TD ∗ ALGÈBRE MODULAIRE

1 CNS pour que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ soit cyclique

Soient $a, b \in \mathbb{N}^*$.
Montrer que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est cyclique si et seulement si $a \wedge b = 1$.

Solution de 1 : CNS pour que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ soit cyclique

- Supposons $a \wedge b = 1$, et $au + bv = 1$ une relation de Bézout.
  Soit $x = (v \bmod a, u \bmod b) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.
  On remarque que $ax = (0 \bmod a, 1 \bmod b)$ et $bx = (1 \bmod a, 0 \bmod b)$.
  Donc pour tout couple $(c, d) \in \mathbb{Z}^2$,

$$(c \bmod a, d \bmod b) = cbx + dax = (cb + da)x$$

  Donc $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} = \langle x \rangle$ et $\boxed{\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \text{ est cyclique.}}$
- Supposons $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ cyclique.
  Pour tout $x \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, $(a \vee b)x = (0 \bmod a, 0 \bmod b)$, donc l'ordre de x dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ divise $a \vee b$.
  En particulier, $ab = |\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}|$ qui est l'ordre d'un élément puisque le groupe est cyclique divise $a \vee b$.
  Comme, par ailleurs, $a \vee b$ divise ab, tout étant positif, nécessairement $a \vee b = ab$ et $\boxed{a \wedge b = 1.}$

2 Mines

Soit $n \in \mathbb{N}^*$.

1. Soit H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$. Montrer qu'il existe a divisant n vérifiant $H = \langle \overline{a} \rangle$.
2. Observer que si $d \mid n$, il existe un unique sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ de cardinal d.
3. Justifier que si $d \mid n$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ possède exactement $\varphi(d)$ éléments d'ordre d (avec φ la fonction indicatrice d'Euler).
4. Montrer

$$\sum_{d \mid n} \varphi(d) = n$$

Solution de 2 : Mines

1. Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.
   Si $H = \{0\}$ alors $H = \langle \overline{0} \rangle$.
   Sinon, on peut introduire

$$a = \min\left\{k \in \mathbb{N}^*,\ \overline{k} \in H\right\}$$

   On a $\overline{a} \in H$ donc $\langle \overline{a} \rangle \subset H$. La division euclidienne de n par a donne $n = qa + r$ avec $q \in \mathbb{Z}$ et $r \in \{0, \dots, a-1\}$.
   On en déduit $\overline{r} = q \cdot \overline{a} \in \langle \overline{a} \rangle \subset H$.
   Par minimalité de a, il vient $r = 0$. Ainsi, $\boxed{a \mid n.}$
   Soit $\overline{x} \in H$. Par division euclidienne, on écrit $x = aq + r$ avec $q \in \mathbb{Z}$ et $r \in \{0, \dots, a-1\}$.
   On en déduit $\overline{r} = \overline{x} - q \cdot \overline{a} \in H$.
   Par minimalité de a, il vient $r = 0$ puis $x = aq$ et donc $\overline{x} \in \langle \overline{a} \rangle$.
   Par double inclusion, $\boxed{H = \langle \overline{a} \rangle.}$
2. Si a divise n, on observe que $\langle \overline{a} \rangle$ est de cardinal $\dfrac{n}{a}$.
   Ainsi, $\left\langle \overline{n/d} \right\rangle$ est l'unique sous-groupe d'ordre d de $(\mathbb{Z}/n\mathbb{Z}, +)$.
3. Un élément d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ est générateur d'un sous-groupe à d éléments donc générateur de $\left\langle \overline{n/d} \right\rangle$.
   Inversement, tout générateur de $\left\langle \overline{n/d} \right\rangle$ est élément d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.
   Or $\left\langle \overline{n/d} \right\rangle$ est cyclique d'ordre d donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$ et possède ainsi $\varphi(d)$ générateurs.
   On peut alors affirmer que $\boxed{\mathbb{Z}/n\mathbb{Z} \text{ possède exactement } \varphi(d) \text{ élément d'ordre } d.}$

4. L'ordre d'un élément de $\mathbb{Z}/n\mathbb{Z}$ est cardinal d'un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ et donc diviseur de n.
En dénombrant $\mathbb{Z}/n\mathbb{Z}$ selon l'ordre de ses éléments, on obtient

$$\boxed{\sum_{d|n}\varphi(d)=n.}$$

3 Centrale – X-ENS : polynômes cyclotomiques et version faible du théorème de Dirichlet

Soit $n\in\mathbb{N}^*$, $\varphi(n)$ l'indicatrice d'Euler de n, $\mathbb{U}_n$ l'ensemble des racines n^{e} de l'unité et $\mathbb{U}_n^*$ l'ensemble des racines de l'unité d'ordre exactement n. Enfin, pour $d\in\mathbb{N}^*$, on pose

$$\Phi_d=\prod_{z\in\mathbb{U}_d^*}(X-z)$$

1. Montrer que $X^n-1=\prod_{d|n}\Phi_d$.
2. Justifier que $\sum_{d|n}\varphi(d)=n$.
3. Montrer que Φ_n est un polynôme à coefficients entiers.
4. **Application**
   (a) Que peut-on dire d'un nombre premier p qui divise $\Phi_n(a)$ où $a\in\mathbb{Z}$, mais aucun des $\Phi_d(a)$ pour d diviseur strict de n ?
   (b) En déduire que pour $n\geqslant 1$ fixé, il existe une infinité de nombres premiers de la forme $kn+1$ avec $k\in\mathbb{N}$.

Solution de 3 : Centrale – X-ENS : polynômes cyclotomiques et version faible du théorème de Dirichlet

1. $\mathbb{U}_n$ est un groupe à n. Les éléments de ce groupe ont un ordre divisant n et pour tout divisant n, les éléments du groupe $\mathbb{U}_n$ d'ordre d sont exactement ceux de $\mathbb{U}_d^*$. On en déduit que $\mathbb{U}_n$ est la réunion disjointe des $\mathbb{U}_d^*$ pour d parcourant les diviseurs de n. On en déduit $\boxed{X^n-1=\prod_{z\in\mathbb{U}_d}(X-z)=\prod_{d|n}\Phi_d.}$
2. Le polynôme Φ_n est de degré $\varphi(n)$ car les racines de l'unité d'ordre n sont les $\mathrm{e}^{2\mathrm{i}k\pi/n}$ avec $k\in[\![1,n]\!]$ et $k\wedge n=1$.
L'identité précédente donne la relation voulue en passant celle-ci au degré.
3. Par récurrence forte sur l'entier $n\geqslant 1$.
La propriété est immédiate quand $n=1$. Soit $n\geqslant 2$. Supposons la propriété vérifiée jusqu'au rang $n-1$. On a

$$X^n-1=\prod_{d|n,d\neq n}\Phi_d\times\Phi_n$$

Le polynôme X^n-1 est à coefficients entiers et $\prod_{d|n,d\neq n}\Phi_d$ l'est aussi. De plus, le coefficient dominant de ce dernier vaut 1. On réalisant une division euclidienne, le calcul de Φ_n détermine un polynôme à coefficients entiers.
4. (a) Soit p premier vérifiant l'hypothèse. Comme p divise $\Phi_n(a)$, il divise aussi a^n-1. Ainsi, l'ordre de $\overline{a}$ dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ divise n. Montrons que cet ordre est exactement n.
Si d divise n, $d<n$, on a dans $\mathbb{Z}/p\mathbb{Z}$

$$\overline{a}^d-1=\prod_{d'|d}\overline{\Phi_{d'}(a)}.$$

Or si d' divise d, d' divise aussi n et par hypothèse, $\overline{\Phi_{d'}(a)}\neq 0$.
Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, le produit de ces éléments non nuls est également non nul, si bien que $\overline{a}^d\neq 1$.
L'ordre de $\overline{a}$ est donc n.
Comme cet ordre divise $p-1$ d'après le théorème de Lagrange, p est de la forme $kn+1$ avec k entier.
(b) Raisonnons par l'absurde et supposons qu'il n'existe qu'un nombre fini d'entiers premiers congrus à 1 modulo n, soit $p_1,\dots,p_q$.
La question précédente, si on arrive à trouver a et p vérifiant les hypothèses, assure que p est congru à 1 modulo n.
Ce sera insuffisant pour aboutir à une contradiction, p pouvant être alors un des p_i.
Pour éviter cela, on va changer n en $N=np_1p_2\cdots p_q$.
Si p est congru à 1 modulo N, p ne peut être un des p_i et pourtant, il est congru à 1 modulo n.

Il faut donc trouver $a \in \mathbb{Z}$ et p premier, tels que p divise $\Phi_N(a)$, mais aucun des $\Phi_d(a)$ pour $d \mid N$, $d < N$.
On note $B = \prod_{d \mid N,\ d<N} \Phi_d$.
Le problème est donc de trouver $a \in \mathbb{Z}$ et p premier tels que p divise $\Phi_N(a)$ et ne divise pas $B(a)$.
Le polynôme B est premier avec Φ_N dans $\mathbb{C}[X]$ (en effet, ils sont scindés sur $\mathbb{C}$ et n'ont aucune racine commune), donc dans $\mathbb{Q}[X]$, puisque ces polynômes sont à coefficients rationnels et que le pgcd est invariant par extension de corps (l'algorithme d'Euclide s'écrit de la même manière dans $\mathbb{C}[X]$ et dans $\mathbb{Q}[X]$).
D'après le théorème de Bézout, il existe donc U et V dans $\mathbb{Q}[X]$ tels que

$$1 = U\Phi_N + VB.$$

Il existe $a \in \mathbb{Z}$ tel que $U_1 = aU$ et $V_1 = aV$ appartiennent à $\mathbb{Z}[X]$ (il suffit de prendre un multiple du ppcm des dénominateurs des cœfficients qui apparaissent dans U et V).
Comme $\Phi_N \neq 0$ et $\Phi_N \neq \pm 1$, on peut même choisir a tel que $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$, étant donné l'infinité de $a \in \mathbb{Z}$ vérifiant $aU \in \mathbb{Z}[X]$ et $aV \in \mathbb{Z}[X]$ (ceci en vue d'avoir des nombres premiers qui divisent $\Phi_N(a)$).
On a donc

$$a = U_1\Phi_N + V_1 B$$

et en particulier

$$a = U_1(a)\Phi_N(a) + V_1(a)B(a). \qquad (*)$$

Soit p un nombre premier qui divise $\Phi_N(a)$. Alors p divise $a^N - 1$, car Φ_N divise $X^N - 1$ dans $\mathbb{Z}[X]$.
Dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^N = 1$ et donc $\overline{a}$ est inversible, ce qui signifie que a est premier avec p.
Si p divisait $B(a)$, il diviserait a, d'après $(*)$, ce qui est exclu.
On est donc dans les hypothèses de la question précédente : p est congru à 1 modulo N, et donc modulo n, avec p forcément distinct des p_i, pour $1 \leqslant i \leqslant q$.
C'est la contradiction voulue.

4 Cyclicité du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$

Soit p un nombre premier.

1. Soit q un nombre premier qui divise $p-1$.
   Établir l'existence d'un élément de $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ d'ordre multiplicatif q.
   On pourra s'intéresser au polynôme $X^{\frac{p-1}{q}} - 1 \in \mathbb{F}_p[X]$.
2. Soit q un nombre premier et $\alpha \in \mathbb{N}^*$ tel que q^α divise $p-1$.
   Montrer l'existence d'un élément de $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ d'ordre q^α.
3. En déduire que $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est cyclique.

Solution de 4 : Cyclicité du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$

1. L'entier p étant premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps et $(\mathbb{Z}/p\mathbb{Z})^*$ est son groupe multiplicatif.
   Pour tout x dans $(\mathbb{Z}/p\mathbb{Z})^*$, notons $y_x = x^{\frac{p-1}{q}}$.
   On a alors, d'après le petit théorème de Fermat (ou le théorème d'Euler), $(y_x)^q = x^{p-1} = 1$.
   L'ordre de y_x divise donc q et puisque q est premier, il est donc égal à q ou à 1 .
   L'ordre de y_x n'est égal à 1 que si $y_x = 1$.
   Imaginons que cela soit le cas pour tout x dans $(\mathbb{Z}/p\mathbb{Z})^*$.
   Le polynôme $X^{\frac{p-1}{q}} - 1$ a alors au moins $p-1$ racines distinctes.
   C'est absurde, car son degré $\frac{p-1}{q}$ est strictement inférieur à $p-1$.
   Il existe donc $x \in (\mathbb{Z}/p\mathbb{Z})^*$ pour lequel $y_x \neq 1$.
   Cet élément y_x est d'ordre q.
2. Inspirons-nous de ce qui précède : pour tout x dans $(\mathbb{Z}/p\mathbb{Z})^*$, on pose maintenant $y_x = x^{\frac{p-1}{q^\alpha}}$.
   On a alors $(y_x)^{q^\alpha} = x^{p-1} = 1$.
   L'ordre de y_x divise donc q^α ; il est de la forme q^{r_x} avec $r_x \leqslant \alpha$.
   Supposons par l'absurde que que pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$, $r_x \leqslant \alpha - 1$.
   Alors pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$, $x^{\frac{p-1}{q}} = (y_x)^{q^{\alpha-1}} = 1$.
   On obtient comme dans la question précédente une contradiction.

On peut aussi effectuer un raisonnement direct : on considère le plus grand des entiers r_x pour x décrivant l'ensemble fini $(\mathbb{Z}/p\mathbb{Z})^*$; on le note r. On a $r \leqslant \alpha$.

On obtient $x^{\frac{p-1}{q^\alpha}q^r} = \left(y_x\right)^{q^r} = \left(\left(y_x\right)^{q^{r_x}}\right)^{q^{r-r_x}} = 1$, pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$.

Le polynôme $X^{\frac{p-1}{q^{\alpha-r}}} - 1$ a donc au moins $p-1$ racines distinctes.

Ce polynôme n'étant manifestement pas le polynôme nul, son degré doit être supérieur ou égal à $p-1$.

On a donc $\dfrac{p-1}{q^{\alpha-r}} = p-1$ et $\alpha = r$.

Étant donné la définition de r, il existe donc dans $(\mathbb{Z}/p\mathbb{Z})^*$ un élément d'ordre q^α.

3. On a classiquement que si G est un groupe abélien et x et y sont deux éléments de G d'ordre p et q respectivement, p et q étant premiers entre eux, alors l'ordre de xy est pq (vrai pour des ordres premiers entre eux plus généralement, voir exercice du cours sur les groupes).

   On établit par récurrence que, si $x_1, \ldots, x_r$ sont d'ordres respectifs $p_1, \ldots, p_r$, les p_i étant deux à deux premiers entre eux, l'ordre de leur produit $x_1 \cdots x_r$ est $p_1 \cdots p_r$.

   Décomposons donc $p-1$ en produit de facteurs premier $q_1^{\alpha_1} \ldots q_r^{\alpha_r}$, les q_i étant des entiers premiers et distincts deux à deux et les α_i des entiers naturels non nuls.

   D'après la question 2 , il existe, pour tout $1 \leqslant i \leqslant r$, un élément x_i de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $q_i^{a_i}$.

   Ainsi, le produit $x_1 \cdots x_r$ est d'ordre $q_1^{\alpha_1} \cdots q_r^{\alpha_r} = p-1$.

   Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ a donc un élément d'ordre $p-1 = |(\mathbb{Z}/p\mathbb{Z})^*|$: il est cyclique.