

Feuille de TD N°1
Autour de l'équation de Fermat

Exercice 1. Pour démontrer le théorème de Fermat, il suffit de montrer que

$$x^n + y^n = z^n \Rightarrow xyz = 0$$

pour $n = 4$ ainsi que pour tous les nombres premiers impairs. Justifier cette assertion.

Exercice 2. Soit K un corps, p sa caractéristique et \overline{K} une clôture algébrique de K .

- (1) Si G est un groupe abélien non cyclique d'ordre n , montrer qu'il existe un diviseur strict d de n tel que $g^d = 1$ pour tout élément g de G .
- (2) Soit $P(X) = X^n - 1 \in K[X]$; à quelle condition sur n le polynôme P admet-il n racines distinctes dans \overline{K} ? Justifier à l'aide de la question précédente que l'ensemble de ses racines forme alors un groupe cyclique d'ordre n (autrement dit, \overline{K} contient «les» racines n -ièmes de l'unité).
- (3) Soit $n \geq 3$ un entier qui n'est pas multiple de p . On désire montrer que toutes les solutions dans $K[t]$ de l'équation de Fermat sont en fait des solutions dans K .
 - Pourquoi suffit-il de montrer le résultat pour $\overline{K}[t]$?
 - Généraliser la démonstration du cours au cas de $\overline{K}[t]$.

Exercice 3. (1) Démontrer que $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel.

- (2) Montrer que $A = \mathbb{C}[X, Y]/(Y^2 - X^3)$ est intègre et que l'image \overline{Y} de Y est irréductible dans A . Justifier que $A/(\overline{Y}) \simeq \mathbb{C}[X]/(X^3)$; en déduire que \overline{Y} n'est pas premier. Qu'en concluez-vous?

Exercice 4. Factoriser en irréductibles $7 + i$ dans $\mathbb{Z}[i]$ et $5 + j$ dans $\mathbb{Z}[j]$.

Exercice 5. (1) Soit p un nombre premier impair; il s'agit de montrer que

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{si } p \equiv \pm 1 \pmod{8}; \\ -1 & \text{si } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Pour cela, on choisit une clôture algébrique $\overline{\mathbb{F}}_p$ de \mathbb{F}_p , un élément u de $\overline{\mathbb{F}}_p$ tel que $u^4 = -1$ et note $z = u + u^{-1}$. Vérifier que $z^2 = 2$. En déduire que $\left(\frac{2}{p}\right) = +1$ si et seulement si $z \in \mathbb{F}_p$, donc si et seulement si $z^p = z$. Conclure en discutant selon la congruence vérifiée par p .

- (2) Poursuivant avec les notations précédentes, on se donne maintenant un nombre premier q impair différent de p . Il s'agit de démontrer que

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \quad (\text{loi de réciprocité quadratique}).$$

Pour cela, on se donne $1 \neq \omega \in \overline{\mathbb{F}}_p$ une racine q -ième de l'unité et considère la «somme de Gauss» $S = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x \in \overline{\mathbb{F}}_p$ (pourquoi ω^x a-t-il bien un sens?)

- Démontrer que $S^2 = \sum_{(x,z) \in \mathbb{F}_q^2} \left(\frac{x(z-x)}{q}\right) \omega^z$; calculer $\sum_{x \in \mathbb{F}_q^\times} \left(\frac{x(z-x)}{q}\right)$ en remarquant que $\sum_{u \in \mathbb{F}_q^\times} \left(\frac{u}{q}\right) = 0$. En déduire que $S^2 = (-1)^{\frac{q-1}{2}} \bar{q} \in \mathbb{F}_p \subset \overline{\mathbb{F}}_p$.
- Calculer S^p . En déduire que $S^{p-1} = \left(\frac{\bar{p}}{q}\right) \in \mathbb{F}_p \subset \overline{\mathbb{F}}_p$.
- On rappelle que $\left(\frac{\bar{q}}{p}\right) = \bar{q}^{\frac{p-1}{2}}$. Démontrer la loi de réciprocité quadratique.

Exercice 6. Fermat a découvert le résultat suivant :

Proposition 1. *Si p est un nombre premier vérifiant $p \equiv \pm 1 \pmod{8}$, alors il existe deux entiers naturels x et y tels que*

$$p = x^2 - 2y^2.$$

Réciproquement, si $p \equiv \pm 3 \pmod{8}$, alors cette équation n'admet pas de solution en entiers.

On se propose de démontrer ce résultat en travaillant dans l'anneau $A = \mathbb{Z}[\sqrt{2}]$. Etant donné $\alpha = x + y\sqrt{2} \in A$, on note $\bar{\alpha} = x - y\sqrt{2}$ son conjugué, $N(\alpha) = \alpha\bar{\alpha}$ la norme et $\phi : \alpha \in A^\times \rightarrow |N(\alpha)|$ le stathme pour lequel A est euclidien. On rappelle également que $A^\times = \{\alpha, N(\alpha) = \pm 1\} = \{\pm(1 + \sqrt{2})^k, k \in \mathbb{Z}\}$ (déterminé en utilisant la méthode de descente de Fermat). On s'inspirera de la preuve donnée en cours pour l'équation $p = x^2 + y^2$, où l'on a travaillé dans l'anneau des entiers de Gauss $\mathbb{Z}[i]$, et montrera :

- On a l'alternative suivante : soit p reste irréductible dans $\mathbb{Z}[\sqrt{2}]$, soit $p = \alpha\bar{\alpha}$, où $\alpha \in \mathbb{Z}[\sqrt{2}]$ est irréductible.
- Si $\left(\frac{2}{p}\right) = +1$ alors p n'est pas premier dans $\mathbb{Z}[\sqrt{2}]$.
- S'il existe une solution en entiers de $p = x^2 - 2y^2$, alors $\left(\frac{2}{p}\right) = +1$.

Exercice 7 (cf. session d'examen de septembre 2004). Fermat a découvert le résultat suivant :

Proposition 2. *Soit p un nombre premier arbitraire. Il existe deux entiers naturels x et y tels que*

$$p = x^2 + 3y^2$$

si et seulement si $p \equiv 1 \pmod{3}$ ou $p = 3$.

On se propose de démontrer ce résultat. Pour cela, on introduit les anneaux $A = \mathbb{Z}[i\sqrt{3}]$ et $B = \mathbb{Z}[j]$, où $i^2 = -1$ et $j = \frac{-1+i\sqrt{3}}{2}$. Etant donné un élément $\alpha = x + iy\sqrt{3}$ de A ou de B , on note $\bar{\alpha} = x - iy\sqrt{3}$ son conjugué et $N(\alpha) = \alpha\bar{\alpha}$ sa norme.

(1) Préliminaires :

- Montrer que $B = \left\{ \frac{m+in\sqrt{3}}{2} \mid m \text{ et } n \text{ sont des entiers relatifs de même parité} \right\}$.
- Déterminer les ensembles A^\times et B^\times .
- Montrer que tout élément β de B s'écrit $\beta = u\alpha$, où $\alpha \in A$ et $u \in B^\times$.
- Montrer que l'anneau A n'est pas factoriel (on pourra exhiber deux décompositions de l'entier 4 en produit d'irréductibles).
- Démontrer que l'anneau B est euclidien.

- (f) Soit p un nombre premier impair différent de 3. Notant $\left(\frac{a}{p}\right)$ le symbole de Legendre, montrer que $\left(\frac{-3}{p}\right) = +1$ si et seulement si $p \equiv 1 \pmod{3}$. On utilisera la loi de réciprocité quadratique.
- (2) Démonstration de l'énoncé de Fermat :
- (a) Traiter les cas $p = 2$ et $p = 3$.
On suppose désormais que p est un nombre premier impair différent de 3.
- (b) Démontrer l'alternative suivante : soit p reste irréductible dans B , soit il s'écrit $p = \beta\bar{\beta}$, pour β un élément irréductible de B .
- (c) Montrer que si $\left(\frac{-3}{p}\right) = +1$ (autrement dit, si -3 est un carré modulo p) alors p n'est pas premier dans B .
- (d) En déduire que p s'écrit sous la forme $p = \alpha\bar{\alpha}$, où $\alpha \in A$.
- (e) On suppose maintenant qu'il existe deux entiers naturels x et y tels que $p = x^2 + 3y^2$. Montrer que $\left(\frac{-3}{p}\right) = +1$.
- (f) Démontrer la proposition de Fermat.