Si $G = \mathbb{Z}$ et $H = m\mathbb{Z}$, alors $G/H = \mathbb{Z}/m\mathbb{Z}$ comme avant.

Exemples

- Si $G = \mathbb{Z}$ et $H = m\mathbb{Z}$, alors $G/H = \mathbb{Z}/m\mathbb{Z}$ comme avant.
- Si $H = \{0\}$, alors $\pi: G \rightarrow G/\{0\}$ est un isomorphisme.

Exemples

- Si $G = \mathbb{Z}$ et $H = m\mathbb{Z}$, alors $G/H = \mathbb{Z}/m\mathbb{Z}$ comme avant.
- Si $H = \{0\}$, alors $\pi: G \rightarrow G/\{0\}$ est un isomorphisme.
- Si $H = G$, alors $G/H = \{\bar{0}\}$ est le groupe trivial.

Exemples

- Si $G = \mathbb{Z}$ et $H = m\mathbb{Z}$, alors $G/H = \mathbb{Z}/m\mathbb{Z}$ comme avant.
- Si $H = \{0\}$, alors $\pi: G \rightarrow G/\{0\}$ est un isomorphisme.
- Si $H = G$, alors $G/H = \{\bar{0}\}$ est le groupe trivial.

Exercice

Soit $\pi: G \rightarrow G/H$ le morphisme quotient. Déterminer $\text{im}(\pi)$ et $\text{ker}(\pi)$.
Déterminer les sous-groupes de G/H en termes des sous-groupes de G .
Illustrer vos résultats par le quotient $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/24\mathbb{Z}$, disons.

Exemples

- Si $G = \mathbb{Z}$ et $H = m\mathbb{Z}$, alors $G/H = \mathbb{Z}/m\mathbb{Z}$ comme avant.
- Si $H = \{0\}$, alors $\pi: G \rightarrow G/\{0\}$ est un isomorphisme.
- Si $H = G$, alors $G/H = \{\bar{0}\}$ est le groupe trivial.

Exercice

Soit $\pi: G \rightarrow G/H$ le morphisme quotient. Déterminer $\text{im}(\pi)$ et $\text{ker}(\pi)$.
Déterminer les sous-groupes de G/H en termes des sous-groupes de G .
Illustrer vos résultats par le quotient $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/24\mathbb{Z}$, disons.



Nous ne discutons ici que les groupes abéliens !

Exemples

- Si $G = \mathbb{Z}$ et $H = m\mathbb{Z}$, alors $G/H = \mathbb{Z}/m\mathbb{Z}$ comme avant.
- Si $H = \{0\}$, alors $\pi: G \rightarrow G/\{0\}$ est un isomorphisme.
- Si $H = G$, alors $G/H = \{\bar{0}\}$ est le groupe trivial.

Exercice

Soit $\pi: G \rightarrow G/H$ le morphisme quotient. Déterminer $\text{im}(\pi)$ et $\text{ker}(\pi)$.
Déterminer les sous-groupes de G/H en termes des sous-groupes de G .
Illustrer vos résultats par le quotient $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/24\mathbb{Z}$, disons.

 Nous ne discutons ici que les groupes abéliens !
La situation est un peu plus compliquée pour les groupes non abéliens.

Exemples

- Si $G = \mathbb{Z}$ et $H = m\mathbb{Z}$, alors $G/H = \mathbb{Z}/m\mathbb{Z}$ comme avant.
- Si $H = \{0\}$, alors $\pi: G \rightarrow G/\{0\}$ est un isomorphisme.
- Si $H = G$, alors $G/H = \{\bar{0}\}$ est le groupe trivial.

Exercice

Soit $\pi: G \rightarrow G/H$ le morphisme quotient. Déterminer $\text{im}(\pi)$ et $\text{ker}(\pi)$. Déterminer les sous-groupes de G/H en termes des sous-groupes de G . Illustrer vos résultats par le quotient $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/24\mathbb{Z}$, disons.

 Nous ne discutons ici que les groupes abéliens !
La situation est un peu plus compliquée pour les groupes non abéliens.

Exemple

Considérons le groupe symétrique $G = \text{Sym}(3)$ et $H = \langle (12) \rangle$. L'ensemble quotient G/H n'admet pas de structure de groupe pour laquelle l'application quotient $\pi: G \rightarrow G/H$ soit un morphisme.

Proposition

Soit G un groupe abélien, soit $K \subset G$ un sous-groupe, et soit $\phi: G \rightarrow H$ un morphisme de groupes.

Proposition

Soit G un groupe abélien, soit $K \subset G$ un sous-groupe, et soit $\phi: G \rightarrow H$ un morphisme de groupes. Les deux conditions suivantes sont équivalentes :

Proposition

Soit G un groupe abélien, soit $K \subset G$ un sous-groupe, et soit $\phi: G \rightarrow H$ un morphisme de groupes. Les deux conditions suivantes sont équivalentes :

1 $K \subset \ker(\phi)$

Proposition

Soit G un groupe abélien, soit $K \subset G$ un sous-groupe, et soit $\phi: G \rightarrow H$ un morphisme de groupes. Les deux conditions suivantes sont équivalentes :

- 1** $K \subset \ker(\phi)$
- 2** *Il existe un morphisme de groupes $\bar{\phi}: G/K \rightarrow H$ tel que $\phi = \bar{\phi} \circ \pi$.*

Proposition

Soit G un groupe abélien, soit $K \subset G$ un sous-groupe, et soit $\phi: G \rightarrow H$ un morphisme de groupes. Les deux conditions suivantes sont équivalentes :

1 $K \subset \ker(\phi)$

2 *Il existe un morphisme de groupes $\bar{\phi}: G/K \rightarrow H$ tel que $\phi = \bar{\phi} \circ \pi$.*

Dans ce cas on dit que ϕ passe au quotient ; le morphisme $\bar{\phi}$ est unique, et on l'appelle le morphisme induit par passage au quotient.

Corollaire

Tout morphisme de groupes $\phi: G \rightarrow H$ induit un isomorphisme de groupes $\bar{\phi}: G/\ker(\phi) \xrightarrow{\sim} \text{im}(\phi)$.

Corollaire

Tout morphisme de groupes $\phi: G \rightarrow H$ induit un isomorphisme de groupes $\bar{\phi}: G/\ker(\phi) \xrightarrow{\sim} \text{im}(\phi)$.

Exemple

Soit G un groupe et $g \in G$.

Corollaire

Tout morphisme de groupes $\phi: G \rightarrow H$ induit un isomorphisme de groupes $\bar{\phi}: G/\ker(\phi) \xrightarrow{\sim} \text{im}(\phi)$.

Exemple

Soit G un groupe et $g \in G$.

On a un morphisme de groupes $\phi: \mathbb{Z} \rightarrow G, k \mapsto g^k$.

Corollaire

Tout morphisme de groupes $\phi: G \rightarrow H$ induit un isomorphisme de groupes $\bar{\phi}: G/\ker(\phi) \xrightarrow{\sim} \text{im}(\phi)$.

Exemple

Soit G un groupe et $g \in G$.

On a un morphisme de groupes $\phi: \mathbb{Z} \rightarrow G, k \mapsto g^k$.

Ici $\text{im}(\phi) = \langle g \rangle$ et $\ker(\phi) = m\mathbb{Z}$, donc ϕ induit $\bar{\phi}: \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$.

Corollaire

Tout morphisme de groupes $\phi: G \rightarrow H$ induit un isomorphisme de groupes $\bar{\phi}: G/\ker(\phi) \xrightarrow{\sim} \text{im}(\phi)$.

Exemple

Soit G un groupe et $g \in G$.

On a un morphisme de groupes $\phi: \mathbb{Z} \rightarrow G, k \mapsto g^k$.

Ici $\text{im}(\phi) = \langle g \rangle$ et $\ker(\phi) = m\mathbb{Z}$, donc ϕ induit $\bar{\phi}: \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$.

Ainsi tout groupe cyclique G d'ordre m est isomorphe au groupe $\mathbb{Z}/m\mathbb{Z}$.

Théorème (version faible)

Tout groupe abélien fini $(G, +)$ est isomorphe à un produit $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$.

Toute partie génératrice $\{g_1, \dots, g_r\} \subset G$ définit un épimorphisme

$$\phi: \mathbb{Z}^r \twoheadrightarrow G, \quad (a_1, \dots, a_r) \mapsto a_1 g_1 + \cdots + a_r g_r.$$

Théorème (version faible)

Tout groupe abélien fini $(G, +)$ est isomorphe à un produit $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$.

Toute partie génératrice $\{g_1, \dots, g_r\} \subset G$ définit un épimorphisme

$$\phi: \mathbb{Z}^r \twoheadrightarrow G, \quad (a_1, \dots, a_r) \mapsto a_1 g_1 + \cdots + a_r g_r.$$

Le théorème dit que l'on peut choisir $\{g_1, \dots, g_r\}$ tel que l'application ϕ associée ait pour noyau $m_1 \mathbb{Z} \times \cdots \times m_r \mathbb{Z}$.

Théorème (version faible)

Tout groupe abélien fini $(G, +)$ est isomorphe à un produit $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$.

Toute partie génératrice $\{g_1, \dots, g_r\} \subset G$ définit un épimorphisme

$$\phi: \mathbb{Z}^r \rightarrow G, \quad (a_1, \dots, a_r) \mapsto a_1 g_1 + \cdots + a_r g_r.$$

Le théorème dit que l'on peut choisir $\{g_1, \dots, g_r\}$ tel que l'application ϕ associée ait pour noyau $m_1 \mathbb{Z} \times \cdots \times m_r \mathbb{Z}$. Il induit donc un isomorphisme

$$\bar{\phi}: \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r \xrightarrow{\sim} G, \quad (\bar{a}_1, \dots, \bar{a}_r) \mapsto a_1 g_1 + \cdots + a_r g_r$$

Classification des groupes abéliens finis

Théorème (version faible)

Tout groupe abélien fini $(G, +)$ est isomorphe à un produit $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$.

Toute partie génératrice $\{g_1, \dots, g_r\} \subset G$ définit un épimorphisme

$$\phi: \mathbb{Z}^r \rightarrow G, \quad (a_1, \dots, a_r) \mapsto a_1 g_1 + \cdots + a_r g_r.$$

Le théorème dit que l'on peut choisir $\{g_1, \dots, g_r\}$ tel que l'application ϕ associée ait pour noyau $m_1 \mathbb{Z} \times \cdots \times m_r \mathbb{Z}$. Il induit donc un isomorphisme

$$\bar{\phi}: \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r \xrightarrow{\sim} G, \quad (\bar{a}_1, \dots, \bar{a}_r) \mapsto a_1 g_1 + \cdots + a_r g_r$$

Théorème (version forte)

Il existe des générateurs $\{g_1, g_2, \dots, g_s\} \subset G$ comme ci-dessus tels que leurs ordres $m_k = \text{ord}(g_k)$ satisfassent

$$2 \leq m_1 \leq m_2 \leq \cdots \leq m_s \quad \text{et} \quad m_1 \mid m_2 \mid \cdots \mid m_s.$$

Classification des groupes abéliens finis

Théorème (version faible)

Tout groupe abélien fini $(G, +)$ est isomorphe à un produit $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$.

Toute partie génératrice $\{g_1, \dots, g_r\} \subset G$ définit un épimorphisme

$$\phi: \mathbb{Z}^r \rightarrow G, \quad (a_1, \dots, a_r) \mapsto a_1 g_1 + \cdots + a_r g_r.$$

Le théorème dit que l'on peut choisir $\{g_1, \dots, g_r\}$ tel que l'application ϕ associée ait pour noyau $m_1 \mathbb{Z} \times \cdots \times m_r \mathbb{Z}$. Il induit donc un isomorphisme

$$\bar{\phi}: \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r \xrightarrow{\sim} G, \quad (\bar{a}_1, \dots, \bar{a}_r) \mapsto a_1 g_1 + \cdots + a_r g_r$$

Théorème (version forte)

Il existe des générateurs $\{g_1, g_2, \dots, g_s\} \subset G$ comme ci-dessus tels que leurs ordres $m_k = \text{ord}(g_k)$ satisfassent

$$2 \leq m_1 \leq m_2 \leq \cdots \leq m_s \quad \text{et} \quad m_1 \mid m_2 \mid \cdots \mid m_s.$$

Dans ce cas la famille (m_1, m_2, \dots, m_s) est uniquement déterminée par G .

Classification des groupes abéliens finis

Théorème (version faible)

Tout groupe abélien fini $(G, +)$ est isomorphe à un produit $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$.

Toute partie génératrice $\{g_1, \dots, g_r\} \subset G$ définit un épimorphisme

$$\phi: \mathbb{Z}^r \rightarrow G, \quad (a_1, \dots, a_r) \mapsto a_1 g_1 + \cdots + a_r g_r.$$

Le théorème dit que l'on peut choisir $\{g_1, \dots, g_r\}$ tel que l'application ϕ associée ait pour noyau $m_1 \mathbb{Z} \times \cdots \times m_r \mathbb{Z}$. Il induit donc un isomorphisme

$$\bar{\phi}: \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r \xrightarrow{\sim} G, \quad (\bar{a}_1, \dots, \bar{a}_r) \mapsto a_1 g_1 + \cdots + a_r g_r$$

Théorème (version forte)

Il existe des générateurs $\{g_1, g_2, \dots, g_s\} \subset G$ comme ci-dessus tels que leurs ordres $m_k = \text{ord}(g_k)$ satisfassent

$$2 \leq m_1 \leq m_2 \leq \cdots \leq m_s \quad \text{et} \quad m_1 \mid m_2 \mid \cdots \mid m_s.$$

Dans ce cas la famille (m_1, m_2, \dots, m_s) est uniquement déterminée par G . On appelle m_1, m_2, \dots, m_s les diviseurs élémentaires de G .

Classification des groupes abéliens finis

Théorème (version faible)

Tout groupe abélien fini $(G, +)$ est isomorphe à un produit $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r$.

Toute partie génératrice $\{g_1, \dots, g_r\} \subset G$ définit un épimorphisme

$$\phi: \mathbb{Z}^r \rightarrow G, \quad (a_1, \dots, a_r) \mapsto a_1 g_1 + \cdots + a_r g_r.$$

Le théorème dit que l'on peut choisir $\{g_1, \dots, g_r\}$ tel que l'application ϕ associée ait pour noyau $m_1 \mathbb{Z} \times \cdots \times m_r \mathbb{Z}$. Il induit donc un isomorphisme

$$\bar{\phi}: \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r \xrightarrow{\sim} G, \quad (\bar{a}_1, \dots, \bar{a}_r) \mapsto a_1 g_1 + \cdots + a_r g_r$$

Théorème (version forte)

Il existe des générateurs $\{g_1, g_2, \dots, g_s\} \subset G$ comme ci-dessus tels que leurs ordres $m_k = \text{ord}(g_k)$ satisfassent

$$2 \leq m_1 \leq m_2 \leq \cdots \leq m_s \quad \text{et} \quad m_1 \mid m_2 \mid \cdots \mid m_s.$$

Dans ce cas la famille (m_1, m_2, \dots, m_s) est uniquement déterminée par G . On appelle m_1, m_2, \dots, m_s les diviseurs élémentaires de G .

Démonstration. Réduction des matrices sur \mathbb{Z} (Jacobson, *Basic Algebra*).

- 1 Groupes
- 2 Applications en cryptographie
- 3 Le théorème de Lagrange et applications
- 4 Groupes quotients dans le cas commutatif
- 5 Exercices**

Exercice

Soit $\phi: G \rightarrow H$ un morphisme de groupes supposé bijectif.

Est-ce que l'application inverse $\phi^{-1}: H \rightarrow G$ est un morphisme ?

Exercice

Soit $\phi: G \rightarrow H$ un morphisme de groupes supposé bijectif.
Est-ce que l'application inverse $\phi^{-1}: H \rightarrow G$ est un morphisme ?

Exercice

Soit G un groupe. Un sous-ensemble $H \subset G$ est un sous-groupe si et seulement si $H \neq \emptyset$ et pour tout $a, b \in H$ on a $ab^{-1} \in H$.

Exercice

Soit $\phi: G \rightarrow H$ un morphisme de groupes supposé bijectif.
Est-ce que l'application inverse $\phi^{-1}: H \rightarrow G$ est un morphisme ?

Exercice

Soit G un groupe. Un sous-ensemble $H \subset G$ est un sous-groupe si et seulement si $H \neq \emptyset$ et pour tout $a, b \in H$ on a $ab^{-1} \in H$.

Exercice

Supposons que $a, b \in G$ commutent. On pose $p = \text{ord}(a)$ et $q = \text{ord}(b)$.

- 1 Montrer que $\text{ord}(ab) \mid m$ où $m = \text{ppcm}(p, q)$.
- 2 Illustrer par un exemple que $\text{ord}(ab) < m$ est possible.
- 3 Si $\text{pgcd}(p, q) = 1$, alors $\text{ord}(ab) = pq$. (Indication : Bézout et Lagrange)

Exercice

Soit $G = \{a, b, c\}$ muni de la loi de composition

\cdot	a	b	c
a	a	b	b
b	b	a	b
c	c	c	a

Est-ce un groupe ? Quels sous-ensembles H forment un groupe ?
Expliciter les classes xH pour $x \in G$. Est-ce que $|H|$ divise $|G|$?

Exercices : autour du théorème de Lagrange

Exercice

Soit $G = \{a, b, c\}$ muni de la loi de composition

\cdot	a	b	c
a	a	b	b
b	b	a	b
c	c	c	a

Est-ce un groupe ? Quels sous-ensembles H forment un groupe ?
Expliciter les classes xH pour $x \in G$. Est-ce que $|H|$ divise $|G|$?

Exercice

Quels sont les ordres des éléments dans $\mathbb{Z}/4$ et de $\mathbb{Z}/2 \times \mathbb{Z}/2$?

Est-ce que tout diviseur de $|G|$ se réalise comme ordre d'un élément $g \in G$?

Exercices : autour du théorème de Lagrange

Exercice

Soit $G = \{a, b, c\}$ muni de la loi de composition

\cdot	a	b	c
a	a	b	b
b	b	a	b
c	c	c	a

Est-ce un groupe ? Quels sous-ensembles H forment un groupe ?
Expliciter les classes xH pour $x \in G$. Est-ce que $|H|$ divise $|G|$?

Exercice

Quels sont les ordres des éléments dans $\mathbb{Z}/4$ et de $\mathbb{Z}/2 \times \mathbb{Z}/2$?

Est-ce que tout diviseur de $|G|$ se réalise comme ordre d'un élément $g \in G$?

Exercice

Le groupe $(\mathbb{Z}/101, +)$ est-il cyclique ? Combien a-t-il de générateurs ?

Le groupe $(\mathbb{Z}/101^\times, \cdot)$ est-il cyclique ? Combien a-t-il de générateurs ?

Exercices : autour du théorème de Lagrange

Exercice

Soit $G = \{a, b, c\}$ muni de la loi de composition

\cdot	a	b	c
a	a	b	b
b	b	a	b
c	c	c	a

Est-ce un groupe ? Quels sous-ensembles H forment un groupe ?
Expliciter les classes xH pour $x \in G$. Est-ce que $|H|$ divise $|G|$?

Exercice

Quels sont les ordres des éléments dans $\mathbb{Z}/4$ et de $\mathbb{Z}/2 \times \mathbb{Z}/2$?

Est-ce que tout diviseur de $|G|$ se réalise comme ordre d'un élément $g \in G$?

Exercice

Le groupe $(\mathbb{Z}/101, +)$ est-il cyclique ? Combien a-t-il de générateurs ?

Le groupe $(\mathbb{Z}/101^\times, \cdot)$ est-il cyclique ? Combien a-t-il de générateurs ?

Exercice

Quels sont les ordres des sous-groupes dans $\text{Sym}(3)$ et dans $\text{Sym}(4)$?

Est-ce que tout diviseur de $|G|$ se réalise comme ordre d'un sous-groupe ?

Exercice

Soit $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ l'application quotient. On pose $a\mathbb{Z}/n\mathbb{Z} = \pi(a\mathbb{Z})$.

- 1 Est-ce que $a\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$?
- 2 Déterminer image et noyau de $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, k \mapsto k\bar{a}$.
- 3 Expliciter un isomorphisme $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} a\mathbb{Z}/n\mathbb{Z}$. Que vaut m ?
- 4 Si $n = ma$, alors $\langle \bar{a} \rangle = a\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe d'ordre m .
- 5 Si $H \subset \mathbb{Z}/n\mathbb{Z}$ est un sous-groupe d'ordre m , alors $H = \langle \bar{a} \rangle$ où $a = n/m$.
- 6 En déduire que $n = \sum_{d|n} \varphi(d)$ où φ est l'indicatrice d'Euler.

Exercice

Soit $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ l'application quotient. On pose $a\mathbb{Z}/n\mathbb{Z} = \pi(a\mathbb{Z})$.

- 1 Est-ce que $a\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$?
- 2 Déterminer image et noyau de $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, k \mapsto k\bar{a}$.
- 3 Expliciter un isomorphisme $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} a\mathbb{Z}/n\mathbb{Z}$. Que vaut m ?
- 4 Si $n = ma$, alors $\langle \bar{a} \rangle = a\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe d'ordre m .
- 5 Si $H \subset \mathbb{Z}/n\mathbb{Z}$ est un sous-groupe d'ordre m , alors $H = \langle \bar{a} \rangle$ où $a = n/m$.
- 6 En déduire que $n = \sum_{d|n} \varphi(d)$ où φ est l'indicatrice d'Euler.

Exercice

Soit G un groupe d'ordre n . Les conditions suivantes sont équivalentes :

- 1 Le groupe G est cyclique.
- 2 Pour tout diviseur $d \mid n$ il existe un unique sous-groupe d'ordre d dans G .
- 3 Pour tout diviseur $d \mid n$ il existe au plus un sous-groupe d'ordre d dans G .

Indication — Utiliser l'exercice précédent.