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

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

Objectifs de ce chapitre

La structure de groupe est une notion centrale pour de nombreux domaines (en mathématiques, physique, chimie, ...). Nous les étudions ici d'un point de vue algébrique et algorithmique avec applications en cryptographie.

Développement mathématique :

- Introduire le vocabulaire des groupes, sous-groupes, quotients.
- Présenter le théorème de Lagrange et quelques applications.
- Énoncer la classification des groupes abéliens finis.

Développement algorithmique :

- Certificat de primalité pour $p \in \mathbb{N}$.
- Calculer l'ordre de x dans le groupe $\mathbb{Z}/p^{\times}$.
- Cryptographie selon Diffie–Hellman et Elgamal.

Sommaire

Groupes

Définition

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

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

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

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

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

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

Proposition

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

Démonstration. Si e et e' sont neutres, alors $e' = e \bullet e' = e$.

Supposons que b et b' sont inverses à a, c'est-à-dire que $a \bullet b = b \bullet a = e$ et $a \bullet b' = b' \bullet a = e$. Alors $b = b \bullet e = b \bullet (a \bullet b') = (b \bullet a) \bullet b' = e \bullet b' = b'$. $\square$

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 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.
$(\mathrm{Sym}(3), \circ)$ et $(\mathrm{GL}(2, \mathbb{R}), \cdot)$ 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 $(G_1, \cdot), \ldots, (G_n, \cdot)$ sont des groupes, alors le produit $G = G_1 \times \cdots \times G_n$ est un groupe pour la loi $(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) := (g_1 h_1, \ldots, g_n h_n)$.

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

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

Démonstration. Exercice facile mais bénéfique.

Morphismes de groupes

Définition

Soient $(G, \circ)$ et $(H, \bullet)$ des groupes. Une application $\phi\colon G \to H$ 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 $\pi\colon (\mathbb{Z}, +) \to (\mathbb{Z}/m, +)$ est un morphisme de groupes.

Exemples

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

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

Proposition

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

Démonstration. Exercice facile mais bénéfique.

L'exponentielle discrète

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 $\exp_g : \mathbb{Z} \to G$ définie par $\exp_g(k) = g^k$ est un morphisme du groupe $(\mathbb{Z}, +)$ dans le groupe $(G, \cdot)$.

Démonstration. Exercice bénéfique.

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 $(-n)g := -(ng)$.

Isomorphismes de groupes

Définition

Un morphisme de groupes $\phi\colon G \to H$ 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 $\pi_m\colon (\mathbb{Z}, +) \to (\mathbb{Z}/m, +)$ est un épimorphisme.

Exemple

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

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

Exemple

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

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 $\cdot : H \times H \to H$ est alors un groupe, et l'inclusion $\iota : H \hookrightarrow G$ est un monomorphisme de groupes.

Démonstration. Exercice facile mais bénéfique.

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.

Sous-groupes 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 $m \in \mathbb{Z}$.

Démonstration. Évidemment $m\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Réciproquement, soit I un sous-groupe de $\mathbb{Z}$.
Par (SG1) on a $0 \in I$. Si $I = \{0\}$, alors $I = 0\mathbb{Z}$.

Si $I \neq \{0\}$, alors il existe $a \in I$, $a \neq 0$.
Grâce à (SG2) on peut supposer $a > 0$.

Soit $m = \min\{a \in I \mid a > 0\}$ le plus petit élément positif de I.

- Pour tout $q \in \mathbb{Z}$ on a $mq \in I$, donc $m\mathbb{Z} \subset I$.
- Pour tout $a \in I$ il existe $q, r \in \mathbb{Z}$ tels que $a = mq + r$ et $0 \leq r < m$.
  Grâce à (SG2/3) on voit que $r = a - mq$ est un élément de I.
  Notre hypothèse exclut que $0 < r < m$, il ne reste donc que $r = 0$.
  On conclut que tout $a \in I$ vérifie $a \in m\mathbb{Z}$, donc $I \subset m\mathbb{Z}$.

Les deux inclusions prouvent que $I = m\mathbb{Z}$. □

Image et noyau

Proposition

Soit $\phi\colon G \to H$ 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.

Démonstration. Exercice facile mais bénéfique.

Corollaire

L'image $\mathrm{im}(\phi) = \phi(G) = \{\phi(g) \mid g \in G\}$ 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 $\phi\colon G \to H$ est surjectif ssi $\mathrm{im}(\phi) = H$.
Pour l'injectivité nous avons le critère suivant :

Proposition

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

Démonstration. «⇒» Tout morphisme vérifie $\phi(e_G) = e_H$.
Si ϕ est injectif, alors $\phi^{-1}(e_H) = \{e_G\}$.
«⇐» Supposons que $\ker(\phi) = \{e_G\}$. Soient $a, b \in G$ tels que $\phi(a) = \phi(b)$.
Alors $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = e_H$, donc $ab^{-1} \in \ker(\phi) = \{e_G\}$.
On conclut que $ab^{-1} = e_G$, donc $a = b$. □

Correspondance des sous-groupes

Exercice

Soit $\phi\colon G \to H$ un morphisme de groupes.
Soit $\mathscr{X}$ l'ensemble des sous-groupes $F \subset G$ contenant $\ker(\phi)$.
Soit $\mathscr{Y}$ l'ensemble des sous-groupes $K \subset H$ contenus dans $\mathrm{im}(\phi)$.
Pour tout $F \in \mathscr{X}$ on a $\phi(F) \in \mathscr{Y}$, et pour tout $K \in \mathscr{Y}$ on a $\phi^{-1}(K) \in \mathscr{X}$.
Les applications

$$\Phi\colon \mathscr{X} \to \mathscr{Y}, F \mapsto \phi(F), \qquad \text{et} \qquad \Psi\colon \mathscr{Y} \to \mathscr{X}, K \mapsto \phi^{-1}(K),$$

sont des bijections mutuellement inverses.

Solution. Pour tout $K \subset H$ on a $\phi(\phi^{-1}(K)) \subset K$. C'est la condition $K \subset \mathrm{im}(\phi)$ qui assure que $\phi(\phi^{-1}(K)) = K$. Ainsi on voit que $\Phi \circ \Psi = \mathrm{id}_{\mathscr{Y}}$.

Pour tout $F \subset G$ on a $\phi^{-1}(\phi(F)) \supset F$. C'est la condition $F \supset \ker(\phi)$ qui assure que $\phi^{-1}(\phi(F)) = F$. Pour montrer «$\subset$» considérons $g \in \phi^{-1}(\phi(F))$. On a alors $\phi(g) = \phi(f)$ pour un certain $f \in F$. Ainsi $k = gf^{-1} \in \ker(\phi) \subset F$, ce qui entraîne que $g = kf \in F$. Ainsi on voit que $\Psi \circ \Phi = \mathrm{id}_{\mathscr{X}}$. ☺

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.

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.

Démonstration. Exercice facile mais bénéfique.

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

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. □

Notation

Si $S = \{g_1, \ldots, g_n\}$, alors on note $\langle S \rangle$ par $\langle g_1, \ldots, g_n \rangle$.
En particulier, si $S = \{g\}$, alors $\langle S \rangle = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.

Parties génératrices et groupes monogènes

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

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 $\mathbb{Z}/_2 \times \mathbb{Z}/_3$?

Groupes cycliques

Définition

L'ordre d'un groupe G est le cardinal $|G| = \mathrm{ord}(G) = \mathrm{card}(G) = \sharp G$.
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 $\phi\colon \mathbb{Z} \to \langle g \rangle$ donné par $k \mapsto g^k$ est surjectif.
Nous avons $\ker(\phi) = m\mathbb{Z}$ et ϕ induit un isomorphisme $\bar{\phi}\colon \mathbb{Z}/_m \xrightarrow{\sim} \langle g \rangle$.

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

Démonstration.
Si $\ker(\phi) = m\mathbb{Z}$, alors $g^{k+mq} = g^k (g^m)^q = g^k e^q = g^k$.
Ainsi on peut définir $\bar{\phi}\colon \mathbb{Z}/_m \to \langle g \rangle$ par $\bar{\phi}(\pi_m(k)) = g^k$.
Par construction $\bar{\phi}$ est un morphisme de groupes et surjectif.

Si $\bar{\phi}(\pi_m(k)) = \bar{\phi}(\pi_m(k'))$, alors $g^k = g^{k'}$, donc $g^{k-k'} = e$.
Ainsi $k - k' \in \ker(\phi) = m\mathbb{Z}$, et on conclut que $\pi_m(k) = \pi_m(k')$.
Ceci prouve que $\bar{\phi}$ est un isomorphisme. □

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 $\mathbb{Z}/_2^\times$, $\mathbb{Z}/_3^\times$, $\mathbb{Z}/_4^\times$, …, $\mathbb{Z}/_{16}^\times$. 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 $\mathbb{Z}/_p$.
On pose $n = p - 1$ puis on effectue / vérifie les calculs suivants :

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

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 $d = 2, \ldots, \sqrt{p}$ sont hors de question !
Solution. Il suffit d'exploiter l'information des calculs ci-dessus :

$$\begin{aligned}
g^n = \bar{1} \quad &\Longrightarrow \quad g \in \mathbb{Z}/_p^\times \quad \text{et} \quad \operatorname{ord}(g) \mid n \\
g^{n/2} \neq \bar{1} \quad &\Longrightarrow \quad \operatorname{ord}(g) \nmid \tfrac{n}{2} \\
g^{n/3} \neq \bar{1} \quad &\Longrightarrow \quad \operatorname{ord}(g) \nmid \tfrac{n}{3} \\
g^{n/5} \neq \bar{1} \quad &\Longrightarrow \quad \operatorname{ord}(g) \nmid \tfrac{n}{5}
\end{aligned}$$

Ceci montre que $\operatorname{ord}(g) = n$.

Nous avons $\langle g \rangle \subset \mathbb{Z}/_p^\times \subset \mathbb{Z}/_p^*$, donc $n = |\langle g \rangle| \leq |\mathbb{Z}/_p^\times| \leq |\mathbb{Z}/_p^*| = p - 1$.
Ici nous avons $n = p - 1$, donc nécessairement $\langle g \rangle = \mathbb{Z}/_p^\times = \mathbb{Z}/_p^*$.
On conclut que p est premier et que g est un générateur de $\mathbb{Z}/_p^\times$. ☺

Certificats de primalité

Définition

Un ***certificat de primalité*** pour $p \in \mathbb{N}$ consiste en la donnée d'entiers positifs $(p_1, e_1, \ldots, p_\ell, e_\ell; g)$ 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 $k = 1, \ldots, \ell$

Proposition

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

Démonstration. Si p est premier, alors $\mathbb{Z}/p^\times$ est un groupe cyclique, et il existe donc $\varphi(p-1)$ générateurs (éléments d'ordre $p-1$).
Si p admet un certificat alors nous avons déjà vu ci-dessus que $\mathbb{Z}/p^\times$ est cyclique d'ordre $p-1$ et donc p est premier. □

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.

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 $\mathrm{ord}(g)$.

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 $k = 0, 1, 2, 3, \ldots$ est trop coûteux en général.
Par contre, étant donné g et a il est facile à calculer g^a.

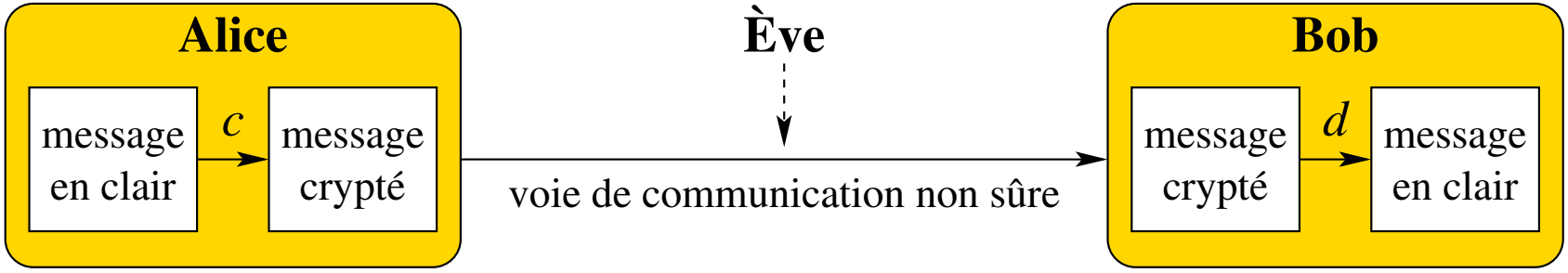
Slogan

La cryptographie repose sur des fonctions $f \colon X \to Y$ 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.



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 !

Implémentations du protocole Diffie–Hellman

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.

Il intercepte la clé g^a envoyé par Alice et envoie à Bob une autre clé $g^{a'}$.
De même, il remplace la clé g^b envoyée par Bob par une autre clé $g^{b'}$.
L'attaquant communique avec Alice en utilisant leur clé commune $g^{ab'}$.
De même, il communique avec Bob en utilisant leur clé commune $g^{a'b}$.

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.

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

Implémentations du protocole Elgamal

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.

Le théorème de Lagrange

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.

Démonstration. On définit une relation d'équivalence $a \sim b$ par $a^{-1}b \in H$.

- Réflexivité : $a \sim a$,
  car $a^{-1}a = e \in H$. (SG1)
- Symétrie : $a \sim b$ implique $b \sim a$,
  car $a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} = b^{-1}a \in H$. (SG2)
- Transitivité : $a \sim b$ et $b \sim c$ entraînent $a \sim c$,
  car $a^{-1}b, b^{-1}c \in H \Rightarrow (a^{-1}b)(b^{-1}c) = a^{-1}c \in H$. (SG3)

Une classe d'équivalence pour $\sim$ est de la forme

$$\mathfrak{cl}(a) = \{b \in G \mid a \sim b\} = \{b \in G \mid a^{-1}b \in H\} = \{ah \mid h \in H\} = aH.$$

On note $G/H = \{aH \mid a \in G\}$ l'ensemble quotient. C'est une partition de G en sous-ensembles disjoints. Pour tout $a \in G$ les applications

$$H \to aH, \quad h \mapsto ah, \qquad \text{et} \qquad aH \to H, \quad g \mapsto a^{-1}g$$

sont des bijections mutuellement inverses, donc $|aH| = |H|$.
On conclut que $|G| = |G/H| \cdot |H|$. □

Les théorèmes de Fermat et d'Euler

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 $\mathrm{ord}(x) \mid p-1$ 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 $\mathrm{ord}(x) \mid \varphi(n)$ 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

Nous savons que $p = 2^{32} \cdot 3^{32} \cdot 5^{32} + 1$ est un nombre premier ($p = 185302018885184100000000000000000000000000001$).

Comment déterminer l'ordre de $x = \bar{3}$ dans $\mathbb{Z}/_p^\times$?
La méthode naïve est de calculer $x^1, x^2, x^3, \ldots$. C'est inefficace !

On sait que $|\mathbb{Z}/_p^\times| = 2^{32} \cdot 3^{32} \cdot 5^{32}$ donc $\mathrm{ord}(x) = 2^a 3^b 5^c$ où $0 \leq a, b, c \leq 32$.
Ceci permet de trouver l'ordre de x par tâtonnement éclairé :

$$
\begin{array}{lcll}
x^{(2^{32}\cdot 3^{32}\cdot 5^{32})} = \bar{1} & & & \\
x^{(2^{31}\cdot 3^{32}\cdot 5^{32})} = \bar{1} & & & \\
\vdots & & & \\
x^{(2^{26}\cdot 3^{32}\cdot 5^{32})} = \bar{1} & \rightarrow & x^{(2^{26}\cdot 3^{32}\cdot 5^{32})} = \bar{1} & \\
x^{(2^{25}\cdot 3^{32}\cdot 5^{32})} \neq \bar{1} & & x^{(2^{26}\cdot 3^{31}\cdot 5^{32})} = \bar{1} & \\
 & & x^{(2^{26}\cdot 3^{30}\cdot 5^{32})} = \bar{1} & \rightarrow \quad x^{(2^{26}\cdot 3^{30}\cdot 5^{32})} = \bar{1} \\
 & & x^{(2^{26}\cdot 3^{29}\cdot 5^{32})} \neq \bar{1} & \quad\;\; x^{(2^{26}\cdot 3^{30}\cdot 5^{31})} \neq \bar{1} \\
\vdots & & \vdots & \vdots \\
x^{(2^{0}\cdot 3^{32}\cdot 5^{32})} \neq \bar{1} & & x^{(2^{26}\cdot 3^{0}\cdot 5^{32})} \neq \bar{1} & \quad\;\; x^{(2^{26}\cdot 3^{30}\cdot 5^{0})} \neq \bar{1}
\end{array}
$$

On trouve ainsi $\mathrm{ord}(\bar{3}) = 2^{26} \cdot 3^{30} \cdot 5^{32}$.

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** ℓ **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.

Calculer l'ordre d'un élément dans un groupe

Solution. Soit G un groupe d'ordre $|G| = p_1^{e_1} \cdots p_\ell^{e_\ell}$.
D'après Lagrange, l'ordre m d'un sous-groupe $\langle g \rangle \subset G$ vérifie $m \mid n$.
Ainsi $m = p_1^{m_1} \cdots p_\ell^{m_\ell}$ où les exposants vérifient $0 \leq m_k \leq e_k$ pour tout k.
La correction de l'algorithme découle de l'observation suivante :

Lemme

Soit $n = p_1^{n_1} \cdots p_\ell^{n_\ell}$. Alors $g^n = 1$ si et seulement si $n_k \geq m_k$ pour tout k.

Démonstration. On a $g^n = 1$ dans G si et seulement si $n \in m\mathbb{Z}$.
Ceci équivaut à dire que $m \mid n$, d'où la conclusion. □

Dans le pire des cas le tâtonnement nécessite $e_1 + \cdots + e_\ell$ essais.
Chaque essaie nécessite une exponentiation dans le groupe G.
L'algorithme est efficace grâce à l'exponentielle rapide ! ☺

Construction du groupe quotient dans le cas commutatif

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 $\mathfrak{cl}(a) = a + H = \{a + h \mid h \in H\}$.
On note $\pi : G \to G/H$, $a \mapsto \mathfrak{cl}(a)$, l'application quotient.

Proposition

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

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

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

Démonstration.
Unicité. — Si une telle structure existe alors $\mathfrak{cl}(a) + \mathfrak{cl}(b) = \mathfrak{cl}(a + b)$.

Existence. — Il faut montrer que $\mathfrak{cl}(a) + \mathfrak{cl}(b) = \mathfrak{cl}(a + b)$ est bien définie.
Soit $\mathfrak{cl}(a) = \mathfrak{cl}(a')$ et $\mathfrak{cl}(b) = \mathfrak{cl}(b')$, c'est-à-dire $a - a' \in H$ et $b - b' \in H$.
La commutativité assure que $(a + b) - (a' + b') = (a - a') + (b - b') \in H$.
Ainsi $\mathfrak{cl}(a + b) = \mathfrak{cl}(a' + b')$. On peut donc poser $\mathfrak{cl}(a) + \mathfrak{cl}(b) := \mathfrak{cl}(a + b)$.
Cette opération est une loi de groupe : on vérifie qu'elle est associative, commutative, l'élément neutre est $\mathfrak{cl}(0)$, et l'inverse de $\mathfrak{cl}(a)$ et $\mathfrak{cl}(-a)$. □

Exemples de groupes quotients

Exemples

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

Exercice

Soit $\pi\colon G \to G/H$ le morphisme quotient. Déterminer $\mathrm{im}(\pi)$ et $\ker(\pi)$.
Déterminer les sous-groupes de G/H en termes des sous-groupes de G.
Illustrer vos résultats par le quotient $\pi\colon \mathbb{Z} \to \mathbb{Z}/24\mathbb{Z}$, 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 $G = \mathrm{Sym}(3)$ et $H = \langle(12)\rangle$.
L'ensemble quotient G/H n'admet pas de structure de groupe
pour laquelle l'application quotient $\pi\colon G \to G/H$ soit un morphisme.

Passage au groupe quotient

Proposition

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

1. $K \subset \ker(\phi)$
2. *Il existe un morphisme de groupes $\bar{\phi}\colon G/K \to H$ 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.*

Démonstration. «⇐» Si $a \in K$ alors $\pi(a) = 0$, donc $\phi(a) = \bar{\phi} \circ \pi(a) = 0$.

«⇒» Supposons que $K \subset \ker(\phi)$, et construisons $\bar{\phi}$ tel que $\phi = \bar{\phi} \circ \pi$
Cette exigence entraîne que $\bar{\phi}(\mathfrak{cl}(a)) = \phi(a)$. Montrons que c'est bien défini.
Si $\mathfrak{cl}(a) = \mathfrak{cl}(b)$, alors $a - b \in K$, donc $a - b \in \ker(\phi)$, puis $\phi(a) = \phi(b)$.
On peut donc définir $\bar{\phi}\colon G/K \to H$ par $\bar{\phi}(\mathfrak{cl}(a)) := \phi(a)$.
On a $\phi = \bar{\phi} \circ \pi$ par construction. C'est un morphisme de groupes :

$$\bar{\phi}(\mathfrak{cl}(a) + \mathfrak{cl}(b)) = \bar{\phi}(\mathfrak{cl}(a+b)) = \phi(a+b) = \phi(a) + \phi(a) = \bar{\phi}(\mathfrak{cl}(a)) + \bar{\phi}(\mathfrak{cl}(b))$$

Ceci prouve la proposition. □

Factorisation canonique des morphismes

Corollaire

Tout morphisme de groupes $\phi\colon G \to H$ induit un isomorphisme de groupes $\bar{\phi}\colon G/\ker(\phi) \xrightarrow{\sim} \mathrm{im}(\phi)$.

Démonstration. D'abord ϕ induit un morphisme surjectif $\tilde{\phi}\colon G \to \mathrm{im}(\phi)$.
Par passage au quotient $\tilde{\phi}$ induit un morphisme $\bar{\phi}\colon G/\ker(\phi) \to \mathrm{im}(\phi)$.
Si $\bar{\phi}(\bar{a}) = \bar{\phi}(\bar{b})$ alors $\phi(a) = \phi(b)$, donc $a - b \in \ker(\phi)$, d'où $\bar{a} = \bar{b}$. □

Exemple

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

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

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

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

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 $\{g_1, \ldots, g_r\} \subset G$ définit un épimorphisme

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

Le théorème dit que l'on peut choisir $\{g_1, \ldots, g_r\}$ 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

$$\bar{\phi}\colon \mathbb{Z}/_{m_1} \times \cdots \times \mathbb{Z}/_{m_r} \xrightarrow{\sim} G, \quad (\overline{a_1}, \ldots, \overline{a_r}) \mapsto a_1 g_1 + \cdots + a_r g_r$$

Théorème (version forte)

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

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

*Dans ce cas la famille $(m_1, m_2, \ldots, m_s)$ est uniquement déterminée par G. On appelle $m_1, m_2, \ldots, m_s$ les **diviseurs élémentaires** de G.*

Démonstration. Réduction des matrices sur $\mathbb{Z}$ (Jacobson, *Basic Algebra*).

Exercices : groupes et sous-groupes

Exercice

Soit $\phi\colon G \to H$ un morphisme de groupes supposé bijectif.
Est-ce que l'application inverse $\phi^{-1}\colon H \to G$ 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 $p = \mathrm{ord}(a)$ et $q = \mathrm{ord}(b)$.

1. Montrer que $\mathrm{ord}(ab) \mid m$ où $m = \mathrm{ppcm}(p, q)$.
2. Illustrer par un exemple que $\mathrm{ord}(ab) < m$ est possible.
3. Si $\mathrm{pgcd}(p, q) = 1$, alors $\mathrm{ord}(ab) = pq$. (Indication : Bézout et Lagrange)

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 $\mathrm{Sym}(3)$ et dans $\mathrm{Sym}(4)$?
Est-ce que tout diviseur de $|G|$ se réalise comme ordre d'un sous-groupe ?

Exercices

Exercice

Soit $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ 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 $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto k\bar{a}$.
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.