

## Rappel de cours

**Definition 1.** La relation  $xRy$  est une relation d'équivalence sur l'ensemble  $E$  ssi:

- $\forall x \in E, xRx$
- $\forall x, y \in E, xRy \Rightarrow yRx$
- $\forall x, y, z \in E, xRy \wedge yRz \Rightarrow xRz$

**Definition 2.** Les équations suivantes sont équivalentes:

- $a \equiv b \pmod{p}$
- $kp + a \equiv b \pmod{p}$
- $\exists k, k', a = kp + r \wedge b = k'p + r \wedge 0 \leq r < p$
- $\exists k, k', a - kp = b - k'p$

**Theorem 1.** Petit Théorème de Fermat 1. Si  $p$  est un nombre premier alors  $\forall a \in \mathbb{N}, a^p \equiv a \pmod{p}$ . ou  $\exists k, a^p - a = kp$

**Theorem 2.** Petit Théorème de Fermat 2. Si  $p$  est un nombre premier alors  $\forall a \in \mathbb{N}, p \nmid a, a^{p-1} \equiv 1 \pmod{p}$ . ou  $\exists k, a^{p-1} - 1 = kp$

## Exercice 1

### Exercice 1.1

La relation  $R$  n'est pas une relation d'équivalence car  $(4, 4) \notin R$ .

Si on ajoute le couple  $(4, 4)$  à la relation  $R$  alors  $R$  est une relation d'équivalence car

- $(1, 1), (2, 2), (3, 3), (4, 4) \in R$
- $(1, 2) \Rightarrow (2, 1), (3, 4) \Rightarrow (4, 3)$
- $(1, 1) \wedge (1, 2) \Rightarrow (1, 2), (1, 2) \wedge (2, 1) \Rightarrow (1, 1), (1, 2) \wedge (2, 2) \Rightarrow (1, 2), \dots$

### Exercice 1.2

La liste des classes d'équivalence est  $\{(1, 1), (1, 2), (2, 1), (2, 2)\}, \{(3, 3), (3, 4), (4, 3), (4, 4)\}$ .

## Exercice 2

### Exercice 2.1

- $\forall a, b \in \mathbb{R}, (a, b)R(a, b) \Leftrightarrow a^2 + b^2 = a^2 + b^2$  est vrai
- $\forall a, b, c, d \in \mathbb{R}, ((a, b)R(c, d) \Rightarrow (c, d)R(a, b)) \Leftrightarrow (a^2 + b^2 = c^2 + d^2 \Rightarrow c^2 + d^2 = a^2 + b^2)$  est vrai car l'égalité est symétrique
- $\forall a, b, c, d, e, f \in \mathbb{R}, ((a, b)R(c, d) \wedge (c, d)R(e, f) \Rightarrow (a, b)R(e, f)) \Leftrightarrow (a^2 + b^2 = c^2 + d^2 \wedge c^2 + d^2 = e^2 + f^2 \Rightarrow a^2 + b^2 = e^2 + f^2)$  est vrai car l'égalité est transitive

### Exercice 2.2

La relation  $R$  est l'ensemble des points du cercle de centre  $(0, 0)$  et de rayon  $\sqrt{a^2 + b^2}$ .

### Exercice 2.3

Pas compris  $|R^2 \setminus \mathbb{R}$ .

## Exercice 3

### Exercice 3.1

Prenons  $x = a + i.b$ ,  $y = c + i.d$  et  $z = e + i.f$

- $\forall x \in \mathbb{C}, xRx \Leftrightarrow |x| = |x| \Leftrightarrow \sqrt{a^2 + b^2} = \sqrt{a^2 + b^2}$  est vrai
- $\forall x, y \in \mathbb{C}, (xRy \Rightarrow yRx) \Leftrightarrow (|x| = |y| \Rightarrow |y| = |x|) \Leftrightarrow (\sqrt{a^2 + b^2} = \sqrt{c^2 + d^2} \Rightarrow \sqrt{c^2 + d^2} = \sqrt{a^2 + b^2})$  est vrai car l'égalité est symétrique
- $\forall x, y, z \in \mathbb{C}, (xRy \wedge yRz \Rightarrow xRz) \Leftrightarrow (|x| = |y| \wedge |y| = |z| \Rightarrow |x| = |z|) \Leftrightarrow (\sqrt{a^2 + b^2} = \sqrt{c^2 + d^2} \wedge \sqrt{c^2 + d^2} = \sqrt{e^2 + f^2} \Rightarrow \sqrt{a^2 + b^2} = \sqrt{e^2 + f^2})$  est vrai car l'égalité est transitive

### Exercice 3.2

- $\forall x \in \mathbb{R}, xRx \Leftrightarrow e^x = e^x$  est vrai
- $\forall x, y \in \mathbb{R}, (xRy \Rightarrow yRx) \Leftrightarrow (e^x = e^y \Rightarrow e^y = e^x)$  est vrai car l'égalité est symétrique
- $\forall x, y, z \in \mathbb{R}, (xRy \wedge yRz \Rightarrow xRz) \Leftrightarrow (e^x = e^y \wedge e^y = e^z \Rightarrow e^x = e^z)$  est vrai car l'égalité est transitive

## Exercice 4

### Exercice 4.1

- $\forall a, b \in \mathbb{R}, (a, b)R(a, b) \Leftrightarrow ab = ba$  est vrai car la multiplication est commutative
- $\forall a, b, c, d \in \mathbb{R}, ((a, b)R(c, d) \Rightarrow (c, d)R(a, b)) \Leftrightarrow (ad = bc \Rightarrow cb = da)$  est vrai car l'égalité est symétrique et la multiplication est commutative
- $\forall a, b, c, d, e, f \in \mathbb{R}, ((a, b)R(c, d) \wedge (c, d)R(e, f) \Rightarrow (a, b)R(e, f)) \Leftrightarrow (ad = bc \wedge cf = de \Rightarrow af = be)$  est vrai car  $a = \frac{bc}{d}$ , donc  $af = \frac{bc}{d}f$  mais  $cf = de$  donc  $af = \frac{bde}{d} = be$ .

### Exercice 4.2

$(p, q)R(x, y) \Leftrightarrow py = qx$  avec  $(p, q)$  premiers entre eux. Le seul couple est  $x = np$  et  $y = nq$ . Donc la relation représente les couples  $\forall n \in \mathbb{N}^*, (np, nq)$  avec  $(p, q)$  premiers entre eux.

## Exercice 5

### Exercice 5.1

- $\forall P \in \mathbb{R}, PRP \Leftrightarrow P - P$  est un multiple de  $X$  est vrai car 0 est un multiple de tous les nombres ( $0 = 0 \cdot X$ )
- $\forall P, Q \in \mathbb{R}, (PRQ \Rightarrow QRP) \Leftrightarrow (P - Q = k \cdot X \Rightarrow Q - P = k' \cdot X)?$  est vrai en prenant  $k' = -k$  car  $Q - P = -(P - Q) = -kX$
- $\forall P, Q, S \in \mathbb{R}, (PRQ \wedge QRS \Rightarrow PRS) \Leftrightarrow (P - Q = kX \wedge Q - S = k'X \Rightarrow P - S = k''X)?$  est vrai  $P - S = (P - Q) - (Q - S) = kX + k'X = (k + k')X$

### Exercice 5.2

$PRP(0) = P - P(0)$  mais  $P(0)$  est le polynôme de degré 0, donc  $P - P(0)$  est un polynôme avec le degré 0 égale à 0. On peut donc le factoriser par  $X$ . Par conséquent  $P - P(0) = X \cdot k$  est un multiple de  $X$

### Exercice 5.3

En prenant par exemple,  $\pi : \mathbb{Z}[X] \rightarrow \mathbb{Z}[X], P \mapsto P - X$ , on a  $\forall P \in \mathbb{Z}[X], P(0) = (P - X)(0)$  car  $P - X$  ne change pas de degré 0 du polynôme  $P$ .

## Exercice 6

Prenons  $a = 7k + r$  et  $b = 7k' + r'$  avec  $r, r' < 7$ . On a

$$a^2 + b^2 = (7k + r)^2 + (7k' + r')^2 = 49k^2 + 14kr + r^2 + 49k'^2 + 14k'r' + r'^2 = 7(7k^2 + 2kr + 7k' + 2k'^2 r') + r^2 + r'^2$$

On a  $7|a^2 + b^2$  donc  $7|7(7k^2 + 2kr + 7k'^2 + 2k'r') + r^2 + r'^2$ , donc  $7|r^2 + r'^2$  et  $r, r' < 7$ . On a

$0^2$	mod 7	0
$1^2$	mod 7	1
$2^2$	mod 7	4
$3^2$	mod 7	2
$4^2$	mod 7	2
$5^2$	mod 7	4
$6^2$	mod 7	1

La seule combinaison possible est  $r = 0$  et  $r' = 0$ . Donc  $7|a$  et  $7|b$ .

## Exercice 7

Preuve par récurrence. Vrai pour  $n = 0$  ( $3^1 + 2^2 = 7$ ). Supposons vrai pour  $n$ ,  $3^{2n+1} + 2^{n+2} = 7k$  est-ce que  $3^{2(n+1)+1} + 2^{(n+1)+2} = 7k'$

$$3^{2(n+1)+1} + 2^{(n+1)+2} = 3^{(2n+1)+2} + 2^{(n+2)+1} = 9 \cdot 3^{2n+1} + 2 \cdot 2^{n+2}$$

On a  $3^{2n+1} = 7k - 2^{n+2}$  (hypothèse)

$$9 \cdot (7k - 2^{n+2}) + 2 \cdot 2^{n+2} = 63k - 7 \cdot 2^{n+2} = 7(9k + 2^{n+2})$$

Donc vrai en prenant  $k' = 9k + 2^{n+2}$ .

## Exercice 8

Preuve par récurrence. pour  $n = 1$ , on a  $2^{3+3} - 7 - 8 = 64 - 15 = 49$ . Supposons vrai pour  $49|2^{3n+3} - 7n - 8$  au rang  $n$ , vérifions que  $49|2^{3(n+1)+3} - 7(n+1) - 8$

$$\begin{aligned} 2^{3(n+1)+3} - 7(n+1) - 8 &= 2^{3n+3+3} - 7(n+1) - 8 = 2^3 \cdot 2^{3n+3} - 7n - 7 - 8 = (7+1)2^{3n+3} - 7n - 7 - 8 = 7 \cdot 2^{3n+3} - 7 + (2^{3n+3} - 7n - 8) \\ &= 7(2^{3n+3} - 1) + (2^{3n+3} - 7n - 8) \end{aligned}$$

On a  $49|(2^{3n+3} - 7n - 8)$  par hypothèse de récurrence. Il reste à montrer que  $49|7(2^{3n+3} - 1)$  ou  $7|2^{3n+3} - 1$ .

Preuve par récurrence, pour  $n=1$ ,  $2^6 - 1 = 64 - 1 = 63$  qui est divisible par 7. Supposons  $7|2^{3n+3} - 1$  et vérifions  $7|2^{3(n+1)+3} - 1$ .

$$2^{3(n+1)+3} - 1 = 2^{3n+3+3} - 1 = 2^3 \cdot 2^{3n+3} - 1 = (7+1) \cdot 2^{3n+3} - 1 = 7 \cdot 2^{3n+3} + 2^{3n+3} - 1$$

On a  $7|2^{3n+3} - 1$  par hypothèse de récurrence. et  $7|7 \cdot 2^{3n+3}$ . donc  $\forall n \in \mathbb{N}, 7|2^{3n+3} - 1$ , et  $\forall n \in \mathbb{N}, 49|7(2^{3n+3} - 1)$ , et  $\forall n \in \mathbb{N}, 49|7(2^{3n+3} - 1) + (2^{3n+3} - 7n - 8)$  et  $\forall n \in \mathbb{N}, 49|2^{3n+3} - 7n - 8$ .

La proposition est vraie.

## Exercice 9

### Exercice 9.1

Preuve par récurrence. Vrai pour  $n = 0$  ( $2^3 + 3^1 = 11$ ). Supposons vrai pour  $n$ ,  $2^{6n+3} + 3^{2n+1} = 11k$  est-ce que  $2^{6(n+1)+3} + 3^{2(n+1)+1} = 11k'$

$$2^{6(n+1)+3} + 3^{2(n+1)+1} = 2^{(6n+3)+6} + 3^{2n+1+2} = 2^6 \cdot 2^{6n+3} + 3^2 \cdot 3^{2n+1}$$

On a  $2^{6n+3} = 11k - 3^{2n+1}$  (hypothèse)

$$2^6 \cdot (11k - 3^{2n+1}) + 3^2 \cdot 3^{2n+1} = 2^6 \cdot 11k - 2^6 \cdot 3^{2n+1} + 3^2 \cdot 3^{2n+1} = 11(2^6 k + 5 \cdot 3^{2n+1})$$

Donc vrai en prenant  $k' = 2^6 k + 5 \cdot 3^{2n+1}$ .

## Exercice 10

- On a  $p^2 - 1 = (p+1)(p-1)$
- $p$  est premier donc il est impair ( $p = 2^n + 1$ ). On a  $(p+1)(p-1) = (2^n + 2)(2^n)$ . Soit  $2|(p+1)$ , soit  $4|(p-1)$ . Donc  $p^2 - 1 = 2k \cdot 4k' = 8(kk')$ .
- $p$  est premier donc  $p \bmod 3 = 1$  ou  $p \bmod 3 = 2$ . Si  $p \bmod 3 = 1$  alors  $(p+1)(p-1) = (p+1) \cdot 3k = 3((p+1)k)$ , et Si  $p \bmod 3 = 2$  alors  $(p+1)(p-1) = 3k \cdot (p-1) = 3(k(p-1))$  donc  $p^2 - 1 = 3k'$

3 et 8 sont premiers entre eux, et  $p$  est premier donc  $p^2 - 1 = 3 * 8 * k = 24k$ .

QED