

Rappel de cours

Definition 1. Un *groupe* $(G, *)$ est un ensemble G auquel est associé une opération $*$ (la *loi de composition*) vérifiant les 4 propriétés suivantes:

- $\forall x, y \in G, x * y \in G$. $*$ est une loi de composition interne.
- $\forall x, y, z \in G, (x * y) * z = x * (y * z)$ la loi est *associative*
- $\exists e \in G, \forall x \in G, x * e = e * x = x$. e est l'élément neutre
- $\forall x \in G, \exists x' \in G, x * x' = e$. x' est l'inverse de x et est noté x^{-1} .

Exercice 1

Pour que \mathbb{R} , muni de la multiplication soit un groupe, il faut qu'il vérifie les 4 propriétés d'un groupe. La multiplication est une loi de composition interne pour \mathbb{R} . La multiplication est associative dans \mathbb{R} . 1 est l'élément neutre pour la multiplication dans \mathbb{R} . Vérifions si tout les éléments de \mathbb{R} ont un inverse dans \mathbb{R} . 0, n'a pas d'inverse dans \mathbb{R} , donc $(\mathbb{R}, *)$ n'est pas un groupe.

Exercice 2

On a $G = \{a, b, e\}$, $(G, .)$ est un groupe et e l'élément neutre du groupe $(G, .)$. Donc $\forall x \in G, \exists x' \in G, x.x' = e$ et $\forall x, y \in G, x.y \in G = \{a, b, e\}$.

Donc $a.b \in a, b, e$. Plusieurs cas possibles:

- b est l'inverse de a dans le groupe. Donc, $a.b = e$
- b n'est pas l'inverse de a dans le groupe. donc $a.b \in a, b$. Soit $a.b = a$, as possible car $a.e = a$ et $b \neq e$, ou $a.b = b$ pas possible car $(a.b).b \neq a.(b.b)$.

Donc $a.b = e$

Exercice 3

Non. a et b premiers entre eux donc $\gcd(a, b) = 1$ et b et c premiers entre eux donc $\gcd(b, c) = 1$. Prenons, $a = 3, b = 5, c = 9$, on a $\gcd(3, 5) = 1$ et $\gcd(5, 9) = 1$ mais $\gcd(3, 9) = 3$. Donc a et c ne sont pas premiers entre eux.

Exercice 4

Preuve par récurrence. Supposons que $7|3^{2n+1} + 2^{n+2}$, montrons que $7|3^{2(n+1)+1} + 2^{(n+1)+2}$.

$$3^{2n+1} + 2^{n+2} = 3.3^{2n} + 4.2^n = 3.9^n + 4.2^n$$

calculons

$$3.9^n + 4.2^n[7] = 3.2^n + 4.2^n[7] = 2^n(3 + 4)[7] = 7.2^n[7] = 0$$

donc $7|3^{2n+1} + 2^{n+2}$.

Exercice 5

Exercice 5.1

$p^2 - 1 = (p + 1)(p - 1)$, comme p est un nombre premier supérieur à 5, p est impair. Donc $p^2 - 1 = (2k + 1 - 1)(2k + 1 + 1) = 2k(2k + 2) = 4k(k + 1)$.

Exercice 5.2

$8|p^2 - 1$ si $\exists n, p^2 - 1 = 8n$.

- k est pair donc $k = 2k'$ et $4k(k + 1) = 8k'(2k' + 1)$ donc $n = k'(2k' + 1)$
- k est impair donc $k = 2k' + 1$ et $4k(k + 1) = 4(2k' + 1)(2k' + 1 + 1) = 4(2k' + 1)(2k' + 2) = 8(2k' + 1)(k' + 1)$ donc $n = (2k' + 1)(k' + 1)$.

n existe, donc $8|p^2 - 1$.

$16|p^4 - 1$ si $\exists n, p^4 - 1 = 16n$. $p^4 - 1 = (p^2 - 1)(p^2 + 1)$ et $8|p^2 - 1$ mais p est impair donc p^2 est impair et $p^2 + 1$ est pair. Par conséquent $2|p^2 + 1$. Par conséquent, $(p^2 - 1)(p^2 + 1) = 8n.2n' = 16nn'$ donc $16|p^4 - 1$.

Exercice 5.3

$3|p^2 - 1$ si $\exists n, p^2 - 1 = 3n$. Chaque entier n peut s'écrire $3k$, $3k + 1$ ou $3k + 2$. Comme p est un nombre premier il ne peut pas être égal à $3n$. Donc il reste 2 cas:

- $p = 3n + 1$, donc $p^2 - 1 = (3n + 1)^2 - 1 = 9n^2 + 6n + 1 - 1 = 3(3n^2 + 2n)$
- $p = 3n + 2$, donc $p^2 - 1 = (3n + 2)^2 - 1 = 9n^2 + 12n + 4 - 1 = 3(3n^2 + 6n + 1)$

Donc $3|p^2 - 1$ pour tout nombre premier p .

Exercice 5.4

$5|p^2 - 1$ si $\exists n, p^2 - 1 = 5n$. $p^4 - 1 = (p^2 - 1)(p^2 + 1)$ Chaque entier n peut s'écrire $5k$, $5k + 1$, $5k + 2$, $5k + 3$ ou $5k + 4$. Comme p est un nombre premier il ne peut pas être égal à $5n$. Donc il reste 4 cas:

- $p = 5n + 1$, donc $p^4 - 1 = ((5n + 1)^2 - 1)((5n + 1)^2 + 1) = (25n^2 + 10n + 1 - 1)((5n + 1)^2 - 1) = 5(n^2 + 2n)((5n + 1)^2 - 1)$
- $p = 5n + 2$, donc $p^4 - 1 = ((5n + 2)^2 - 1)((5n + 2)^2 + 1) = ((5n + 2)^2 - 1)(25n^2 + 10n + 4 + 1) = 5((5n + 2)^2 - 1)(5n^2 + 2n + 1)$
- $p = 5n + 3$, donc $p^4 - 1 = ((5n + 3)^2 - 1)((5n + 3)^2 + 1) = ((5n + 2)^2 - 1)(25n^2 + 30n + 9 + 1) = 5((5n + 2)^2 - 1)(5n^2 + 6n + 2)$
- $p = 5n + 4$, donc $p^4 - 1 = ((5n + 4)^2 - 1)((5n + 4)^2 + 1) = (25n^2 + 40n + 16 - 1)((5n + 2)^2 + 1) = 5(5n^2 + 8n + 3)((5n + 2)^2 - 1)$

Donc $5|p^4 - 1$ pour tout nombre premier p .

Exercice 5.5

$a|c$ donc $c = k_1a$ et $b|c$ donc $c = k_2b$. il faut montrer que $ab|c$ ou $c = kab$. En partant de l'identité de Bezout on a $\gcd(a, b) = ax + by$ donc $ax + by = 1$, en multipliant par c on a $cax + cby = c$, cela fait $k_2bax + k_1aby = c$ et $ab(k_2x + k_1y) = c$. Donc $ab|c$.

Exercice 5.6

On a $16|p^4 - 1$ et $5|p^4 - 1$, et $\gcd(16, 5) = 1$ donc d'après la question 5 on a $80|p^4 - 1$.

On a $p^4 - 1 = (p^2 - 1)(p^2 + 1)$ et $3|p^2 - 1$ donc $p^2 - 1 = 3n$ et $p^4 - 1 = 3n(p^2 + 1)$ donc $3|p^4 - 1$, $\gcd(3, 80) = 1$ donc d'après la question 5, on a $240|p^4 - 1$.

Exercice 6

Exercice 6.1

Non, car $N = 2u_1u_2u_3 \dots u_n - 1$ avec $\gcd(2, u_1, u_2, \dots, u_n) = 1$ (car tous u_n premiers et $u_1 = 3$). Prenons un u_i , on a $N = u_i(2u_1u_2u_3 \dots u_n) - 1$ avec $2u_1u_2u_3 \dots u_n$ non divisible par u_i . donc le reste de la division $\frac{N}{u_i} = u_i - 1$ qui est différent de 0.

Exercice 6.2

Exercice 7

Exercice 7.1

$$\gcd(171, 160), 171 = 160 * 1 + 11$$

$$\gcd(11, 160), 160 = 11 * 14 + 6$$

$$\gcd(11, 6), 11 = 6 * 1 + 5$$

$$\gcd(5, 6), 6 = 5 * 1 + 1$$

$$\gcd(5, 1), 5 = 1 * 5 + 0$$

$$\gcd(0, 1) = 1$$

Exercice 7.2

On a $\gcd(171, 160) = 1$, donc $\exists x, y, 171x + 160y = 1$.

$$1 = 6 - 1 * 5 = 6 - (11 - 6 * 1) = 2 * 6 - 11 = 2 * (160 - 11 * 14) - 11 = 2 * 160 - 29 * 11 = 2 * 160 - 29 * (171 - 160) = 31 * 160 - 29 * 171$$

Identité de Bezout: $31 * 160 - 29 * 171 = 1$.

Exercice 7.3

QED