L2 UE Arithmétique dans Z

Daouda Sangare
Université Nangui Abrogoua
Abidjan, Côte d'Ivoire

February 24, 2016

Chapitre 1

Entiers naturels - Dénombrement

Prérequis : Relation d'ordre sur un ensemble, relation d'équivalence, classe d'équivalence, ensemble quotient.

1.1. Les ensembles usuels de nombres

On note :
$\mathbb{N}$ l'ensemble des **entiers naturels** $\mathbb{N} = \{0, 1, 2, ...\}$,
$\mathbb{Z}$ l'ensemble des **entiers relatifs**
$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$
$\mathbb{Z}$ est donc l'ensemble des entiers naturels et leurs opposés
L'ensemble des **nombres rationnels** se note $\mathbb{Q} = \{r = p/q,\ p, q \in \mathbb{Z}$, avec $q \neq 0\}$
L'ensemble $\mathbb{R}$ des **nombres réels** est formé des nombres rationnels et des nombres irrationnels tels que, $\sqrt{2}, \pi, e$ etc.
L'ensemble $\mathbb{C}$ des **nombres complexes** est formé des nombres de la forme $x = a + ib$, où $a, b \in \mathbb{R}$ et où i est un élément vérifiant l'équation $i^2 = -1$.

Propriétés de $\mathbb{N}$
L'ensemble $\mathbb{N}$ est muni d'une **relation d'ordre total notée** $\leq$. Cette relation d'ordre vérifie les propriétés suivantes :

Propriété 1($\mathbb{N}$ est bien ordonné)
Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Propriété 2
Toute partie non vide majorée de $\mathbb{N}$ admet un plus grand élément.

1.2. Raisonnement par récurrence

On a souvent besoin de montrer que certaines propriétés sont vraies pour tous les entiers naturels n. Comme l'ensemble des entiers naturels est infini, on ne peut donc pas tester la propriété en question sur chaque entier naturel. On utilise l'artifice du **raisonnement** dit **par récurrence** dont voici quelques exemples.

Quelques exemples

Théorème1
Soit $P(n)$ une propriété portant sur l'entier $n \in \mathbb{N}$.
Pour que $P(n)$ soit vraie pour tout $n \in \mathbb{N}$ il faut et il suffit que l'on ait :
$\begin{cases} \text{(i) } P(o) \text{ est vraie} \\ \text{(ii) Pour chaque } n \in \mathbb{N}, \text{ si } P(n) \text{ est vraie, alors } P(n+1) \text{ est vraie} \end{cases}$
Dans le théorème 1 on peut supposer que les choses se passent seulement à partir d'un certain rang n_0.

Théorème2
Soit $P(n)$ une propriété portant sur l'entier $n \in \mathbb{N}$.
Pour que $P(n)$ soit vraie pour tout $n \geq n_0$, il faut et il suffit que l'on ait :
$\begin{cases} \text{(i) } P(n_0) \text{ est vraie} \\ \text{(ii) Pour tout entier } n \geq n_0, \text{ si } P(n) \text{ est vraie, alors } P(n+1) \text{ est vraie} \end{cases}$

Exercice:
1. Montrer par récurrence l' identité suivante :
$0 + 1 + 2 + ... + n = \dfrac{n(n+1)}{2}$

Réponse :
Soit $P(n)$ cette propriété. $P(0)$ est vraie
Supposons que $P(n)$ soit vrai. Alors
$0+1+2+...+n+n+1 = \dfrac{n(n+1)}{2} + n + 1 = (n+1)[\dfrac{n}{2}+1] = \dfrac{(n+1)(n+2)}{2}$
Donc $\forall\, n \in \mathbb{N}$, $[P(n) \Longrightarrow P(n+1)]$. Par conséquent $\forall\, n \in \mathbb{N}$ $P(n)$ est vraie.

2. Montrer par récurrence l' identité suivante :
$0^2 + 1^2 + 2^2 + ... + n^2 = \dfrac{n(n+1)(2n+1)}{6}$

Réponse :
Soit $P(n)$ cette propriété. $P(0)$ est vraie
Supposons que $P(n)$ soit vraie. Montrons que $P(n+1)$ est vraie.
On a $0^2 + 1^2 + 2^2 + ... + n^2 + (n+1)^2 = \dfrac{n(n+1)(2n+1)}{6} + (n+1)^2$
$= (n+1)[\dfrac{n(2n+1)}{6} + (n+1)] = (n+1)\dfrac{(2n^2+7n+6)}{6}$
$= \dfrac{(n+1)(n+2)(2n+3)}{6}$

Donc $P(n+1)$ est vraie.

Exercice
Montrer que $\forall n \in \mathbb{N}$, $2^n > n$

Réponse :
Pour $n = 0$, on a $2^0 = 1 > 0$
Soit $n \geq 1$ tel que que $2^n > n$.
Alors $2^{n+1} = 22^n > 2n \geq n + 1$

Remarque
On pouvait utiliser la formule du binôme
$2^n = (1+1)^n = \sum_{p=0}^{n} \binom{n}{p} = 1 + \binom{n}{1} + ...$
$> 1 + \binom{n}{1} = 1 + n > n$

Exercice
Trouver toutes les applications $f : \mathbb{N} \longrightarrow \mathbb{N}$ telles que $\forall m, n \in \mathbb{N}$, on ait $f(m+n) = f(m) + f(n)$

Réponse :
Soit f une telle application.
On a $f(0+0) = f(0) + f(0)$
Donc $f(0) = 2f(0)$, d'où $f(0) = 0$
Posons $a = f(1)$
Alors $f(2) = f(1+1) = 2f(1) = 2a$
Supposons que $f(n) = na$
Alors $f(n+1) = f(n) + f(1) = na + a = (n+1)a$
Donc on a nécessairement $f(n) = na$ $\forall n \in \mathbb{N}$
Réciproquement si $f(n) = na$ $\forall n \in \mathbb{N}$ alors $f(m+n) = (m+n)a = ma + na = f(m) + f(n)$
Donc les solutions sont exactement les fonctions de la forme $f(n) = na$ où a est une constante $\in \mathbb{N}$.

Exercice
Trouver toutes les applications $f : \mathbb{N} \longrightarrow \mathbb{N}$ injectives telles que $n \in \mathbb{N}$, on ait $f(n) \leq n$.

Réponse :
On montre par récurrence que $f(n) = n$ $\forall n \in \mathbb{N}$

Il y a des situations où l'on a besoin de la **récurrence forte** suivante :

Théorème3
Soit $P(n)$ une propriété portant sur l'entier $n \in \mathbb{N}$.

Pour que $P(n)$ soit vraie pour tout $n \geq n_0$, il faut et il suffit que l'on ait :

$$\begin{cases} \text{(i) } P(n_0) \text{ est vraie} \\ \text{(ii) } \forall n \in \mathbb{N} \text{ tel que } n \geq n_0, \text{ si } P(k) \text{ est vraie pour tout } k = n_0, n_0+1, ..., n \text{ alors } P(n+1) \text{ est vraie} \end{cases}$$

Exemple 1

Soit (u_n) la suite définie par

$$\begin{cases} u_0 = 2 \\ u_1 = 3 \\ \forall n \in \mathbb{N},\ u_{n+2} = 3u_{n+1} - 2u_n \end{cases}$$

Tableau des premières valeurs prises par la suite

n	0	1	2	3	4	5	6
u_n	2	3	5	9	17	33	65

Ce tableau suggère la proprié $P(n) : u_n = 2^n + 1 \ \forall \ n \in \mathbb{N}$

Vérifions cette propriété par récurrence

$P(0)$ et $P(1)$ sont vraies.

Supposons que $P(n)$ et $P(n+1)$ soient vraies. Alors

$\forall n \in \mathbb{N},\ u_{n+2} = 3u_{n+1} - 2u_n = 3(2^{n+1} + 1) - 2(2^n + 1)$

$= 2^{n+1}(3-1) + 1 = 2^{n+2} + 1$

Donc $P(n)$ et $P(n+1)$ vraies implique $P(n+2)$

Par conséquent pout tout entier $n \geq 0$, la propriété $P(n)$ est vraie.

Exemple 2

Voir la preuve du résultat qui affirme que tout nombre admet au moins un diviseur premier

1.3. Divisibilité dans $\mathbb{N}$

Soient a, b deux entiers naturels. On dit que a *divise* b et l'on écrit a/b, s'il existe $c \in \mathbb{N}$ tel que $b = ac$. On dit aussi que b est un multiple de a.

Un entier n est dit *pair* si $2/n$, *impair* si $2/(n+1)$

Exercices

1. Montrer que la relation a *divise* b est une relation d'ordre partiel dans $\mathbb{N}$.

2. $\forall (a, b, c, d) \in \mathbb{N}^4$, montrer que :

(i) $a/b \Longrightarrow a/bc$

(ii) a/b et $a/c \Longrightarrow a/(b+c)$

(iii) a/b et $c/d \Longrightarrow ac/bd$

(iv) $a/b \Longrightarrow \forall\ n \in \mathbb{N},\ a^n/b^n$.

Définition

Un nombre $p \in \mathbb{N}$ est **premier** si $p \geq 2$ et si les seuls diviseurs de p sont 1 et p.

Exemples

$2, 3, 5, 7, 11, ...,$

Voici un exemple d'application de **la récurrence forte**

Proposition
Tout entier naturel n admet au moins un diviseur premier

Preuve
soit $P(n)$ la propriété "n admet au moins un diviseur premier"
$P(2)$ est vraie.

Soit n un entier ≥ 2. Supposons la propriété vraie jusqu'au rang n, c'est à dire que $P(2)$, $P(3)$, $P(4), ...P(n)$ soient vraies. Montrons que $P(n+1)$ est vraie.

Si $n+1$ est premier , alors il est diviseur premier de lui-même et $P(n+1)$ est vraie.

Si $n+1$ n'est pas premier, alors il existe un entier $d, 1 \leq d < n+1$, tel que d divise $n+1$.

Comme $d \leq n$, alors d'après l'hypothèse de récurrence, d admet au moins un diviseur premier qui est donc un diviseur premier de $n+1$ Donc $P(n+1)$ est vraie, c.q.f.d.

Proposition
L'ensemble $\mathcal{P}$ des nombres premiers est infini

Preuve
Raisonnons par l'absurde. Si $\mathcal{P}$ était fini, soit $k = card\ \mathcal{P}$. Ecrivons $\mathcal{P} = \{p_1, p_2, ..., p_k\}$. Soit
$m = 1 + p_1 p_2 ... p_k$.

m admet au moins un facteur premier p.Comme $p \in \mathcal{P}$ il existe $j \in \{1, 2, ..., k\}$ tel que $p = p_j$

Par conséquent p divise $p_1 p_2 ... p_k$ et p divise $m = 1 + p_1 p_2 ... p_k$, donc p divise $m - p_1 p_2 ... p_k = 1$, ce qui est absurde.

1.4. Coefficients binomiaux

Soient $0 \leq p \leq n$ deux entiers naturels. On pose
$$\binom{n}{p} = \frac{n(n-1)(n-2)...(n-p+1)}{p!} = \frac{n!}{p!(n-p)!}$$

Pour $p > n$, on pose $\binom{n}{p} = 0$

Remarque
Les $\binom{n}{p}$ s'appellent **coefficients binomiaux**. En réalité $\binom{n}{p}$ est la notation anglo saxonne correspondant à C_n^p. La notation $\binom{n}{p}$ est la plus utilisée sur le plan international. C'est pourquoi nous l'avons adoptée.

Propriétés essentielles des coefficients $\binom{n}{p}$

Proposition

$\binom{n}{p}$ est le nombre de parties à p éléments d'un ensemble à n éléments

Proposition

$\binom{n}{p} = \binom{n}{n-p}$ si $p \leq n$

$\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$ si $n \geq 1$ et $p \geq 1$.

Exercice

Montrer que

a) $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$

b) $\binom{n}{p} = \frac{n-p+1}{p}\binom{n}{p-1}$

Formule du binôme

$\forall\ a,\ b \in \mathbb{Z},\ (a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^{n-p}b^p$ où n est un entier naturel.

Preuve

La formule est vraie pour $n = 0$. En effet $1 = (a+b)^0 = \binom{0}{0}a^0b^0$

Supposons que la propriété soit vraie pour n. Montrons qu'elle est vraie pour $n+1$

Par hypotèse $(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^{n-p}b^p$

Il s'agit de montrer que $(a+b)^{n+1} = \sum_{p=0}^{n+1} \binom{n+1}{p} a^{n+1-p}b^p$

On utilisera la formule $\binom{n+1}{p} = \binom{n}{p} + \binom{n}{p-1}$

On a $(a+b)^{n+1} = (a+b)\sum_{p=0}^{n} \binom{n}{p} a^{n-p}b^p$

$= \sum_{p=0}^{n} \binom{n}{p} a^{n+1-p}b^p + \sum_{p=0}^{n} \binom{n}{p} a^{n-p}b^{p+1}$

$= \binom{n}{0}a^{n+1} + \binom{n}{1}a^n b + \binom{n}{2}a^{n-1}b^2 + \ldots\ldots + \binom{n}{p}a^{n+1-p}b^p + \ldots\ldots + \binom{n}{n-1}a^2b^{n-1} + \binom{n}{n}ab^n$

$\binom{n}{n}b^{n+1} + \binom{n}{0}a^n b + \binom{n}{1}a^{n-1}b^2 + \binom{n}{2}a^{n-2}b^3 + \ldots + \binom{n}{p}a^{n-p}b^{p+1} + \ldots + \binom{n}{n-1}ab^n +$

$= a^{n+1} + b^{n+1} + (\binom{n}{0} + \binom{n}{1})a^n b + (\binom{n}{1} + \binom{n}{2})a^{n-1}b^2 + ... + (\binom{n}{n-1} + \binom{n}{n})ab^n$

$a^{n+1} + b^{n+1} + \binom{n+1}{1}a^{n+1-1}b + \binom{n+1}{2}a^{n-2+1}b^2 + ... + \binom{n+1}{n}ab^n$

$= \binom{n+1}{0}a^{n+1} + \binom{n+1}{1}a^{n+1-1}b + \binom{n+1}{2}a^{n-2+1}b^2 + ... + \binom{n+1}{n}ab^n + \binom{n+1}{n+1}b^{n+1}$

Donc $(a+b)^{n+1} = \sum_{p=0}^{n+1} \binom{n+1}{p} a^{n+1-p}b^p$

Remarque

On peut montrer que la formule précédente est vraie dans un anneau A quelconque si $ab = ba$.

Proposition

Le nombre de parties d'un ensemble fini E de cardinal n est égal à 2^n.

Preuve

$2^n = (1+1)^n = \sum_{p=0}^{n} \binom{n}{p}$

Il suffit ensuite de constater que E est la réunion disjointe de l'ensemble de ses parties à 0 élément, à 1 élément, à 2 éléments, etc. sachant que $\binom{n}{p}$ est le cardinal d'une partie à p éléments de E.

Chapitre 2

Arithmétique dans $\mathbb{Z}$

2.1. **Propriétés de** $\mathbb{Z}$

On rappelle que $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$

$(\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire intègre.

$(\mathbb{Z}, \leq)$ est un ensemble totalement ordonné.

Toute partie non vide minorée de $\mathbb{Z}$ admet un plus petit élément. Toute partie non vide majorée de $\mathbb{Z}$ admet un plus grand élément.

2.2. **Divisibilité dans** $\mathbb{Z}$

On prolonge à $\mathbb{Z}$ la divisibilité dans $\mathbb{N}$.

Soient $a, b \in \mathbb{Z}$. On dit que a divise b et l'on écrit a/b, s'il existe $c \in \mathbb{Z}$ tel que $b = ac$. On dit aussi que b est un multiple de a.

Exemples

1. Tout entier $k \in \mathbb{Z}$ divise 0 car $0 = k \times 0$. Mais si 0 divise k, alors $k = 0$

1. 1 et -1 divisent tous les autres entiers. En ffet $\forall\ k \in \mathbb{Z},\ k = 1.k = (-1)(-k)$

Mais les seuls diviseurs de 1 (resp. -1) sont 1 et -1.

2.3. **Division euclidienne dans** $\mathbb{Z}$

Soit $a \in \mathbb{Z}$ et soit $b \in \mathbb{N}^*$.. Alors il existe un couple unique d'entiers relatifs $(q,\ r)$ tel que

$a = bq + r$ avec $0 \leq r < b$.

q s'appelle **le quotient** de la division euclidienne de a par b

r s'appelle **le reste** de la division euclidienne de a par b

Remarque

Si q est le quotient et r le reste de la division euclidienne de a par $b \neq 0$, alors $q = [\frac{a}{b}]$

En effet $bq \leq a < bq + b = (q+1)b$, c'est à dire

$q \leq \dfrac{a}{b} < q + 1$

2.4. **Congruence**

Définition

Soit $n \in \mathbb{N}^*$.

$\forall a,\ b \in \mathbb{Z}\ \ a \equiv b\ [\text{mod } n] \iff n/(b-a) \iff \exists\ k \in \mathbb{Z},\ b = a + kn$

Exercice

Montrer que la congrence modulo n est une relation d'équivalence dans $\mathbb{Z}$

Notations

$\forall a \in \mathbb{Z}$ on note $cla = \overline{a} = \widehat{a} = \{x \in \mathbb{Z}\ ;\ a \equiv x\ [\text{mod } n]\ \} = \{x \in \mathbb{Z}\ ;\ \exists\ k \in \mathbb{Z},\ x = a + kn\}$

Remarques

1. $\forall a \in \mathbb{Z},\ a \in \overline{a}$ car la congruence modulo n est réflexive
2. $\forall a,\ b \in \mathbb{Z}\ \ a \equiv b\ [\text{mod } n] \iff b \in \overline{a} \iff \overline{a} = \overline{b}$

On note $\dfrac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n$ l'ensemble de toutes les classes d'équivalence. Cet ensemble est appelé **l'ensemble quotient modulo** n.

Soit $a \in \mathbb{Z}$. Alors d'après la division euclidienne, il existe un couple unique d'entiers relatifs $(q,\ r)$ tel que

$a = qn + r$ avec $0 \leq r < n$. Donc $a \equiv r\ [\text{mod } n]$, c'est à dire $\overline{a} = \overline{r}$ avec $r \in \{0,\ 1,\ 2, ...,\ n-1\}$

Ce qui prouve que $\dfrac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0},\ \overline{1},\ \overline{2}, ...,\ \overline{n-1}\}$. C'est un ensemble fini de cardinal n

Exemple

$$\frac{\mathbb{Z}}{6\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, .\ \overline{3}, \overline{4}, \overline{5}\}$$

Propriétés de la congruence

Soient $a, b, c \in \mathbb{Z}$. Alors

(i) Si $a \equiv b \ [\text{mod } n]$ et $c \equiv d \ [\text{mod } n]$, alors $a + c \equiv b + d \ [\text{mod } n]$ et $ac \equiv bd \ [\text{mod } n]$

(ii) Si $a \equiv b \ [\text{mod } n]$ alors $a + c \equiv b + c \ [\text{mod } n]$ et $ac \equiv bc \ [\text{mod } n]$

(iii) Si $a \equiv b \ [\text{mod } n]$ alors $\forall\ m \in \mathbb{N}$, $a^m \equiv b^m [\text{mod } n]$

Addition et multiplication dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Soient α et β deux éléments de $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Alors il existe $a, b \in \mathbb{Z}$ tels que $\alpha = \overline{a}$ et $\beta = \overline{b}$

On pose alors $\alpha + \beta = \overline{a + b}$ et $\alpha\ \beta = \overline{ab}$.

Ces définitions ont un sens car si $a' \in \overline{a} = \alpha$ et si $b' \in \overline{b} = \beta$, alors

$a \equiv a' \ [\text{mod } n]$ et $b \equiv b' \ [\text{mod } n]$, alors $a + b \equiv a' + b' \ [\text{mod } n]$,

c'est à dire $\overline{a + b} = \overline{a' + b'}$

De même $ab \equiv a'b' \ [\text{mod } n]$, donc $\overline{ab} = \overline{a'b'}$

Proposition

$(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times)$ est un anneau commutatif unitaire.

Remarque :

L'élément nul de cet anneau est $\overline{0} = n\mathbb{Z}$, tandis que l'élément neutre pour la multiplicatin est $\overline{1} = 1 + n\mathbb{Z}$.

Exemple

Dans $\frac{\mathbb{Z}}{4\mathbb{Z}}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Le petit Théorème de Fermat

Pour tout entier naturel n et pour tout nombre premier p, on a :

$(*)$ $n^p - n \equiv 0 (\text{mod } p)$

En particulier si p ne divise pas n, alors $n^{p-1} \equiv 1 (\text{mod } p)$

Preuve

Nous allons procéder par récurrence sur n.
Si $n = 0$, on a $0^p - 0 \equiv 0(\text{mod } p)$
Supposons la propriété vraie pour un entier $n \in \mathbb{N}$
Montrons qu'elle est vraie pour $n + 1$
On a
$(n+1)^p = \sum_{k=0}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) n^{p-k} = n^p + \sum_{k=1}^{p-1} \left(\begin{array}{c} p \\ k \end{array} \right) n^{p-k} + 1$
$\equiv n^p + 1$ [mod p] $\equiv n + 1$ [mod p] (d'après l'hypothèse de récurrence), la première congreunce ci-dessu provient du fait que pour $1 \leq k \leq p-1$, $\left(\begin{array}{c} p \\ k \end{array} \right) \equiv 0[\text{mod } p]$
En effet $l = \left(\begin{array}{c} p \\ k \end{array} \right) = \dfrac{p!}{k!(p-k)!}$,
$p! = k!(p-k)!l$
$p/k!(p-k)!l$, $(p,k) = 1 = (p, p-k)$, car $1 \leq k \leq p-1$
Donc $(p, k!) = 1 = (p, (p-k)!)$
Donc p/l
Si p ne divise pas n, alors $n(n^{p-1} - 1) \equiv 0(\text{mod}\, p)$, c'est à dire que $p/\ n(n^{p-1} - 1)$
Comme $(p, n) = 1$, alors $p/\ (n^{p-1} - 1)$. Donc $n^{p-1} \equiv 1(\text{mod } p)$.

Exemple :
Donner le reste de la division de 10^{15} par 13

Solutions
$p = 13$, $n = 10$, $n^{p-1} \equiv 1(\text{mod } p)$.
Donc $10^{12} \equiv 1(\text{mod } 13)$ et $10^{15} = 10^{12}10^3 \equiv 10^3(\text{mod } 13)$
$= 10^2 10(\text{mod } 13)$
$10^2 = 13 \times 7 + 9 \equiv 9(\text{mod } 13)$
Donc $10^{15} \equiv 90(\text{mod } 13)$
$90 = 13 \times 7 - 1 \equiv -1(\text{mod } 13) \equiv 12(\text{mod } 13)$
Donc $10^{15} \equiv 12(\text{mod } 13)$ et le reste de la division de 10^{15} par 13 est égal à 12.

Exercice résolu
Trouver le reste de la division de 10^{100} par $247 = 13 \times 19$

Solution

Modulo 13 :
On a $10^{13} \equiv 10[13]$. Comme $(10, 13) = 1$, alors $10^{12} \equiv 1$ [13]

$100 = 8 \times 12 + 4 \equiv 4$ [12]
Donc $10^{100} = 10^{8 \times 12 + 4} \equiv 10^4$ [13]
On a $10^2 = 100 = 7 \times 13 + 9 \equiv 9$ [13]

Donc $10^4 \equiv 9^2$ [13]
$9^2 = 81 = 7 \times 13 - 10 \equiv -10[13] = 3$ [13]
Donc $10^{100} \equiv 3$ [13]

Modulo 19 :
$10^{19} \equiv 10[19]$. Comme $(10, 19) = 1$, alors $10^{18} \equiv 1$ [19]

$100 = 5 \times 18 + 10 \equiv 10$ [18]
Donc $10^{100} = 10^{5\times 18+10} \equiv 10^{10}$ [19]
$10^{10} = (10^2)^5 = 100^5$

$100 = 5 \times 19 + 5 \equiv 5$ [19]
Donc $10^{100} \equiv 10^{10}$ [19] $\equiv 5^5$ [19] $= 5^2\ 5^2\ 5$ [19]
$= 6^2 \times 5$ [19] $= -10$ [19] $= 9$ [19]
Donc $10^{100} \equiv 9$ [19]
On a $3 \times 13 - 2 \times 19 = 39 - 38 = 1$
Donc $3 = 9 \times 13 - 2 \times 3 \times 19$ et $9 = 3 \times 9 \times 13 - 2 \times 9 \times 19$
Donc $3 \equiv -2\times 3\times 19 + 3\times 9\times 13$ [13] $\equiv 3(-38+117)$ [13] $= 3\times 79$ [13] $= 237$ [13]
De même $9 \equiv -2 \times 3 \times 19 + 3 \times 9 \times 13$ [19] $\equiv 237$ [19]
Finalement
$10^{100} \equiv 237$ [13] et $10^{100} \equiv 237$ [19]. Comme $(13, 19) = 1$, alors $10^{100} \equiv 237$ [13×19]
Donc le reste de la division de 10^{100} par $247 = 13 \times 19$ est 237.

Exercices (à faire en TD)
1. Montrer que $\forall\ n \in \mathbb{Z}$, $\dfrac{n^7}{7} + \dfrac{n^5}{5} + \dfrac{23n}{35} \in \mathbb{Z}$
Réponse :
$\dfrac{n^7}{7} + \dfrac{n^5}{5} + \dfrac{23n}{35} = \dfrac{5n^7 + 7n^5 + 23n}{35}$
Soit $u_n = 5n^7 + 7n^5 + 23n$.. Il suffit de mntrer que $u_n \equiv 0$[mod 35]
D'après le petit théorème de Fermat, $n^7 \equiv n$[mod 7]
Donc $u_n \equiv 5n + 2n$[mod 7] $\equiv 0$[mod 7]
De même

$n^5 \equiv n$[mod 5], Donc $u_n \equiv 7n + 3n$[mod 5] $\equiv 0$[mod 5]
Finalement comme $(5, 7) = 1$, on a $u_n \equiv 0$[mod 35].
2. Monrer que pour tout n,
a) $42/n^7 - n$
R.
$n^2 \equiv n$[mod 2], donc $n^7 \equiv n$[mod 2],
$n^3 \equiv n$[mod 3], donc $n^7 \equiv n$[mod 3]
$n^7 \equiv n$[mod 7],
Comme (2, 3, 7) = 1, $n^7 \equiv n$[mod 42].
b) Monrer que pour tout n, $2730/n^{13} - n$

R. $2730 = 2 \times 3 \times 5 \times 7 \times 13$

On termine comme en a)

2.5. PGCD, PPCM

Soient $a, b \in \mathbb{Z}$ l'un au moins étant non nul .

Si $(a, b) \neq (0, 0)$, alors l'ensemble des diviseurs communs de a et b est une partie non vide de $\mathbb{Z}$. En effet il contien 1. Cet ensemble est majoré par min $(|a|, |b|)$ Il admet donc un plus grand élément appelé **le plus grand commun diviseur,** en abrégé $p\,\text{gcd}$, de a et b.

Donc le $p\,\text{gcd}$ de a et b est l'unique **entier naturel** d vérifiant les deux propriétés suivantes :

(i) d/a et d/b

(ii) Si d' est un entier relatif tel que d'/a et d'/b alors d'/d

Le $p\,\text{gcd}$ de a et b sera noté $d = p\,\text{gcd}\ (a\ ,\ b)$ ou (a, b) ou $a \vee b$

De même si $a \neq 0$ et $b \neq 0$, alors l'ensemble des multiples > 0 communs de a et b est une partie non vide de $\mathbb{N}$. En effet il contient $|a|\ |b|$ . . Cet ensemble admet donc un plus petit élément appelé **le plus petit commun multiple,** en abrégé *ppcm*, de a et b.

Donc le *ppcm* de a et b est l'unique entier naturel m vérifiant les deux roprétés suivantes :

(i) m est un multiple de a et m est un multiple de b

(ii) Si m' est un entier relatif tel que m' est un multiple de a et m' est un multiple de b, alors m' est un multiple de m

Le *ppcm* de a et b sera noté $m = ppcm\ (a\ ,\ b)$ ou $m = a \wedge b$

Remarques

On a :

1. $p\,\text{gcd}\ (a\ ,\ b) = p\,\text{gcd}\ (|a|\ ,\ |b|)$
2. $ppcm(a\ ,\ b) = ppcm\ (|a|\ ,\ |b|)$

C'est pourquoi on supposera souvent que a et b sont des entiers naturels.

Exemple

$p\,\text{gcd}\ (12\ ,\ 18) = 6$

$ppcm(12, 18) = 36$

2.6. Algorithme d'Euclide

Soient $a, b \in \mathbb{N}^*$.

Alors par division euclidienne de a par b, il existe un couple unique d'entiers relatifs (q, r) tel que

$a = bq + r$ avec $0 \leq r < b$.

Si $r = 0$, alors $a = bq$ et $(a\ ,\ b) = b$

Supposons $r \neq 0$.

Alors $(a\ ,\ b) = (b\ ,\ r\ )$

En effet soit $c \in \mathbb{Z}$

Si c/a et c/b alors c/a et c/bq. Donc $c/a - bq = r$

Récproquement si c/r et c/b, alors c/r et c/bq. Donc $c/bq + r = a$

Donc l'ensemble des diviseurs commun de a et b est égal à l'ensemble des diviseurs communs de b et r.

Alors par division euclidienne de b par r, il existe un couple unique d'entiers relatifs (q_1, r_1) tel que

$b = q_1 r + r_1$ avec $0 \leq r_1 < r$.

Si $r_1 = 0$, alors $r = (b, r) = (a, b)$

Si $r_1 \neq 0$, alors d'après ce qui précède, $(b, r) = (r, r_1)$

$r = q_2 r_1 + r_2$, avec $0 \leq r_2 < r_1$.

On construit ainsi une suite de couples $(q, r), (q_1, r_1), (q_2, r_2), ...$, tels que

$a = bq + r$, $b = q_1 r + r_1$, $r = q_2 r_1 + r_2, ...$,

$r_{n-2} = q_n r_{n-1} + r_n$, $0 \leq r_n < r_{n-1}$, etc..

On a

$r > r_1 > r_2 > ..... > r_{n-1} > r_n > ...$

Donc il existe un entier N tel que $r_{N+1} = 0$. Donc $r_{N-1} = q_{N+1}\ r_N$

D'où $(a\ ,\ b) = (b\ ,\ r\ ) = (r, r_1) = ... = (r_{N-2},\ r_{N-1}) = (r_{N-1}, r_N) = r_N$

Ainsi $(a\ ,\ b)$ est le dernier reste non nul.

Proposition

Soient $a,\ b \in \mathbb{Z}^*$ et soit $d = (a,\ b)$

Alors il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tels $ua + bv = d$

Preuve

Quitte à remplacer a et b par leus valeur absolue, on peut supposer $a,\ b \in \mathbb{N}^*$.

Soit $b \in \mathbb{N}$ et soit $P(b)$. la propriété : Pour tout entier naturel $a \in \mathbb{N}$, il existe $u, v \in \mathbb{Z}$ tels que

$ua + bv = d$

$P'0)$ est vraie. En effet $\forall\ a \in \mathbb{N}$, $1a + 0v = a = (a, 0) = d$

Supposons $P(b-1)$ vraie où $b > 1$. Soit $a \in \mathbb{N}$ et soit $d = (a,\ b)$.

Par division euclidienne de a par b, on a $a = bq + r$ avec $0 \leq r < b$.

$(a, b) = (b, r) = d$

D'après l'hypothèse de récurrence, $P(r)$ est vraie. Donc il existe $u, v \in \mathbb{Z}$ tels que

$ub + rv = d = ub + (a - bq)v = av + (u - qv)b$

Donc il existe $u', v' \in \mathbb{Z}$ tels que

$u'a + bv' = d$, c.q.f.d.

2.7. Nombres premiers entre eux

Définition

Deux nombres $a, b \in \mathbb{Z}$ sont dits *premiers entre eux* si $(a, b) = 1$

donc si leurs seuls diviseurs communs sont 1 et -1.

Proposition (identité de Bezout)

Les entiers a et b sont premiers entre eux si et seulement si $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tels $ua + vb = 1$

Preuve

Si a et b sont premiers entre eux alors $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tels $ua + bv = 1$ (Proposition précédente)

Réciproquement supposons que $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tels $ua + bv = 1$

Soit c un diviseur commun de a et b . Alors $a = cq$, $b = cq'$

$ua + bv = ucq + vcq' = c(uq + vq') = 1$. Donc $c = \pm 1$ et a et b sont premiers entre eux.

Remarque

Soit $d = (a,b)$ et soient q_1 tels que $a = q_1 d$ et $b = q_2 d$

Alors $(q_1, q_2) = 1$. En effet soient $u, v \in \mathbb{Z}$ tels $ua + vb = d$

Alors $uq_1 d + vq_2 d = d$, donc $uq_1 + vq_2 = 1$ d'où $(q_1, q_2) = 1$ d'après Bézout.

Corollaire

Si $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tels $ua + vb = 1$, alors $(a,b) = (u,v) = (a,v) = (u,b) = 1$

Thèorème de Gauss

Soient $a, b, c \in \mathbb{Z}$.

Si a/bc et si $(a,b) = 1$, alors a/c

Preuve

Il existe $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tels $ua + vb = 1$

Alors $c = uac + bvc$

Come a/bc, alors $\exists\ q$ tel que $bc = qa$

Donc $c = uac + qav = a(uc + qv)$

Corollaire Soient $a, b, c \in \mathbb{Z}$. On a ce qui suit :

(i) Si a est premier avec b et si a est premier avec c, alors a est premier avec bc

(ii) Si a est premier avec b, alors a est premier avec b^n $\forall n \geq 1$.

(iii) Si a est premier avec b, alors a^m est premier avec b^n $\forall m, n \geq 1$.

(iv) Réciproquement, s'il existe $m, n \geq 1$, tels que a^m soit premier avec b^n, alors a est premier avec b.

Preuve

(i) Par hypothèse il existe $u_1\ , u_2, v_1,\ v_2 \in \mathbb{Z}$ tels que $u_1 a + v_1 b = 1$ et $u_2 a + v_2 c = 1$

Alors $1 = (u_1 a + v_1 b)(u_2 a + v_2 c) = a(u_1 u_2 a + u_1 v_2 c + u_2 v_1 b) + v_1 v_2 bc$

Donc d'après Bézout, a est premier avec bc.

(ii) Provient de (i) en prenant $b = c$, puis par récurrence sur n.

(iii) Echanger les rôles de a et b.

(iv) Il existe $(u,v) \in \mathbb{Z} \times \mathbb{Z}$ tels $ua^m + vb^n = 1$.

$(ua^{m-1})a + (vb^{n-1})b = 1$. Donc d'après Bézout, a est premier avec b

Proposition
Soient $a,\ b \in \mathbb{Z}^{\bullet}$

Alors $p\gcd\ (a,b)\ ppcm\ (a,b) = |a|\ |b|$
Preuve
On peut supposer $a,\ b \in \mathbb{N}^{\bullet}$. Soit $d = p\gcd\ (a,b)$. Alors $a = q_1 d,\ \ b = q_2 d$.
On doit montrer que $d\ ppcm\ (a,b) = q_1 q_2 d^2$, c'est à dire $ppcm\ (a,b) = q_1 q_2 d$
Or $q_1 q_2 d$ est un multiple comun de a et b. Soit m' un multiple commun de a et b.
Alors $m' = q_1' a = q_2' b$
Donc $m' = q_1' q_1 d = q_2' q_2 d$.
Par simplification par d, $q_1' q_1 = q_2' q_2$, donc $q_2 / q_1' q_1$. Comme $(q_2, q_1) = 1$, alors q_2 / q_1'
$q_1' = q_2 c$, donc $m' = q_1' q_1 d = c q_2 q_1 d$

Chapitre3

Groupes, Anneaux, Corps

3.1. Groupes

L'Algèbre est la branche des Mathématiques qui étudie les structures algébriques, c'est à dire les lois de composition. La structure classique de base est celle de groupe. On s'en sert ensuite pour définir la structure d'anneau, de corps, d'espace vectoriel etc...Les groupes interviennent dans des domaines variés : Géométrie, cristallographie, théorie de Galois qui en est le point de départ etc..

Définition
Soit E un ensemble. On appelle loi de composition interne sur E, toute application de $E \times E$ dans E notée généralement par le symbole de la multiplication

$(x,y) \longmapsto xy$. Mais ce n'est pas nécessairement la multiplication au sens habituel!

On appelle **groupe**, tout ensemble G muni d'une loi de composition interne $(x,y) \longmapsto xy$ qui vérifie les propriétés suivantes :

1. Cette loi est associative, c'est à dire que $\forall\ (x,y,z) \in G^3$, on a $(xy)z = x(yz)$

2. G possède un élément neutre, c'est à dire un élément généralement noté e tel que $\forall\ x \in G, xe = ex = x$. Un tel élément est unique.

3. Tout élément x de G admet un symétrique dans G, c'est à dire un élément $x' \in G$ tel que $xx' = x'x = e$. Ce symétrique est unique. Généralement on le note x^{-1}. Le **groupe** G est dit **abélien** ou **commutatif** si sa loi est commutative, c'est à dire si $\forall\ x, y \in G$, on a $xy = yx$.

La loi d'un groupe abélien est généralement notée additivement, c'est à dire par le signe $+$. Dans ce cas l'élément neutre est noté 0.

Exemples

1. $(\mathbb{N}, +)$ et $(\mathbb{R}, \times)$ ne sont pas des groupes
2. $(\mathbb{Z}, +), (\mathbb{Q}, +)(\mathbb{R}, +), (\mathbb{C}, +)$ sont des groupes additifs abéliens
3. $(\mathbb{R}^*, \times), (\mathbb{Q}^*, \times), (\mathbb{C}^*, \times)$ sont des groupes multiplicatifs abéliens.
4. $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$ est un groupe multiplicatif abélien.
5. Soit E un ensemble quelconque. On note $\mathfrak{S}_E$ l'ensemble des bijections de E dans E. Alors $(\mathfrak{S}_E, \circ)$ est un groupe généralement non abélien, appelé le groupe symétrique de E . Si $E = E_n$ est un ensemble fini de n éléments, alors on note $\mathfrak{S}_{E_n} = \mathfrak{S}_n$.

Exercice

Soit $E_3 = \{1, 2, 3\}$. Alors le cardinal de $\mathfrak{S}_3$ est $3! = 6$. Les éléments de $\mathfrak{S}_3$ sont :

$i = \binom{123}{123}$, $\tau_1 = \binom{123}{132}$, $\tau_2 = \binom{123}{321}$, $\tau_3 = \binom{123}{213}$, $\sigma_1 = \binom{123}{231}$, $\sigma_2 = \binom{123}{312}$.

Donner la table de $\mathfrak{S}_3$.

3.2 Sous groupes

Soit G un groupe. On appelle sous groupe de G toute partie H de G qui est un groupe pour la loi induite par celle de G. Une telle partie H est nécessairement non vide. En effet H contient un élément eutre qui est d'ailleurs celui de G.

Exercice

Soit H une partie non vide du groupe G. Montrer que les assertions suivantes sont équivalentes :

(i) H est un sous groupe de G

(ii) a) $\forall x, y \in H$, $xy \in H$

b) $\forall x \in H$, $x^{-1} \in H$.

(iii) $\forall x, y \in H$, $xy^{-1} \in H$.

Exercice

Ecrire l'énoncé de l'exercice précédent en notation additive.

Exemples

1 $(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{Q}, +)$. $(\mathbb{Q}^*, \times)$ est un sous groupe de $(\mathbb{R}^*, \times)$

2. $(\mathbb{R}_+^*, \times)$ est un sous groupe de $(\mathbb{R}^*, \times)$ mais pas de $(\mathbb{R}, +)$

3. $\mathbb{U} = \{z \in \mathbb{C}, |z| = 1\}$ est un sous groupe de $(\mathbb{C}^*, \times)$.

et l'ensemble $\mathbb{U}_n$ des racines nièmes de l'unité est un sous groupe de $(\mathbb{C}^*, \times)$.

Exercice

Soit G un groupe. On note $Z(G) = \{x \in G; xy = yx \ \forall \ y \in G\}$. Montrer que $Z(G)$ est un sous groupe de G appelé le centre de G.

3.3 Morphismes de groupes.

La notion de morphisme de groupes permet de transposer les opérations d'un groupe donné G dans un groupe G', ce qui peut être avantageux si la loi de G' est plus simple.

Soient G et G'deux groupes. On appelle morphisme (ou homomorphisme) de G dans G', toute application $f : G \rightarrow G'$telle que $\forall\ x, y \in G$, $f(xy) = f(x)f(y)$.

Dans cette définition on a noté multiplicativement les lois des deux groupes. Mais dans la pratique, ces deux lois sont quelconques l'une par rapport à l'autre.

Soit $f : G \rightarrow G'$ un morphisme de groupes. On note

$Kerf = \{x \in G$ tels que $f(x) = e'\}$, où e' est l'élément neutre de G',

$Imf = \{f(x), x \in G\}$

$Kerf$ s'appelle le noyau de f tandis que Imf s'appelle l'image de f.

$Kerf$ est un sous groupe de G. Imf est un sous groupe de G'.

Exercice

Soit $f : G \rightarrow G$' un morphisme de groupes. Montrer que :

(i) $f(e) = e$'

(ii) $f(x^{-1}) = f(x)^{-1} \forall x \in G$

(iii) f est injective $\Longleftrightarrow Kerf = (e)$

Remarque

En notation additive :

(i) $Kerf = \{x \in G$ tels que $f(x) = 0\}$.

(ii) f est injective $\Longleftrightarrow Kerf = (o)$

Un morphisme de groupes $f : G \rightarrow G$' est appelé isomorphisme si f est bijectif

3.4 Sous groupes distingués

Soit G un groupe et soit H un sous groupe de G. On définit les deux relations suivantes qui déterminées par la donnée de H.

$\forall\ x, y \in G$,

$x \underset{g}{\equiv} y \ \ (modH) \Longleftrightarrow x^{-1}y \in H \Longleftrightarrow y \in xH = \{xh,\ h \in H\}$

C'est une relation d'équivalence. On l'appelle la congruence à gauche modulo H

La classe d'un élément x de G est $\overline{x} = clx = \{y \in G$ tels que $x \underset{g}{\equiv} y \ (Mod\ H\}$

Donc $\overline{x} = xH$

L'ensemble quotient de G par cette relation d'équivalence, c'est à dire l'ensemble des différentes classes d'équivalence se note $(G/H)_g$.

On définit de manière duale la congruence à droite modulo H par :

$\forall\ x, y \in G$,

$x \underset{d}{\equiv} y \ \ (modH) \Longleftrightarrow yx^{-1} \in H \Longleftrightarrow y \in Hx = \{hx,\ h \in H\}$

C'est une relation d'équivalence. On l'appelle la congruence à droite modulo H

La classe d'un élément x de G est $\overline{x} = clx = \{y \in G$ tels que $x \underset{g}{\equiv} y \ (Mod\ H\} = Hx$

L'ensemble quotient de G par cette relation d'équivalence, c'est à dire l'ensemble des différentes classes à droite se note $(G/H)_d$.

On remarquera les deux ensembles quotients $(G/H)_g$ et $(G/H)_d$ sont différents en général mais ils ont le même nombre d'éléments. En effet l'application $\theta : xH \longmapsto Hx^{-1}$ de $(G/H)_g$ dans $(G/H)_d$ est bien définie car si $x \underset{g}{\equiv} y \ \ (modH)$, alors $x^{-1}y \in H$, $x^{-1} \in Hy^{-1}$, donc $H\ x^{-1} = H\ y^{-1}$. θ est trivialement surjective. D'autre part si $Hx^{-1} = Hy^{-1}$, alors $x^{-1} \in H\ y^{-1}$, donc $x^{-1}y \in H$, c'est à dire $y \in xH$ et $xH = yH$. θ est donc une bijection. Donc les deux ensembles ont même cardinal, $|(G/H)_g| = |(G/H)_d|$

Ce nombre commun s'appelle l'indice de H dans G et se note $[G/H]$.

Donc

$[G : H] = |(G/H)_g| = |(G/H)_d|$

On appelle ordre du groupe G le nombre (fini ou infini) de ses éléments. On le note $|G|$.

Définition

Un sous-groupe H du groupe G est dit distingué ou invariant ou normal et l'on écrit alors $H \lhd G$ si

$\forall\ x \in G, \forall\ y \in H$, on a $xyx^{-1} \in H$

Exercice

Soit H un sous-groupe du groupe G. Montrer que les quatre propriétés suivantes sont équivalents :

(i) $H \lhd G$

(ii) $\forall\ x \in G,\ xH \subseteq Hx$

(iii) $\forall\ x \in G,\ xH = Hx$

(iv) $(G/H)_g = (G/H)_d$

3.5 Groupe quotient

Soit H un sous groupe distingué du groupe G. Alors d'après l'exercice précédent $(G/H)_g = (G/H)_d$. On note G/H cet ensemble.

On définit dans G/H une multiplication par :

$\forall\ x, y \in G,\ xH\ yH = xyH$

On vérifie que cette loi est bien définie c'est à dire qu'elle ne dépend pas des représentants des classes. On vérifie également aisément que G/H muni de cette multiplication est un groupe appelé groupe quotient de G par H. L'élément de G/H pour cette loi est $eH = H$, où e est l'élément neutre de G. Le symétrique de xH est $x^{-1}H$.

L'application $p : G \to G/H$ définie par $p(x) = \overline{x} = xH$ est un morphisme de groupes dit canonique.

Remarque

Si le groupe G est abélien, alors le groupe quotient G/H est abélien.

Exemple

$(G, \times) = (\mathbb{Z}, +)$, $H = n\mathbb{Z}$, où $n \geq 1$ est un entier.

Il est clair que $n\mathbb{Z} \lhd \mathbb{Z}$ D'une manière générale tout sous groupe d'un groupe abélien est abélien. On retrouve ici la congruence $Modulo\ n$ telle que définie dans le chapitre précédent. On a déjà étudié dans le chapitre en question les propriétés du groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

Exercice

Montrer que si $f : G \to G$' un morphisme de groupes, alors $Ker\ f \lhd G$.

Théorème de Lagrange

Soit G un groupe fini et soit H un sous groupe de G.

Alors $|G| = |H|\,[G : H]$

Exercice

Etudier le groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

Théorème d'isomorphisme

Soit $f : G \to G$' un morphisme de groupes. Alors il existe un isomorphisme unique $\overline{f} : G/kerf \to Imf$ tel que $\overline{f}\ (xN) = f(x)\ \forall\ x \in G$, où $N = kerf$.

Remarques

1. On retiendra le théorème d'isomorphisme sous sa forme pratique $G/kerf \simeq Imf$.

2. Lorsque les groupes G et G' sont abéliens alors l'isomorphisme $\overline{f} : G/kerf \to Imf$ ci-dessus s'écrit $\overline{f}(xN) = f(x) \forall x \in G$, où $N = Kerf$.

Exercice : Le groupe symétrique $\mathfrak{S}_n$

Soit E un ensemble quelconque. On note $\mathfrak{S}_E$ l'ensemble des bijections de Edans E.

1. Montrer que ($\mathfrak{S}_E$, $\circ$) est un groupe généralement non abélien, appelé le groupe symétrique de E .

Si $E = E_n$ est un ensemble fini de n éléments, alors on note $\mathfrak{S}_{E_n} = \mathfrak{S}_n$.

Désormais on note $E_n = \{1, 2, ..., n\}$ Le cardinal de E_n est $n!$ Les éléments $\sigma \in \mathfrak{S}_n$ seront représentés par

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$$

2. Soit $E_3 = \{1, 2, 3\}$. Alors le cardinal de $\mathfrak{S}_3$ est $3! = 6$. Les éléments de $\mathfrak{S}_3$ sont :

$i = \binom{1\ 2\ 3}{1\ 2\ 3}$, $\tau_1 = \binom{1\ 2\ 3}{1\ 3\ 2}$, $\tau_2 = \binom{1\ 2\ 3}{3\ 2\ 1}$, $\tau_3 = \binom{1\ 2\ 3}{2\ 1\ 3}$, $\sigma_1 = \binom{1\ 2\ 3}{2\ 3\ 1}$, $\sigma_2 = \binom{1\ 2\ 3}{3\ 1\ 2}$.

Donner la table de $\mathfrak{S}_3$.

3. Soient $H = \{i, \tau_1\}$ et $A = \{i, \sigma_1, \sigma_2\}$

a) Montrer que H et A sont des sous groupes de $\mathfrak{S}_3$

b) Déterminer l'ensemble quotient $(\frac{\mathfrak{S}_3}{H})_g$ et $(\frac{\mathfrak{S}_3}{H})_d$

c) H est- t- il un sous groupe distingué de $\mathfrak{S}_3$?

d) Montrer que $A \rhd \mathfrak{S}_3$

3.On appelle transposition de E_n toute permutation τ de E_n qui échange deux éléments et laisse invariants les n-2 autres. Si τ échange les élément i et j , on écrit

$$\tau = \tau_{ij} = \begin{pmatrix} 1 & 2 & ... & i & ... & j & ... & n \\ 1 & 2 & ... & j & ... & i & ... & n \end{pmatrix}$$

a) Montrer qu'il y a $n(n-1)/2$ trnspositions

b) Montrer que $\tau_{ij}^2 = id$. Donc $\tau_{ij}^{-1} = \tau_{ij}$.

3.7. Exercice (Le théorème chinois des restes)

1.Soient m et n deux entier premiers entre eux.

Montrer que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est naturellemet muni d'une structure d'anneau unitaire.

2. Montrer que le morphisme d'anneaux

$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ défini par

$\forall\ k \in \mathbb{Z}$, $\varphi(k) = (k + m\mathbb{Z},\ k + n\mathbb{Z})$ induit un isomorphisme

$\overline{\varphi} : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

3. Montrer que $\forall\ (a, b) \in \mathbb{Z}^2$, le système de congruences

$$(\mathrm{S}) \begin{cases} x \equiv a[m] \\ x \equiv b[n] \end{cases},$$

admet au moins une solution $x_1 \in \mathbb{Z}$.

4. Soient $k_1, k_2 \in \mathbb{Z}$ deux solutions su système (S). Montrer que

$k_1 \equiv k_2[mn]$.

5. Montrer que $U(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z})$

6. Montrer que les groupes $U(\mathbb{Z}/mn\mathbb{Z}$ et $U(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ sont isomorphes.

Réponse :

1.$\forall\ x, y, x', y' \in \mathbb{Z}$, $(x + m\mathbb{Z},\ y + n\mathbb{Z})+(x' + m\mathbb{Z},\ y' + n\mathbb{Z}) =(x + x' + m\mathbb{Z},\ y + y' + n\mathbb{Z})$

$(x + m\mathbb{Z},\ y + n\mathbb{Z})(x' + m\mathbb{Z},\ y' + n\mathbb{Z}) =(xx' + m\mathbb{Z},\ yy' + n\mathbb{Z})$

Ces deux lois confèrent à $\mathbb{Z}/m\mathbb{Z} \times\mathbb{Z}/n\mathbb{Z}$ une structure d'anneau commutatif unitaire.

2. L'application $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times\mathbb{Z}/n\mathbb{Z}$ définie par

$\forall\ x \in \mathbb{Z},\ \varphi(x) = (x + m\mathbb{Z},\ x + n\mathbb{Z})$ est un morphisme d'anneaux défini à l'aides des morphismes canoniques. Il est surjectif d'après la question 3 ci-dessous

Il est clair que $mn\mathbb{Z} \subseteq Ker\ \varphi$.

Réciproquement soit $x \in Ker\varphi$. Alors $x \in m\mathbb{Z}\cap\ n\mathbb{Z} = mn\mathbb{Z}$ car $(m, n) = 1$.

Donc $Ker\ \varphi = mn\mathbb{Z}$

Il en résulte que $\mathbb{Z}/m\mathbb{Z} \times\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$

3.Considérons le système de congruences

(S)$\begin{cases} x \equiv\ a[m] \\ x \equiv\ b[n] \end{cases}$, où $(a, b) \in \mathbb{Z}^2$.

Comme m et n sont premiers entre eux, alors d'après le théorème de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $um + vn = 1$

Posons $x_1 = vn$ et $x_2 = um$. Alors :

$\begin{cases} x_1 \equiv\ 1[m] \\ x_1 \equiv\ 0[n] \end{cases}$ et $\begin{cases} x_2 \equiv\ 0[m] \\ x_2 \equiv\ 1[n] \end{cases}$

Alors $(a, b) \in \mathbb{Z}^2$, $ax_1 + bx_2$ est une solution de (S)

4. Soient k_1 et k_2 deux solutions du Système (S). Alors k_1-$k_2 \in Ker\varphi = mn\mathbb{Z}$.

5.. Soit $(x, y) \in U(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$. Alors il existe $(x', y') \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tel que

$(x, y)(x', y') = (1, 1)$. Donc $xx' = 1$, $yy' = 1$. par conséquent $x \in U(\mathbb{Z}/m\mathbb{Z})$, $y \in U(\mathbb{Z}/n\mathbb{Z})$ et $(x, y) \in U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z})$

La réciproque se montre de façon analogue.

6. $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times\mathbb{Z}/n\mathbb{Z}$

Donc $U(\mathbb{Z}/mn\mathbb{Z}) \simeq U(\mathbb{Z}/m\mathbb{Z} \times\mathbb{Z}/n\mathbb{Z})$

3.8 Exercice (Indicateur d'Euler)

Soient n un entier naturel non nul, $x \in \mathbb{Z}$, $\overline{x}\ = x+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$. On suppose que $1 \leq x \leq n - 1$.

1. Montrer que les assertions suivantes sont équivalentes :

(i) $(x, n) = 1$

(ii) $\overline{x} \in U(\mathbb{Z}/n\mathbb{Z})$

(iii) $\overline{x}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$

2. On note $\varphi(n)$ le cardinal de $U(\mathbb{Z}/n\mathbb{Z})$, c'est à dire le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Donc d'après la question 1. ci-dessus, $\varphi(n)$ est le nombre d'entiers x tels que $1 \leq x \leq n - 1$ avec $(x, n) = 1$.

$\varphi(n)$ s'appelle **l'indicateur d'Euler de** n. On dit aussi que φ est **la fonction indicatrice d'Euler**. Dans ce qui suit, on se propose de calculer $\varphi(n)$ en fonction des facteurs premiers de n.

a) Montrer que si $(m,n)=1$, alors $\varphi(mn)=\varphi(m)\varphi(n)$

b) Soit p un nombre premier

Calculer $\varphi(p)$

Montrer que pour tout entier $k\geq 1$, $\varphi(p^k)=(p-1)p^{k-1}=p^k(1-\frac{1}{p})$

c) Montrer que si

$n=p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$, où $p_1,p_2,..p_r$ sont premiers et où $\alpha_i\geq 1\ \forall\ i$,

alors $\varphi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_r})$

Réponse

1. (i) $\Rightarrow$ (ii) Si $(x,n)=1$, alors il existe $u,v\in\mathbb{Z}$ tels que $ux+nv=1$

Donc $\overline{ux}=\overline{1}$ et $\overline{x}\in U(\mathbb{Z}/n\mathbb{Z})$.

(ii) $\Rightarrow$ (iii) Soit $y\in\mathbb{Z}$ tel que $\overline{xy}=\overline{1}$. Alors il existe $q\in\mathbb{Z}$ tels que $xy=1+qn$ et $\forall\ k\in\mathbb{Z}$, $\overline{k}=\overline{kxy}=ky\overline{x}$ et $\overline{x}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$

(iii) $\Rightarrow$ (i) $\forall\ k\in\mathbb{Z}$, il existe $q\in\mathbb{Z}$, tel que $\overline{k}=q\overline{x}$. En particulier pour $k=1,\overline{1}=\overline{qx}$, $1-qx=q'n$ et d'après Bezout $(x,n)=1$

2. a) Si $(m,n)=1$, alors $\varphi(mn)=cardU(\mathbb{Z}/mn\mathbb{Z}=card\ U(\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z})$

$=card(U(\mathbb{Z}/m\mathbb{Z})\times U(\mathbb{Z}/n\mathbb{Z}))=\varphi(m)\varphi(n)$.

b) Soit p un nombre premier. On $\varphi(p)=p-1$

Soit $k\geq 1$. Un élément $\overline{x}$ avec $0\leq x\leq p^k-1$, n'est pas inversible dans $\mathbb{Z}/p^k\mathbb{Z}$ si et seulement si x n'est pas premier avec p^k, donc si et seulement si p divise x. Il y a p^{k-1} éléments non inversibles dans $\mathbb{Z}/p^k\mathbb{Z}$.

Donc $\varphi(\ p^k)=p^k-\ p^{k-1}=p^k(1-\frac{1}{p})$

c) Si $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$, où $p_1,p_2,..p_r$ sont premiers et où $\alpha_i\geq 1\ \forall\ i$, alors

$\varphi(n)=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})...\varphi(.p_r^{\alpha_r})=p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_r})$

$=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_r})$.

3.9. Groupes cycliques

Soit G un groupe et soit F un sous ensemble de G. On s'intéresse à tous les sous groupes de G contenant F, et plus exactement au plus petit d'entre eux. On notera celui-là $<F>$. On vérifie que $<F>$ est l'intersection des sous groupes de G contenant F. On l'appelle **le sous groupe de G engendré par F**. Si $<F>=G$, on dit que F est un système générateur ou une partie génératrice de G.

Exemples

1. Si $F=\{a\}$ est un singleton où $a\in G$, alors le groupe multiplicatif engendré par F est

$<F>=\{a^k,k\in\mathbb{Z}\}=a^{\mathbb{Z}}$, tandis que si G était un groupe additif, le sous groupe additif de G engendré par F est

$<F>=\{ka,k\in\mathbb{Z}\}=a\mathbb{Z}$

2. Si F est un ensemble fini du groupe multiplicatif G, par exemple $F = \{a_1, a_2, ..., a_r\}$, et si ces éléments commutent deux à deux, alors on vérifie que le sous groupe de G engendré par F est égal à l'ensemble des éléments x de G qui sont de la forme

$x = a_1^{k_1} a_2^{k_2} ... a_r^{k_r}$, où $k_1, k_2, ..., k_r \in \mathbb{Z}$.

Si G est un groupe additif, alors

$< F > = \{x \in G, x = k_1 a_1 + k_2 a_2 + ... + k_r a_r\}$ où $k_i \in \mathbb{Z} \ \forall \ i$

$= a_1\mathbb{Z} + a_2\mathbb{Z} + ... + a_r\mathbb{Z}$

Définition

Le groupe G est dit **de type fini** s'il possède un système générateur fini.

Il est **monogène** s'il posséde un sytème générateur formé d'un seul élément.

Il est **cyclique** s'il est monogène fini.

Exemples

1. Le groupe $\mathbb{Z} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ est de type fini engendré par $\{(0, \overline{1}), (1, \overline{0})\}$

En effet tout élément z de $\mathbb{Z} \times \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ s'écrit $z = (k, \overline{l})$, où $k \in \mathbb{Z}$ et $\overline{l} = l + 2\mathbb{Z} \in \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ avec $l \in \mathbb{Z}$.

On a $z = (k, \overline{l}) = k(1, \overline{0}) + l(0, \overline{1}) \in < (0, \overline{1}), (1, \overline{0}) >$

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

3. Soit $n \geq 1$ un entier. Le groupe $\mathbb{U}_n = \{z \in \mathbb{C}, z^n = 1\}$ (groupe des racines nièmes de l'unité) est un groupe multiplicatif cyclique d'ordre n. En effet

$\mathbb{U}_n = \{1, e^{\frac{2i\pi}{n}}, e^{\frac{4i\pi}{n}}, ..., e^{(n-1)\frac{2i\pi}{n}}\} = < e^{\frac{2i\pi}{n}} >$

Proposition

Tout groupe monogène est commutatif

Preuve

Soit $G = (a)$ un groupe monogène. Alors $\forall \ x, y \in G, \exists \ m, n \in \mathbb{Z}$ tels que $x = a^m$, $y = a^n$. Donc $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$

Proposition

Tout groupe monogène G est :

i) isomorphe à $\mathbb{Z}$ s'il est infini

ii) isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ s'il est fini d'ordre n

Preuve

Supposons que $G = < a > = \{a^k, k \in \mathbb{Z}\}$

Considérons l'application $\varphi : \mathbb{Z} \to G$ telle que $\forall \ k \in \mathbb{Z}$, $\varphi(k) = a^k$.

φ est un morphisme surjectif de groupes. $Ker \ \varphi$ est un sous groupe de $\mathbb{Z}$. Donc il existe $n \in \mathbb{N}$ tel que $Ker \ \varphi = n\mathbb{Z}$

Si $n = 0$, alors φ est injectif. Dans ce cas φ est un isomorphisme. Donc $G \simeq \mathbb{Z}$.

Si $n > 0$, $\dfrac{\mathbb{Z}}{Ker\ \varphi} \simeq G$, c'est à dire $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \simeq G$

Définition

Soit G un groupe et soit $a \in G$. **L'ordre de** a est par définition l'ordre du groupe monogène $H = < a >$.

Proposition

Soit $G = < a >$ un groupe cyclique d'ordre n. Alors

(i) $G = \{e, a, a^2, ..., a^{n-1}\}$

(ii) On a $a^n = e$ et si un entier $m > 0$ vérifie l'équation $a^m = e$, alors n divise m.

Preuve

Cela provient du fait que $Ker\ \varphi = n\mathbb{Z}$

Proposition

Soit G un groupe fini d'ordre n. Alors $\forall\ a \in G$, l'ordre de a est fini et divise n.

En particulier, $\forall\ a \in G$ on a $a^n = e$

Preuve

L'ordre de a est par définition l'ordre m du sous groupe $H = < a >$. D'après le Théorème de Lagrange, m divise n. Si $n = qm$, alors $a^n = a^{qm} = (a^m)^q = e$

Chapitre4

Anneaux et Corps

4.1. Anneaux

Définition

On appelle anneau tout ensemble $(A, +, .)$ muni de deux loi internes notées ici additivement et mumtiplicativement tel que :

(i) $(A, +)$ est un groupe abélien

(ii) La multiplication est

associative, c'est à dire $\forall x, y, z \in A, (xy)z = x(yz)$

distributive par rapport à l'addition, c'est à dire

$\forall\ x, y, z \in A, x(y + z) = xy + xzet(y + z)x = yx + zx$

L'anneau A est dit :

- commutatif si sa multiplication est commutative c'est à dire $\forall x, y, \in A, xy = yx$

- unitaire si sa multiplication admet un élément neutre généralement noté 1 ou 1_A appelé l'unité de A. 1 est l'unique élément de A verifiant $\forall x \in A, 1x = x1 = x$

Exemples

1. $\mathbb{Z}$ l'anneau des entiers relatifs
2. $\mathbb{Z}/n\mathbb{Z}$ l'anneau des entiers modulo n
3. $\mathbb{R}[X]$ (resp. $\mathbb{C}[X]$) l'anneau des polynômes à coefficients réels (resp. complexes) etc... Tous ces anneaux sont commutatifs
4. $\mathbb{M}_n(\mathbb{R})$ l'anneau des matrices carrées d'ordre $n \geq 1$ à coefficients réels est un anneau non commutatif

Exercice

Soit A un anneau commutatif unitaire et soient $a, b \in A$. Montrer que $(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^{n-p} b^p$

Indication : Procéder par récurrence et utiliser la formule $\binom{n+1}{p} = \binom{n}{p} + \binom{n}{p-1}$

4.2. Sous anneau

Définition.

Soit B un anneau commutatif unitaire. Un sous ensemble A de B est appelé **sous anneau** de B si A est un sous groupe additif de B tel que $1_B \in A$ et $\forall\, x, y \in A, xy \in A$.

4.3. Morphisme d'anneaux

Définition.

Un morphisme d'anneaux est défini par la donnée de deux anneaux commutatifs unitaires A et B et d'une application $\varphi : A \to B$ vérifiant les propriétés suivantes

Un morphisme d'anneaux est défini par la donnée de deux anneaux commutatifs unitaires A et B et d'une application $\varphi : A \to B$ vérifiant les propriétés suivantes :

1. $\varphi(1_A) = 1_B$
2. $\varphi\ (a+b) = \varphi(a) + \varphi(b)$
3. $\varphi(ab) = \varphi(a)\varphi(b)$

Un isomorphisme d'anneaux est un morphisme d'anneaux qui et bijectif. On dit dans ce cas que les deux anneaux sont isomorphes

Si $\varphi : A \to B$ est un morphisme d'anneaux, on pose

$Ker\ \varphi = \varphi^{-1}(0) = \{x \in A; \varphi(x) = 0\ \}$

$Im\ \varphi = \{y \in B; \exists x \in A$ tel que $y = \varphi(x)\}$

4.4. Eléments inversibles d'un anneau

Définition

Un élément a de l'anneau commutatif unitaire A est dit **inversible dans** A s'il existe $b \in A$ tel que $ab = 1$. Cet élément b qui est unique s'appelle **l'inverse** de a. On le note généralement $b = a^{-1}$. Un élément inversible de A s'appelle également **une unité** de A, à ne pas confondre avec l'élément unité de A qui est 1. En accord avec cette derniére appellation, on désigne par $U(A)$ l'ensemble des éléments inversibles de A.

Exercice

Montrer que $U(A)$ est un groupe multiplicatif de A appelé le groupe des unités de A.

Exercice

Déterminer la table de multiplication de $\mathbb{Z}/4\mathbb{Z}$. En déduire $U(\mathbb{Z}/4\mathbb{Z}.)$

Exercice

Soient n un entier naturel non nul, $x \in \mathbb{Z}$, $\overline{x} = x + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$. On suppose que $1 \leq x \leq n-1$.

1. Montrer que les assertions suivantes sont équivalentes :

(i) $(x, n) = 1$

(ii) $\overline{x} \in U(\mathbb{Z}/n\mathbb{Z})$

(iii) $\overline{x}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$

2. On note $\varphi(n)$ le cardinal de $U(\mathbb{Z}/n\mathbb{Z})$, c'est à dire le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Donc d'après la question 1. ci-dessus, $\varphi(n)$ est le nombre d'entiers x tels que $1 \leq x \leq n-1$ avec $(x, n) = 1$.

$\varphi(n)$ s'appelle l'indicateur d'Euler de n. On dit aussi que φ est la **la fonction indicatrice d'Euler**. Dans ce qui suit, on se propose de calculer $\varphi(n)$ en fonction des facteurs premiers de n.

2.1 Soient r, s deux entiers naturels tels que $(r, s) = 1$.

a) Montrer que

$r\mathbb{Z} \cap s\mathbb{Z} = rs\mathbb{Z}$

b) Montrer que le système de congruences

$$(\mathrm{S}) \begin{cases} x \equiv x_1 [r] \\ x \equiv x_2 [s] \end{cases},$$

où x_1 et x_2 sont donnés dans $\mathbb{Z}$, possède des solutions dans $\mathbb{Z}$.

C'est un cas particulier du Théorème chinois des restes.

c) Montrer que deux solutions quelconques du système (S) sont congrues modulo rs.

d) Montrer que $U(\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}) = U(\mathbb{Z}/r\mathbb{Z}) \times U(\mathbb{Z}/s\mathbb{Z})$

e) Montrer que les anneaux $\mathbb{Z}/rs\mathbb{Z}$ et $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ sont isomorphes. En déduire que les groupes $U(\mathbb{Z}/rs\mathbb{Z})$ et $U(\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z})$ sont isomorphes.

2.2 a) Déduire de 2.1 que si $(r, s) = 1$, alors $\varphi(rs) = \varphi(r)\varphi(s)$

b) Calculer $\varphi(p)$ pour tout nombre premier p

c) Montrer que pour tout entier $k \geq 1$, $\varphi(p^k) = (p-1)p^{k-1} = p^k(1 - \frac{1}{p})$

d) Montrer que si

$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$, où $p_1, p_2, ..p_r$ sont premiers et où $\alpha_i \geq 1 \ \forall \ i$,
alors $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_r})$

4.5. Diviseurs de zéro, anneaux intègres

Définition :

Soit A un anneau commutatif unitaire. Un élément a de A est appelé **diviseur de zéro** s'il existe $b \in A, b \neq 0$ tel que $ab = 0$. On notera $Z(A)$ l'ensemble des diviseurs de zéro de A. Si l'anneau A est non trivial, c'est à dire si $0 \neq 1$, alors 0 est diviseur de zéro car $01 = 0$. L'anneau commutatif A est intègre si A est non trivial et s'il n'admet pas de diviseur de zéro autre que 0 i.e. si $Z(A) = \{0\}$

Donc A est intègre si $A \neq (0)$ et si $\forall \ a, b \in A$, la relation $ab = 0$ implique $a = 0$ ou $b = 0$.

On remarquera que tout sous anneau d'un anneau intègre est intègre.

Exemples

$\mathbb{Z}$ est intègre. $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre.

Exercice

Soit $n \geq 0$ un entier. Montrer que $\mathbb{Z}/n\mathbb{Z}$ est intègre $\Longleftrightarrow$ n est premier.

4.6. Corps

Définition

Un corps est un anneau commutatif non réduit à $\{0\}$ dont tous les éléments non nuls sont inversibles.

Exemples

$\mathbb{Q}$ le corps des rationnels, $\mathbb{R}$ le corps des nombres réels, $\mathbb{C}$ le corps des nombres complexes etc.

Proposition Le petit théorème de Fermat revu

Soit p un nombre premier. Alors pour tout entier naturel $n \geq 1$, on a $n^p \equiv n \ [p]$

Preuve

Dans le corps $\mathbb{Z}/p\mathbb{Z}$, il s'agit de montrer que $\overline{n}^p = \overline{n}$

Or $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z}$-$\{0\}$ est un groupe multiplicatif d'ordre p-1. Donc $\overline{n}^{p-1} = \overline{1}$

D'où en multipliant par n, on obtient l'égalité.