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 véfifie 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 él'éments 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 lélément 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 récurence. Suppusons que $7 | 3^{2n+1} + 2^{n+2}$, montrons que $7 | 3^{2(n+1)+1} + 2^{(n+1)+2}$.

$$3^{2n+1} + 2^{n+2} = 3.3^{2n} + 42^n = 3.9^n + 4.2^n$$

cqlculons

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

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

QED