Chapitre 12

Les entiers naturels

12.1 Les entiers naturels

12.1.1 Propriétés fondamentales

Muni de la relation d'ordre :

$$\forall (n,m) \in \mathbb{N}^2, n \leq m \iff \exists k \in \mathbb{N}, m = n + k$$

l'ensemble des entiers naturels possède les trois propriétés suivantes :

DÉFINITION 12.1 : **Propriétés de $\mathbb{N}$**

1. **plus petit élément :** toute partie $A \subset \mathbb{N}$ non-vide possède un plus petit élément :
$$\exists a \in A \text{ tq } \forall x \in A, a \leq x$$
2. **plus grand élément :** toute partie $A \subset \mathbb{N}$ non-vide et majorée possède un plus grand élément :
$$\exists b \in A \text{ tq } \forall x \in A, x \leq b$$
3. **axiome de récurrence :** soit une partie $A \subset \mathbb{N}$ telle que :
   - $0 \in A$
   - $\forall n \in \mathbb{N}$, $(n \in A) \Rightarrow \big((n+1) \in A\big)$

   Alors $A = \mathbb{N}$.

THÉORÈME 12.1 : **Division euclidienne**
Soient deux entiers $(a,b) \in \mathbb{N}^2$ avec $b \neq 0$. Alors $\exists !(q,r) \in \mathbb{N}^2$ tels que :
1. $a = bq + r$
2. $0 \leq r < b$

THÉORÈME 12.2 : **Le principe de récurrence**
Soit une proposition $\mathcal{P}(n)$ dépendant d'un entier n. On suppose que :
(H1) $\exists n_0 \in \mathbb{N}$ tel que $\mathcal{P}(n_0)$ est VRAI ;
(H2) $\forall n \geq n_0$, $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$.
Alors $\forall n \geq n_0$, la proposition $\mathcal{P}(n)$ est vraie.

COROLLAIRE 12.3 : **Récurrence forte**
On considère une proposition $\mathcal{P}(n)$ dépendant d'un entier n. On suppose que :
(H1) $\exists n_0 \in \mathbb{N}$ tel que $\mathcal{P}(n_0)$ est VRAI ;
(H2) $\forall n \geq n_0$, $\big(\mathcal{P}(n_0)$ et $\mathcal{P}(n+1)$ et $\ldots$ et $\mathcal{P}(n)\big) \Rightarrow \mathcal{P}(n+1)$.
Alors $\forall n \geq n_0$, la proposition $\mathcal{P}(n)$ est vraie.

Remarque 113. La récurrence forte est plus facile à utiliser : l'hypothèse $\mathcal{P}(1)$ et $\ldots$ et $\mathcal{P}(n)$ est plus forte que l'hypothèse $\mathcal{P}(n)$.

Exercice 12-1

Montrer par récurrence que $\forall n \in \mathbb{N}$,

$$1^2 + 2^2 + \cdots + n^2 = \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$1^3 + 2^3 + \cdots + n^3 = \sum_{k=1}^{n} k^3 = \frac{[n(n+1)]^2}{4}$$

12.1.2 Ensembles finis

On définit pour $(p,q) \in \mathbb{N}^2$, $(p \leq q)$, l'intervalle d'entiers :

$$[\![p,q]\!] = \{k \in \mathbb{N} \text{ tq } p \leq k \leq q\}$$

LEMME 12.4 : **Injections, surjections d'intervalles entiers**
Soient deux entiers $(p,q) \in \mathbb{N}^2$ non-nuls. On a :

$$(p \leq q) \iff (\exists f : [\![1,p]\!] \mapsto [\![1,q]\!] \text{ injective})$$

$$(p \geq q) \iff (\exists f : [\![1,p]\!] \mapsto [\![1,q]\!] \text{ surjective})$$

DÉFINITION 12.2 : **Ensembles finis**
Soit E un ensemble. On dit que l'ensemble E est *fini* lorsqu'il existe un entier non nul $n \in \mathbb{N}^*$ et une bijection $\phi : E \mapsto [\![1,n]\!]$. Par convention, on dira que l'ensemble vide $\emptyset$ est également un ensemble fini.

THÉORÈME 12.5 : **Unicité du cardinal**
Si E est un ensemble fini, alors l'entier n de la définition précédente est unique.

DÉFINITION 12.3 : **Cardinal**
Soit un ensemble fini E non-vide. L'unique entier n tel qu'il existe une bijection entre E et $[\![1,n]\!]$ est appelé le *cardinal* de l'ensemble E, que l'on note $|E|$ (ou Card(E) ou encore $\sharp E$).
Par convention, le cardinal de l'ensemble vide vaut 0.

THÉORÈME 12.6 : **Comment montrer qu'un ensemble est fini**
Soit un ensemble fini F et un ensemble E. S'il existe une injection $\phi : E \mapsto F$, alors l'ensemble E est fini et $|E| \leq |F|$.

DÉFINITION 12.4 : **Ensembles équipotents**
Soient deux ensembles E et F. On dit qu'ils sont *équipotents* et l'on note $E \approx F$ lorsqu'il existe une bijection ϕ entre ces deux ensembles.

COROLLAIRE 12.7 : **Pour montrer que deux ensembles ont même cardinal**
Soient deux ensembles finis E et F. Les deux ensembles E et F sont équipotents si et seulement si ils ont même cardinal

THÉORÈME 12.8 : **Applications entre ensembles finis**
Soient deux ensembles finis E et F de même cardinal n, et une application $f : E \mapsto F$. On a :

$$(f \text{ injective }) \iff (f \text{ surjective }) \iff (f \text{ bijective })$$

COROLLAIRE 12.9 : **Comment montrer que deux ensembles de même cardinal sont égaux**
Soient E et F deux ensembles finis de même cardinal. Alors

$$E \subset F \Rightarrow E = F$$

12.1.3 Dénombrements fondamentaux

LEMME 12.10 : **Lemme des Bergers**
Si A et B sont deux ensembles finis, on a :

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Plus généralement, si $\mathcal{P} = (A_1, \ldots, A_p)$ est un *partage* d'un ensemble fini E en classes disjointes, on a :

$$|E| = |A_1| + \cdots + |A_p|$$

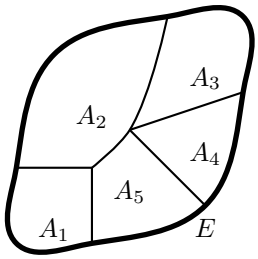


FIG. 12.1 – *Lemme des bergers*

THÉORÈME 12.11 : **Dénombrements fondamentaux**
Soient deux ensembles finis E et F, avec $|E| = n, |F| = p$. Alors :

1. $E \times F$ est fini et $\boxed{|E \times F| = np}$
2. $\mathcal{F}(E,F)$ est fini et $\boxed{|\mathcal{F}(E,F)| = p^n}$
3. $\mathcal{P}(E)$ est fini et $\boxed{|\mathcal{P}(E)| = 2^n}$

DÉFINITION 12.5 : **Arrangements, coefficients binômiaux**
Soient $(n,p) \in \mathbb{N}^2$. On définit :

- $n! = \begin{cases} 1 & \text{si } n = 0 \\ n \times (n-1) \times \ldots 2 \times 1 & \text{si } n \geq 1 \end{cases}$
- Si $0 \leq p \leq n$, $\boxed{A_n^p = \dfrac{n!}{(n-p)!}} = n \times (n-1) \times \cdots \times (n-p+1)$
- Si $0 \leq p \leq n$, $\boxed{C_n^p = \binom{n}{p} = \dfrac{n!}{(n-p)!p!} = \dfrac{A_n^p}{p!} = \dfrac{n \times (n-1) \times \cdots \times (n-p+1)}{p \times (p-1) \times \cdots \times 1}}$

Remarque 114. En particulier, on a les relations :

$$\binom{n}{0} = 1 = \binom{n}{n}, \quad \binom{n}{1} = \binom{n}{n-1} = n, \quad \binom{n}{2} = \frac{n(n-1)}{2}$$

THÉORÈME 12.12 : **Nombre d'injections, de bijections**

1. Si $|E| = p$, $|F| = n$, avec $p \leq n$ (attention aux notations !), le nombre d'applications injectives de E vers F vaut A_n^p ;
2. Si $|E| = |F| = n$, le nombre d'applications bijectives de E vers F vaut $n!$

THÉORÈME 12.13 : **Nombres de parties à p éléments**
Soit un ensemble fini E, de cardinal n, et un entier $0 \leq p \leq n$. Le nombre de parties de E de cardinal p vaut $\binom{n}{p}$ (c'est le nombre de façons différentes de choisir p éléments parmi n).

Remarque 115. Soit un ensemble fini E de cardinal n. Une p-liste de E est une application de $[\![1,p]\!]$ vers E, notée en informatique $l = [a_1, \ldots, a_n]$.

- n^p est le nombre de p-listes ;
- A_n^p est le nombre de p-listes sans répétition. (l'ordre des éléments compte) ;
- $\binom{n}{p}$ représente le nombre de sous-ensembles de E à p éléments (l'ordre n'est pas important et il n'y a pas de répétitions).

Exercice 12-2

Quel est le nombre de façons de placer k boules identiques dans n urnes pouvant contenir au plus 1 boule ?
Quel est le nombre de façons de placer k boules numérotées dans n urnes pouvant contenir au plus 1 boule ?

Exercice 12-3

Trouver le nombre de diviseurs de 1800.

Exercice 12-4

Soit E un ensemble fini de cardinal n. Quel est le nombre de couples de parties $(X,Y) \in \mathcal{P}(E)^2$ vérifiant $X \subset Y$?

Exercice 12-5

Trouver le nombre d'applications strictement croissantes de l'intervalle entier $[\![1,p]\!]$ vers l'intervalle entier $[\![1,n]\!]$.

Exercice 12-6

Soient $0 \leq p \leq n$ deux entiers. On veut trouver le nombre de p-uplets $(\alpha_1, \ldots, \alpha_p)$ d'entiers vérifiant :

$$\alpha_1 + \cdots + \alpha_p = n$$

Pour cela, étant donné un tel p-uplet, considérer α_1 cases blanches, 1 case noire, α_2 cases blanches ... :

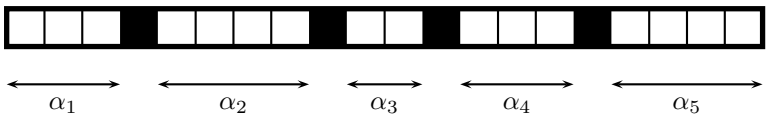


FIG. 12.2 – *Transformation du problème*

Déterminer ensuite le nombre de p-uplets vérifiant :

$$\alpha_1 + \cdots + \alpha_p \leq n$$

Exercice 12-7

Combien y a-t-il d'applications croissantes de $[\![1,k]\!]$ vers $[\![1,p]\!]$?

12.1.4 Propriétés des coefficients binômiaux

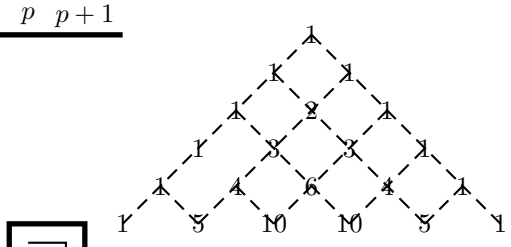
THÉORÈME 12.14 : **Propriété des coefficients binômiaux**
Soient $0 \leq p \leq n$ deux entiers. Les coefficients binômiaux vérifient les propriétés suivantes :

- *Symétrie* : $\binom{n}{p} = \binom{n}{n-p}$
- *Factorisation* : $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$ (si $p \geq 1$)
- *Additivité* : $\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$

De l'additivité, on obtient le *triangle de Pascal* qui permet de calculer de proche en proche tous les coefficients binômiaux.

FIG. 12.3 – *Triangle de Pascal*

	0	1	2	3	p	$p+1$
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
n						
$n+1$						



THÉORÈME 12.15 : **Formule du binôme de Newton**
Soient deux réels a,$b \in \mathbb{R}$ et un entier $n \in \mathbb{N}$. Alors

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

Exercice 12-8
Calculer les sommes

$$\sum_{k=1}^{n} \binom{n}{k} \quad \sum_{k=0}^{n-1} \frac{1}{3^k} \binom{n}{k}$$

Exercice 12-9
Calculer les sommes

$$S_1 = \sum_{\substack{0 \le k \le n \\ k \text{ pair}}} \binom{n}{k} \quad S_2 = \sum_{\substack{0 \le k \le n \\ k \text{ impair}}} \binom{n}{k}$$

Exercice 12-10
Calculer les sommes

$$S_1 = \sum_{k=0}^{n} k \binom{n}{k} \quad S_2 = \sum_{k=0}^{n} \frac{1}{k+1} \binom{n}{k} \quad S_3 = \sum_{k=0}^{n} k^2 \binom{n}{k}$$

Exercice 12-11
Quelques propriétés des coefficients binômiaux.

a. Montrer que $\forall 1 \le k \le n$, on a

$$\binom{n}{k} = \frac{n-k+1}{k} \binom{n}{k-1}$$

b. En déduire les inégalités suivantes selon la parité de n :

$$n = 2p \ : \quad \binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{p-1} < \binom{n}{p} > \binom{n}{p+1} > \cdots > \binom{n}{n}$$

$$n = 2p+1 \ : \quad \binom{n}{0} < \cdots < \binom{n}{p-1} = \binom{n}{p+1} > \cdots > \binom{n}{n}$$

c. En déduire que $\forall n \ge 1$,

$$\binom{2n}{n} \ge \frac{4^n}{2n+1}$$

12.1.5 Numérotation en base b

THÉORÈME 12.16 : **Numérotation en base p**
Soit un entier $n \in \mathbb{N}$. Il s'écrit de façon unique :

$$n = a_k 10^p + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \quad 0 \leq a_i < 10$$

Plus généralement, si $p \in \mathbb{N}^\star$ est un entier non nul, l'entier n s'écrit de façon unique :

$$n = b_k p^k + b_{k-1} p^{k-1} + \cdots + b_1 p + b_0 \quad 0 \leq b_i < p$$

On dit que $(a_p, \ldots, a_0)_{10}$ sont les *chiffres* de l'entier n en base 10 et que $(b_k, \ldots, b_0)_p$ sont les chiffres de l'entier n en base p.

Exercice 12-12
En base 16, les chiffres sont notés $\{0,1,\ldots,9,A,B,C,D,E,F\}$. Déterminer les chiffres de l'entier 95 en base 16.

Calcul des chiffres d'un entier en base p
Une fonction récursive qui renvoie la liste $[b_k, \ldots, b_0]$ des chiffres d'un entier n en base p :

```
chiffres := proc(n)
  if n < p then
    [n]
  else
    [op(chiffres( iquo(n, p) ), n mod p ) ]
  fi;
end;
```

La même fonction programmée avec une boucle :

1. **Arguments :** n (entier) ;
2. **Variables :** a (entier), l (liste), r (entier)
3. **Initialisation :** $a \leftarrow n$, $l \leftarrow []$
4. **Corps :** Tant que $a <> 0$, faire :
   - $r \leftarrow a \bmod p$,
   - $l \leftarrow [r, op(l)]$,
   - $a \leftarrow \dfrac{a - r}{p}$,

   Fin tant que
5. **Fin :** renvoyer l.

en Maple :

Maple
```
conversion := proc(n, b)
  local a, l, r;
  while (a <> 0) do
    r := irem(a, p);
    l := [r, op(l)];
    a := (a - r) / p;
  od;
  l;
end;
```

Exercice 12-13
Combien y a-t-il d'entiers qui s'écrivent avec moins de k chiffres en base p ? Avec exactement k chiffres ?

Algorithme d'exponentiation rapide
On veut calcuer a^n. Pour cela, on peut effectuer $n-1$ multiplications en utilisant la formule :

$$a^n = a \times \cdots \times a$$

ce qui conduit à l'algorithme :

1. **Arguments :** a (entier), n (entier ≥ 1)

2. **Variables :** P entier
3. **Initialisation :** $P \leftarrow a$
4. **Corps :** Pour i de 1 à $n-1$ faire :
   - $P \leftarrow P \times a$
5. **Fin :** renvoyer P

Maple
```
expo := proc(a, n)
  local P;
  P := a;
  for i from 1 to n - 1 do
     P := P * a
  od;
  P;
end;
```

Mais on remarque que pour calculer a^8, on peut se contenter de 3 multiplications :
- $b = a \times a$ ($b = a^2$)
- $c = b \times b$ ($c = a^4$)
- $d = c \times c$ ($d = a^8$)

L'idée de l'algorithme d'exponentiation rapide est la formule récursive :

$$a^n = \begin{cases} x \times x & \text{si } n \text{ pair} \\ a \times x \times x & \text{si } n \text{ impair} \end{cases} \qquad \text{où } x = a^{n/2}$$

Exercice 12-14

Déterminer le nombre de multiplications nécessaires pour calculer a^n avec cet algorithme en fonction des chiffres de n en base 2, et montrer que ce nombre $T(n)$ vérifie :

$$\lfloor \log_2(n) \rfloor \leq T(n) \leq 2 \lfloor \log_2(n) \rfloor$$

12.2 Les entiers relatifs

12.2.1 Congruences

THÉORÈME 12.17 : **Division euclidienne dans $\mathbb{Z}$**
Soient deux entiers $(a,b) \in \mathbb{Z} \times \mathbb{N}$ avec $b \neq 0$. Alors $\exists!(q,r) \in \mathbb{Z}^2$ tels que :
1. $a = bq + r$
2. $0 \leq r < b$

On dit que l'entier q est le *quotient* et l'entier r le *reste* de la division euclidienne de a par b.

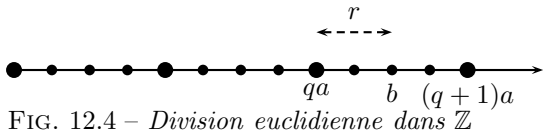


FIG. 12.4 – *Division euclidienne dans $\mathbb{Z}$*

DÉFINITION 12.6 : **Divisibilité**
Soient deux entiers relatifs $(a,b) \in \mathbb{Z}^2$. On dit que l'entier a *divise* l'entier b si et seulement si $\exists k \in \mathbb{Z}$ tq $b = ka$.

Remarque 116.
- $\forall n \in \mathbb{N}$, $n/0$;
- $\forall n \in \mathbb{N}$, $0/n \Rightarrow n = 0$;
- $\forall (a,b,c,d) \in \mathbb{Z}^4$, $\begin{cases} a/b \\ c/d \end{cases} \Rightarrow ac/bd$.

PROPOSITION 12.18 : **Propriétés de la divisibilité**

– Soit $(a,b) \in \mathbb{Z}^2$. On a l'équivalence

$$(a/b) \iff (b \in a\mathbb{Z}) \iff (b\mathbb{Z} \subset a\mathbb{Z})$$

– Si $(a,b) \in \mathbb{Z}^2$,

$$\big(a/b \text{ et } b/a\big) \iff (a = b \text{ ou } a = -b\big)$$

– Si $(a,b) \in {\mathbb{N}^\star}^2$, $a\mathbb{Z} = b\mathbb{Z} \Rightarrow a = b$.

DÉFINITION 12.7 : **Congruence**

Considérons un entier strictement positif $n \in \mathbb{N}^\star$ et deux entiers $(a,b) \in \mathbb{Z}^2$. On dit que l'entier a est *congru* à l'entier b modulo n, et l'on note $a \equiv b\ [n]$ lorsque l'entier n divise l'entier $(b-a)$:

$$a \equiv b\ [n] \iff n/(b-a)$$

PROPOSITION 12.19 : **Caractérisation par les restes**

Soit un entier $n \in \mathbb{N}^\star$ et deux entiers $(a,b) \in \mathbb{Z}^2$. On note r_a le reste de la division euclidienne de a par n et r_b le reste de la division euclidienne de b par n. Alors :

$$a \equiv b\ [n] \iff r_a = r_b$$

PROPOSITION 12.20 : **La relation de congruence est une relation d'équivalence**

Soit un entier $n \in \mathbb{N}^\star$. La relation $\equiv$ définie sur $\mathbb{Z}$ par :

$$\forall (a,b) \in \mathbb{Z}^2,\ a \equiv b \iff a \equiv b\ [n]$$

est une relation d'équivalence.

PROPOSITION 12.21 : **Compatibilité des lois avec les congruences**

Soient quatre entiers $(a,b,c,d) \in \mathbb{Z}^4$ et un entier $n \in \mathbb{N}^\star$. On suppose que

1. $a \equiv b\ [n]$;
2. $c \equiv d\ [n]$.

Alors

1. $a + c \equiv b + d\ [n]$;
2. $a \times c \equiv b \times d\ [n]$;
3. $\forall k \in \mathbb{N},\ a^k \equiv b^k\ [n]$.

Exercice 12-15

1. Trouver le reste de l'entier 126745 dans la division par 9.
2. Trouver le reste de la division de l'entier 121^{1256} par 7.
3. Trouver le reste de la division euclidienne de $(1001)^{77}$ par 3.

12.3 Structure de groupe

DÉFINITION 12.8 : **Groupe**

On appelle *groupe* un ensemble G muni d'une lci $\star$ vérifiant :

1. la loi $\star$ est associative ;
2. G possède un élément neutre ;
3. Tout élément x de G admet un symétrique.

Si de plus la loi $\star$ est commutative, on dit que le groupe est *abélien* (ou *commutatif*).

THÉORÈME 12.22 : **Groupe produit**
On considère deux groupes $(G,.)$ et $(H,\star)$ et sur l'ensemble $G \times H$, on définit la loi T par :

$$\forall((x,y),(x',y')) \in (G \times H)^2, \quad (x,y)T(x',y') = (x.x',y \star y')$$

Alors $(G \times H,T)$ est un groupe appelé *groupe produit.*

DÉFINITION 12.9 : **Sous-groupe**
Soit $(G,\star)$ un groupe. On dit qu'une partie $H \subset G$ est un *sous-groupe* de G ssi :

1. $e \in H$;
2. la partie H est *stable* par la loi : $\forall(x,y) \in H^2$, $x \star y \in H$.
3. $\forall x \in H$, $x^{-1} \in H$.

THÉORÈME 12.23 : **Une caractérisation équivalente**
Les trois conditions précédentes sont équivalentes aux deux conditions :

1. $e \in H$;
2. $\forall(x,y) \in H^2$, $x \star y^{-1} \in H$.

Pour montrer que $H \subset G$ est un sous-groupe du groupe $(G,\star)$:

1. $e \in H$;
2. *Soit* $(x,y) \in H^2$;
3. Calculons $x \star y^{-1}, \ldots$;
4. On a bien $x \star y^{-1} \in H$;
5. Donc H est un sous-groupe de G.

THÉORÈME 12.24 : **Un sous-groupe a une structure de groupe**
Si la partie H est un sous-groupe de $(G,\star)$, alors puisque cette partie est stable pour la lci, on peut définir la restriction de la loi $\star$ à H qui est une lci sur H. Muni de cette loi restreinte, $(H,\star)$ est un groupe.

Pour montrer qu'un ensemble a une structure de groupe, on essaie de montrer que c'est un sous-groupe d'un groupe connu

`Exemple 20.` On considère l'ensemble $U = \{z \in \mathbb{C} \text{ tq } |z| = 1\}$. Montrer que $(U,\times)$ est un groupe.

Exercice 12-16
Soit un ensemble E non-vide et un élément $a \in E$. On note

$$G = \{f \in \mathcal{B}(E,E), \text{ tq } f(a) = a\}$$

(c'est l'ensemble des bijections de G laissant invariant l'élément a). Montrer que $(G,\circ)$ est un groupe.

Exercice 12-17
Soit $(G,.)$ un groupe. On note

$$C = \{x \in G \mid \forall g \in G,\ g.x = x.g\}$$

C'est l'ensemble des éléments de G qui commutent avec tous les éléments de G. Montrer que $(C,.)$ est un sous-groupe de G (appelé *centre* du groupe G).

THÉORÈME 12.25 : **L'intersection de sous-groupes est un sous-groupe**
Si H_1 et H_2 sont deux sous-groupes d'un groupe G, alors $H_1 \cap H_2$ est un sous-groupe de G

Remarque 117. $H_1 \cup H_2$ n'est pas un sous-groupe de G en général.

Exercice 12-18
Soient H_1 et H_2 deux sous-groupes d'un groupe $(G,.)$. Montrer que

$$(H_1 \cup H_2 \text{ est un sous-groupe de } G) \iff (H_1 \subset H_2 \text{ ou } H_2 \subset H_1)$$

THÉORÈME 12.26 : **Sous-groupes de $\mathbb{Z}$**
Les sous groupes du groupe $(\mathbb{Z},+)$ sont les ensembles de la forme :

$$a\mathbb{Z} = \{ka;\ k \in \mathbb{Z}\}$$

où $a \in \mathbb{N}$

DÉFINITION 12.10 : **Morphismes de groupes**
Soient deux groupes $(G_1,\star)$ et $(G_2,\bullet)$. Une application $f\ :\ G_1 \mapsto G_2$ est un *morphisme* de groupes si et seulement si :

$$\forall (x,y) \in G_1^2,\quad f(x \star y) = f(x) \bullet f(y)$$

Pour montrer que $f : G_1 \mapsto G_2$ est un morphisme :
1. *Soit* $(x,y) \in G_1^2$;
2. On a bien $f(x \star y) = f(x) \bullet f(y)$.

PROPOSITION 12.27 : **Propriétés d'un morphisme de groupes**
Si e_1 est l'élément neutre de G_1 et e_2 l'élément neutre de G_2, alors
1. $f(e_1) = e_2$;
2. $\forall x \in G_1$, $[f(x)]^{-1} = f(x^{-1})$.

THÉORÈME 12.28 : **Image directe et réciproque de sous-groupes par un morphisme**
Soit $f\ :\ G_1 \mapsto G_2$ un morphisme de groupes.
1. Si H_1 est un sous-groupe de G_1, alors $f(H_1)$ est un sous-groupe de G_2 ;
2. Si H_2 est un sous-groupe de G_2, alors $f^{-1}(H_2)$ est un sous-groupe de G_1.

DÉFINITION 12.11 : **Noyau, image d'un morphisme**
On considère un morphisme de groupes $f\ :\ G_1 \mapsto G_2$. On note e_1 l'élément neutre du groupe G_1 et e_2 l'élément neutre du groupe G_2. On définit
- le *noyau* du morphisme f :

$$\mathrm{Ker}(f) = \{x \in G_1 \mid f(x) = e_2\} = f^{-1}\big(\{e_2\}\big)$$

- l'*image* du morphisme f :

$$\mathrm{Im}\, f = f(G_1) = \{y \in G_2 \mid \exists x \in G_1\ f(x) = y\}$$

$\mathrm{Ker}\, f$ est un sous-groupe de G_1 et $\mathrm{Im}\, f$ est un sous-groupe de G_2.

THÉORÈME 12.29 : **Caractérisation des morphismes injectifs, surjectifs**
Soit un morphisme de groupes $f\ :\ G_1 \mapsto G_2$. On note e_1 l'élément neutre du groupe G_1 et e_2 l'élément neutre du groupe G_2. On a les propriétés suivantes :
- (f injective) $\iff$ ($\mathrm{Ker}\, f = \{e_1\}$) ;
- (f surjective) $\iff$ ($\mathrm{Im}\, f = G_2$).

Pour montrer qu'un morphisme $f\ :\ (G_1,\star) \mapsto (G_2,\bullet)$ est injectif :
1. *Soit* $x \in G_1$ tel que $f(x) = e_2$
2. Alors $x = e_1$;
3. Donc $\mathrm{Ker}\, f = \{e_1\}$, et puisque f est un morphisme, f est injectif.

DÉFINITION 12.12 : **Isomorphisme**
On dit qu'une application $f\ :\ G_1 \mapsto G_2$ est un isomorphisme de groupes si et seulement si
1. l'application f est un morphisme de groupes ;
2. l'application f est bijective.

Remarque 118. Un isomorphisme d'un groupe G vers lui-même est appelé un *automorphisme*.

THÉORÈME 12.30 : **La bijection réciproque d'un isomorphisme est un isomorphisme**
Si f est un isomorphisme de groupes, sa bijection réciproque $f^{-1}\ :\ G_2 \mapsto G_1$ est aussi un isomorphisme de groupes.

`Exemple 21.` Soit

$$f \ : \ \left\{ \begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathbb{R}^{+*},\times) \\ x & \mapsto & e^x \end{array} \right.$$

Vérifier que l'application f est un isomorphisme de groupes. Quel est son isomorphisme réciproque ?

Exercice 12-19

Trouver tous les morphismes du groupe $(\mathbb{Z},+)$ vers lui-même. Lesquels sont-ils des isomorphismes ?

12.4 Structure d'anneau

DÉFINITION 12.13 : **anneau**

Soit A un ensemble muni de deux lci notées $+$ et $\times$. On dit que $(A,+,\times)$ est un *anneau* ssi :

1. $(A,+)$ est un groupe commutatif ;
2. la loi $\times$ est associative ;
3. la loi $\times$ est *distributive* par rapport à la loi $+$:

$$\forall (x,y,z) \in A^3, \quad \begin{array}{l} x \times (y+z) = x \times y + x \times z \\ (x+y) \times z = x \times z + y \times z \end{array}$$

4. Il existe un élément neutre pour $\times$, noté 1.

Si en plus la loi $\times$ est commutative, on dit que $(A,+,\times)$ est un anneau commutatif.

Remarque 119. Dans un anneau $(A,+,\times)$, on note $-x$ le symétrique de l'élément x pour la loi $+$ et 0 l'élément neutre de la loi $+$. Attention, un élément $x \in A$ n'a pas forcément de symétrique pour la loi $\times$, la notation x^{-1} n'a pas de sens en général.

`Exemple 22.` $(\mathbb{Z},+,\times)$ et $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\times)$ sont des anneaux commutatifs.

DÉFINITION 12.14 : $\mathbb{Z}/n\mathbb{Z}$

Soit un entier strictement positif $n \in \mathbb{N}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de la relation de congruence modulo n. Il y a n classes distinctes, notées

$$\mathbb{Z}/n\mathbb{Z} = \{\widehat{0}, \ldots, \widehat{n-1}\}$$

Ces classes correspondent aux restes possibles dans la division euclidienne par l'entier n. On définit sur $\mathbb{Z}/n\mathbb{Z}$ les « lois quotient » notées $\widehat{+}$ et $\widehat{\times}$. Muni de ces deux lois, $\left(\mathbb{Z}/n\mathbb{Z},\widehat{+},\widehat{\times}\right)$ est un anneau commutatif d'éléments neutres $\widehat{0}$ et $\widehat{1}$.

THÉORÈME 12.31 : **Règles de calcul dans un anneau**

On considère un anneau $(A,+,\times)$. On a les règles de calcul suivantes :

- $\forall a \in A$, $a \times 0 = 0 \times a = 0$;
- $\forall a \in A$, $(-1) \times a = -a$;
- $\forall (a,b) \in A^2$, $(-a) \times b = -(a \times b)$.

Remarque 120. Si $(A,+,\times)$ est un anneau, $(A,\times)$ n'est pas un groupe en général (par exemple lorsque $A = \mathbb{Z}$).

Remarque 121. En général, (par exemple dans l'anneau $\mathcal{F}(\mathbb{R},\mathbb{R})$),

$$\boxed{a \times b = 0 \not\Rightarrow a = 0 \text{ ou } b = 0}$$

On dit que de tels éléments a et b sont des *diviseurs de zéro*.

DÉFINITION 12.15 : **Anneau intègre**

Soit un anneau $(A,+,\times)$. On dit que cet anneau est *intègre* si et seulement si :

1. $A \neq \{0\}$;
2. la loi $\times$ est commutative ;
3. $\forall (x,y) \in A^2$, $x \times y = 0 \Rightarrow x = 0$ ou $y = 0$.

Remarque 122. Dans un anneau *intègre*, on peut « simplifier » à gauche et à droite : Si $(a,y,z) \in A^3$, avec $ax = ay$, et si $a \neq 0$, alors $x = y$. Cette propriété est fausse dans un anneau général.

DÉFINITION 12.16 : **Notations**
On considère un anneau $(A, +, \times)$. Soit un élément $a \in A$ et un entier $n \in \mathbb{N}$. On note

- $na = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ fois}} & \text{si } n \neq 0 \\ 0 & \text{si } n = 0 \end{cases}$
- $(-n)a = n(-a) = \underbrace{(-a) + \cdots + (-a)}_{n \text{ fois}}$
- $a^n = \begin{cases} \underbrace{a \times \cdots \times a}_{n \text{ fois}} & \text{si } n \neq 0 \\ 1 & \text{si } n = 0 \end{cases}$
- a^{-n} n'a pas de sens si a n'est pas inversible pour $\times$.

DÉFINITION 12.17 : **Élément nilpotent**
Soit un anneau $(A, +, \times)$. On dit qu'un élément $a \in A$ $(a \neq 0)$ est *nilpotent* s'il existe un entier $n \in \mathbb{N}^\star$ tel que $a^n = 0$.
Le plus petit entier n vérifiant $a^n = 0$ s'appelle l'indice de nilpotence de l'élément a.

Remarque 123. Si l'anneau A est intègre, il n'y a pas d'élément nilpotent dans cet anneau.

Exercice 12-20
Soit un anneau $(A, +, \times)$ vérifiant :

$$\forall x \in A, \quad x^2 = x$$

Montrer que l'anneau A est commutatif.

THÉORÈME 12.32 : **Binôme de Newton et formule de factorisation dans un anneau**
Dans un anneau $(A, +, \times)$, si $(a,b) \in A^2$ vérifient

$$\boxed{a \times b = b \times a}$$

Alors $\forall n \in \mathbb{N}$,

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

et $\forall n \geq 1$,

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k$$

THÉORÈME 12.33 : **Calcul d'une progression géométrique**
Soit un anneau $(A, +, \times)$ et un élément $a \in A$. On considère un entier $n \in \mathbb{N}$, $n \geq 1$. De la formule de factorisation, on tire :

$$\boxed{1 - a^n = (1-a)(1 + a + a^2 + \cdots + a^{n-1})}$$

En particulier, si l'élément a est *nilpotent* d'indice n : $a^n = 0$, alors l'élément $(1-a)$ est inversible pour la loi $\times$ et on sait calculer son inverse :

$$(1-a)^{-1} = 1 + a + a^2 + \cdots + a^{n-1}$$

DÉFINITION 12.18 : **Sous-anneau**
On considère un anneau $(A, +, \times)$ et une partie $A' \subset A$ de cet anneau. On dit que la partie A' est un sous-anneau de A si et seulement si :

1. $(A',+)$ est un sous-groupe du groupe $(A,+)$;
2. la partie A' est *stable* pour la loi$\times$: $\forall (a,b) \in {A'}^2$, $a \times b \in A'$;
3. l'élément neutre de l'anneau A est dans A' : $1 \in A'$.

Définition 12.19 : **Morphisme d'anneaux**
Soient deux anneaux $(A,+,\times)$ et $(A',+,\times)$. On dit qu'une application $f : A \mapsto A'$ est *morphisme d'anneaux* si et seulement si :

1. $\forall (x,y) \in A^2,\ f(x+y) = f(x)+f(y)$;
2. $f(x \times y) = f(x)\times f(y)$;
3. $f(1_A) = 1_{A'}$.

Remarque 124. On dit que l'application f est un *isomorphisme* lorsque c'est un morphisme bijectif.

Exercice 12-21
Déterminer tous les morphismes d'anneaux de l'anneau $(\mathbb{Z},+,\times)$ vers lui-même.

Théorème 12.34 : **Groupe des unités d'un anneau**
Soit un anneau $(A,+,\times)$. On note U l'ensemble des éléments inversibles pour la loi $\times$:

$$U = \{a \in A \mid \exists a' \in A \text{ tq } a \times a' = a' \times a = 1_A\}$$

Alors muni de la seconde loi de l'anneau, l'ensemble $(U,\times)$ a une structure de groupe : c'est le *groupe des unités* de l'anneau A.

`Exemple 23.` Dans l'anneau $(\mathbb{Z},+,\times)$, le groupe des unités est $U = \{1,-1\}$. Dans l'anneau $\big(\mathcal{F}(I,\mathbb{R}),+,\times\big)$, le groupe des unités est constitué des fonctions qui ne s'annulent pas.

Définition 12.20 : **Idéal d'un anneau**
On considère un anneau $(A,+,\times)$ et une partie $I \subset A$ de cet anneau. On dit que la partie I est un *idéal* de l'anneau A lorsque :

1. la partie I est un sous-groupe du groupe $(A,+)$;
2. la partie I est « absorbante » : $\forall x \in I,\ \forall a \in A,\ a \times x \in I$.

Remarque 125. La notion d'idéal d'un anneau est plus riche que celle de sous-anneau. Elle fournit un cadre général à l'arithmétique.

Exercice 12-22
Montrez qu'il n'existe pas de couple d'entiers $(x,y) \in \mathbb{Z}^2$ vérifiant

$$x^2 - 5y^2 = 3$$

Exercice 12-23
Trouvez les entiers $x \in \mathbb{Z}$ tels que $x^2 - 4x + 3$ soit divisible par 6.

12.4.1 Arithmétique dans $\mathbb{Z}$

Définition 12.21 : **PGCD, PPCM**
Soient deux entiers non nuls $(a,b) \in \mathbb{Z}^{\star\,2}$.

1. L'ensemble des diviseurs de $\mathbb{N}^\star$ communs à a et b admet un plus grand élément δ noté $\delta = a \wedge b$. C'est le *plus grand commun diviseur* des entiers a et b.
2. L'ensemble des entiers de $\mathbb{N}^\star$ multiples communs de a et b admet un plus petit élément μ noté : $\mu = a \vee b$. C'est le *plus petit commun multiple* des entiers a et b.

Exercice 12-24
Soient H_1 et H_2 deux sous-groupes du groupe $(\mathbb{Z},+)$. On définit l'ensemble

$$H_1 + H_2 = \{h_1 + h_2 \ ;\ (h_1,h_2) \in H_1 \times H_2\}$$

a. Montrer que $H_1 + H_2$ est le plus petit (au sens de l'inclusion) sous-groupe de $(\mathbb{Z},+)$ qui contient la partie $H_1 \cup H_2$;
b. Déterminer le sous-groupe $4\mathbb{Z} + 6\mathbb{Z}$;
c. Comment interpréter l'inclusion $a\mathbb{Z} \cup b\mathbb{Z} \subset c\mathbb{Z}$ en termes de divisibilité ?

THÉORÈME 12.35 : **Caractérisation du ppcm et du pgcd avec les sous-groupes de $\mathbb{Z}$**
Soient deux entiers non nuls $(a,b) \in \mathbb{Z}^{\star 2}$, δ leur pgcd et μ leur ppcm. Alors :

$$\delta\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = \{au + bv \ ; \ (u,v) \in \mathbb{Z}^2\}$$

$$\mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$$

PROPOSITION 12.36 : **Caractérisation des diviseurs (multiples) de a et b**
Soient deux entiers $(a,b) \in \mathbb{Z}^2$.

1. Soit un entier $d \in \mathbb{Z}$. $\begin{cases} d/a \\ d/b \end{cases} \iff d/(a \wedge b)$
2. soit un entier $m \in \mathbb{Z}$. $\begin{cases} a/m \\ b/m \end{cases} \iff (a \vee b)/m.$

PROPOSITION 12.37 : **Le pgcd et le ppcm sont associatifs**

$$\forall (a,b,c) \in \mathbb{Z}^{\star 3},\ (a \wedge b) \wedge c = a \wedge (b \wedge c) \text{ et } (a \vee b) \vee c = a \vee (b \vee c)$$

On définit par récurrence le pgcd et le ppcm de n entiers par :

$$\text{pgcd}(x_1, \ldots, x_n) = x_1 \wedge \cdots \wedge x_n$$

$$\text{ppcm}(x_1, \ldots, x_n) = x_1 \vee \cdots \vee x_n$$

PROPOSITION 12.38 :
Soient deux entiers non nuls $(a,b) \in \mathbb{Z}^{\star 2}$. Pour un entier $k \in \mathbb{N}^\star$, $\begin{cases} (ka) \wedge (kb) = k(a \wedge b) \\ (ka) \vee (kb) = k(a \vee b) \end{cases}$.

THÉORÈME 12.39 : **Théorème d'Euclide**
Soient deux entiers $(a,b) \in \mathbb{Z}^{\star 2}$. Effectuons la division euclidienne de l'entier a par l'entier b :

$$\exists !(q,r) \in \mathbb{N}^2 \text{ tq } \begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

Alors :

$$\text{pgcd}(a,b) = \text{pgcd}(b,r)$$

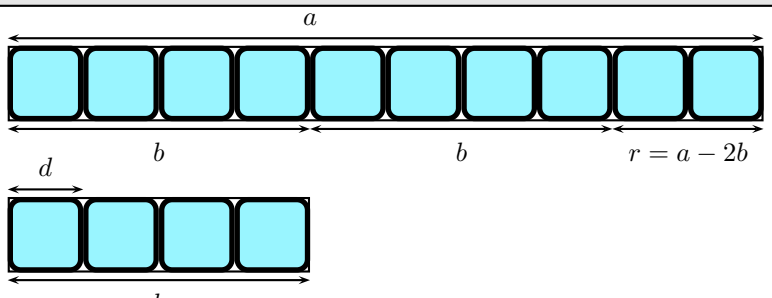


FIG. 12.5 – *Euclide : si d/b et d/a, alors d/r*

Le théorème précédent justifie l'algorithme d'Euclide pour trouver le pgcd de deux entiers non nuls $(a,b) \in \mathbb{N}^{\star 2}$. On pose $r_0 = a$, $r_1 = b$ et on définit ensuite $\forall k \geq 1$, les couples (q_k,r_k) en utilisant une division euclidienne :

$$\text{si } r_k \neq 0,\ \exists !(q_k,r_{k+1}) \in \mathbb{Z}^2 \text{ tq } r_{k-1} = q_k r_k + r_{k+1} \text{ et } 0 \leq r_{k+1} < r_k$$

Comme la suite d'entiers (r_k) est strictement décroissante, il existe un rang $n \geq 1$ tel que $r_n \neq 0$ et $r_{n+1} = 0$. D'après le théorème d'Euclide, on a $\forall k \in [0,n-1]$, $a \wedge b = r_k \wedge r_{k+1}$. Comme r_n divise r_{n-1}, on a $r_n \wedge r_{n-1} = r_n$. Par conséquent, le dernier reste non-nul r_n est le pgcd des entiers (a,b).

`Exemple 24.` Déterminez le pgcd des entiers 366 et 43 en utilisant l'algorithme d'Euclide, et en éliminant les restes « à la main ».

- **Paramètres :** a, b (entiers).
- **Variables locales :** A,B,r.
- **Initialisation :**
  - $A \leftarrow a$,
  - $B \leftarrow b$,
- **Corps :** Tant que $b \neq 0$ faire :
  - $r \leftarrow A \bmod B$,
  - $A \leftarrow B$,
  - $B \leftarrow r$,

  Fin tant que
- Renvoyer A ($A = \text{pgcd}(a,b)$).

Maple
```
pgcd := proc(a, b)
  local A, B, r;
  A := a;
  B := b;
  while (b > 0) do
     r := irem(A, B);
     A := B;
     B := r;
  od;
  A;
end;
```

ou sous une forme récursive :

Maple
```
pgcd := proc(a, b)
   if b = 0 then a
   else
     pgcd(b, irem(a, b))
   fi;
end;
```

DÉFINITION 12.22 : **Nombres premiers entre eux**
Soient n entiers non nuls $(x_1,\dots,x_n) \in \mathbb{Z}^{\star n}$. On dit que :
- les entiers $(x_1,\dots,x_n)$ sont premiers entre eux si et seulement si et seulement si $x_1 \wedge \dots \wedge x_n = 1$;
- les entiers $(x_1,\dots,x_n)$ sont premiers entre eux deux à deux si et seulement si $\forall (i,j) \in [1,n]^2$, $i \neq j \Rightarrow x_i \wedge x_j = 1$.

Remarque 126. Les entiers (3,6,7) sont premiers entre eux, mais pas premiers entre eux deux à deux. Si des entiers sont premiers deux à deux entre eux, ils sont premiers entre eux.

THÉORÈME 12.40 : **Théorème de Bezout** [a]
Soient deux entiers non nuls $(a,b) \in \mathbb{Z}^{\star 2}$. On a

$$(a \wedge b = 1) \Longleftrightarrow (\exists (u,v) \in \mathbb{Z}^2 \text{ tq } 1 = au + bv)$$

[a] Étienne Bezout, (31/03/1730- 27/09/1783), Français, auteur de livres d'enseignement, célèbre pour ce théorème mais a travaillé également sur les déterminants

Exercice 12-25
Soient deux entiers non nuls $(a,b) \in \mathbb{Z}^{\star 2}$ premiers entre eux. Montrez qu'il existe deux entiers $(u,v) \in \mathbb{Z}^2$ tels que

$$au + bv = 1 \text{ et } |u| < |b|,\ |v| \leq |a|$$

Exercice 12-26

Trouver grâce à l'algorithme d'Euclide un couple de Bezout pour $a = 22$ et $b = 17$.

Remarque 127. Soient deux entiers $(a,b) \in \mathbb{Z} \times \mathbb{N}^\star$ premiers entre eux. L'algorithme d'Euclide permet de trouver un couple de Bezout $(u,v) \in \mathbb{Z}^2$ tel que $au+bv = 1$. On définit les suites (r_k) et (q_k) des restes dans l'algorithme d'Euclide. Notons $r_n = a \wedge b = 1$ le dernier reste non-nul. On pose $r_0 = a$, $r_1 = b$ et par récurrence, on définit

$$\forall k \geq 1,\ r_{k-1} = q_k r_k + r_{k+1}\ 0 < r_{k+1} \leq r_k$$

On définit simultanément deux suites (u_k) et (v_k) telles que

$$\forall k \in [0,n],\ r_k = u_k a + v_k b$$

Pour que cette propriété soit vraie pour tout $k \in [0,n]$, on doit poser :

$$(u_0,v_0) = (1,0),\ (u_1,v_1) = (0,1) \ \text{ et } \forall k \in [2,n],\ \begin{cases} u_{k+1} = u_{k-1} - q_k u_k \\ v_{k+1} = v_{k-1} - q_k v_k \end{cases}$$

On a alors $1 = au_n + bv_n$.

$r_0 = a$	$r_1 = b$	r_2	$\ldots$	r_k	$\ldots$	1
X	q_1	q_2	$\ldots$	q_k	$\ldots$	q_n
1	0	u_2	$\ldots$	u_k	$\ldots$	$u_n = u$
0	1	v_2	$\ldots$	v_k	$\ldots$	$v_n = v$

Voici une procédure Maple qui prend comme paramètres a et b et qui retourne $a \wedge b$, ainsi qu'un couple de Bezout (U,V)

Maple

```
bezout := proc(a, b)
  local R, RR, Q, U, UU, V, VV, temp;
  R := a;
  RR := b;
  U := 1;
  UU := 0;
  V := 0;
  VV := 1;
  #Cond entrée :  R = r0, RR = r1, U = u0, V = v0, UU = u1, VV = v1
  while (RR > 0) do
    Q := iquo(R, RR);
    temp := UU;
    UU := U - Q * UU;
    temp := VV;
    VV := V - Q * VV;
    V := temp;
    temp := RR;
    RR := irem(R, RR);
    R := temp;
    #INV : R = rk, RR = r_{k+1}, U = uk, UU = u_{k+1}, V = vk, VV = v_{k+1},
    #    Q = qk,  k : nombre de passages dans la boucle while
  od;
    #Cond sortie : RR = u_{n+1}=0, R = r_n = pgcd(a, b), U = u_n, V = v_n
  R, U, V;
end;
```

THÉORÈME 12.41 : **Théorème de Gauss** [a]

Soient trois entiers non nuls $(a,b,c) \in \mathbb{Z}^{\star 3}$.

$$\begin{cases} a/bc \\ a \wedge b = 1 \end{cases} \Rightarrow a/c$$

[a] Carl Friedrich Gauss (30/04/1777 – 23/02/1855), Allemand. Considéré comme un des plus grand mathématicien de tous les temps avec Henri Poincaré. Il a permi des avancées énormes en théorie des nombres, géométrie non-euclidienne, ...

Exercice 12-27

Considérons deux entiers $(a,b) \in \mathbb{Z}^{\star 2}$ premiers entre eux : $a \wedge b = 1$ et un couple de Bezout $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Déterminer l'ensemble de tous les couples de Bezout $(u',v') \in \mathbb{Z}^2$ vérifiant $au' + bv' = 1$.

PROPOSITION 12.42 : **Autres propriétés du PGCD**

Soient trois entiers non nuls $(a,b,c) \in \mathbb{Z}^{\star 3}$.

1. Soient trois entiers $(\delta,a',b') \in \mathbb{N}^\star \times \mathbb{Z}^2$ tels que $a = \delta a'$, $b = \delta b'$, alors
$$\big(\delta = a \wedge b\big) \Longleftrightarrow \big(a' \wedge b' = 1\big)$$
2. $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Rightarrow a \wedge (bc) = 1$;
3. $\begin{cases} a/c \\ b/c \\ a \wedge b = 1 \end{cases} \Rightarrow ab/c$;
4. pour tous entiers $(k,p) \in \mathbb{N}^{\star 2}$, si $a \wedge b = 1$, alors $a^k \wedge b^p = 1$;
5. pour tout entier $k \in \mathbb{N}^\star$, $a^k \wedge b^k = (a \wedge b)^k$

Exercice 12-28

On se donne trois entiers non nuls $(A,B,C) \in \mathbb{Z}^{\star 3}$, et on considère l'équation diophantienne :

$$(E) \ : \ Ax + By = C \quad (x,y) \in \mathbb{Z}^2$$

Résoudre cette équation consiste à déterminer l'ensemble des solutions $\mathcal{S} = \{(x,y) \in \mathbb{Z}^2 \mid Ax + By = C\}$.

1. Notons $\delta = A \wedge B$. Montrez que si δ ne divise pas C, alors $\mathcal{S} = \emptyset$;
2. On suppose désormais que δ/C. Il existe trois entiers non nuls $(A',B',C') \in \mathbb{Z}^{\star 3}$ tels que $A = \delta A'$, $B = \delta B'$ avec $A' \wedge B' = 1$, et $C = \delta C'$. Montrez que l'équation (E) a même ensemble de solutions que l'équation
$$(E') \ : \ A'x + B'y = C'$$
3. Comment trouver une solution particulière de l'équation (E') ?
4. En déduire l'ensemble $\mathcal{S}$ de toutes les solutions ;
5. résoudre dans $\mathbb{Z}$ l'équation
$$(E) \ : \ 24x + 20y = 36$$

THÉORÈME 12.43 : **Relation entre PGCD et PPCM**

Soient deux entiers non nuls $(a,b) \in \mathbb{Z}^{\star 2}$.

1. Si $a \wedge b = 1$, alors $a \vee b = |ab|$;
2. $(a \wedge b)(a \vee b) = |ab|$.

12.4.2 Nombres premiers

DÉFINITION 12.23 : **Nombres premiers**

Un entier $n \in \mathbb{N}$ est dit *premier* si $n \geq 2$ et si ses seuls diviseurs dans $\mathbb{N}$, sont 1 ou lui-même :

$$\forall k \in \mathbb{N}^\star,\ k/n \Rightarrow k \in \{1,n\}$$

On note $\mathcal{P}$ l'ensemble des nombres premiers.

PROPOSITION 12.44 : **Propriétés des nombres premiers**

1. Soit un entier $n \in \mathbb{N}$ premier, et un entier $a \in \mathbb{Z}$. Alors, n/a ou bien $n \wedge a = 1$.
2. Si n et m sont deux nombres premiers distincts, ils sont premiers entre eux : $n \neq m \Rightarrow n \wedge m = 1$.
3. Si n est un nombre premier et si $(a_1,\ldots,a_k) \in \mathbb{Z}^k$,
$$n/a_1 \ldots a_k \Rightarrow \exists i \in [\![1,n]\!] \text{ tq } n/a_i$$

PROPOSITION 12.45 : **Existence d'un diviseur premier**
Tout entier $n \geq 2$ possède au moins un diviseur premier.

THÉORÈME 12.46 : **Décomposition en facteurs premiers**
Soit un entier $n \in \mathbb{N} \setminus \{0,1\}$. Cet entier n s'écrit de façon unique (à l'ordre des facteurs près) comme :

$$n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$$

où $\nu_p(n) \in \mathbb{N}$ est appelé la *p-valuation* de l'entier n.

Remarque 128. Tout entier relatif $n \in \mathbb{Z}$ non nul s'écrit de façon unique sous la forme :

$$n = \pm \prod_{p \in \mathcal{P}} p^{\nu_p(|n|)}$$

Pour des entiers $a,b \in \mathbb{N}^\star$, et $p \in \mathcal{P}$,

$$\nu_p(a \times b) = \nu_p(a) + \nu_p(b) \quad a/b \Rightarrow \nu_p(a) \leq \nu_p(b)$$

THÉORÈME 12.47 : **Il existe une infinité de nombres premiers**
L'ensemble $\mathcal{P}$ des nombres premiers est infini.

THÉORÈME 12.48 : **Expression du PGCD et du PPCM à l'aide des facteurs premiers**
Soient deux entiers non-nuls $(a,b) \in {\mathbb{N}^\star}^2$. Leur décomposition en facteurs premiers s'écrit :

$$a = \prod_{p \in \mathcal{P}} p^{\nu_p(a)} \quad b = \prod_{p \in \mathcal{P}} p^{\nu_p(b)}$$

Alors la décomposition de $a \wedge b$ et de $a \vee b$ en facteurs premiers s'écrit :

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min\{\nu_p(a),\nu_p(b)\}} \quad a \vee b = \prod_{p \in \mathcal{P}} p^{\max\{\nu_p(a),\nu_p(b)\}}$$

COROLLAIRE 12.49 :
Dans l'ensemble $\mathbb{Z}^\star$, les lois $\wedge$ et $\vee$ sont distributives. Pour tous entiers non nuls $(a,b,c) \in {\mathbb{Z}^\star}^3$,
- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;
- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Exercice 12-29
On considère un entier n décomposé en produit de facteurs premiers :

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

où $\forall i \in [1,k]$, $\alpha_i \in \mathbb{N}^\star$. Calculez la somme de tous les diviseurs de l'entier n :

$$S = \sum_{d/n} d$$

12.4.3 Applications de l'arithmétique

THÉORÈME 12.50 : **Éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$**
Soit un entier $x \in [0,n-1]$. L'élément $\widehat{x}$ est inversible pour la multiplication dans l'anneau $\left(\mathbb{Z}/n\mathbb{Z},\widehat{+},\widehat{\times}\right)$ si et seulement si $x \wedge n = 1$.

COROLLAIRE 12.51 :
Soit un entier $n \in \mathbb{N}^\star$. L'anneau $\left(\mathbb{Z}/n\mathbb{Z},\widehat{+},\widehat{\times}\right)$ est un corps si et seulement si l'entier n est un nombre premier.

Exercice 12-30
Déterminez tous les entiers $x \in \mathbb{Z}$ tels que $x^2 + 5x - 3$ soit divisible par 7.

Exercice 12-31

On considère un entier non nul $n \in \mathbb{N}^\star$ et le groupe $(U_n,\times)$ des racines nièmes de l'unité. On note $\omega = e^{2i\pi/n}$ la racine nième primitive de l'unité et $\alpha = \omega^p$. À quelle condition, a-t-on $U_n = \{\alpha^k;\ k \in \mathbb{N}\}$?