Corrigé de l'examen du Module Algèbre 1

Problème 1. Soient $f : E \to F$ une application. A et B deux parties de E.

1. Montrer que $f(A \cup B) = f(A) \cup f(B)$.

2. Montrer que $f(A \cap B) \subset f(A) \cap f(B)$.

3. Donner un exemple d'une application $f : \mathbb{R} \to \mathbb{R}$ et de deux parties A et B de $\mathbb{R}$ telles que $f(A) \cap f(B) \neq f(A \cap B)$.

4. Montrer que

$$f \text{ est injective } \iff \forall A, B \subset E, \text{ on a } \ f(A) \cap f(B) \subset f(A \cap B)$$

Solution du Problème 1.

1. Montrons que $f(A) \cup f(B) \subset f(A \cup B)$ et $f(A \cup B) \subset f(A) \cup f(B)$.
On a $A \subset A \cup B$, donc $f(A) \subset f(A \cup B)$, de même $B \subset A \cup B$, donc $f(B) \subset f(A \cup B)$.
D'où $f(A) \cup f(B) \subset f(A \cup B)$.
Réciproquement, soit $y \in f(A \cup B)$, il existe $x \in A \cup B$, tel que $y = f(x)$.
Si $x \in A$, alors $y \in f(A) \subset f(A \cup B)$.
Si $x \in B$, alors $y \in f(B) \subset f(A \cup B)$.
Dans tous les cas, $y \in f(A \cup B)$. D'où $f(A \cup B) \subset f(A) \cup f(B)$.

2. Puisque $A \cap B \subset A$. On a $f(A \cap B) \subset f(A)$. De même $A \cap B \subset B$, donc $f(A \cap B) \subset f(B)$.
Par conséquent $f(A \cap B) \subset f(A) \cap f(B)$.

3.. Prenons $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$ et $A = \{0, -1\}$, $B = \{0, 1\}$. On a $f(A) = f(B) = \{0, 1\}$ et $f(A \cap B) = f(\{0\}) = \{0\}$ alors que $f(A) \cap f(B) = \{0, 1\}$.

4.
$\Rightarrow$ Supposons que f est injective. Montrons que $\forall A, B \subset E$, on a $f(A) \cap f(B) \subset f(A \cap B)$.
Soit $y \in f(A) \cap f(B)$, alors $y \in f(A)$ et $y \in f(B)$. Par suite, il existe $x \in A : y = f(x)$ et il existe $x' \in B : y = f(x')$. Comme f est injective, on a $x = x'$. Donc $x \in A \cap B$. D'où $y = f(x) \in f(A \cap B)$.
$\Leftarrow$ Supposons que $\forall A, B \subset E$, on a $f(A) \cap f(B) \subset f(A \cap B)$. Montrons que f est injective. Soient $x, x' \in E$ tels que $f(x) = f(x') = y$. Posons $A = \{x\}$ et $B = \{x'\}$. On a $f(A) \cap f(B) = \{y\}$. Par hypothèse $f(A) \cap f(B) \subset f(A \cap B)$. Donc $y \in f(A \cap B)$. Par conséquent $A \cap B \neq \varnothing$. D'où $x = x'$. f est injective.

Problème 2. Dans tout ce problème, p désigne un nombre premier $\neq 2$ et α un élément primitif modulo p. On rappelle que $\forall k \in \mathbb{N}$, on a :

$$\alpha^k \equiv 1 \text{ modulo } p \iff p-1 \mid k$$

En particulier on a $\alpha^{p-1} \equiv 1$ modulo p.

1. Montrer que ou bien $4 \mid p-1$ ou bien $4 \mid p-3$.
2. Montrer que $\alpha^{\frac{p-1}{2}} \equiv -1$ modulo p.
3. On suppose que $4 \mid p-1$ et on pose $\beta = \alpha^{\frac{p-1}{4}}$. Montrer que $\beta^2 \equiv -1$ modulo p.
4. Réciproquement, on suppose qu'il existe un entier β tel que $\beta^2 \equiv -1$, modulo p. Montrer que $4 \mid p-1$.
5. On suppose que $8 \mid p-1$. On pose $u = \alpha^{\frac{p-1}{8}}$ et $v = \alpha^{7(\frac{p-1}{8})}$. Montrer que $(u+v)^2 \equiv 2$ modulo p.
6. Dans cette question, on suppose que $4 \mid p-3$.

6.1. Montrer que $\forall x, y \in \mathbb{Z}$ on a :

$$p \mid x^2 + y^2 \Longleftrightarrow p \mid x \text{ et } p \mid y$$

6.2. Montrer qu'il n'existe pas de nombres entiers x, y tels que $x^2 + y^2 = p$.

Solution du Problème 2.

1. Posons $p = 4k + r$, avec $r \in \{0, 1, 2, 3\}$. Les cas $r = 0$ ou $r = 2$ sont impossibles car cela implique $2 \mid p$, en contradiction avec p premier et $p \neq 2$. Donc on a $r = 1$ ou $r = 3$.
2. Posons $z = \alpha^{\frac{p-1}{2}}$. On a $z^2 = \alpha^{p-1} \equiv 1$. Donc $z^2 - 1 = (z-1)(z+1) \equiv 0$ modulo p. Comme p est un nombre premier, on a $z - 1 \equiv 0$, ou $z + 1 \equiv 0$. Si $z - 1 \equiv 0$ alors $z \equiv 1$. Donc $\alpha^{\frac{p-1}{2}} \equiv 1$ ce qui implique $p - 1 \mid \frac{p-1}{2}$ ce qui est impossible. Donc $z \equiv -1$.
3. Soit $\beta = \alpha^{\frac{p-1}{4}}$. $\beta^2 = \alpha^{\frac{p-1}{2}} \equiv -1$.
4. Soit $\beta^2 \equiv -1$, Posons $\beta = \alpha^k$. On a $(\alpha^k)^2 \equiv -1 \equiv \alpha^{\frac{p-1}{2}}$. On a alors $\alpha^{2k-\frac{p-1}{2}} \equiv 1$. Donc $p - 1 \mid 2k - \frac{p-1}{2}$. Il existe alors $m \in \mathbb{Z}$ tel que $m(p-1) = 2k - \frac{p-1}{2}$. D'où $2m(p-1) = 4k - (p-1)$. Donc $(2m+1)(p-1) = 4k$. Finalement $4 \mid p-1$.
5. $(u+v)^2 = u^2 + v^2 + 2uv$. $uv = \alpha^{\frac{p-1}{8}}.\alpha^{7(\frac{p-1}{8})} = \alpha^{p-1} = 1$. Donc $2uv \equiv 2$
Par ailleurs, $u^2(u^2+v^2) \equiv u^4 + 1 \equiv \alpha^{\frac{p-1}{2}} + 1 \equiv -1 + 1 \equiv 0$. Comme u est inversible modulo p, on a $u^2 + v^2 \equiv 0$. Par suite $(u+v)^2 \equiv 2$.
6. On suppose que $4 \mid p-3$.

6.1.
$\Leftarrow$ Si $p \mid x$ et $p \mid y$, $x = kp$ et $y = mp$. On a alors $x^2 + y^2 = p^2(k^2 + m^2)$. D'où $p \mid x^2 + y^2$.
$\Rightarrow$ Soient $x, y \in \mathbb{Z}$ tels que $p \mid x^2 + y^2$. Supposons que $p \nmid x$ ou $p \nmid y$. On peut supposer que $p \nmid y$. Alors y est inversible modulo p. Soit u un inverse de y modulo p. On a alors $u^2(x^2 + y^2) = (ux)^2 + 1 \equiv 0$. Alors $(ux)^2 \equiv -1$ modulo p. Ce qui entraîne d'après la question **4** que $4 \mid p-1$. Contradiction car $4 \mid p-3$.

6.2. Supposons qu'il existe deux nombres entiers x, y tels que $x^2 + y^2 = p$. En réduisant modulo p. On a $x^2 + y^2 \equiv 0$. D'après 6.1, on a $p \mid x$ et $p \mid y$. Posons alors $x = kp$ et $y = mp$. Alors $x^2 + y^2 = k^2p^2 + m^2p^2 = p$. Donc $k^2p + m^2p = p(k^2 + m^2) = 1$. Contradiction. Donc $\forall x, y \in \mathbb{Z}$, $x^2 + y^2 \neq p$.