HAX501X – Groupes et anneaux 1

CM1 07/09/2023

Clément Dupont

Organisation

- Poly, feuilles de TD, slides de CM, etc. disponibles sur Moodle.

- Amphi : Clément Dupont.
- TD groupe A : Philippe Castillon.
- TD groupe B : Clément Dupont.
- TD groupe C : Thierry Mignon.

- Évaluation : deux contrôles continus (vendredi 20/10 et vendredi 15/12) et un examen terminal en janvier. La note finale est calculée grâce à la **règle du max** (40-60) entre la moyenne des deux CC et la note du contrôle terminal.

Travail

- Je considère la présence en amphi et en TD **obligatoire** pendant tout le semestre pour pouvoir réussir.

- Après un cours en amphi, il est impératif de relire et d'apprendre la partie du cours correspondante. Le cours doit être su **par coeur**.
- Il y aura des questions de cours à toutes les évaluations. Cela inclut les démonstrations.

- Le poly contient des exercices, qui seront corrigés en amphi, ou parfois en TD. Il est impératif de les préparer avant le cours suivant en amphi, **en relisant le cours**.

- Posez-moi des questions !

Programme

1 – Rappels d'arithmétique des entiers

2 – Étude de $\mathbb{Z}/n\mathbb{Z}$

3 – Introduction à la théorie des groupes

4 – Introduction à la théorie des anneaux et des corps

1 – Rappels d'arithmétique des entiers

1. Addition et multiplication des entiers relatifs

2. Divisibilité, division euclidienne, congruences

3. PGCD et PPCM

4. Gauss, Euclide, et factorisation en produit de nombres premiers

1. Addition et multiplication des entiers relatifs

2. Divisibilité, division euclidienne, congruences

3. PGCD et PPCM

4. Gauss, Euclide, et factorisation en produit de nombres premiers

$\mathbb{Z}$ est un groupe abélien

▶ L'ensemble $\mathbb{Z}$, muni de la loi $+$ de l'addition, est un **groupe**. Cela veut dire qu'on a les propriétés suivantes.

1) Associativité de $+$: $\forall a, b, c \in \mathbb{Z}\,,\ (a+b)+c = a+(b+c)$.
2) Élément neutre pour $+$: 0 est l'élément neutre, c'est-à-dire que $\forall a \in \mathbb{Z}\,,\ a+0 = a = 0+a$.
3) Inverse pour $+$: pour tout $a \in \mathbb{Z}$ il existe $b \in \mathbb{Z}$ tel que $a+b = 0 = b+a$. Il est appelé l'opposé de a et noté $-a$.

▶ Comme la loi $+$ est commutative, on dit que $\mathbb{Z}$ est un **groupe abélien**.

4) Commutativité de $+$: $\forall a, b \in \mathbb{Z}\,,\ a+b = b+a$.

$\mathbb{Z}$ est un anneau commutatif

▶ L'ensemble $\mathbb{Z}$, muni des lois $+$ et $\times$, est un **anneau**. Cela veut dire qu'on a les propriétés suivantes.

1) $(\mathbb{Z}, +)$ est un groupe abélien.
2) Associativité de $\times$: $\forall a, b, c \in \mathbb{Z}\,,\ (a \times b) \times c = a \times (b \times c)$.
3) Élément neutre pour $\times$: 1 est l'élément neutre, c'est-à-dire que $\forall a \in \mathbb{Z}\,,\ a \times 1 = a = 1 \times a$.
4) Distributivité de $\times$ par rapport à $+$: $\forall a, b, c \in \mathbb{Z}\,,\ a \times (b + c) = (a \times b) + (a \times c)$ et $(a + b) \times c = (a \times c) + (b \times c)$.

▶ Comme la loi $\times$ est commutative, on dit que $\mathbb{Z}$ est un **anneau commutatif**.

5) Commutativité de $\times$: $\forall a, b \in \mathbb{Z}\,,\ a \times b = b \times a$.

1. Addition et multiplication des entiers relatifs

2. Divisibilité, division euclidienne, congruences

3. PGCD et PPCM

4. Gauss, Euclide, et factorisation en produit de nombres premiers

Divisibilité

- **Divisibilité** des entiers (relatifs) : pour $a, b \in \mathbb{Z}$, on dit que a divise b et on écrit $a|b$ s'il existe $k \in \mathbb{Z}$ tel que $b = ak$.

- **Nombre premier** : un entier naturel p qui a exactement deux diviseurs positifs distincts (1 et p). Par convention, 1 n'est pas premier.

- **Division euclidienne** : pour tous $a, b \in \mathbb{Z}$ avec $b \neq 0$, on peut écrire de manière unique

$$a = bq + r \quad \text{avec } q, r \in \mathbb{Z} \text{ et } 0 \leqslant r < |b|.$$

Congruences

- **Congruences** : pour $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$,

$$a \equiv b \pmod{n} \quad \Longleftrightarrow \quad n | (a - b).$$

  Cela revient à dire que a et b ont le même reste dans la division euclidienne par n.

- La relation de congruence modulo n est une **relation d'équivalence** (réflexive, symétrique, transitive).

- La relation de congruence modulo n est compatible à la somme et au produit : si $a \equiv b \pmod{n}$ et $a' \equiv b' \pmod{n}$ alors on a :

$$a + a' \equiv b + b' \pmod{n} \quad \text{et} \quad aa' \equiv bb' \pmod{n}.$$

Inversion modulo un entier

Définition

On dit qu'un $a \in \mathbb{Z}$ est **inversible modulo** n *s'il existe $b \in \mathbb{Z}$ tel que*

$$ab \equiv 1 \pmod{n}.$$

On dit alors que b est **un inverse de** a **modulo** n.

- On ne parle pas de **l'**inverse de a modulo n puisqu'il n'y a pas unicité : si b est un inverse de a modulo n, alors tout b' qui est congru à b modulo n l'est aussi.

Exemple

On a

$$5 \times 7 \equiv 1 \pmod{17}$$

et donc 5 est inversible modulo 17, et 7 est **un** inverse de 5 modulo 17. Un autre inverse de 5 modulo 17 est $7 - 17 = -10$.

Un inverse modulo n est unique... modulo n

Proposition

Si $b, b' \in \mathbb{Z}$ sont deux inverses de a modulo n alors $b \equiv b' \pmod{n}$.

Démonstration.

- En multipliant des deux côtés la congruence $ab \equiv 1 \pmod{n}$ par b' on obtient $abb' \equiv b' \pmod{n}$.
- En multipliant des deux côtés la congruence $ab' \equiv 1 \pmod{n}$ par b on obtient $abb' \equiv b \pmod{n}$.
- Comme la relation de congruence modulo n est symétrique et transitive, on en conclut que $b \equiv b' \pmod{n}$.

□

À quoi ça sert ?

Proposition

Soit $a \in \mathbb{Z}$ un entier inversible modulo n, et soit $b \in \mathbb{Z}$ un inverse de a. Alors on a, pour tous $x, y \in \mathbb{Z}$, l'équivalence :

$$ax \equiv y \pmod{n} \iff x \equiv by \pmod{n}.$$

Démonstration.

$\Longrightarrow$: En multipliant des deux côtés par b on obtient :

$$abx \equiv by \pmod{n}.$$

D'autre part, comme $ab \equiv 1 \pmod{n}$ par hypothèse, on a en multipliant des deux côtés par x :

$$abx \equiv x \pmod{n}.$$

Comme la relation de congruence modulo n est symétrique et transitive, on en conclut que $x \equiv by \pmod{n}$.

$\Longleftarrow$: Même démonstration en multipliant des deux côtés par a.

□

1. Addition et multiplication des entiers relatifs

2. Divisibilité, division euclidienne, congruences

3. PGCD et PPCM

4. Gauss, Euclide, et factorisation en produit de nombres premiers

Sous-groupes de $\mathbb{Z}$

Définition

Un **sous-groupe de** $\mathbb{Z}$ *est un sous-ensemble* $H \subset \mathbb{Z}$ *qui vérifie les conditions suivantes :*

1) $0 \in H$;
2) H *est stable par somme :* $\forall a, b \in H,\ a + b \in H$;
3) H *est stable par passage à l'opposé :* $\forall a \in H,\ -a \in H$.

- Soit H un sous-groupe de $\mathbb{Z}$. Pour $a \in H$ et $k \in \mathbb{Z}$, on a : $ka \in H$.
- Pour tout entier naturel n, l'ensemble des multiples de n, noté

$$n\mathbb{Z} = \{nk\,,\ k \in \mathbb{Z}\}$$

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

- Dans la suite du cours on l'appellera le **sous-groupe de** $\mathbb{Z}$ **engendré par** n.

Classification des sous-groupes de $\mathbb{Z}$

Théorème
Soit H un sous-groupe de $\mathbb{Z}$. Il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Définition
On appelle n le **générateur positif** *de H.*

Démonstration.

- Commençons par l'unicité. Soient $m, n \in \mathbb{N}$ tels que $m\mathbb{Z} = n\mathbb{Z}$. Comme $m \in m\mathbb{Z}$, on a donc $m \in n\mathbb{Z}$ et donc $n|m$. De même, comme $n \in n\mathbb{Z}$ on a $n \in m\mathbb{Z}$ et donc $m|n$. Comme m et n sont $\geqslant 0$, on a donc $m = n$.
- Démontrons maintenant l'existence ...

□

Définition du PGCD

Proposition

Soient $a, b \in \mathbb{Z}$. L'ensemble

$$a\mathbb{Z} + b\mathbb{Z} = \{au + bv \, , \, u, v \in \mathbb{Z}\}$$

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

Définition

Le générateur positif de $a\mathbb{Z} + b\mathbb{Z}$ est appelé le **plus grand commun diviseur (PGCD)** *de a et b. On le note $\mathrm{PGCD}(a, b)$ ou $a \wedge b$.*

- On a donc :

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}.$$

Le PGCD comme plus grand diviseur commun

Proposition

Soient $a, b \in \mathbb{Z}$. Alors $a \wedge b$ est l'unique $d \in \mathbb{N}$ qui vérifie les deux conditions suivantes :

1) $d|a$ *et* $d|b$;
2) *pour tout* $e \in \mathbb{N}$, $(e|a$ *et* $e|b) \Longrightarrow e|d$.

- Dit autrement : l'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de $a \wedge b$.

Remarque

Il est vrai que le PGCD de a et b est le plus grand (au sens de l'ordre usuel $\leqslant$) entier naturel qui divise à la fois a et b. Mais c'est surtout, d'après la proposition précédente, le plus grand au sens de la divisibilité, ce qui est plus fort !

Propriétés du PGCD

Pour $a, b \in \mathbb{Z}$ on a :

1) $b \wedge a = a \wedge b$.
2) $(-a) \wedge b = a \wedge b$.
3) si $a \in \mathbb{N}$ alors $a \wedge a = a$.
4) Pour tout $k \in \mathbb{N}$ alors $(ka) \wedge (kb) = k(a \wedge b)$.

- Pour $a, b, k \in \mathbb{Z}$ on a :

$$(a + kb) \wedge b = a \wedge b.$$

- "Le PGCD de a et b ne change pas si on remplace a par $a + kb$. "
- Cela permet de calculer $a \wedge b$ par divisions euclidiennes successives. C'est l'**algorithme d'Euclide**.

Entiers premiers entre eux

- On dit que $a, b \in \mathbb{Z}$ sont **premiers entre eux** si $a \wedge b = 1$.
- Cela revient à dire que le seul diviseur positif commun à a et b est 1.
- Pour $a, b \in \mathbb{Z}$, si on pose $d = a \wedge b$, on peut écrire

$$a = da' \quad \text{et} \quad b = db' \quad \text{avec} \quad a' \wedge b' = 1.$$

- Si p est un nombre premier, on a l'équivalence, pour tout $a \in \mathbb{Z}$:

$$a \wedge p = 1 \quad \Longleftrightarrow \quad p \text{ ne divise pas } a.$$

PPCM

Proposition

Soient $a, b \in \mathbb{Z}$. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Définition

Le générateur positif de $a\mathbb{Z} \cap b\mathbb{Z}$ est appelé le **plus petit commun multiple (PPCM)** *de a et b. On le note $\mathrm{PPCM}(a, b)$ ou $a \vee b$.*

On a donc :

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

Le PPCM comme plus petit multiple commun

Proposition

Soient $a, b \in \mathbb{Z}$. Alors $a \vee b$ est l'unique $m \in \mathbb{N}$ qui vérifie les deux conditions suivantes :

1) $a|m$ *et* $b|m$;
2) *pour tout* $n \in \mathbb{N}$, $(a|n$ *et* $b|n) \Longrightarrow m|n$.

- Dit autrement : l'ensemble des multiples communs à a et b est l'ensemble des multiples de $a \vee b$.

Remarque

Il est vrai que le PPCM de a et b est le plus petit (au sens de l'ordre usuel $\leqslant$) entier naturel qui est un multiple de a et de b. Mais c'est surtout, d'après la proposition précédente, le plus petit au sens de la divisibilité, ce qui est plus fort !

Propriétés du PPCM

Pour $a, b \in \mathbb{Z}$, on a :

1) $b \vee a = a \vee b$.
2) $(-a) \vee b = a \vee b$.
3) si $a \in \mathbb{N}$ alors $a \vee a = a$.
4) $(a \vee b) | ab$.
5) Pour tout $k \in \mathbb{N}$ on a : $(ka) \vee (kb) = k(a \vee b)$.

- Relation entre PGCD et PPCM : pour $a, b \in \mathbb{N}$, si on note $d = a \wedge b$ et $m = a \vee b$, on a :

$$ab = dm.$$

1. Addition et multiplication des entiers relatifs

2. Divisibilité, division euclidienne, congruences

3. PGCD et PPCM

4. Gauss, Euclide, et factorisation en produit de nombres premiers

Le lemme de Gauss, le lemme d'Euclide

Théorème (Lemme de Gauss)

Soient $a, b, c \in \mathbb{Z}$. *Si* $a|bc$ *et* $a \wedge b = 1$ *alors* $a|c$.

Théorème (Variante du lemme de Gauss)

Soient $a, b, c \in \mathbb{Z}$. *Si* $a|c$, $b|c$, *et* $a \wedge b = 1$, *alors* $ab|c$.

Théorème (Lemme d'Euclide)

Soient $a, b \in \mathbb{Z}$, *et soit* p *un nombre premier. Si* $p|ab$, *alors* $p|a$ *ou* $p|b$.

Factorisation en produit de nombres premiers

Théorème (Factorisation en produit de nombres premiers)

Tout entier $n \in \mathbb{N}^*$ peut s'écrire comme un produit de nombres premiers, de manière unique à l'ordre des facteurs près.

- L'existence est facile. L'unicité se base sur le lemme d'Euclide.

Proposition

Soient deux entiers $n, n' \in \mathbb{N}^*$ écrits comme des produits de nombres premiers :

$$n = \prod_{p \text{ premier}} p^{a_p} \quad \text{et} \quad n' = \prod_{p \text{ premier}} p^{a'_p}.$$

Alors on a :

$$n \wedge n' = \prod_{p \text{ premier}} p^{\min(a_p, a'_p)} \quad \text{et} \quad n \vee n' = \prod_{p \text{ premier}} p^{\max(a_p, a'_p)}.$$