1 Exercices

Exercice 1 :

Soit G un groupe fini de cardinal p premier. Montrer que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Exercice 2 :

Soit G un groupe fini additif (donc commutatif) et A, B deux parties de G.

1. Montrer que si $\text{card}(A)+\text{card}(B) > \text{card}(G)$, alors $A+B = G$. $(A+B = \{x+y \mid (x,y) \in A\times B\})$
   On montrera que, si $x \in G$, $\{x-a \mid a \in A\} \cap B \neq \emptyset$.

2. Soit $H = \{x \in G\ ;\ A = x+A\}$. Montrer que H est un sous-groupe de G. $(x+A = \{x+y \mid y \in A\})$

3. Montrer que $\text{card}(A+B) = \text{card}(A)$ si et seulement si il existe $b \in G$ tel que $B \subset b+H$.

Exercice 3 :

Soit G un groupe n'ayant qu'un nombre fini de sous-groupes.

1. Montrer que tout élément de G est d'ordre fini.

2. En notant que $G = \bigcup_{x\in G} Gr(x)$, montrer que G est fini.

Exercice 4 :

Soit G un groupe fini. On note $Z = \{x \in G \mid \forall y \in G,\ xy = yx\}$ le centre de G, $C = \{(x,y) \in G^2 \mid xy = yx\}$, et, si $x \in G$, $C_x = \{y \in G \mid xy = yx\}$.

1. Vérifier que Z et C_x, $x \in G$, sont des sous-groupes de G.

2. Si $\text{card}(G)/\text{card}(Z)$ est premier, montrer que G est commutatif.

   On suppose désormais G non commutatif.

3. Justifier que $\text{card}(G)/\text{card}(Z) \geq 4$

4. Montrer que $\text{card}(C) = \sum_{x\in G} \text{card}(C_x) \leq \text{card}(G)\text{card}(Z) + (\text{card}(G) - \text{card}(Z))\frac{\text{card}(G)}{4}$ puis que $\text{card}(C) \leq \frac{5}{8}\text{card}(G)^2$.

Exercice 5 :

Soit G un groupe fini de cardinal n. Montrer qu'il existe une partie génératrice de G de cardinal $\leq \log_2(n)$.

Exercice 6 :

Soit G un sous-groupe additif de $\mathbb{Q}$ engendré par un nombre fini d'éléments. Montrer que G est monogène.
Trouver un sous-groupe non trivial de $\mathbb{Q}$ non monogène.

Exercice 7 :

1. Soit G un groupe fini de cardinal pair.
   En associant x à x^{-1}, si $x \in G$, montrer que G possède un élément d'ordre 2.

2. Soit G un groupe fini de cardinal impair $2q+1$. Montrer que $\forall x \in G$, $\exists! y \in G$; $x = y^2$.

Exercice 8 : Sous-groupes de $\mathbb{R}^n$ et critère de densité de Kronecker

$\mathbb{R}^n$ est muni de la norme euclidienne usuelle.

1. Soit G un sous-groupe de $(\mathbb{R}^n, +)$.

   (a) On suppose ici G discret: toute partie de G bornée est finie.
   $V = vect(G)$. On se donne $B = (e_1, ..., e_p)$ une base de V formée d'éléments de G.
   Soit $P = \left\{ \sum_{i=1}^{p} \alpha_i e_i \mid \alpha_p \in [0,1] \text{ et } \forall i \leq p-1, \alpha_i \in [0,1[\right\}$.

   i. Justifier l'existence de $h \in P \cap G$ de dernière coordonnée dans B minimale parmi les éléments de $P \cap G$ de dernière coordonnée strictement positive.
   On se fixe h ainsi. Soit $W = vect(e_1, ..., e_{p-1})$.

   ii. Si $g \in G$, montrer qu'il existe $k \in \mathbb{Z}$ tel que $g - kh \in W$. En déduire $G = (G \cap W) + \mathbb{Z}h$.

   iii. Montrer qu'il existe $h_1, ..., h_p \in \mathbb{R}^n$ linéairement indépendants tels que $G = \mathbb{Z}h_1 + ... + \mathbb{Z}h_p$.

   (b) On suppose ici G non discret: il existe une partie de G bornée et infinie.

   i. Montrer que pour tout $r > 0$, $G \cap \overline{B(0,r)}$ est infini.
   On note $V_r = vect(G \cap \overline{B(0,r)})$.

   ii. Montrer qu'il existe $r_0 > 0$ tel que $V_{r_0} = \bigcap_{r>0} V_r$, et que $\dim(V_{r_0}) > 0$.

   iii. Montrer que $G \cap V_{r_0}$ est dense dans V_{r_0}.
   Soit S un supplémentaire de V_{r_0} et p la projection sur S parallèlement à V_{r_0}.

   iv. Si $p(G) \neq \{0\}$, ie $G \cap V_{r_0} \neq G$, montrer que $p(G)$ est un sous-groupe discret de $\mathbb{R}^n$, puis qu'il existe $g_1, ..., g_k \in G$ formant une famille libre tels que
   $vect(g_1, ..., g_k) \cap V_{r_0} = \{0\}$, et $G = (G \cap V_{r_0}) + \mathbb{Z}g_1 + ... + \mathbb{Z}g_k$.

2. Critère de densité de Kronecker.
   Soit G un sous-groupe de $\mathbb{R}^n$. Montrer que sont équivalents:

   (a) G est dense dans $\mathbb{R}^n$

   (b) La seule forme linéaire sur $\mathbb{R}^n$ prenant des valeurs entières sur G est la forme nulle.

3. Une application.
   Soient $x_1, ..., x_n \in \mathbb{R}^n$ $\mathbb{Q}$-linéairement indépendants, et $x = (x_1, ..., x_n)$.

   (a) Montrer que $G := \mathbb{R}x + \mathbb{Z}^n$ est dense dans $\mathbb{R}^n$.

   (b) Soient $a_1, ..., a_n, b_1, ..., b_n \in \mathbb{R}$.
   Montrer que $\sup_{t \in \mathbb{R}} \sum_{i=1}^{n} a_i \cos(t x_i + b_i) = \sum_{i=1}^{n} |a_i|$.

Exercice 9 :

Soit G un groupe fini de neutre 1 tel que $\forall x \in G,\ x^2 = 1$.

1. Montrer que G est commutatif

2. Soit $\{x_1, ..., x_n\}$ un système générateur minimal de G.
   Montrer que $\Phi : \begin{cases} (\{0,1\})^n \to G \\ (e_1, ..., e_n) \mapsto x_1^{e_1}...x_n^{e_n} \end{cases}$ est bijective, et que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.

Exercice 10 :

Quels sont les sous-groupes connexes par arc de $\mathbb{C}$, de $\mathbb{C}^*$?

Exercice 11 :

Soit G un sous-groupe de $GL_n(\mathbb{C})$ tel que

$$\forall A \in G, A^2 = I_n$$

1. Montrer que tous les éléments de G sont diagonalisables et que G est commutatif.
   Ainsi (cours : codiagonalisation) il existe une matrice P inversible telle que pour toute matrice A de G, $P^{-1}AP$ soit diagonale.

2. Montrer que G possède un nombre fini d'éléments et que le cardinal de G est de la forme 2^d avec d entier naturel tel que $d \leq n$.

3. Montrer que les groupes $GL_n(\mathbb{C})$ et $GL_m(\mathbb{C})$ ne sont pas isomorphes si $n \neq m$.

Exercice 12 :

1. $SL_n(\mathbb{Z}) = \{M \in \mathcal{M}_n(\mathbb{Z}) \mid \det(M) = 1\}$. Montrer que $SL_n(\mathbb{Z})$ est un sous-groupe de $GL_n(\mathbb{R})$, infini si $n \geq 2$.

2. Soit $A \in SL_2(\mathbb{Z})$ d'ordre fini d. Montrer que d divise 12.

3. Déterminer les cardinaux possibles d'un sous-groupe fini commutatif de $SL_2(\mathbb{Z})$.

Exercice 13 : Théorème de structure des groupes abéliens finis

Soit $(G, .)$ un groupe fini commutatif.
Si $x \in G$, on notera $|x|$ l'ordre de x.

1. Soient $x, y \in G$ tels que $|x| \wedge |y| = 1$. Montrer que $|xy| = |x||y|$.

2. Si $x \in G$, et d divise $|x|$, montrer que $|x^d| = \dfrac{|x|}{d}$.

3. Soit $d = ppcm(\{|x| \mid x \in G\}$ (exposant de G). On note $d = p_1^{\alpha_1}...p_k^{\alpha_k}$ sa décomposition en produit de nombres premiers.
   En utilisant cette décomposition, montrer qu'il existe $x \in G$ d'ordre d.

   On se fixe un tel x. $H := Gr(x)$ est le sous-groupe engendré par x. Il est donc isomorphe à U_d et $\mathbb{Z}/d\mathbb{Z}$.

4. Prolongement des caractères.
   Soient V un sous-groupe strict de G, et $\phi : V \to \mathbb{C}^*$ un morphisme de groupe.
   Soit $y \in G \backslash V$, et $F = Gr(V \cup y)$.
   Comme G est commutatif, tout élément de F s'écrit (de manière non unique) vy^n avec $v \in V$ et $n \in \mathbb{Z}$.

(a) Montrer que $W := \{k \in \mathbb{Z} \mid y^k \in V\}$ est un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$.
Soient r l'unique entier > 0 tel que $W = r\mathbb{Z}$.
Soit θ une racine r-ième de $\phi(y^r)$ (dans $\mathbb{C}$).

(b) Soit $g : \begin{cases} F \to \mathbb{C}^* \\ vy^n \mapsto \phi(v)\theta^n \end{cases}$.
Montrer que g a un sens, est un morphisme de groupes, et coïncide avec ϕ sur V.

(c) Montrer que ϕ se prolonge en un morphisme de G dans $\mathbb{C}^*$.

On se donne f un isomorphisme de H dans U_d. En vertu de la question 4, on peut le prolonger en un morphisme de G dans $\mathbb{C}^*$, que l'on appelle toujours f.

5. Montrer que $Im(f) = U_d$, et que $\begin{cases} \mathcal{K}er(f) \times H \to G \\ (k,h) \mapsto kh \end{cases}$ est un isomorphisme de groupes.

6. Montrer qu'il existe $k \in \mathbb{N}^*$, et $n_1|n_2|...|n_k$ tels que G soit isomorphe à $\mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}$.

7. En considérant des invariants par isomorphisme comme les ordres, le nombre d'éléments d'ordre donné, etc..., montrer que $k \in \mathbb{N}^*$, et $n_1, ..., n_k$ sont uniques.

Exercice 14 : Groupe diédral

On assimile $\mathbb{R}^2$ canoniquement euclidien et $\mathbb{C}$. $n \geq 3$.
Soit P le n-èdre convexe dont les sommets sont les éléments de U_n.
Soit $G = \{f \in \mathcal{L}(\mathbb{R}^2) \mid f(P) = P\}$.

1. Si $f \in G$, montrer que $f \in GL(\mathbb{R}^2)$, puis établir de G est un sous-groupe de $GL(\mathbb{R}^2)$.

2. Si $a \in U_n$, montrer que $f(a) \in U_n$.

3. Si $a, b \in U_d$ sont "voisins", montrer que $f(a)$ et $f(b)$ aussi.

4. Montrer que G est engendré par une rotation et une réflexion, est de cardinal $2n$, et non commutatif.

Exercice 15 : Action de groupe et colliers de Pólya

$|A|$ désigne le cardinal de A.
Soit G un groupe de neutre 1, et E un un ensemble non vide.
Soit $*$, opération de $G \times E$ dans E vérifiant:
$\forall x \in E,\ 1 * x = x$
$\forall x \in E, \forall g_1, g_2 \in G,\ g_1 * (g_2 * x) = (g_1 g_2) * x$
On dit que $*$ est une action de G sur E.
Si $x \in E$, soient $O(x) = \{g * x \mid g \in G\}$ (orbite de x) et $stab(x) = \{g \in G \mid g * x = x\}$ (stabilisateur de x).
Si $g \in G$, soit $N(g) = \{x \in E \mid g * x = x\}$ (normalisateur de g)

1. Vérifier que $stab(x)$ est un sous-groupe de G.

2. Soient $x, y \in E$. Montrer que $O(x) \cap O(y) \neq \emptyset \Longrightarrow O(x) = O(y)$.

On suppose désormais G fini.

3. Montrer que, si $x \in E$, $|O(x)| = \dfrac{|G|}{|stab(x)|}$.
On pourra, si $y \in O(x)$, regarder combien il y a de $g \in G$ tels que $g * x = y$.

On suppose désormais de plus E fini.

4. Soit NO le nombre d'orbites distinctes, et donc disjointes deux à deux par la question 2.
Montrer que
$$NO = \sum_{x\in E} \frac{1}{|O(x)|} = \frac{1}{|G|}\sum_{x\in E} |stab(x)| = \frac{1}{|G|}|\{(g,x)\in G\times E \mid g*x=x\}| = \frac{1}{|G|}\sum_{g\in G}|N(g)|.$$

Une application combinatoire:
$n, q \in \mathbb{N}$, $n, q \geq 2$.
On veut calculer le nombre de colliers que l'on peut fabriquer avec n perles pouvant avoir q couleurs enfilées régulièrement sur un cercle, en considérant comme équivalents deux colliers se déduisant l'un de l'autre par rotation.
On prend $G = \mathbb{Z}/n\mathbb{Z}$, qui va jouer le rôle des point portant les perles.
$E = \mathcal{F}(G, [\![1, q]\!])$ va modéliser l'ensemble des colliers.
Une rotation va être une translation de G.
On définit donc, si $g \in G$, et $f \in E$, $g * f : \begin{cases} G \to [\![1,q]\!] \\ y \mapsto f(y+g) \end{cases}$.

5. Vérifier que $*$ est une action de G sur E.

6. Soit d un diviseur de n, et $g \in G$ d'ordre d. Montrer que $|N(g)| = q^{n/d}$.

7. Montrer que le nombre recherché est $\dfrac{1}{n}\displaystyle\sum_{d|n} \varphi(d) q^{n/d}$.

Exercice 16 :

Dans la suite, $C_n^p = \dfrac{n!}{p!(n-p)!}$ désigne un coefficient binomial.

p est un nombre premier. Si $n \in \mathbb{N}^*$, $v_p(n)$ désigne la valuation en p de n, ie la puissance à laquelle apparaît p dans la factorisation de n : $n = p^{v_p(n)}m$ avec $p \wedge m = 1$.

1. Si $n, m \in \mathbb{N}^*$, $v_p(nm) =$?. Si $n, m \in \mathbb{N}^*$ et m divise n, $v_p(n/m) =$?

2. On pose $\theta(i,j) = \begin{cases} 1 \text{ si } p^i \text{ divise } j \\ 0 \text{ sinon} \end{cases}$. Que vaut $\displaystyle\sum_{i=1}^{+\infty} \theta(i,j)$?

3. Montrer que $v_p(n!) = \displaystyle\sum_{k=1}^{+\infty} E(n/p^k)$.

4. q est un entier > 0 non divisible par p, et $k \in \mathbb{N}$. Montrer que $v_p\left(C_{p^k q}^{p^k}\right) = 0$.

5. $n \in \mathbb{N}$, $n \geq 2$. Montrer que p divise tous les C_n^k, $k = 1, ..., n-1$, si et seulement si n est une puissance de p.

Exercice 17 : Inégalités de Tchebychev

On utilisera: si p est premier et $n \in \mathbb{N}^*$, $v_p(n!) = \displaystyle\sum_{k\geq 1} E\left(\frac{n}{p^k}\right)$ (voir exercice précédant)

Si $\mathbf{x} \in \mathbb{R}^+$ notons $\pi(\mathbf{x})$ le nombre de nombres premiers inférieurs ou égaux à x.
Un célèbre théorème stipule que $\pi(x) \underset{x\to+\infty}{\sim} \dfrac{x}{\ln(x)}$.
On établit un résultat plus faible, le premier obtenu par Tchebychev.

1. Montrer que $\forall k \in \mathbb{N}$, $\pi(2^{k+1}) \leq 2^k$.

2. Soit $n \in \mathbb{N}^*$. Si $p \leq 2n$ premier et $r \in \mathbb{N}^*$ est l'unique entier tel que $p^r \leq 2n < p^{r+1}$ (justifier) montrer que $v_p(C_{2n}^n) \leq r$ puis que: $\prod_{\substack{p \text{ premier} \\ \text{dans }]n,2n]}} p \mid C_{2n}^n \mid \prod_{\substack{p \text{ premier} \leq 2n \text{ et } r \\ \text{tel que } p^r \leq 2n < p^{r+1}}} p^r$

   En déduire que $n^{\pi(2n)-\pi(n)} < C_{2n}^n \leq (2n)^{\pi(2n)}$.

3. Montrer que $\forall n \in \mathbb{N}^*$, $2^n \leq C_{2n}^n \leq 2^{2n}$ et en déduire en prenant $n = 2^k$ pour $k \in \mathbb{N}$ que:

$$k(\pi(2^{k+1}) - \pi(2^k)) < 2^{k+1} \text{ et } 2^k \leq (k+1)\pi(2^{k+1})$$

4. Montrer que si $k \in \mathbb{N}$: $\dfrac{2^{k+1}}{2(k+1)} \leq \pi(2^{k+1}) \leq 3\dfrac{2^{k+1}}{k+1}$

5. Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$ tel que $2^k \leq n < 2^{k+1}$. Montrer que: $\dfrac{n \ln 2}{4 \ln(n)} \leq \pi(n) < \dfrac{(6 \ln 2)n}{\ln(n)}$

Exercice 18 :

Si $n \in \mathbb{N}^*$, montrer que $n(n+1)(n+2)$ n'est pas le carré d'un entier.

Exercice 19 :

Quel est le dernier chiffre de l'écriture en base 10 de $7^{7^{7^{7^{7^7}}}}$?

Exercice 20 : Contenu d'un polynôme.

Si $P = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$, avec $a_n \neq 0$, on appelle contenu de P la quantité $cont(P) := pgcd(a_0, ..., a_n)$.

1. $A, B \in \mathbb{Z}[X]\backslash\{0\}$. On suppose qu'un nombre premier q divise tous les coefficients de AB. Montrer que q divise tous les coefficients de A, ou tous les coefficients de B.

2. Montrer, si $A, B \in \mathbb{Z}[X]\backslash\{0\}$, que $cont(AB) = cont(A)cont(B)$.

Exercice 21 : Entiers de Gauss

On note $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.

1. Vérifier que $\mathbb{Z}[i]$ est un anneau commutatif.

2. En utilisant $|z|^2$, $z \in \mathbb{Z}[i]$, déterminer les inversibles de $\mathbb{Z}[i]$.

3. Soit $z \in \mathbb{C}$. Justifier qu'il existe $y \in \mathbb{Z}[i]$ tel que $|y - z| < 1$.

4. Division euclidienne dans $\mathbb{Z}[i]$.
   Soient $a, b \in \mathbb{Z}[i]$, $b \neq 0$. Montrer qu'il existe $q, r \in \mathbb{Z}[i]$ tels que $a = bq + r$ et $|r| < |b|$.

5. Soit I un idéal de $\mathbb{Z}[i]$.
   En considérant un élément de $I\backslash\{0\}$, si $I \neq \{0\}$, de module minimal, montrer qu'il existe $a \in \mathbb{Z}[i]$ tel que $I = a\mathbb{Z}[i]$.

Exercice 22 : Équation de Pell Fermat

$d \in \mathbb{N}^*$ n'est pas un carré d'entier.
Si $k \in \mathbb{Z}$, soit $S_k = \{(a,b) \in \mathbb{Z}^2 \mid a^2 - db^2 = k\}$.
On pose $A = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ (souvent noté $\mathbb{Z}[\sqrt{d}]$).

1. Si $z \in A$, montrer qu'il existe un unique $(a,b) \in \mathbb{Z}^2$ tel que $z = a + b\sqrt{d}$.
   On peut ainsi définir, si $z = a + b\sqrt{d} \in A$, $\overline{z} = a - b\sqrt{d}$ et $N(z) = a^2 - b^2 d$.

2. Montrer que A est un sous-anneau de $\mathbb{R}$, dense dans $\mathbb{R}$ (utiliser les sous-groupes de $\mathbb{R}$).

3. Vérifier, si $z, z' \in A$, $N(zz') = N(z)N(z')$, $N(\overline{z}) = N(z)$.
   Soit G le groupe des inversibles de A. (parfois appelé groupe des unités de A)

4. Si $z \in A$, montrer que $z \in G \iff N(z) = \pm 1$, et que si $N(z) = \pm 1$, l'inverse de z dans A $(= z^{-1})$, est $\pm\overline{z}$. Vérifier que si $z \in G$, $-z$, $\overline{z}$, $-\overline{z}$ sont aussi dans G.

5. Soit $z = a + b\sqrt{d} \in G$ tel que $z > 1$. Localiser $-z$, $\overline{z}$, $-\overline{z}$, et en déduire $a, b > 0$.
   Montrer que pour tout $x \geq 1$, $G \cap [1, x]$ est fini.

6. Supposons $G \neq \{-1, 1\}$.
   Justifier l'existence de $\theta = \min G \cap]1, +\infty[$.
   Si $z \in G$ et $z \geq 1$, montrer qu'il existe $n \in \mathbb{N}$ tel que $z = \theta^n$ (écrire $\theta^n \leq z < \theta^{n+1}$).
   En déduire que $\{z \in A \mid N(z) = \pm 1\} = \{\varepsilon\theta^n \mid \varepsilon = \pm 1,\ n \in \mathbb{Z}\}$.

7. Approximation de Dirichlet.

   (a) En considérant $k\sqrt{d} - E(k\sqrt{d})$, $k = 0..n$, et le principe des tiroirs, montrer que pour tout $n \in \mathbb{N}^*$, il existe $(p,q) \in \mathbb{Z} \times [\![1, n]\!]$ tels que $\left|\sqrt{d} - p/q\right| \leq \dfrac{1}{nq}$.

   (b) En déduire qu'il existe $(p_n), (q_n) \in \mathbb{N}^{\mathbb{N}}$ telles que (p_n/q_n) soit injective et $\left|\sqrt{d} - p_n/q_n\right| \leq \dfrac{1}{q_n^2} \xrightarrow[n \to +\infty]{} 0$.

   On se fixe de telles suites.

8. Majorer $|p_n^2 - dq_n^2|$, et en déduire qu'il existe $k \in \mathbb{Z}^*$ tel que S_k contient une infinité de (p_n, q_n).
   On se fixe k ainsi.

9. Justifier qu'il existe $x = (a,b), y = (a',b') \in S_k$ tels que $a'b - ab' \neq 0$, $a \equiv a'[k]$, $b \equiv b'[k]$.

10. En écrivant $N(x\overline{y}) = k^2$, montrer l'existence de $(c,d) \in S_1$ avec $d \neq 0$.

11. En déduire que $G \neq \{-1, 1\}$ et que S_1 est infini.

12. Ici, $d = 2$. Déterminer θ (Q.6) et S_1.

Exercice 23 :

1. Soient $n \in \mathbb{N}^*$, $a_0, ..., a_{n-1} \in \mathbb{Z}$ et $r \in \mathbb{Q}$ tels que $a_0 + a_1 r + ... + a_{n_1} r^{n-1} + r^n = 0$.
   En écrivant r sous forme irréductible, montrer que $r \in \mathbb{Z}$.

2. Si $x \in \mathbb{R}$ et $n \in \mathbb{N}$, montrer que $\cos((n+1)x) = 2\cos(x)\cos(nx) - \cos((n-1)x)$.

3. Montrer que pour tout $n \in \mathbb{N}$ il existe P_n, polynôme à coefficients entiers relatifs du type $P_n(X) = X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0$ tel que $\forall x \in \mathbb{R}$, $P_n(2\cos(x)) = 2\cos(nx)$.

4. Soit $n \in \mathbb{N}^*$. Si $r \in \mathbb{Q}$ vérifie $P_n(r) = 2$ montrer que $r \in \mathbb{Z}$.

5. Si $x \in \mathbb{R}$ est tel que $\cos(x) \in \mathbb{Q}$ et $\dfrac{x}{\pi} \in \mathbb{Q}$, montrer que $\cos(x) \in \{-1, -1/2, 0, 1/2, 1\}$

Exercice 24 : Soit $a \in \mathbb{N}$ premier à 10.

1. Montrer que pour tout entier $k \in \mathbb{N}$, $a^{4\times 10^k} \equiv 1[10^{k+1}]$.

2. En déduire qu'il existe un nombre $x \in \mathbb{N}$ tel que x^3 se termine par 123456789 en base 10.

Exercice 25 :
Pour $n \in \mathbb{N}^*$, on note d_n le nombre de diviseurs positifs de n.

1. Montrer que si $n = ab$ avec $a \wedge b = 1$, alors $d_n = d_a d_b$.

2. Montrer que n est un carré parfait si et seulement si d_n est impair.

3. Montrer que : $\displaystyle\prod_{d|n} d = \sqrt{n}^{d_n}$.

4. Montrer que $\displaystyle\sum_{k=1}^{n} d_k = \sum_{k=1}^{n} E(n/k)$, et donner un équivalent de cette somme quand $n \to +\infty$.

Exercice 26 :
Montrer qu'il y a une infinité de nombres premiers p tels que $p \equiv -1[4]$.

Exercice 27 :

1. Montrer que tout entier > 6 peut s'écrire $a + b$ où $a, b \geq 2$ et $a \wedge b = 1$.

2. Soit $(p_n)_{n\in\mathbb{N}}$ la suite croissante des nombres premiers. ($p_1 = 2,\ p_2 = 3,\ p_3 = 5, ...$)
   Montrer que pour $n \geq 3$, $p_1 p_2 ... p_n \geq p_{n+1} + p_{n+2}$.

Exercice 28 :
On dit qu'un entier $n \in \mathbb{N}^*$ a un facteur carré si et seulement si il existe p premier tel que p^2 divise n.
Montrer qu'il existe 1000 entiers consécutifs ayant un facteur carré.

Exercice 29 :
Soit $n \geq 3$. Montrer que $\varphi(n)$ est pair et que $\displaystyle\sum_{\substack{x\wedge n=1\\ 1\leq x\leq n}} x = \frac{n\varphi(n)}{2}$.

Exercice 30 :

1. Dresser la liste des cubes dans $\mathbb{Z}/13\mathbb{Z}$.

2. Soient $x, y, z \in \mathbb{Z}$ tels que $5x^3 + 11y^3 + 13z^3 = 0$. Montrer que 13 divise x, y, z.

3. Quelles sont les solutions entières de $5x^3 + 11y^3 + 13z^3 = 13$?

Exercice 31 : p est un nombre premier. Montrer que $(p-1)! \equiv -1[p]$. (ind : quels sont les $x \in \mathbb{Z}/p\mathbb{Z}^*$ tels que $x^{-1} = x$?)

Exercice 32 :
$m, n \in \mathbb{N}^*$. Déterminer les morphismes de groupe de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 33 :

1. p est premier. Montrer que tout élément de $\mathbb{Z}/p\mathbb{Z}$ est somme de deux carrés. (regarder, si $k \in \mathbb{Z}/p\mathbb{Z}$, les cardinaux de $\{a^2 \mid a \in \mathbb{Z}/p\mathbb{Z}\}$, et $\{k - a^2 \mid a \in \mathbb{Z}/p\mathbb{Z}\}$)

2. n est un produit de nombres premiers distincts deux à deux. Montrer que tout élément de $\mathbb{Z}/n\mathbb{Z}$ est somme de deux carrés.

3. Pour $n = 9$ et $n = 25$, regarder si tout élément de $\mathbb{Z}/n\mathbb{Z}$ est somme de deux carrés.

Exercice 34 :

1. p est un nombre premier ≥ 3. Si $x \in \mathbb{Z}$, $\overline{x}$ est la classe de x dans $\mathbb{Z}/p\mathbb{Z}$. On pose $K = \mathbb{Z}/p\mathbb{Z}$.
   Un élément $a \in K$ est dit carré si et seulement si il existe $b \in K$ tel que $b^2 = a$.

   (a) Montrer que le nombre de carrés de K est $\dfrac{p+1}{2}$.

   (b) Montrer que, si $x \in K$, x est un carré si et seulement si $x^{(p+1)/2} = x$. (se simplifie en $x^{(p-1)/2} = 1$ si $x \neq 0$)

   On pourra utiliser que $X^{(p+1)/2} - X \in K[X]$ a au plus $\dfrac{p+1}{2}$ racines dans K.

   (c) A quelle condition nécessaire et suffisante (sur p) $-\overline{1}$ est-il un carré dans K?

2. Soit $n \in \mathbb{N}$ et $p \geq 3$ un diviseur premier de $n^2 + 1$. Montrer que $p \equiv 1[4]$.

3. En déduire qu'il y a une infinité de nombres premiers de la forme $4k + 1$.

Exercice 35 :

p est un nombre premier ≥ 3. Si $x \in \mathbb{Z}$, $\overline{x}$ est la classe de x dans $\mathbb{Z}/p\mathbb{Z}$.
On pose, si $k \in \mathbb{Z}/p\mathbb{Z}$, $S_k = \{(x, y) \in (Z/p\mathbb{Z})^2 \mid x^2 + y^2 = k\}$.

1. Si $p \equiv 1[4]$, en notant que $-\overline{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ (cf exercice précédent) déterminer $card(S_1)$.

2. On suppose $p \equiv 3[4]$.

   (a) $Card(S_0) =?$

   (b) Si $k \neq 0$, montrer que $S_k \neq \emptyset$

   (c) Soit $(a, b) \in S_k$. Montrer que $(x, y) \mapsto (xa - yb, xb + ya)$ est une bijection de S_1 dans S_k.
   $card(S_1) =?$.

Exercice 36 :

Si $n \in \mathbb{N}^*$, $x \in \mathbb{C}$ est dit racine primitive n-ième de l'unité si et seulement si x est d'ordre n dans $\mathbb{C}^*$.
Un tel x est donc dans U_n
On notera R_n l'ensemble des racines primitives n-ième de l'unité.

1. Soit $x = e^{2ik\pi/n}$. Montrer que x est racine primitive n-ième de l'unité si et seulement si $k \wedge n = 1$.
   card$(R_n) =?$.

2. On note $\Phi_n = \prod_{x \in R_n} (X - x)$ (polynôme cyclotomique).
   Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$.

3. Montrer que pour tout $n \in \mathbb{N}^*$, Φ_n est à coefficients entiers relatifs, de terme constant ± 1.

Exercice 37 : Cyclicité de $(\mathbb{Z}/p\mathbb{Z})^*$

1. Soit K un corps et G un sous-groupe fini de K^*.
   Soit $x \in G$ d'ordre le ppcm des ordres des éléments de G (cf exercice 13)
   Soit n l'ordre de x.
   Montrer que $G = Gr(x)$. (On utilisera une considération sur $X^n - 1 \in K[X]$)

   En particulier, si K est fini, K^* est cyclique, et donc si p est premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

2. $(\mathbb{Z}/7\mathbb{Z})^*$ est donc cyclique isomorphe à $\mathbb{Z}/6\mathbb{Z}$. Déterminer ses générateurs.

3. $(\mathbb{Z}/8\mathbb{Z})^*$ est-il cyclique?

2 Complément de cours sur les corps

2.1 Caractéristique d'un corps

Définition 1: Caractéristique d'un corps
Soit K un corps. Si $n \in \mathbb{Z}$, et $x \in K$, $n \cdot x$ désigne l'itéré n-ième additif de x, et x^n l'itéré n-ième multiplicatif.
Le produit de $x, y \in K$ sera simplement noté xy, et les neutres 0 et 1.
On dit que K est de caractéristique nulle si et seulement si $\forall n \in \mathbb{N}^*$, $n \cdot 1 \neq 0$ (itéré de 1).
Si K n'est pas de caractéristique nulle, on définit sa caractéristique par $car(K) = \min\{n \in \mathbb{N}^* \mid n \cdot 1 = 0\}$.

Propriété 1:

1. Tout corps fini est de caractéristique non nulle.

2. Si K est un corps de caractéristique non nulle non réduit à un élément, $car(K)$ est un nombre premier

3. Si $car(K) = n \in \mathbb{N}^*$, $\forall x \in K^*$, $\forall m \in \mathbb{N}$, $m \cdot x = 0 \iff n|m$.

4. Si p est premier, $car(\mathbb{Z}/p\mathbb{Z}) = p$.

Démonstration:

1. Soit K un corps fini de cardinal n.
   Alors $1, 2 \cdot 1, ..., (n+1) \cdot 1$ sont $n+1$ éléments de K, donc deux sont égaux. Il existe $p, q \in \mathbb{N}$, $p < q$, tels que $p \cdot 1 = q \cdot 1$, et alors $(q - p) \cdot 1 = 0$.

2. On suppose $car(K) = n \in \mathbb{N}^*$.
   Si $n = 1$, $0 = 1$ et K est réduit à un élément, cas sans intérêt...
   Sinon: $n \geq 2$. Supposons n non premier. On écrit alors $n = ab$ avec $a, b \geq 2$.
   Notons qu'on a $(a \cdot 1)(b \cdot 1) = \underbrace{(1 + ... + 1)}_{a \text{ termes}} \underbrace{(1 + ... + 1)}_{b \text{ termes}} = n \cdot 1 = 0$.
   Par intégrité de K, $a \cdot 1 = 0$ ou $b \cdot 1 = 0$ ce qui contredit la minimalité de n.

3. Si $n|m$: $m = an$. $(an) \cdot x = a \cdot ((n \cdot 1)x) = 0$.
   Si $m \cdot x = 0$: $0 = m \cdot x = (m \cdot 1)x$. Comme $x \neq 0$, par intégrité de K, $m \cdot 1 = 0$.
   On écrit $m = pn + r$ avec $r \in [\![0, n-1]\!]$ la division euclidienne de m par n.
   $0 = m \cdot 1 = (p \cdot \underbrace{(n \cdot 1)}_{=0}) + r \cdot 1 = r \cdot 1$. Par définition de $n = car(K)$, $r = 0$.

4. Facile.

♣

2.2 $K[X]$

La construction des polynômes ne change pas, la notion de degré et ses propriétés non plus.
$K[X]$ est intègre.
Le théorème de division euclidienne reste inchangé (même démonstration), ainsi que ses conséquences sur la factorisation, et le fait qu'un polynôme de degré n a au plus n racines.
En revanche, il y a des problèmes avec le polynôme dérivé si la caractéristique est $\neq 0$.
Si $P = a_nX^n + ... + a_1X + a_0$, $P' = na_nX^n + ... + a_1$. na_n s'entend comme l'itéré n-ième de a. $na_n = (n \cdot 1)a_n = 0$ si $car(K)|n$.
Ainsi, si $car(K) = n$, et $P = X^n - 1$, $P' = nX^{n-1} = 0$.
Dans la formule de Taylor, $\frac{1}{n!}$ s'entend $((n!) \cdot 1)^{-1}$, et $(n!) \cdot 1$ peut être nul.
Il faut donc oublier en caractéristique non nulle formule de Taylor, caractérisation de l'ordre des racines avec les dérivées, sauf à être très prudent.

2.3 Algèbre linéaire sur un corps quelconque

Les résultats du cours sont inchangés, dont les résultats sur diagonalisation/trigonalisation et polynôme minimal, polynôme caractéristique, polynômes annulateurs.
Le théorème de Cayley-Hamilton subsiste.
Mais on ne peut pas nécessairement trigonaliser, $P \in K[X]$ n'étant pas nécessairement scindé.
On peut faire certaines choses en utilisant des dénombrements sur les corps finis.
Un exemple:

Propriété 2:
Soit K un corps de cardinal q. Alors $\text{card}(GL_n(K)) = (q^n - 1)(q^n - q)(q^n - q^2)...(q^n - q^{n-1})$

Démonstration:
Définir $A \in GL_n(K)$ revient à définir ses colonnes, ie une famille libre $(C_1, ..., C_n)$ dans K^n.
On commence par choisir $C_1 \neq 0$: $q^n - 1$ choix.
Ensuite, ayant choisi C_1, il faut choisir $C_2 \in \mathbb{K}^n \backslash vect(C_1)$. $\text{card}(K^n) = q^n$. $vect(C_1) = KC_1$ est de cardinal q, car $k \to kC_1$ est injective.
D'où $q^n - q$ choix pour C_2.
Ensuite, comme (C_1, C_2) est libre, $(k_1, k_2) \mapsto k_1C_1 + k_2C_2$ est injective, $vect(C_1, C_2)$ est de cardinal q^2, et il y a $q^n - q^2$ choix pour C_3.
Etc... D'où $(q^n - 1)(q^n - q)(q^n - q^2)...(q^n - q^{n-1})$ choix.
♣

2.4 Extension de corps

Nous nous limiterons ici aux prémisses, bien loin d'aller jusqu'à la théorie de Galois.
En fait, essentiellement le lemme de la base télescopique, et les conséquences sur les nombres algébriques.

La remarque fondamentale de départ est que si K_1 et K_2 sont deux corps avec $K_1 \subset K_2$, K_2 a une structure naturelle de K_1-ev, le produit extérieur $\lambda \cdot x$, avec $\lambda \in K_1$ et $x \in K_2$ étant simplement le produit λx dans K_2.
On note $[K_2 : K_1] \in \mathbb{N}^* \cup \{\infty\}$ la dimension de K_2 comme K_1-ev.

Propriété 3: Soient $K_1 \subset K_2 \subset K_3$ trois corps tels que $[K_3 : K_1] < \infty$.
Alors $[K_2 : K_1] \leq [K_3 : K_1]$.

Démonstration:
Soit $n = [K_3 : K_1] < \infty$. Si $[K_2 : K_1] > n$, on peut se donner $(e_1, ..., e_{n+1})$ famille d'éléments de K_2 qui est K_1-libre.
Alors a fortiori, c'est une famille de $n+1$ éléments de K_3 qui est K_1-libre, ce qui contredit $n = [K_3 : K_1]$.

Propriété 4: Base télescopique
Soient trois corps K_1, K_2, K_3 tels que $[K_3 : K_2]$ et $[K_2 : K_1]$ soient finis.
Alors $[K_3 : K_1]$ est finie, et $[K_3 : K_1] = [K_3 : K_2][K_2 : K_1]$.

Démonstration Soient $(e_1, ..., e_d)$ une base de K_3 comme K_2-ev, et $(f_1, ..., f_n)$ une base de K_2 comme K_1-ev.
Montrons que $B = (e_i f_j)_{\substack{1 \leq i \leq d \\ 1 \leq j \leq n}}$ est une base de K_3 comme K_1-ev, ce qui donnera le résultat par cardinalité des bases. (B est appelée base télescopique)
Caractère générateur: Soit $x \in K_3$. x s'écrit $x = \sum_i y_i e_i$ avec $y_1, ..., y_d \in K_2$. Ensuite, pour tout i, y_i s'écrit $y_i = \sum_j k_{i,j} f_j$ avec $k_{i,j} \in K_1$.
Il en résulte $x = \sum_{i,j} k_{i,j} f_j e_i$.

Liberté: Si $\sum_{i,j} k_{i,j} f_i e_j = 0$ avec $\forall i, j,\ k_{i,j} \in K_1$: $\sum_j \underbrace{\left(\sum_i k_{i,j} f_i \right)}_{\in K_2} e_j = 0$.

Par K_2-liberté de $(e_1, ..., e_d)$, $\forall j$, $\sum_i \underbrace{k_{i,j}}_{\in K_1} f_i = 0$, puis par K_1-liberté de $(f_1, ..., f_n)$, $\forall j, i,\ k_{i,j} = 0$.

♣

Définition 2: Nombres algébriques
$x \in \mathbb{R}$ est dit algébrique si et seulement si il existe $Q \in \mathbb{Q}[X]$ non nul tel que $Q(x) = 0$.

Définition 3: polynôme minimal
Si $x \in \mathbb{R}$, $Ann(x) = \{Q \in \mathbb{Q}[X] \mid Q(x) = 0\}$ est facilement un idéal de $\mathbb{Q}[X]$.
Si x est algébrique, $Ann(x) \neq \{0\}$, donc il existe un unique $P \in \mathbb{Q}[X]$ unitaire tel que $Ann(x) = P\mathbb{Q}[X]$, et ce polynôme P est appelé polynôme minimal de x. Nous le noterons π_x.

Propriété 5: Avec les mêmes notations, si x est algébrique, π_x est un irréductible de $\mathbb{Q}[X]$.

Démonstration: Par l'absurde, sinon, il existe $A, B \in \mathbb{Q}[X]$ non constants tels que $\pi_x = AB$. Alors $A(x)B(x) = 0$, et par intégrité de $\mathbb{R}$, $A(x) = 0$ ou $B(x) = 0$, disons $A(x) = 0$. Alors π_x divise A, mais $1 \leq deg(A) < deg(\pi_x)$. C'est absurde.

Définition 4: Soit $x \in \mathbb{R}$, et K un sous-corps de $\mathbb{R}$. On note $K(x) = \bigcap_{\substack{K_2 \text{ sous-corps de } \mathbb{R} \\ \text{contenant } \{x\} \cup K}} K_2$.
L'intersection de sous-corps étant un sous corps, $K(x)$ est un sous-corps de $\mathbb{R}$, et de par sa définition, le plus petit (au sens de l'inclusion) sous-corps de $\mathbb{R}$ contenant K et x.
Dit plus simplement, $K(x)$ est tout ce qui peut s'obtenir à partir de $K \cup \{x\}$ en utilisant un nombre quelconque de fois les opérations $+$, $\times$, passage à l'inverse et à l'opposé.
De ce fait, $K(x)$ est en fait facilement l'ensemble des évaluations en x des fractions rationnelles à coefficients dans K qui n'ont pas x comme pôle: $K(x) = \{F(x) \mid F \in K(X),\ x \text{ non pôle de } F\}$.

La propriété essentielle est la suivante:

Propriété 6:
$x \in \mathbb{R}$ est algébrique si et seulement si $[\mathbb{Q}(x) : \mathbb{Q}] < \infty$.
De plus, si x est algébrique, $n := [\mathbb{Q}(x) : \mathbb{Q}]$ est le degré de π_x, et $\mathbb{Q}(x) = \mathbb{Q}_{n-1}[x] = \{P(x) \mid P \in \mathbb{Q}_{n-1}[X]\}$.

Démonstration:
Supposons x algébrique. Notons $\pi_x = X^n + a_{n-1}X^{n-1} + ... + a_0$. $a_i \in \mathbb{Q}$.
En premier, voyons que $\mathbb{Q}(x) = \mathbb{Q}[x]$. Il n'y a qu'une inclusion non triviale.
$\mathbb{Q}[x]$ est facilement un anneau.
Soit $F \in \mathbb{Q}(X)$, $F = \dfrac{A}{B}$, $A, B \in \mathbb{Q}[X]$, avec $B(x) \neq 0$.
Si on montre que $\dfrac{1}{B(x)} \in \mathbb{Q}[x]$, on aura $F(x) = A(x) \times \dfrac{1}{B(x)} \in \mathbb{Q}[x]$.
π_x ne divise pas B, et est irréductible dans $\mathbb{Q}[X]$, donc, dans $\mathbb{Q}[X]$, $B \wedge \pi_x = 1$.
Donc (Bezout), il existe $U, V \in \mathbb{Q}[X]$ tels que $UB + V\pi_x = 1$. Alors $U(x)B(x) = 1$, et $\dfrac{1}{B(x)} = U(x) \in \mathbb{Q}[x]$.
Ainsi $\mathbb{Q}(x) = \mathbb{Q}[x]$.
Ensuite, par division euclidienne par π_x, on a $\mathbb{Q}[X] = \mathbb{Q}_{n-1}[x]$.
$\mathbb{Q}_{n-1}[x] = vect_{\mathbb{Q}}(1, x, ..., x^{n-1})$. $(1, ..., x^{n-1})$ est $\mathbb{Q}$-libre sans quoi on aurait un $P \in \mathbb{Q}[X]$ non nul de degré $< n$ annulant x, donc divisé par π_x, ce qui est impossible.
Donc $[\mathbb{Q}(x) : \mathbb{Q}] = n$.

Supposons maintenant $n := [\mathbb{Q}(x) : \mathbb{Q}] < \infty$.
Comme $1, x, ..., x^n$ sont $(n+1)$ éléments de $\mathbb{Q}(x)$, la famille est $\mathbb{Q}$-liée, ce qui donne un polynôme non nul $P \in \mathbb{Q}[X]$ tel que $P(x) = 0$, et x est algébrique.
♣.

La propriété précédente s'étend sans changement de démonstration à des corps quelconques, et on a notamment:

Propriété 7: Soit $K_1 \subset K_2$ deux corps, et $x \in K_2$. Il existe $P \in K_1[X]$ non nul tel que $P(x) \neq 0$ si et seulement si $[K_1(x) : K_1] < \infty$.

Propriété 8: L'ensemble A des réels algébriques est un sous-anneau de $\mathbb{R}$.

Démonstration: Remarque: on l'a déjà vu avec le résultant.
Soient $x, y \in A$. $-x \in A$ trivialement (on change des signes dans π_x).
$(\mathbb{Q}(x))(y)$ est un corps contenant x et y, donc xy et $x + y$.
On a les inclusions de corps $\mathbb{Q} \subset \mathbb{Q}(x) \subset (\mathbb{Q}(x))(y)$.
$[\mathbb{Q}(x) : \mathbb{Q}] < \infty$ car x est algébrique.
y est algébrique, d'où l'existence de $\pi_y \in \mathbb{Q}[X]$. A fortiori, $\pi_y \in \mathbb{Q}(x)[X]$, et annule y, donc par la propriété 7, $[(\mathbb{Q}(x))(y) : \mathbb{Q}(x)] < \infty$.
Alors, par la propriété 4, $[(\mathbb{Q}(x))(y) : \mathbb{Q}] < \infty]$.
$\mathbb{Q} \subset \mathbb{Q}(x + y) \subset (\mathbb{Q}(x))(y)$, et $[(\mathbb{Q}(x))(y) : \mathbb{Q}] < \infty]$, donc par la propriété 3, $[\mathbb{Q}(x + y) : \mathbb{Q}] < \infty$, et $x + y$ est algébrique.
Idem pour xy.
♣.

Une dernière chose, lié à des considérations d'algèbre linéaire:

Propriété 9:
Soit K un corps fini de cardinal ≥ 2.
Alors il existe p nombre premier et $n \in \mathbb{N}^*$ tels que $\text{card}(K) = p^n$.

Remarque: réciproquement, pour tous p, n il existe un corps de cardinal p^n.

Démonstration:
Soit $p = car(K)$. On a vu que p est un nombre premier.
Notons $K_2 = \{0, 1, 2 \cdot 1, ..., (p-1) \cdot 1\}$.
K_2 est de cardinal p car s'il existait $1 \leq n < m \leq p-1$ tels que $n \cdot 1 = m \cdot 1$, on aurait $(m-n) \cdot 1 = 0$, avec $1 \leq m - n < p$, ce qui contredirait la définition de p.
K_2 est un sous-corps de K: stable par somme, produit, passage à l'opposé, en utilisant des divisions euclidiennes par p, comme dans la démonstration de la propriété 1.
Il reste à voir la stabilité par passage à l'inverse: soit $n \in [\![1, p-1]\!]$.
On a $n \wedge p = 1$ car p est premier. On écrit une relation de Bezout $1 = un + vp$.
Alors $1 = 1 \cdot 1 = (un + vq) \cdot 1 = (un) \cdot 1 + \underbrace{(vp) \cdot 1}_{=0} = (u \cdot 1)(n \cdot 1)$.
Donc l'inverse de $n \cdot 1$ est $u \cdot 1$, qui est dans K_2 comme dit précédemment, en faisant la division euclidienne de u par p.
$K_2 \subset K$, donc K est un K_2-ev, de dimension finie car fini. Notons $n = [K : K_2]$.
Soit $(e_1, ..., e_n)$ une base de K comme K_2-ev.
Par liberté et caractère générateur, $\begin{cases} K_2^n \to K \\ (k_1, ..., k_n) \mapsto k_1 e_1 + ... + k_n e_n \end{cases}$ est bijective, donc $\text{card}(K) = p^n$.
♣