MA435 Introduction aux corps finis

Alena Pirutka

École Polytechnique & Courant Institute, NYU

Paris Tech Shanghai, 18 Septembre 2015

Programme :

- relations d'equivalence, groupes, exemples;
- anneaux, propriétés;
- extensions de corps, corps finis;
- initiation aux applications cryptographiques.

Programme :

- relations d'equivalence, groupes, exemples;
- anneaux, propriétés;
- extensions de corps, corps finis;
- initiation aux applications cryptographiques.

Documents : lien sur ma page web pour acceder

- à la polycopie, qui contient plus d'exercices
- aux slides.

Cours 1 :
Relations d'equivalence
Groupes

Exemple : Quand on dit *les nombres pairs* ou *les nombres impairs* on identifie les nombres entiers selon un critère : s'ils sont divisibles par 2 ou pas.

Exemple : Quand on dit *les nombres pairs* ou *les nombres impairs* on identifie les nombres entiers selon un critère : s'ils sont divisibles par 2 ou pas.

Un principe : une *relation d'équivalence* sur un ensemble E (resp. une *relation binaire* entre E et F) permet d'identifier certains éléments de E (resp. de E et F).

Définition. Soient E et F deux ensembles. Le *produit cartésien* de E et F noté $E \times F$ est l'ensemble des couples (x, y) où $x \in E$ et $y \in F$:

$$E \times F = \{(x, y) \,|\, x \in E, y \in F\}.$$

Définition. Soient E et F deux ensembles. Le *produit cartésien* de E et F noté $E \times F$ est l'ensemble des couples (x, y) où $x \in E$ et $y \in F$:

$$E \times F = \{(x, y) \,|\, x \in E, y \in F\}.$$

Définition. Une relation binaire entre deux ensembles E et F est une partie (un sous-ensemble) $\mathcal{R}$ du produit cartesien $E \times F$. Pour $x \in E$ et $y \in F$ on note $x\mathcal{R}y$ ou $x \sim_{\mathcal{R}} y$ (où même simplement $x \sim y$) si $(x, y) \in \mathcal{R}$. Si $E = F$ on dit qu'on a une relation binaire sur E.
(voir les exemples 1.1.2 poly)

$\mathcal{R}$ une relation binaire sur l'ensemble E est

$\mathcal{R}$ une relation binaire sur l'ensemble E est

1. *réflexive* si pour tout $x \in E$ on a $x \sim x$;

$\mathcal{R}$ une relation binaire sur l'ensemble E est

1. *réflexive* si pour tout $x \in E$ on a $x \sim x$;
2. *transitive* si pour tous $x, y, z \in E$ on a $x \sim y$ et $y \sim z \Rightarrow x \sim z$;

$\mathcal{R}$ une relation binaire sur l'ensemble E est

1. *réflexive* si pour tout $x \in E$ on a $x \sim x$;
2. *transitive* si pour tous $x, y, z \in E$ on a $x \sim y$ et $y \sim z \Rightarrow x \sim z$;
3. *symétrique* si pour tous $x, y \in E$ on a $x \sim y \Leftrightarrow y \sim x$;

$\mathcal{R}$ une relation binaire sur l'ensemble E est

1. *réflexive* si pour tout $x \in E$ on a $x \sim x$;
2. *transitive* si pour tous $x, y, z \in E$ on a $x \sim y$ et $y \sim z \Rightarrow x \sim z$;
3. *symétrique* si pour tous $x, y \in E$ on a $x \sim y \Leftrightarrow y \sim x$;
4. *antisymétrique* si pour tous $x, y \in E$ on a $x \sim y$ et $y \sim x \Leftrightarrow x = y$.

$\mathcal{R}$ une relation binaire sur l'ensemble E est

1. *réflexive* si pour tout $x \in E$ on a $x \sim x$;
2. *transitive* si pour tous $x, y, z \in E$ on a $x \sim y$ et $y \sim z \Rightarrow x \sim z$;
3. *symétrique* si pour tous $x, y \in E$ on a $x \sim y \Leftrightarrow y \sim x$;
4. *antisymétrique* si pour tous $x, y \in E$ on a $x \sim y$ et $y \sim x \Leftrightarrow x = y$.

Une *relation d'équivalence* sur l'ensemble E est une relation réflexive, transitive et symétrique.

$\mathcal{R}$ une relation binaire sur l'ensemble E est

1. *réflexive* si pour tout $x \in E$ on a $x \sim x$;
2. *transitive* si pour tous $x, y, z \in E$ on a $x \sim y$ et $y \sim z \Rightarrow x \sim z$;
3. *symétrique* si pour tous $x, y \in E$ on a $x \sim y \Leftrightarrow y \sim x$;
4. *antisymétrique* si pour tous $x, y \in E$ on a $x \sim y$ et $y \sim x \Leftrightarrow x = y$.

Une *relation d'équivalence* sur l'ensemble E est une relation réflexive, transitive et symétrique.
Une *relation d'ordre* sur l'ensemble E est une relation réflexive, transitive et antisymétrique.
(voir les exemples 1.1.3-4 poly)

Un principe : Soit $\mathcal{R}$ une relation d'equivalence sur l'ensemble E (par exemple, la relation de congruence modulo 2), on peut alors voir l'ensemble E comme l'union de *classes* des éléments équivalents (par exemple, les nombres paires et impaires).

Un principe : Soit $\mathcal{R}$ une relation d'equivalence sur l'ensemble E (par exemple, la relation de congruence modulo 2), on peut alors voir l'ensemble E comme l'union de *classes* des éléments équivalents (par exemple, les nombres paires et impaires).
Définition. Soit E un ensemble. Une *partition* de E est un ensemble des parties non vides deux à deux disjointes de E dont E est la réunion.
(voir les exemples 1.1.5 poly)

Definition. Soit E un ensemble. Soit $\mathcal{R}$ une relation d'équivalence sur E. On définit, pour tout $x \in E$

$$\bar{x} = \{y \in E \,|\, x \sim y\}$$

la *classe d'équivalence* de x pour $\mathcal{R}$.

Definition. Soit E un ensemble. Soit $\mathcal{R}$ une relation d'équivalence sur E. On définit, pour tout $x \in E$

$$\bar{x} = \{y \in E \,|\, x \sim y\}$$

la *classe d'équivalence* de x pour $\mathcal{R}$.

Proposition. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. Les différentes classes d'équivalence forment une partition de E. (la preuve est au tableau)

Définition. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. *L'ensemble quotient* $E/\mathcal{R}$ est l'ensemble des classes d'équivalence pour $\mathcal{R}$. On note $E \to E/\mathcal{R}, x \mapsto \bar{x}$ la surjection canonique.

Définition. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. *L'ensemble quotient* $E/\mathcal{R}$ est l'ensemble des classes d'équivalence pour $\mathcal{R}$. On note $E \to E/\mathcal{R}, x \mapsto \bar{x}$ la surjection canonique.

Un principe : toute relation d'équivalence provient d'une application : la surjection canonique $E \to E/\mathcal{R}$. Dans l'ensemble $E/\mathcal{R}$ on *identifie* certains éléments de E (ceux qui sont équivalents par la relation $\mathcal{R}$).

Définition. Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. *L'ensemble quotient* $E/\mathcal{R}$ est l'ensemble des classes d'équivalence pour $\mathcal{R}$. On note $E \to E/\mathcal{R}, x \mapsto \bar{x}$ la surjection canonique.

Un principe : toute relation d'équivalence provient d'une application : la surjection canonique $E \to E/\mathcal{R}$. Dans l'ensemble $E/\mathcal{R}$ on *identifie* certains éléments de E (ceux qui sont équivalents par la relation $\mathcal{R}$).

Corollaire. Soit E un ensemble fini muni d'une relation d'équivalence $\mathcal{R}$. Soient $E_1, \dots E_r$ les différentes classes d'équivalence.

(i) $\mathrm{Card}(E) = \sum_{i=1}^{r} \mathrm{Card}(E_r)$;

(ii) si toutes les classes ont le même nombre d'éléments, on a $\mathrm{Card}(E) = m \cdot \mathrm{Card}(E/\mathcal{R})$.

(voir exemples 1.1.9 poly)

Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$ et soit $f : E \to F$ une application. On dit que f *passe au quotient* par $\mathcal{R}$ si

$$x \sim y \Rightarrow f(x) = f(y).$$

On peut alors définir une applicaition $\bar{f} : E/\mathcal{R} \to F$ par $\bar{f}(\bar{x}) = f(x)$; cette application est bien définie.
(voir exemples 1.1.10 poly)

Un principe: $\mathbb{Z}$ est naturellement muni des lois de composition comme l'addition et la multiplication.

Un principe: $\mathbb{Z}$ est naturellement muni des lois de composition comme l'addition et la multiplication.
Définition: X un ensemble. Une *loi de composition interne* sur X est une application $X \times X \to X$.
(voir exemples 1.2.1 poly)

Un principe: $\mathbb{Z}$ est naturellement muni des lois de composition comme l'addition et la multiplication.
Définition: X un ensemble. Une *loi de composition interne* sur X est une application $X \times X \to X$.
(voir exemples 1.2.1 poly)
Définition Une loi de composition interne $*$ sur un ensemble X est dite:
associative si $\forall a, b, c \in X, (a * b) * c = a * (b * c)$,
commutative si $\forall a, b \in X, a * b = b * a$.

Un principe: $\mathbb{Z}$ est naturellement muni des lois de composition comme l'addition et la multiplication.
Définition: X un ensemble. Une *loi de composition interne* sur X est une application $X \times X \to X$.
(voir exemples 1.2.1 poly)
Définition Une loi de composition interne $*$ sur un ensemble X est dite:
associative si $\forall a, b, c \in X, (a * b) * c = a * (b * c)$,
commutative si $\forall a, b \in X, a * b = b * a$.
Question. Lesquelles parmi les lois des exemples précédents sont associatives? Commutatives?

Définition. Soit X un ensemble muni d'une loi de composition interne $*$. Un élément $e_g \in X$ est *un élément neutre à gauche* si $\forall a \in X, e_g * a = a$. Un élément $e_d \in X$ est *un élément neutre à droite* si $\forall a \in X, a * e_d = a$.

Définition. Soit X un ensemble muni d'une loi de composition interne $*$. Un élément $e_g \in X$ est *un élément neutre à gauche* si $\forall a \in X, e_g * a = a$. Un élément $e_d \in X$ est *un élément neutre à droite* si $\forall a \in X, a * e_d = a$.

Exercice! Montrer que s'il existe un élément neutre à gauche et un élément neutre à droite, alors ils coïncident. On appelle l'élément ainsi défini *l'élément neutre* tout court.

Definition Un *groupe* est un ensemble G muni d'une loi de composition interne . telle que

(i) . est associative;

(ii) il existe un élément neutre $e \in G$: $\forall a \in X, e.a = a.e = a$;

(iii) pour chaque élément $a \in G$ il existe un élément que l'on note $a^{-1} \in G$ et qu'on appelle *l'inverse de a*, tel que $a.a^{-1} = a^{-1}.a = e$.

Si de plus la loi est commutative, on dit que le groupe est *abélien* ou *commutatif*.
(voir exemples 1.2.4 poly)

Definition Un *groupe* est un ensemble G muni d'une loi de composition interne . telle que

(i) . est associative;

(ii) il existe un élément neutre $e \in G$: $\forall a \in X, e.a = a.e = a$;

(iii) pour chaque élément $a \in G$ il existe un élément que l'on note $a^{-1} \in G$ et qu'on appelle *l'inverse de a*, tel que $a.a^{-1} = a^{-1}.a = e$.

Si de plus la loi est commutative, on dit que le groupe est *abélien* ou *commutatif*.
(voir exemples 1.2.4 poly)
Remarque : Soit $a \in G$, l'inverse de a est unique.

Défintion. Soient G et G' deux groupes. Une application $f : G \to G'$ est un *morphisme de groupes* si $f(x.y) = f(x).f(y)$ pour tous $x, y \in G$. Si f est bijective et f^{-1} est aussi un morphisme, on dit que f est un *isomorphisme*, si de plus $G = G'$ on dit que f est un automorphisme.
On dit parfois *homomorphisme* pour un morphisme de groupes.
(voir exemples 1.2.5 poly)

Définition. Un sous-ensemble H d'un groupe G est un *sous-groupe* G' s'il vérifie :

- $e \in H$;
- pour tous $x, y \in H$, $xy \in H$;
- pour tout $x \in H$, $x^{-1} \in H$.

Définition. Un sous-ensemble H d'un groupe G est un *sous-groupe* G' s'il vérifie :

- $e \in H$;
- pour tous $x, y \in H$, $xy \in H$;
- pour tout $x \in H$, $x^{-1} \in H$.

Proposition. Soit $f : G \to G'$ un morphisme de groupes, soient H (resp. H') un sous-groupe de G (resp. de G'). Alors

- $f(H)$ est un sous-groupe de G', en particulier $Im\, f = f(G)$ est un sous-groupe de G';
- $f^{-1}(H')$ est un sous-groupe de G, en particulier $Ker f = f^{-1}(e_H)$ est un sous-groupe de G.

(voir exemples 1.2.6-7 poly)

Définition. Soit G un groupe. Un sous-groupe H de G est *distingué* (ou *normal*) s'il est stable par des automorphismes intérieurs : pour tous $g \in G, h \in H$ on a $ghg^{-1} \in H$. On écrit alors $H \triangleleft G$.
(voir exemples 1.2.8 poly)

Définition. Soit G un groupe. Un sous-groupe H de G est *distingué* (ou *normal*) s'il est stable par des automorphismes intérieurs : pour tous $g \in G, h \in H$ on a $ghg^{-1} \in H$. On écrit alors $H \triangleleft G$.
(voir exemples 1.2.8 poly)
Proposition. Soit $f : G \to G'$ un morphisme de groupes, soient $H \triangleleft G$ et $H' \triangleleft G'$. Alors

- $f(H)$ est un sous-groupe distingué dans $f(G)$ (mais pas dans G en général);
- $f^{-1}(H')$ est distingué dans G, en particulier $Kerf$ est un sous-groupe distingué de G.

Soient G un groupe et soit $H \subset G$ un sous-groupe de G. On définit une partition de G en classes à gauche (resp. à droite) selon H comme suit :

à gauche $x \sim y$ si $x^{-1}y \in H$. L'ensemble quotient est noté G/H (ses éléments sont les classes aH, $a \in G$).

à droite $x \sim y$ si $xy^{-1} \in H$. L'ensemble quotient est noté $H \setminus G$ (ses éléments sont les classes Ha, $a \in G$).

Soient G un groupe et soit $H \subset G$ un sous-groupe de G. On définit une partition de G en classes à gauche (resp. à droite) selon H comme suit :

à gauche $x \sim y$ si $x^{-1}y \in H$. L'ensemble quotient est noté G/H (ses éléments sont les classes aH, $a \in G$).

à droite $x \sim y$ si $xy^{-1} \in H$. L'ensemble quotient est noté $H \setminus G$ (ses éléments sont les classes Ha, $a \in G$).

Proposition. Soit G un groupe et $H \triangleleft G$ est un sous-groupe distingué de G. Alors pour tout $a \in G$ les classes aH et Ha coïncident et $G/H = H \setminus G$. Il existe une unique structure de groupe sur G/H telle que la surjection canonique $G \to G/H$ soit un morphisme de groupes.
(voir exemples 1.2.10 poly)

Proposition. Soit $f : G \to G'$ un morphisme de groupes. Alors le morphisme f passe au quotient par $H = ker(f)$: il existe un unique homomorphisme $\bar{f} : G/ker(f) \to G'$ tel que $f = \bar{f} \circ \pi$ où π est la surjection canonique $G \to G/ker(f)$. De plus, $\bar{f}$ induit un isomorphisme entre $G/ker(f)$ et $Im(f)$.

Proposition. Soit $f : G \to G'$ un morphisme de groupes. Alors le morphisme f passe au quotient par $H = ker(f)$: il existe un unique homomorphisme $\bar{f} : G/ker(f) \to G'$ tel que $f = \bar{f} \circ \pi$ où π est la surjection canonique $G \to G/ker(f)$. De plus, $\bar{f}$ induit un isomorphisme entre $G/ker(f)$ et $Im(f)$.

Une suite $1 \to G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \to 1$ de groupes et de morphismes de groupes est *exacte* si

- f_1 est injectif ($ker(f_1) = e_{G_1}$);
- f_2 est surjectif;
- $Im(f_1) = ker(f_2)$: f_2 induit un isomorphisme $G_2/G_1 \xrightarrow{\sim} G_3$.

Exemple : $1 \to SL_n(\mathbb{R}) \to GL_n(\mathbb{R}) \to \mathbb{R}^* \to 1$.