École Normale Supérieure, Année 2021-2022

1e année, Algèbre 1

TD n° 2 : Notes et corrections

Exercice 1.

Montrer que tout sous-groupe de type fini de $\mathbb{Q}$ est de la forme $\lambda\mathbb{Z} \subset \mathbb{Q}$ pour $\lambda \in \mathbb{Q}$.

Correction exercice 1

Soit $H \subset \mathbb{Q}$ un sous-groupe non-trivial de type fini noté additivement. Soit $\{\lambda_1, \dots, \lambda_r\} \subset H$ un ensemble fini de générateurs de H. Pour tout indice i, $\lambda_i \in \mathbb{Q}$ donc il existe $b_i \in \mathbb{N}$ tel que $b_i \cdot \lambda_i \in \mathbb{Z}$. Posons $b = b_1 \cdot b_r$ le produit des b_i, alors $b \cdot H \subset \mathbb{Z}$ puisque $b \cdot H$ est le sous-groupe de $\mathbb{Q}$ engendré par la partie $\{b \cdot \lambda_1, \dots, b \cdot \lambda_r\} \subset \mathbb{Z}$ ce qui en fait un sous-groupe de $\mathbb{Z}$. On connait les sous-groupes de $\mathbb{Z}$ qui sont monogènes : il existe $a \in \mathbb{Z}$ tel que $b \cdot H = a\mathbb{Z}$. Pour $\lambda = a/b$ on obtient que $\lambda \in H$ et finalement $H = \lambda\mathbb{Z} \subset \mathbb{Q}$.

Exercice 2.

Soient a et b des entiers avec $a, b \geqslant 3$. On pose $\zeta_n = e^{2i\pi/n}$ pour $n \geqslant 1$ et l'on considère les éléments A, B et $U(t)$ de $\mathrm{SL}_2(\mathbb{C})$ définis par

$$A \coloneqq \begin{bmatrix} \zeta_a & 0 \\ 0 & \zeta_a^{-1} \end{bmatrix}, \; B \coloneqq \begin{bmatrix} 0 & -1 \\ 1 & \zeta_b + \zeta_b^{-1} \end{bmatrix}, \; U(t) \coloneqq \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}.$$

1. Montrer que $C \in \mathrm{SL}_2(\mathbb{C})$ est d'ordre a si, et seulement si $\mathrm{tr}(C) = \zeta + \zeta^{-1}$ pour ζ une racine primitive a-ième de l'unité.
2. Montrer que A est d'ordre a, et que B est d'ordre b, dans le groupe $\mathrm{SL}_2(\mathbb{C})$.
3. On pose $B(t) \coloneqq U(t)BU(t)^{-1}$. Calculer la trace de $AB(t)$.
4. On suppose $c \geqslant 3$ entier, ou $c = \infty$. Montrer que pour t bien choisi, le produit $AB(t)$ est d'ordre c.
5. En travaillant dans $\mathbb{Z}/p\mathbb{Z}$ pour $p \equiv 1 \pmod{a}bc$ (avec p premier), à la place du corps $\mathbb{C}$, montrer que pour tous entiers $a, b, c \geqslant 3$, il existe un groupe fini possédant un élément d'ordre a, un autre d'ordre b, de produit d'ordre c.

Correction exercice 2

1. Remarquons que si C est d'ordre a il est annulé par le polynôme $P(X) = X^a - 1$ et ses valeurs propres sont des racines de l'unité $\zeta_1, \zeta_2 \in \mu_a(\mathbb{C})$. Comme $\zeta_1\zeta_2 = 1$, on pose $\zeta = \zeta_1$ et alors $\mathrm{tr}(C) = \zeta + \zeta^{-1}$. Finalement, l'ordre de ζ est l'ordre de C donc $\zeta \in \mu_a(\mathbb{C})$ est primitive. Réciproquement, si $\mathrm{tr}(C) = \zeta + \zeta^{-1}$, C est annulé par le polynôme $X^2 - (\zeta + \zeta^{-1})X + 1 = (X - \zeta)(X - \zeta^{-1})$ donc a fortiori annulé par le polynôme $X^a - 1 = \prod_{\xi \in \mu_a(\mathbb{C})}(X - \xi)$. Ainsi l'ordre de C divise a et puisque $\zeta \in \mu_a(\mathbb{C})$ est primitive, C est exactement d'ordre a.
2. D'après la question précédente c'est immédiat puisque $\mathrm{tr}(A) = \zeta_a + \zeta_a^{-1}$ et $\mathrm{tr}(B) = \zeta_b + \zeta_b^{-1}$.
3. Notons $A(t) = U(t)^{-1}AU(t)$, alors $\mathrm{tr}(AB(t)) = \mathrm{tr}(A(t)B)$. De plus $U(t) = (\mathrm{id}_2 + tE_{12})$ et $U(t)^{-1} = (\mathrm{id}_2 - tE_{12})$ donc $A(t) = A + t(\zeta_a - \zeta_a^{-1})E_{12}$ donc $\mathrm{tr}(A(t)B) = \mathrm{tr}(AB) + t(\zeta_a - \zeta_a^{-1})\mathrm{tr}(E_{12}B)$. Or $\mathrm{tr}(AB) = \zeta_a^{-1}(\zeta_b + \zeta_b^{-1})$ et $\mathrm{tr}(E_{12}B) = 1$ donc on obtient $\mathrm{tr}(AB(t)) = \zeta_a^{-1}(\zeta_b + \zeta_b^{-1}) + t(\zeta_a - \zeta_a^{-1})$.
4. L'application $t \mapsto \mathrm{tr}(AB(t))$ est affine en t et c'est donc une bijection de $\mathbb{C}$ dans $\mathbb{C}$. Ainsi pour tout $c \in \mathbb{N}$, soit ζ_c une racine primitive c-ième de l'unité alors il existe (un unique) $t_c \in \mathbb{C}$ tel que $\mathrm{tr}(AB(t_c) = \zeta_c + \zeta_c^{-1}$ et donc $AB(t_c)$ est d'ordre c d'après la première question. De plus, en posant par exemple $t_\infty = 0$ comme $\mathrm{tr}(AB(0)) \notin \mathbb{R}$, la trace de $AB(t_\infty)$ n'est pas somme de deux racines de l'unité conjuguées et donc n'est pas d'ordre fini. Ceci conclut.

Exercice 3. Le symbole de Legendre

Soient p un nombre premier impair et $a \in \mathbb{Z}$ premier à p.

1. En utilisant l'application $x \mapsto a/x$, montrer
$$(p-1)! \equiv -\left(\frac{a}{p}\right) a^{(p-1)/2} \pmod{p}.$$
2. En déduire
$$(p-1)! \equiv -1 \pmod{p} \text{ (théorème de Wilson)}, \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \text{ (congruence d'Euler)}.$$
3. Retrouver $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ pour tout $a, b \in \mathbb{Z}$.

Correction exercice 3

1. Posons $\Pi_p \in \mathbb{F}_p^\times$ tel que
$$\Pi_p = \prod_{x \in \mathbb{F}_p^\times} x \in \mathbb{F}_p^\times, \quad \text{i.e. } \Pi_p \equiv (p-1)! \pmod{p}.$$
On veut montrer $\Pi_p = -\left(\frac{a}{p}\right) a^{\frac{(p-1)}{2}}$.

Remarquons que $\iota_a \colon x \mapsto a/x$ est une involution de $\mathbb{F}_p^\times$. Si $x \in \mathbb{F}_p^\times$ est un point fixe de ι_a, alors $x^2 = a$ et réciproquement. Ainsi
$$\mathrm{Fix}(\iota_a) = \{x \in {\mathbb{F}_p}^\times \mid x^2 = a\}$$
Cette involution induit une partition de $\mathbb{F}_p^\times$. On sait décrire la partition donnée par une involution, elle est constituée de paires et de singletons où les singletons sont les points fixes de l'involution. On est emmené à distinguer deux cas, suivant que $|\mathrm{Fix}(\iota_a)| = 0$ ou 2.

- Le cas où a n'est pas un carré modulo p : $\boxed{\left(\frac{a}{p}\right) = -1}$: Dans ce cas $\mathrm{Fix}(\iota_a) = \emptyset$ et donc la partition induite par ι_a sur $\mathbb{F}_p^\times$ est uniquement constitué de paires de la forme $\{x, \frac{a}{x}\}$. On peut donc choisir une partie de représentants X tels que $\mathbb{F}_p^\times = X \sqcup \iota_a(X) = \bigsqcup_{x \in X} \{x, \frac{a}{x}\}$, en particulier $|X| = (p-1)/2$. On peut alors calculer Π_p :
$$\Pi_p = \prod_{x \in X} x \cdot \frac{a}{x} = a^{\frac{(p-1)}{2}} = -\left(\frac{a}{p}\right) a^{\frac{(p-1)}{2}}.$$
Ce qui conclut ce cas.
- Le cas où a est un carré modulo p : $\boxed{\left(\frac{a}{p}\right) = 1}$: Posons α tel que $\alpha^2 = a$, on a alors $\mathrm{Fix}(\iota_a) = \{\alpha, -\alpha\}$ dont le produit vaut $-a$. Soit $Y = \mathbb{F}_p^\times \setminus \{\alpha, -\alpha\}$, alors Y est stable par ι_a et la partition induite par ι_a est constitué de paires de la forme $\{y, \frac{a}{y}\}$. Comme dans le premier cas, on peut choisir une partie $X \subset Y$ telle que $Y = X \sqcup \iota_a(X) = \bigsqcup_{y \in X} \{y, \frac{a}{y}\}$ et en particulier $|X| = (p-3)/2$. On peut alors calculer Π_p :
$$\Pi_p = -a \cdot \prod_{y \in X} y \cdot \frac{a}{y} = -a \cdot a^{\frac{(p-3)}{2}} = -\left(\frac{a}{p}\right) a^{\frac{(p-1)}{2}}.$$
Ce qui termine la preuve.
2. On applique l'égalité précédente à $a \equiv 1 \pmod{p}$ pour obtenir que $(p-1)! \equiv -1 \pmod{p}$ puis on obtient que $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.
3. On peut conclure puisque $\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. On a ainsi obtenu que pour deux entiers qui ne sont pas des carrés modulo p leur produit est un carré modulo p.

Exercice 4.

Soit p un nombre premier.

1. Montrer que pour $p \equiv 1 \pmod 4$, et $x = \left(\frac{p-1}{2}\right)!$, on a $x^2 \equiv -1 \pmod p$.
2. En considérant le polynôme $X^2 + X + 1$, montrer que -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, on a $p \equiv 1 \pmod 3$ ou $p = 3$.
3. En déduire une condition nécessaire et suffisante sur p pour que 3 soit un carré dans $\mathbb{Z}/p\mathbb{Z}$.
4. *(Euler)* On suppose $p \equiv 1 \pmod 8$. En s'inspirant de l'écriture $\sqrt{2} = e^{2i\pi/8} + e^{-2i\pi/8}$ dans $\mathbb{C}$, montrer que 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Correction exercice 4

1. Soit $y \in \mathbb{Z}$ choisi tel que $x \cdot y = (p-1)! \in \mathbb{Z}$ i.e. $y = \frac{(p-1)!}{x} = (p-1) \cdot (p-2) \cdot \dots \cdot \frac{(p+3)}{2} \cdot \frac{(p+1)}{2}$. D'après Wilson, on a $(p-1)! \equiv -1 \pmod p$ et donc il suffit de montrer $y \equiv x \pmod p$ pour avoir $x^2 \equiv -1 \pmod p$. Or $(p-i) \equiv -i \pmod p$ pour tout $i \in \mathbb{Z}$ et donc

$$y \equiv \prod_{i=1}^{\frac{(p-1)}{2}} (p-i) \equiv \prod_{i=1}^{\frac{(p-1)}{2}} (-i) \equiv (-1)^{\frac{(p-1)}{2}} \prod_{i=1}^{\frac{(p-1)}{2}} i \equiv (-1)^{\frac{(p-1)}{2}} x \pmod p$$

   Mais comme $p \equiv 1 \pmod p$ on a $(-1)^{\frac{(p-1)}{2}} = 1$ et donc $x \equiv y \pmod p$ ce qui fini de montrer que x est une racine carré de -1 modulo p.
2. Remarquons que le polynôme $X^2 + X + 1$ est de discriminant -3. Donc le polynôme $X^3 - 1$ admet des racines non-triviales dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, -3 est un carré modulo p. Pour p=3 le résultat est clair, sinon il faut montrer que $\mathbb{Z}/p\mathbb{Z}$ contient une racine 3-ième de l'unité primitive ou bien $(\mathbb{Z}/p\mathbb{Z})^\times$ contient un élément d'ordre 3 si et seulement si $3 \mid (p-1)$ ce qui est bien le cas.
3. On veut calculer $\left(\frac{3}{p}\right)$. D'après la multiplicativité du symbole de Legendre établie à l'exercice précédent on a

$$\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{-3}{p}\right)$$

   et on vient de déterminer $\left(\frac{-3}{p}\right)$. Ainsi, comme 3 et 4 sont premiers entre eux, 3 est un carré modulo p si, et seulement si, $p \equiv 1, 6 \mod 12$.
4. Comme $8 \mid (p-1)$ le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ contient un élément d'ordre 8, ou en d'autres termes, le polynôme $X^4 + 1$ admet une racine. Notons ζ_8 l'une de ses racines et posons $\alpha = \zeta_8 + \zeta_8^{-1}$. Alors, remarquons que ζ_8^2 est une racine de -1 ce qui en fait l'opposé de son inverse i.e. $\zeta_8^{-1} = -\zeta_8$. Ainsi $\alpha^2 = 2$ et 2 est bien un carré modulo p si $p \equiv 1 \pmod 8$.

Exercice 13. Lemme chinois

Soit $n, m \in \mathbb{N}$ deux entiers premiers entre eux. Montrer que pour tout couple $(k_1, k_2) \in \mathbb{N}^2$ l'équation

$$\begin{cases} x \equiv k_1 \pmod n \\ x \equiv k_2 \pmod m, \end{cases}$$

admet une unique solution entière telle que $1 \leqslant x \leqslant nm$. En déduire un isomorphisme naturel d'anneaux $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/nm\mathbb{Z}$ puis montrer $\varphi(nm) = \varphi(m)\varphi(n)$ où $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Correction exercice 13

Posons l'application $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ donnée par la diagonale $x \mapsto (x \pmod n, x \pmod m)$. Remarquons qu'alors, comme $(n, m) = 1$, deux entiers sont dans la même classe modulo nm si, et seulement si, ils ont même image sous cette application, ce qui montre l'unicité.

On peut de plus factoriser l'application en $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, qui est une application injective entre ensembles de même cardinal donc une bijection.

Finalement, c'est un morphisme d'anneaux donc : c'est un isomorphisme de groupes additifs mais il induit aussi un isomorphisme $(\mathbb{Z}/nm\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ qui justifie que ϕ est bien multiplicative.

Exercice 14.

Le but de cet exercice est de déterminer, pour tout entier n, la structure du groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^\times$. L'isomorphisme de $(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ pour n et m deux entiers premiers entre eux nous permet de se ramener au cas $n = p^k$. En particulier, on veut montrer pour $k \geqslant 2$ un entier et p un nombre premier impair

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(p^k)\mathbb{Z} \text{ puis que } (\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^{k-2}\mathbb{Z}).$$

1. Montrer, sans utiliser le résultat, que $(\mathbb{Z}/187\mathbb{Z})^\times$ n'est pas cyclique puis qu'il est isomorphe au produit de deux groupes cycliques.
2. Montrer que $(\mathbb{Z}/p^k\mathbb{Z})^\times$ contient un élément[1] d'ordre $p-1$.
3. Montrer pour tout entier $k \geqslant 1$, $\forall a, b \in \mathbb{Z}$, $a \equiv b \pmod{p}^k \implies a^p \equiv b^p \pmod{p^{k+1}}$. En déduire l'ordre de $\overline{(1+p)} \in (\mathbb{Z}/p^k\mathbb{Z})^\times$.
4. Conclure si $p \neq 2$.
5. Traiter le cas[2] $p = 2$.
6. En guise d'application, déterminer les entiers $n \in \mathbb{N}$ tels que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Correction exercice 14

1. On remarque que $187 = 11 \cdot 17$ et donc d'après l'exercice précédent, $(\mathbb{Z}/187\mathbb{Z})^\times \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ qui n'est pas un groupe cyclique puisqu'il contient le groupe de Klein.
2. Comme $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ il contient un élément d'ordre $p-1$. Soit $\pi\colon \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la réduction modulo p^k. Comme c'est un morphisme d'anneaux on obtient $\pi^\times\colon (\mathbb{Z}/p^k\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ qui est surjectif puisque $1, 2, \ldots, p-1$ ont des images distinctes. On choisit $x_0 \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ tel que $\pi^\times(x_0)$ engendre $(\mathbb{Z}/p\mathbb{Z})^\times$. L'ordre de x_0 est donc divisible par $p-1$ mais divise aussi $\varphi(p^k)$: il est de la forme $p^i(p-1)$. Posons $x \coloneqq x_0^{p^i}$, alors x est d'ordre $(p-1)$.
3. Comme on a formellement[3] $p(X-Y) \mid [(X-Y)^p - (X^p - Y^p)]$ en déduit pour tout $a, b \in \mathbb{Z}$,

$$\frac{(a-b)^p - (a^p - b^p)}{p(a-b)} \in \mathbb{Z}.$$

   Ainsi, supposons que $a \equiv b \pmod{p}^k$, alors $p^{k+1} \mid p(a-b)$ et $p^{k+1} \mid (a-b)^p$ donc $p^{k+1} \mid (a^p - b^p)$ et on a bien ce qu'on voulait. On obtient une réciproque en remarquant que formellement $[(X-Y)^p - (X^p - Y^p)]$ n'est pas divisible par p^2.

   Supposons $p \neq 2$. On va montrer que la classe de $(1+p)$ est d'ordre p^k dans $(\mathbb{Z}/p^{k+1}\mathbb{Z})^\times$ pour $k \geqslant 1$. Par récurrence sur ce qui précède, comme $(1+p) \equiv 1 \pmod{p}$ on obtient $(1+p)^{p^k} \equiv 1 \pmod{p}^{k+1}$ donc son ordre divise p^k. Par la réciproque précédente on en déduit bien l'ordre de $(1+p)$.
4. Soit $y = x(1+p)$, comme on est dans un groupe abélien et que l'ordre de x et l'ordre de $1+p$ sont premiers entre eux on conclut que y est d'ordre $p^{k-1}(p-1)$. Ainsi, le sous-groupe engendré par y est du même cardinal que $(\mathbb{Z}/p^k\mathbb{Z})^\times$ ce qui en fait un groupe cyclique et $(\mathbb{Z}/p^k\mathbb{Z})^\times \xrightarrow{\sim} \mathbb{Z}/\varphi(p^k)\mathbb{Z}$ est donné par $y^k \mapsto k$.
5. On a bien $(\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$ engendré par les classes de 5 et -1. Pour $k \geqslant 3$ on montre comme précédemment que $5 \in (\mathbb{Z}/2^k\mathbb{Z})^\times$ est d'ordre 2^{k-2} puisque $5 \equiv 1 \pmod{4} \implies 5^{2^{k-2}} \equiv 1 \pmod{2}^k$, puis comme par la réduction $(\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/8\mathbb{Z})^\times \cong \langle\bar{5}\rangle \times \langle\overline{-1}\rangle$ on en déduit que -1 n'est pas dans le sous-groupe engendré par 5 ce qui nous permet de construire l'isomorphisme $(\mathbb{Z}/2^k\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z})$ donné par $(-1)^\epsilon 5^j \mapsto (\epsilon, j)$.
6. Remarquons que dans ls cas où on a $8 \mid n$, $p, q > 2$ premiers distincts tels que $pq \mid n$ le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique puisqu'il contient deux sous-groupes d'ordre 2. Cependant $(\mathbb{Z}/4\mathbb{Z})^\times$ est bien cyclique et $(\mathbb{Z}/2p^k\mathbb{Z})^\times \cong (\mathbb{Z}/p^k\mathbb{Z})^\times$ le sont aussi. Ainsi, $n \in \mathbb{N}$ est tel que $(\mathbb{Z}/n\mathbb{Z})^\times$ soit cyclique si et seulement si $n = 4$ ou bien s'il est de la forme p^k ou $2p^k$ pour p premier impair.

[1] *Indication* : On pourra considérer $a \in \mathbb{Z}$ dont la classe engendre $(\mathbb{Z}/p\mathbb{Z})^\times$
[2] *Indication* : Calculer l'ordre de $\overline{5} \in (\mathbb{Z}/2^k\mathbb{Z})^\times$ pour $k \geqslant 2$.
[3] Si la formulation est désagréable on peut la traduire en ajoutant $\forall X, Y \in \mathbb{Z}$ devant.