Un peu de combinatoire

Soient n un entier naturel non nul et p un nombre premier. Calculer l'ordre de $GL_n(\mathbb{Z}/p\mathbb{Z})$ et de $SL_n(\mathbb{Z}/p\mathbb{Z})$.

Lemme de Gauss et critère d'Eisenstein

Lorsque $P \in \mathbb{Z}[X]$ est un polynôme non nul à coefficients entiers, on appelle *contenu* de P et on note $c(P)$ le pgcd des coefficients de P.

1. Soient $P, Q \in \mathbb{Z}[X]$ tous non nuls. Montrer que $c(PQ) = c(P)c(Q)$. Ceci est le lemme de Gauss.
2. Soit $P \in \mathbb{Z}[X]$ un polynôme irréductible dans $\mathbb{Z}[X]$. Montrer qu'il est aussi irréductible dans $\mathbb{Q}[X]$.
3. Quel est le polynôme minimal sur $\mathbb{Q}$ de $\sqrt{2} + \sqrt{3}$?
4. Soit $P = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p qui divise tous les a_i sauf a_n, et dont le carré ne divise pas a_0 (on dit que P est *d'Eisenstein en* p). Montrer que P est irréductible dans $\mathbb{Q}[X]$.

Algorithme de Berlekamp

Cet exercice établit un algorithme permettant la factorisation des polynômes à coefficients dans le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1. Soit $P \in \mathbb{F}_p[X]$ un polynôme unitaire. A quelle condition P' est-il nul ?
2. On cherche à factoriser complètement P. Expliquer comment on peut tout d'abord savoir si P a un facteur carré, et comment réagir dans ce cas. On prendra garde au cas où P' est nul.
3. On suppose désormais P sans facteur carré. On peut donc écrire

$$P = \prod_{i=1}^{m} P_i,$$

les P_i étant irréductibles unitaires et distincts deux-à-deux.

Soit A la $\mathbb{F}_p$-algèbre $A = \mathbb{F}_p[X]/(P)$. Montrer qu'on a un isomorphisme de $\mathbb{F}_p$-algèbres

$$A \simeq \prod_{i=1}^{m} \mathbb{F}_p[X]/(P_i).$$

4. On munit A du *morphisme de Frobenius* $Fr\colon A \to A,\ f \mapsto f^p$. Vérifier qu'il s'agit bien d'un endomorphisme de A, puis démontrer que

$$\dim \ker(Fr - Id_A) = m.$$

Expliquer alors comment on peut déterminer si P est irréductible.

5. Si P est n'est pas irréductible, on souhaite pouvoir calculer les P_i. Expliquer pourquoi il existe un polynôme non-constant $Q \in \mathbb{F}_p[X]$, de degré strictement moindre que celui de P, qui soit tel que $P | Q^p - Q$. Montrer qu'on a alors une factorisation non-triviale

$$P = \prod_{a \in \mathbb{F}_p} P \wedge (Q + a),$$

où $\wedge$ désigne le pgcd. En déduire comment trouver les P_i.

Algèbre commutative

Dans cet exercice, on *admettra* et on utilisera librement le *lemme de Zorn*, dont voici l'énoncé :

▷ Soit E un ensemble non vide partiellement ordonné. Si E est *inductif*, c'est-à-dire si toute partie non vide totalement ordonnée de E admet un majorant, alors E admet (au moins) un élément maximal. ◁

Soit A un anneau commutatif et unitaire.

1. On dit qu'un idéal $\mathfrak{P}$ de A est *premier* si

$$\forall x, y \in A,\ xy \in \mathfrak{P} \Longrightarrow x \in \mathfrak{P} \text{ ou } y \in \mathfrak{P}.$$

   Soit I un idéal de A, montrer que I est premier si et seulement si le quotient A/I est intègre.

   On notera $Spec\, A$ l'ensemble des idéaux premiers de A.

2. On dit qu'un idéal $\mathfrak{M}$ de A est *maximal* s'il est maximal au sens de l'inclusion, autrement dit si

$$\forall I \text{ idéal de } A,\ \mathfrak{M} \subseteq I \Longrightarrow I = \mathfrak{M} \text{ ou } I = A.$$

   Soit I un idéal de A, montrer que I est maximal si et seulement si le quotient A/I est un corps.

   En utilisant le lemme de Zorn, montrer que tout idéal propre de A est contenu dans un idéal maximal.

   On notera $Specmax\, A$ l'ensemble des idéaux premiers de A.

3. Montrer que $Specmax\, A \subseteq Spec\, A$.

4. A tout idéal I de A, on associe son *radical*

$$\sqrt{I} = \{a \in A \mid \exists n \in \mathbb{N} \colon a^n \in I\}.$$

   Montrer que $\sqrt{I}$ est encore un idéal. Si $n \in \mathbb{Z}$, quel est le radical de l'idéal $n\mathbb{Z}$ de $\mathbb{Z}$? A l'aide du lemme de Zorn, démontrer l'identité

$$\sqrt{I} = \bigcap_{\mathfrak{P} \in Spec\, A,\, \mathfrak{P} \supseteq I} \mathfrak{P}.$$

   Soit $Nilrad\, A$ le *nilradical* de A, c'est-à-dire l'ensemble des éléments nilpotents de A. Montrer que

$$Nilrad\, A = \bigcap_{\mathfrak{P} \in Spec\, A} \mathfrak{P}.$$

5. En déduire quels sont les éléments inversibles de l'anneau de polynômes $A[X]$.
6. On considère le *radical de Jacobson*

$$Rad\, A = \{a \in A \mid \forall x \in A,\ 1 + ax \text{ est inversible}\}.$$

Montrer l'identité

$$Rad\, A = \bigcap_{\mathfrak{M} \in Specmax\ A} \mathfrak{M}.$$

Polynômes cyclotomiques

Lorsque $n \geqslant 1$ est un entier, on appelle Π_n l'ensemble des racines n-ièmes primitives de l'unité, et on définit le *n-ième polynôme cyclotomique* par

$$\phi_n(X) = \prod_{\zeta \in \Pi_n} (X - \zeta) \in \mathbb{C}[X].$$

Que vaut $\prod_{d|n} \phi_d$? En déduire qu'en fait $\phi_n \in \mathbb{Z}[X]$.

Actions de groupes

Soit X un ensemble, et soit G un groupe. On dit que G *agit* (ou *opère*) sur X si on s'est donné un morphisme (pas forcément injectif, et même éventuellement trivial) de G dans le groupe des permutations $\mathfrak{S}(X)$. On note alors $g \cdot x \in X$ l'action d'un élément $g \in G$ sur un élément $x \in X$. Si $x \in X$, on dispose de son *stabilisateur*

$$Stab_x = \{g \in G \mid g \cdot x = x\} \subseteq G$$

et de son *orbite*

$$G \cdot x = \{g \cdot x,\ g \in G\} \subseteq X.$$

On note Ω l'ensemble des orbites. Enfin, lorsque $g \in G$, on peut aussi considérer ses *points fixes*

$$Fix_g = \{x \in X \mid g \cdot x = x\} \subseteq X.$$

On suppose dans cet exercice G et X finis.

1. Montrer la *formule des classes* :

$$\exists R \subseteq X : \quad Card\ X = \sum_{x \in R} \frac{Card\ G}{Card\ Stab_x}.$$

2. Démontrer la *formule de Burnside* :

$$Card\ \Omega = \frac{1}{Card\ G} \sum_{g \in G} Card\ Fix_g.$$

3. On note $\mathcal{Z}_G$ le centre de G, c'est-à-dire le sous-groupe formé des éléments de G qui commutent avec tous les autres. Montrer qu'on a une identité de la forme

$$\exists \Theta \subseteq G : \quad Card\ G = Card\ \mathcal{Z}_G + \sum_{g \in \Theta} \frac{Card\ G}{Card\ N_g}$$

où les N_g sont des sous-groupes de G que l'on précisera.

4. Montrer que tous les groupes d'ordre p^2, avec p premier, sont abéliens.
5. On souhaite démontrer le *théorème de Wedderburn*, qui affirme que tout corps fini est commutatif. Soit donc K un corps fini. On pose $q - 1 = Card\ \mathcal{Z}_{K^*}$. Montrer qu'on peut écrire

$$q^n - 1 = q - 1 + \sum_{d|n} \lambda_d \frac{q^n - 1}{q^d - 1},$$

où n et les λ_d sont entiers. Conclure en utilisant l'exercice précédent.

Symbole de Legendre

Soit p un nombre premier impair fixé une fois pour toutes. Afin d'alléger les notations, on appelle $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, et on pose $p' = (p-1)/2$. On note aussi $(\mathbb{F}_p^*)^2$ l'ensemble des carrés de $\mathbb{F}_p^*$. Enfin, si x est réel, on note $\lfloor x \rfloor$ sa partie entière.

1. Quel est le cardinal de $(\mathbb{F}_p^*)^2$?
2. Si $x \in \mathbb{Z}$ n'est pas divisible par p, on définit le *symbole de Legendre*

$$\left(\frac{x}{p}\right) = 1 \text{ si } x \in (\mathbb{F}_p^*)^2, \ -1 \text{ sinon.}$$

Montrer que $\left(\frac{x}{p}\right) \equiv x^{p'} \mod p$. En déduire la valeur de $\left(\frac{-1}{p}\right)$, puis montrer que $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.

3. On souhaite montrer que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Pour cela, on considère α une racine huitième primitive de l'unité de $\mathbb{F}_p$ dans la clôture algébrique de celui-ci. Que vaut α^4 ? On pose $\beta = \alpha + \alpha^{-1}$. Montrer que $2 \in (\mathbb{F}_p^*)^2$ si et seulement si $\beta \in \mathbb{F}_p$, et conclure.
4. Notre objectif est à présent de démontrer la *loi de réciprocité quadratique*, qui affire que si p et q sont premiers impairs distincts, alors

$$\left(\frac{p}{q}\right) = (-1)^{p'q'} \left(\frac{q}{p}\right).$$

   Ceci nous permettrait de calculer le sybole de Legendre efficacement. Pour s'en convaincre, *en admettant teporarement la loi de réciprocité quadratique*, déterminer si 19 est un carré modulo 283.
5. On pose $S = \{1, 2, \cdots, p'\} \subset \mathbb{F}_p^*$, et on fixe $a \in \mathbb{Z}$ non-divisible par p. Vérifier que pour tout $s \in S$, on peut écrire $as = \epsilon_a(s)s_a$ avec $s_a \in S$ et $\epsilon_a(s) = \pm 1$, et montrer que l'application ainsi définie $S \to S$, $s \mapsto s_a$ est bijective.
6. Soit $\mu_a = Card\ \{s \in S | \epsilon_a(s) = -1\}$. Montrer que $\left(\frac{a}{p}\right) = (-1)^{\mu_a}$.
7. On pose

$$S_{p,q} = \sum_{s=1}^{p'} \left\lfloor \frac{sq}{p} \right\rfloor \quad \text{et} \quad S_{q,p} = \sum_{s=1}^{q'} \left\lfloor \frac{sp}{q} \right\rfloor.$$

   En considérant un rectangle de côtés p et q, démontrer que $S_{p,q} + S_{q,p} = p'q'$.
8. Montrer que $S_{p,q} \equiv \mu_q \mod 2$, et conclure.

Une petite dernière pour la route

Existe-t-il un polynôme $P \in \mathbb{R}[X]$ tel que $\forall x \in [0, 1],\ P(x) = \cos x$?