Examen du 18 février 2021

1 heure 30

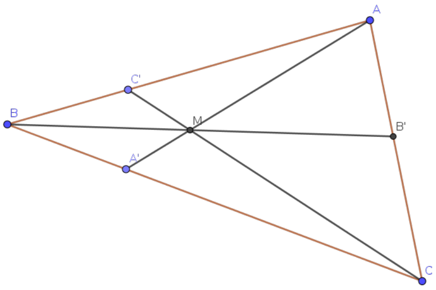
La correction tiendra grandement compte de la clarté et de la concision de la rédaction.
L'utilisation de calculatrice, de téléphone portable et autre gadget est interdite.

Exercice 1. — Les questions de cet exercice sont indépendantes entre elles.

1) Énoncer sans démonstration le critère d'Eisenstein.
Le polynôme $P := X^2Y^7 + X^5 - 1$ est-il irréductible dans $\mathbf{Z}[X,Y]$?

2) Soit $P \in \mathbf{C}[X,Y]$ un polynôme *non constant.*
Montrer que $\{(x,y) \in \mathbf{C}^2,\ P(x,y) = 0\}$ est infini.
Donner un exemple de P tel que $\{(x,y) \in \mathbf{R}^2,\ P(x,y) = 0\}$ est fini.

3) **Théorème de Gergonne** : soient ABC un triangle non aplati, et A' , B' , C' trois points appartenant respectivement aux droites (BC), (CA) et (AB). On suppose que les droites (AA'), (BB') et (CC') sont concourantes en un point M.



Montrer que les mesures algébriques vérifient :

$$\frac{\overline{A'M}}{\overline{A'A}} + \frac{\overline{B'M}}{\overline{B'B}} + \frac{\overline{C'M}}{\overline{C'C}} = 1$$

[**Indication:** Soient (α,β,γ) les coordonnées barycentriques normalisées de M dans le repère (A,B,C). Montrer que $\beta+\gamma \neq 0$. Identifier le barycentre $\mathrm{Bar}[(B,\beta),(C,\gamma)]$.]

* *
*

Exercice 2. — **1)** Soient $\mathbf{K} \subset \mathbf{L}$ une extension de corps, et $x, y \in \mathbf{L}$ des éléments algébriques. Montrer que l'on a $[\mathbf{K}(x,y) : \mathbf{K}(x)] \leqslant [\mathbf{K}(y) : \mathbf{K}]$.
[**Indication:** Montrer qu'une $\mathbf{K}$-base de $\mathbf{K}(y)$ engendre $\mathbf{K}(x,y)$ comme $\mathbf{K}(x)$-espace vectoriel.]

Pour tout entier $k \geqslant 1$, on note $\zeta_k := e^{\frac{2i\pi}{k}} \in \mathbf{C}$.
Dans toute la suite, on fixe deux entiers n et m premiers entre eux. Le but de cet exercice est de montrer qu'on a $\mathbf{Q}[\zeta_n] \cap \mathbf{Q}[\zeta_m] = \mathbf{Q}$. Pour cela, on pose $\mathbf{K} := \mathbf{Q}[\zeta_n] \cap \mathbf{Q}[\zeta_m]$.

2) Montrer qu'on a $\mathbf{K}(\zeta_m) = \mathbf{Q}(\zeta_m), \mathbf{K}(\zeta_n) = \mathbf{Q}(\zeta_n)$ et $\mathbf{K}(\zeta_{mn}) = \mathbf{Q}(\zeta_{mn})$.

3) Montrer que l'on a $\mathbf{K}(\zeta_m, \zeta_n) = \mathbf{K}(\zeta_{mn})$.

4) Montrer que $[\mathbf{Q}(\zeta_{mn}) : \mathbf{Q}(\zeta_m)] = \varphi(n)$.

5) En utilisant **1)**, en déduire que $[\mathbf{Q}(\zeta_n) : \mathbf{K}] \geqslant \varphi(n)$ et conclure.

* *
*

Exercice 3. — Soient $n \geqslant 1$, $p \in \mathcal{P}$ un nombre premier, $q := p^n$ et $\mathbf{F}_q$ un corps fini à q éléments. On note $\mathbf{F}_p$ le sous corps premier de $\mathbf{F}_q$ (il est donc isomorphe à $\mathbf{Z}/p\mathbf{Z}$).

1) Montrer que $\varphi : \mathbf{F}_q \to \mathbf{F}_q$, $x \mapsto x^p$ est un automorphisme de corps et qu'il est d'ordre n.

2) Pour tout $a \in \mathbf{F}_q$, on note $K_a := \mathbf{F}_p[a]$ et on note d_a le degré de l'extension $[K_a : \mathbf{F}_p]$.
Montrer que d_a est égal à l'ordre de $\varphi_{|K_a}$ (la restriction de φ à K_a).
En déduire que $d_a = \mathrm{Inf}\{d \geqslant 1,\ a^{p^d} = a\}$.

3) On suppose désormais $a \neq 0$. Soit N_a l'ordre de a dans le groupe $\mathbf{F}_q^\times$.
Montrer que N_a est premier avec p, puis que d_a est l'ordre de $\overline{p}$ dans le groupe $(\mathbf{Z}/N_a\mathbf{Z})^\times$.