10.15 Exercice

$$x \mapsto x^{-1} \text{ est un morphisme de } G \Leftrightarrow \forall (x,y) \in G^2, (xy)^{-1} = x^{-1}y^{-1}$$

Or :

$$\begin{aligned} (xy)^{-1} &= y^{-1}x^{-1} \\ \Leftrightarrow x^{-1}y^{-1} &= y^{-1}x^{-1} \end{aligned}$$

Donc G est commutatif.

11.1 Exercice

$$\begin{aligned} AB \text{ est symétrique } &\Leftrightarrow AB = {}^t(AB) \\ &\Leftrightarrow AB = {}^tB \times {}^tA \\ &\Leftrightarrow AB = BA \end{aligned}$$

11.4 Exercice

Analyse :
On suppose que :

$$\begin{aligned} X + tr(X)A &= B \\ \text{Donc } X &= B - tr(X)A \\ \text{Donc } tr(X) &= tr(B) - tr(X)tr(A) \\ \text{Donc } tr(X) &= \begin{cases} \frac{tr(B)}{1+tr(A)} \text{ si } tr(A) \neq -1 \\ tr(X) + tr(B) \text{ si } tr(A) = -1 \end{cases} \\ \text{Donc } X &= B - \frac{tr(B)}{1+tr(A)}A \end{aligned}$$

Synthèse :
On pose $X = B - \frac{tr(B)}{1+tr(A)}A$

11.15 Exercice

$$MX = 0 \Leftrightarrow \exists (x,y,z) \in \mathbb{R}^3, \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & 3 \\ -1 & 4 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

$$\Leftrightarrow \begin{cases} x - 2y + z = 0 \\ y + 3z = 0 \\ -x + 4y + 7z = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x - 2y + z = 0 \\ y + 3z = 0 \\ 2y + 8z = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x - 2y + z = 0 \\ y + 3z = 0 \\ 2z = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 0 \\ y = 0 \\ z = 0 \end{cases}$$

12.1 Exercice

On remarque que $2^{10} \equiv 1 \pmod{11}$ et que $3^5 \equiv 1 \pmod{11}$.
Donc $2^{123} \equiv 2^3 \equiv 8 \pmod{11}$ et $3^{121} \equiv 3^1 \equiv 3 \pmod{11}$.
Donc $\boxed{2^{123} + 3^{121} \equiv 0 \pmod{11}}$.

12.2 Exercice

On raisonne par disjonction de cas :

$n \pmod 6$	$n+2 \pmod 6$	$7n-5 \pmod 6$	$n(n+2)(7n-5) \pmod 6$
0	2	1	0
1	3	2	0
2	4	3	0
3	5	4	0
4	0	5	0
5	1	0	0

Donc $\boxed{\forall n \in \mathbb{Z}, n(n+2)(7n-5) \equiv 0 \pmod{6}}$.

12.3 Exercice

1. On cherche une puissance cyclique de $3 \pmod{25}$.

$$\begin{aligned} 3 &\equiv 3 \pmod{25} \\ 3^2 &\equiv 9 \pmod{25} \\ 3^3 &\equiv 2 \pmod{25} \\ 3^4 &\equiv 6 \pmod{25} \\ 3^5 &\equiv 18 \pmod{25} \\ 3^6 &\equiv 4 \pmod{25} \\ 3^7 &\equiv 12 \pmod{25} \\ 3^8 &\equiv 11 \pmod{25} \\ 3^9 &\equiv 8 \pmod{25} \\ 3^{10} &\equiv 24 \equiv -1 \pmod{25} \end{aligned}$$

   Donc $\boxed{3^{2189} \equiv 3^{2180} \times 3^9 \equiv (3^{10})^{218} \times 3^9 \equiv (-1)^{218} \times 8 \equiv 8 \pmod{25}}$.

2. On cherche une puissance cyclique de $55 \pmod{8}$.

$$\begin{aligned} 55 &\equiv 7 \pmod{8} \\ 55^2 &\equiv 1 \pmod{8} \end{aligned}$$

   Donc $\boxed{55^{970321} \equiv 55^1 \equiv 7 \pmod{8}}$.

3. On cherche une puissance cyclique de $1234^{4312} \pmod{7}$ et de $4321^{1234} \pmod{7}$.

$$\begin{aligned} 1234^1 &\equiv 2 \pmod{7} \text{ et } 4321^1 \equiv 2 \pmod{7} \\ 1234^2 &\equiv 4 \pmod{7} \text{ et } 4321^2 \equiv 4 \pmod{7} \\ 1234^3 &\equiv 1 \pmod{7} \text{ et } 4321^3 \equiv 1 \pmod{7} \end{aligned}$$

   Donc $1234^{4312} \equiv 1234^{3\times 1437+1} \equiv 2 \pmod{7}$ et $4321^{1234} \equiv 4321^{3\times 411+1} \equiv 2 \pmod{7}$.
   Donc $\boxed{1234^{4321} + 4321^{1234} \equiv 4 \pmod{7}}$.

12.4 Exercice

1. Soit $n \in \mathbb{N}$.
   On remarque que $4|100$, donc $\forall k \geq 2 \in \mathbb{N}, 4|a_k$.
   Et :

$$\begin{aligned} 4|n &\Leftrightarrow k|\sum_{k=0}^{r} a_k \times 10^k \\ &\Leftrightarrow k|\sum_{k=2}^{r}(a_k \times 10^k) + a_1 \times 10 + a_0 \end{aligned}$$

   Or comme on sait que $k|\sum_{k=2}^{r}(a_k \times 10^k)$, nécessairement, $k|(a_0 + a_1 \times 10)$.

12.8 Exercice

1. Soit $a \geq 2$ et $n \geq 2$.

$$a^n - 1 = (a-1)\sum_{k=0}^{n-1} a^k$$

   On a donc :

$$\begin{aligned} a^n - 1 \in \mathbb{P} \text{ donc } (a-1)\sum_{k=0}^{n-1} a^k &\in \mathbb{P} \\ \text{donc } a-1 = 1 \text{ et } \sum_{k=0}^{n-1} = a^n - 1 &\text{ ou } a-1 = a^n - 1 \text{ et } \sum_{k=0}^{n-1} a^k = 1 \\ \text{donc } a-1 = 1 \text{ et } \sum_{k=0}^{n-1} a^n - 1 & \\ \text{donc } a = 2 & \end{aligned}$$

2. On raisonne par l'absurde : supposons que $n \notin \mathbb{P}$. Alors $n = ab$ avec $a > 1$ et $b > 1$. Donc on a :

$$\begin{aligned} 2^n - 1 \in \mathbb{P} &\Leftrightarrow 2^{ab} - 1 \in \mathbb{P} \\ &\Leftrightarrow (2^a - 1)(\sum_{k=0}^{b-1} 2^{ak}) \in \mathbb{P} \end{aligned}$$

   Absurde.
   Donc, nécessairement, n est premier.

12.10 Exercice

1. (a) Soit $k \in \mathbb{N}$ tel que $k \equiv 3 \pmod 4$. k est donc impair.
   On note $(p_i)_{i\in\mathbb{N}}$ les diviseurs premiers de k.
   Nécessairement, pour tout $i \in \mathbb{N}$ on a $p_i \equiv 1 \pmod 4$ ou $p_i \equiv 3 \pmod 4$ (k est impair, donc p_i est impair).
   On raisonne par l'absurde : supposons que $\forall i \in \mathbb{N}, p_i \equiv 1 \pmod 4$.
   Alors $\prod_{i=0}^{n} p_i^{\alpha_i} \equiv 1 \pmod 4 \Leftrightarrow k \equiv 1 \pmod 4$.
   Absurde.
   Donc tout entier naturel congru à 3 modulo 4 possède au moins un diviseur premier congru à 3 modulo 4.

   (b) On raisonne par l'absurde : on suppose que l'ensemble des nombres premiers congrus à 3 modulo 4 est fini. On note cet ensemble $\mathbb{P}_3$.

$$\mathbb{P}_3 = \{p_1, p_2, \ldots, p_n | \, n \in \mathbb{N}\}$$

Soit $n = |\mathbb{P}_3|$. On remarque que pour tout $k \in [\![1, n]\!]$,

$$4 \times \prod_{k=1}^{n} p_k - 1 \equiv 3 \pmod 4$$

n'est pas divisible par p_k et n'appartient pas à $\mathbb{P}_3$.
Or cette quantité possède forcément au moins un diviseur premier congru à 3 modulo 4 (cf. (a)).
Absurde.
Donc il existe une infinité de nombres premiers congrus à 3 modulo 4.

2. De la même manière, on montre que tout entier congru à 5 modulo 6 possède au moins un diviseur congru à 5 modulo 6.
   De la même manière, on raisonne par l'absurde en supposant que l'ensemble des nombres premiers congrus à 5 modulo 6 noté $\mathbb{P}_5$ est fini.
   On remarque qu'il existe un facteur premier $p \equiv 5 \pmod 6 \notin \mathbb{P}_5$ qui divise $6 \prod_{k=1}^{|\mathbb{P}_5|} p_k - 1$.
   Absurde.
   Donc il existe une infinité de nombres premiers congrus à 5 modulos 6.

12.11 Exercice

1. Soit $p \in \mathbb{P}$, $y \in [\![1, p-1]\!]$.

$$\exists! x \in [\![1, p-1]\!], xy \equiv 1 \pmod p$$

12.12 Exercice

Soit $(a, b, c) \in \mathbb{N}^3$.
On suppose que $b \wedge c = 1$.
Donc :

$$\begin{aligned}
\forall p \in \mathbb{P}, v_p(a \wedge (bc)) &= \min(v_p(a), v_p(bc)) \\
&= \min(v_p(a), v_p(b) + v_p(c)) \\
&= \min(v_p(a), v_p(b), v_p(c)) \text{ (car } b \text{ et } c \text{ sont premiers entre eux)} \\
&= v_p(a \wedge b, a \wedge c)
\end{aligned}$$

Donc $\boxed{a \wedge (bc) = a \wedge b, a \wedge c}$.

12.13 Exercice

Soit $(a, b) \in (\mathbb{Z}^*)^2$.
On suppose que $a^2 | b^2$.
On a :

$$\begin{aligned}
\forall p \in \mathbb{P}, v_p(a^2) \leq v_p(b^2) &\text{ donc } \forall p \in \mathbb{P}, 2v_p(a) \leq 2v_p(b) \\
&\text{donc } \forall p \in \mathbb{P}, v_p(a) \leq v_p(b) \\
&\text{donc } a | b
\end{aligned}$$

12.14 Exercice

Soit $(a, b) \in (\mathbb{N}^*)^2$.

$$\begin{aligned}
(a \wedge b)^n = a^n \wedge b^n &\Leftrightarrow \forall p \in \mathbb{P}, v_p((a \wedge b)^n) = v_p(a^n \wedge b^n) \\
&\Leftrightarrow \forall p \in \mathbb{P}, n \times v_p(a \wedge b) = \min(v_p(a)^n, v_p(b)^n) \\
&\Leftrightarrow \forall p \in \mathbb{P}, n \times \min(v_p(a), v_p(b)) = \min(n \times v_p(a), n \times v_p(b))
\end{aligned}$$

12.15 Exercice

1. Soit $(a,b) \in (\mathbb{N}^*)^2$ et $k \geq 2$ entier.
   On suppose que $a \wedge b = 1$ et que $\exists \lambda \in \mathbb{N}, ab = \lambda^k$.
   On note λ l'entier tel que $ab = \lambda^k$.

$$\begin{aligned} ab = \lambda^k &\Leftrightarrow v_\lambda(ab) = v_\lambda(\lambda^k) \\ &\Leftrightarrow v_\lambda(a) + v_\lambda(b) = k \end{aligned}$$

   Or si $\lambda \neq 1$:

$$v_\lambda(a \wedge b) = 0 = \min(v_\lambda(a), v_\lambda(b))$$

   Donc, par disjonction de cas :

   - si $\lambda = 1$, alors $ab = 1^k$ et on a bien $a = 1^k$ et $b = 1^k$.
   - si $\lambda \neq 1$, alors :

$$\begin{aligned} v_\lambda(a) + v_\lambda(b) = k &\Leftrightarrow \max(v_\lambda(a), v_\lambda(b)) = k \\ &\Leftrightarrow \max(a,b) = \lambda^k \text{ et } \min(a,b) = 1^k \ (\forall d \neq \lambda \in \mathbb{P}, d \not| \lambda, \ v_d(ab) = 0) \end{aligned}$$

2. Le résultat ne persiste pas pour $(a,b) \in \mathbb{Z}^2$:
   On choisit a et b négatifs tels que $a \wedge b = 1$ et $ab = \lambda^k$.
   Ainsi, il n'existe pas de $n \in \mathbb{N}$ tel que $a = n^k$ (car a est négatif).

12.16 Exercice

1. <u>Première méthode</u>
   Soit $p \in \mathbb{P}$ et $n \in \mathbb{N}$.
   On note $A_k = \{q \in [\![1,n]\!], p^q | k\}$ et $a_k = |A_k|$.
   On note $V_l = \{k \in [\![1,n]\!], v_p(k) = l\}$ et on note $m_l = |V_l|$.
   Lien entre V_k, A_k :

$$V_k = A_k \backslash A_{k+1}$$

   Par ailleurs, $A_{k+1} \subset A_k$.

$$m_k = a_k - a_{k+1}$$

   On a :

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{n} v_p(k) \\ &= \sum_{l \geq 0} l \times m_l \text{ (définition de } V_l) \\ &= \sum_{l \geq 0} l(a_l - a_{l+1}) \\ &= \sum_{l \geq 0} l a_l - \sum_{l \geq 0} l a_{l+1} \\ &= \sum_{l \geq 1} l a_l - \sum_{l \geq 1} (l-1) a_l \\ &= \sum_{l \geq 1} a_l \end{aligned}$$

   On explicite le cardinal de A_l.
   Déterminer le nombre de $k, 1 \leq kp^l \leq n$.
   Soit :

$$\frac{1}{p^l} \leq k \leq \frac{n}{p^l}$$

   Soit :

$$1 \leq k \leq \frac{n}{p^l}$$

Il y en a $\lfloor \frac{n}{p^l} \rfloor$.

Deuxième méthode
On peut montrer que :

$$\left\lfloor \frac{\lfloor \frac{a}{b} \rfloor}{c} \right\rfloor = \left\lfloor \frac{a}{bc} \right\rfloor$$

En particulier :

$$\left\lfloor \frac{\lfloor \frac{n}{p^k} \rfloor}{p} \right\rfloor = \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$$

On raisonne par récurrence forte.
Initialisation :
On vérifie que ça fonctionne pour $n = 0$.

Hérédité :

$$\begin{aligned}
v_p((n+1)!) &= v_p(n+1) + v_p(n!) \\
&= v_p(n+1) + \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \\
&= \sum_{1 \leq i \leq n+1} v_p(i) \\
&= \sum_{1 \leq i \leq n+1, p \mid i} v_p(i) \text{ (si } p \not| i \text{, alors } v_p(i) = 0) \\
&= \sum_{1 \leq kp \leq n+1} v_p(p \times k) \\
&= \sum_{1 \leq k \leq \frac{n+1}{p}} v_p(p \times k) \\
&= \sum_{1 \leq k \leq \frac{n+1}{p}} (v_p(k) + 1) \\
&= \left\lfloor \frac{n+1}{p} \right\rfloor + \sum_{1 \leq k \leq \frac{n+1}{p}} v_p(k) \\
&= \left\lfloor \frac{n+1}{p} \right\rfloor + v_p\left(\left\lfloor \frac{n+1}{p}! \right\rfloor \right) \\
&= \left\lfloor \frac{n+1}{p} \right\rfloor + \sum_{k \geq 1} \left\lfloor \frac{\lfloor \frac{n}{p} \rfloor}{p^k} \right\rfloor \\
&= \left\lfloor \frac{n+1}{p} \right\rfloor + \sum_{k \geq 1} \left\lfloor \frac{n+1}{p^{k+1}} \right\rfloor \\
&= \sum_{k \geq 1} \left\lfloor \frac{n+1}{p^k} \right\rfloor
\end{aligned}$$

2.

$$\begin{aligned} v_2(100!) &= \sum_{j\geq 1} \left\lfloor \frac{100}{2^k} \right\rfloor \\ &= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{4} \right\rfloor + \left\lfloor \frac{100}{8} \right\rfloor + \left\lfloor \frac{100}{16} \right\rfloor + \left\lfloor \frac{100}{32} \right\rfloor + \left\lfloor \frac{100}{64} \right\rfloor \\ &= 50 + 25 + 12 + 6 + 3 + 1 \\ &= 97 \\ v_5(100)! &= \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor \\ &= 20 + 4 \\ &= 24 \end{aligned}$$

100! s'achève donc par $\min(v_2(100!), v_5(100!)) = 24$.

13.1 Exercice

Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme de $\mathbb{K}[X]$.

On suppose que P^{-1} existe. Alors :

$$\begin{aligned} PP^{-1} = 1 &\Leftrightarrow \deg(PP^{-1}) = 0 \\ &\Leftrightarrow \deg P + \deg P^{-1} = 0 \text{ ($\mathbb{K}$ est un corps, donc est intègre)} \\ &\Leftrightarrow \deg P = 0 \end{aligned}$$

Ainsi, Comme $\mathbb{K}$ est un corps, on a :

$$\forall P \neq 0 \in \mathbb{K}[X], \deg P = 0, P \in U(\mathbb{K}[X])$$

13.2 Exercice

$$\begin{aligned} P_n &= (1 + X + X^2 + \cdots + X^n)^2 \\ &= \left(\sum_{k=0}^{n} X^k \right)^2 \\ &= \left(\frac{1 - X^{n+1}}{1 - X} \right)^2 \\ &= \frac{X^{2(n+1)} - 2X^{n+1} + 1}{X^2 - 2X + 1} \end{aligned}$$

$$\begin{aligned} Q_n &= (1 + X) \times (1 + X^2) \times (1 + X^4) \times \cdots \times (1 + X^{2^n}) \\ &= \prod_{k=0}^{n} (1 + X^{2^k}) \end{aligned}$$

14.6 Exercice

1. Soit $n \in \mathbb{N}$. Lorsque $a = 1$, on a la relation $u_{n+1} = u_n + b$. Ainsi, (u_n) est une suite arithmétique d'expression :
$$u_n = u_0 + nb$$

2. (a) Pour $n \in \mathbb{N}$:

$$\begin{aligned} v_n &= u_n + \lambda \\ \text{donc } v_{n+1} &= u_{n+1} + \lambda \\ &= au_n + b + \lambda \end{aligned}$$

On remarque que pour $\lambda = \frac{b}{a-1}$ avec $a \neq 1$, on a :

$$\begin{aligned} v_{n+1} &= au_n + b + \frac{b}{a-1} \\ &= \frac{(a-1)(a)u_n + (a-1)b + b}{a-1} \\ &= a \times \frac{(a-1)u_n + b}{a-1} \\ &= a\left(u_n + \frac{b}{a-1}\right) \\ &= av_n \end{aligned}$$

Donc pour $\lambda = \frac{b}{a-1}$, (v_n) est géométrique.

(b)

$$\begin{aligned} v_n &= u_n + \frac{b}{a-1} \\ \text{donc } u_n &= v_n - \frac{b}{a-1} \\ &= \left(u_0 + \frac{b}{a-1}\right) \times a^n - \frac{b}{a-1} \\ &= u_0 a^n + (a^n - 1)\frac{b}{a-1} \end{aligned}$$

14.2 Exercice

1. Soit $k \geq 2 \in \mathbb{N}$.

$$\begin{aligned} \frac{1}{k^2} \leq \frac{1}{k-1} - \frac{1}{k} &\Leftrightarrow \frac{1}{k^2} \leq \frac{1}{k(k-1)} \\ &\Leftrightarrow \frac{1}{k} \leq \frac{1}{k-1} \\ &\Leftrightarrow k \geq k-1 \ (x \mapsto \frac{1}{x} \text{ est décroissante}) \end{aligned}$$

2. On suppose que S_n converge. Ainsi, pour $n \in \mathbb{N}$, on a d'une part :

$$\begin{aligned} \frac{1}{k^2} \leq \frac{1}{k-1} - \frac{1}{k} &\Leftrightarrow S_n \leq 1 + \sum_{k=2}^{n} \left(\frac{1}{k-1} - \frac{1}{k}\right) \\ &\Leftrightarrow S_n \leq 1 + 1 - \frac{1}{n} \text{ (télescopage)} \\ &\Leftrightarrow \lim_{n\to+\infty} S_n \leq \lim_{n\to+\infty} 2 + \frac{1}{n} \text{ (Hypothèse)} \\ &\Leftrightarrow \lim_{n\to+\infty} S_n \leq 2 \end{aligned}$$

D'autre part, la suite est strictement croissante, donc d'après le théorème de la limite monotone, (u_n) converge.