Colle du 11 janvier 2012 (MPSI3)

Coniques

Exercice Soit $\mathscr{C}$ une conique non vide, et M un point de cette conique. Montrer d'abord qu'il existe une bijection entre $\mathscr{C}$ et les droites du plan euclidien passant par l'origine, puis qu'il existe une paramétrisation rationnelle de $\mathscr{C} \setminus \{M\}$. Montrer que si les coefficients de la conique sont rationnels, et que la conique a un point à coordonnées rationnelles, alors elle en a une infinité.

Exercice Soit R le repère orthonormé traditionnel, et $\mathscr{C}$ une conique d'équation $x^2 - dy^2 = 1$ dans ce repère, où d est un entier naturel supérieur à 2. De quel type est la conique $\mathscr{C}$? Si M et N sont deux points de la conique qui ont pour coordonnées (x, y) et (x', y') dans R, montrer que $M(x, y)_R + N(x', y')_R = (M + N)(xx' + dyy', xy' + x'y)_R$ définit une loi de groupe commutatif sur la conique. Et si M et N sont à coordonnées (x, y) et (x', y') dans le repère porté par les asymptotes, que dire des coordonnées de $M + N$? En déduire un isomorphisme de groupes entre $(\mathbb{R}^*, \times)$ et $(\mathcal{C}, +)$.

Si M et N sont deux points de la conique, soit R le point d'intersection autre que $(1, 0)$ entre la conique la droite passant par $(1, 0)$ et parallèle à (MN). Montrer que $R = M + N$.

Exercice Montrer que par cinq points du plan, il passe au moins une conique.

Exercice Montrer que six points A, B, C, A', B', C', dont trois ne sont jamais alignés, sont sur une même conique si et seulement si les intersections P de (AB') et (BA'), N, de (AC') et (CA') et M de (BC') et (CB') sont trois points alignés. Montrer comment construire géométriquement cette conique.

Exercice Donner une condition nécessaire et suffisante pour qu'une hyperbole soit équilatère.

Exercice Soit C l'enveloppe convexe de n points s_1, …, s_n. Montrer que si $\mathcal{E}$ est un disque elliptique inclus dans C et contenant s_1, alors $\mathcal{E}$ est dégénérée (c'est-à-dire réduite à un segment).

Applications

Exercice Montrer qu'une sphère privée d'un point est en bijection avec le plan euclidien.

Exercice Soit $\phi : \begin{cases} \mathbb{Z} \times \mathbb{N}^* & \to & \mathbb{Q} \\ (p, q) & \mapsto & p + \frac{1}{q} \end{cases}$. Est-ce que ϕ est injective ? Surjective ? Bijective ?

Exercice Montrer que s'il existe une injection de $[\![1, n]\!]$ dans $[\![1, m]\!]$, alors $n \leq m$.

Exercice Soit $f : E \to F$ une application. Montrer que $x \sim y \Leftrightarrow f(x) = f(y)$ est une relation d'équivalence, et que l'application $\tilde{f} : \begin{cases} E/\sim & \to & F \\ \mathfrak{cl}_\sim(x) & \mapsto & f(x) \end{cases}$ est bien définie, et est injective, et que $\tilde{f}(E) = f(E)$. Calculer $\mathbb{R}^*/\sim$ si $f : \mathbb{R}^* \to \mathbb{R}^*$ est l'application $x \mapsto x^2$, et en déduire qu'il existe une bijection entre $\mathbb{R}^*/\{\pm 1\}$ et $(\mathbb{R}_+^*)^2$. Trouver un analogue en remplaçant $\mathbb{R}$ par $\mathbb{Q}$.

Exercice Montrer que la relation sur $\mathbb{C}^*$ définie par « $x \sim y \Leftrightarrow x/y$ est un carré » est une relation d'équivalence, et déterminer combien il y a de classes d'équivalence. Même question en remplaçant $\mathbb{C}$ par $\mathbb{R}$, puis $\mathbb{Q}$.

Exercice Montrer que s'il existe une injection de E dans F, alors il existe une surjection de F dans E (et réciproquement).

Exercice Montrer qu'il n'existe pas de surjection de E dans $\mathcal{P}(E)$.

Exercice Montrer qu'il existe une injection de $\mathbb{Z}$ dans $\mathbb{N}$, puis de $\mathbb{Q}$ dans $\mathbb{N}$ (ou une surjection de $\mathbb{N}$ dans $\mathbb{Z}$, puis $\mathbb{Q}$).

Exercice Montrer que s'il existe une surjection de $\mathbb{N}$ dans A et B, alors il existe une surjection de $\mathbb{N}$ dans $A \times B$. En déduire l'existence d'une surjection de $\mathbb{N}$ dans $\mathbb{N}^k$, mais montrer qu'il n'existe pas de surjection de $\mathbb{N}$ dans $\mathbb{N}^{\mathbb{N}}$.

Groupes – Anneaux – Corps

Exercice Soit K un corps. montrer que les groupes $(K, +)$ et $(K^*, \cdot)$ ne sont pas isomorphes.

Exercice Montrer qu'un sous-groupe de $(\mathbb{R}, +)$ est soit de la forme $a\mathbb{Z}$, soit dense.

Exercice Soit p un nombre premier. Montrer qu'un diviseur premier de $2^p - 1$ est strictement plus grand que p.

Exercice Déterminer les automorphismes de $\mathbb{R}$, puis ceux de $\mathbb{C}$ laissant fixe $\mathbb{R}$.

Exercice Soit $f : G \to H$ un morphisme de groupes. On note $xRy \Leftrightarrow f(x) = f(y)$. Montrer que c'est une relation d'équivalence, que l'ensemble des classes de G pour R est un groupe (noté $G/\ker(f)$), et que $\tilde{f} : \begin{cases} G/\ker(f) & \to & H \\ \mathfrak{cl}_R(x) & \mapsto & f(x) \end{cases}$ est une application bien définie, et un morphisme de groupe injectif pour ne rien gâcher. En déduire que $\mathrm{card}(G) = \mathrm{card}(\ker(f))\mathrm{card}(f(G))$.

Exercice Soit K un corps. Montrer que K contient un sous-corps isomorphe soit à $\mathbb{Q}$, soit à $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Exercice Soit A un anneau commutatif, et I un sous-groupe de $(A,+)$ tel que $IA = I$. Montrer que A/I est un anneau, pour les lois $(a+I)+(b+I) = (a+b)+I$ et $(a+I)(b+I) = (ab)+I$. En déduire que si a est un entier et p un nombre premier qui ne divise pas a, alors $a^{p-1} \equiv 1 \mod p$.

Exercice Montrer que $\mathbb{Z}[i]$ est un anneau. Montrer l'existence d'une division euclidienne sur $\mathbb{Z}[i]$. On dit qu'un élément p de $\mathbb{Z}[i]$ est premier s'il est non nul, et si $p = ab$ implique a ou $b \in \{\pm 1, \pm i\}$. Montrer que tout élément de $\mathbb{Z}[i]$ s'écrit de manière unique comme produit de nombres premiers. En déduire que les triplets pythagoriciens sont de la forme $(a^2 - b^2, 2ab, a^2 + b^2)$ (avec a et b deux entiers).

Exercice Montrer que $A = (\mathbb{C}^{\mathbb{N}^*}, +, *)$ est un anneau unitaire commutatif, où $f * g$ est définie par $(f * g)(n) = \sum_{ij=n} f(i)g(j)$. Quel est l'élément neutre e pour $*$? Caractériser les éléments de A^*. Montrer que $\mu * 1 = e$, où μ est la fonction de Möbius ($\mu(p) = -1$ si p est premier, $\mu(p^k) = 0$ si $k \geq 1$, et on étend par multiplicativité), puis $\Lambda * 1 = \ln$ où Λ est la fonction de Van Mangoldt ($\Lambda(p^k) = \ln(p)$, $\Lambda(n) = 0$ sinon).

Exercice Montrer qu'il existe un isomorphisme d'anneaux entre $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ pour m et n premiers entre eux, puis un isomorphisme de groupes entre $(\mathbb{Z}/mn\mathbb{Z})^*$ et $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. Montrer que si m et n ne sont pas premiers entre eux, ces groupes ne sont jamais isomorphes.

Expliciter l'isomorphisme de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/mn\mathbb{Z}$. Déterminer les entiers n tels que $n \equiv 2 \mod 15$ et $m \equiv 4 \mod 17$. On note $\varphi(n)$ l'ensemble des entiers entre 1 et n premiers avec n. Montrer que $\varphi(n) = \mathrm{card}((Z/nZ)^*)$. En déduire que $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont premiers entre eux, et en déduire une formule pour $\varphi(n)$ pour tout n.

Exercice Montrer que $\mathbb{Q}$ n'a pas un nombre fini de générateurs.

Exercice Montrer que l'ensemble des automorphismes d'un corps forme un groupe. Calculer ce groupe dans les cas suivants : $K = \mathbb{Q}$, $K = \mathbb{Q}(i)$, $K = \mathbb{Q}(\sqrt{2})$, et $K = \mathbb{Q}(\zeta_5)$. Montrer que si $K = \mathbb{Q}(a)$ où a est annulé par un polynôme de degré n, alors l'ensemble des automorphismes de K est, au plus, de cardinal $n!$ (et s'injecte en fait dans $\mathfrak{S}_n$).

Exercice Soit G un groupe, X un ensemble (tous deux finis), et $\varphi : G \to \mathrm{Bij}(X)$ un morphisme de groupes. On introduit la relation d'équivalence sur G définie, pour tout x, par $gR_xg' \Leftrightarrow \exists\varphi(g)(x) = \varphi(g')(x) \Leftrightarrow \varphi(gg'^{-1})(x) = x$. Vérifier que c'est une relation d'équivalence, et montrer qu'il y a une bijection entre G/R_x et $G \cdot x = \{\varphi(g)(x); g \in G\}$. En déduire que

$$\mathrm{card}(G) = \mathrm{card}(G \cdot x)\mathrm{card}(\mathrm{Stab}_G(x)).$$

Application : on prend $G = \mathfrak{S}_n$, $X = \mathcal{P}([\![1, n]\!])$, et le morphisme $\varphi : G \to \mathrm{Bij}(X)$ définie par $\varphi(\sigma)(x) = \sigma(x)$. Montrer que φ est un morphisme bien défini, puis calculer le cardinal de G. En déduire C_n^k, puis A_n^k.

Exercice Montrer que le groupe des isométries du polygone à n côtés est un groupe, et déterminer ses éléments.

Exercice Soit G l'ensemble des isométries du plan qui laissent fixe l'origine. Montrer que c'est un groupe. Soit $\varphi : G \to \mathrm{Bij}(X)$ définie par $\varphi(f)(\vec{x}) = f(\vec{x})$. Montrer que φ est un morphisme, puis déterminer (pour $\vec{x}$ non nul) les ensembles $\{f(\vec{x}); f \text{ est une rotation}\}$ et $\{f \in G; f(\vec{x}) = \vec{x})$. En déduire que toute isométrie s'écrit comme produit de rotations et de symétries.

Exercice Montrer que dans un anneau commutatif, la somme d'un élément inversible et d'un élément nilpotent est un élément inversible.