Devoir sur table n° 4

(corrigé)

Table des matières

1 Commentaires

Ce sujet est une adaptation de l'épreuve de Mathématiques de six heures du concours ENS (Paris et Lyon), année 2001, filière MP. Pour tenir compte de la durée de votre devoir, j'ai retranché huit questions sur les trente-quatre d'origine, et simplifié deux d'entre elles (les questions 4 et 5 qui étaient posées avec des endomorphismes quelconques) ; j'en ai certes rajouté, mais ce sont presque toutes des subdivisions de questions d'origine (donc elles ne rallongent pas le problème, au contraire : si l'épreuve initiale dure six heures, c'est parce que le temps de recherche sur certaines questions le mérite ; en rajoutant quelques questions intermédiaires, je raccourcis ce temps de réflexion).

Mon seul ajout réel est l'avant-dernière question, parce que je ne voulais pas que votre seule application de la loi de réciprocité quadratique soit aussi subtile ; surtout en fin d'épreuve où il n'y a plus beaucoup de temps pour réfléchir...

Vous avez vu en travaux dirigés que les nombres algébriques sur $\mathbb{Q}$ forment un corps. Ce sujet vous fait étudier le cas des *entiers* algébriques (ce sont des nombres algébriques avec la contrainte supplémentaire qu'ils doivent être annulés par un polynôme à coefficients entiers et unitaires). Ils forment un anneau noté $\mathcal{O}$, ou $\mathcal{O}_K$ si l'on considère uniquement les entiers algébriques d'un corps K de dimension finie sur $\mathbb{Q}$. Ce sont les « meilleurs » anneaux pour faire de l'arithmétique : d'abord, ils s'obtiennent très naturellement à partir de $\mathbb{Z}$, par simple adjonction de racines (ainsi obtient-on l'anneau $\mathbb{Z}[i]$ des entiers de Gauß), et ensuite il s'avère qu'ils sont souvent principaux, et même quand ils ne le sont pas : ce sont des anneaux de *Dedekind* (c'est-à-dire : tout *idéal* est un produit d'idéaux premiers ; c'est pour pallier l'absence de théorème fondamental de l'arithmétique dans ces anneaux, que les idéaux ont été historiquement introduits), et ils sont « presque » principaux (il existe un entier k tel que pour tout idéal, I^k soit principal, à une subtilité près que j'omets). C'est donc un moindre mal. Ils permirent de démontrer l'inexistence de solutions entières non triviales à l'équation de Fermat $x^n + y^n = z^n$ pour tout entier naturel entre 3 et 100, sauf 37, 59 et 67 (ces nombres premiers sont liés au cardinal de ce qu'on appelle le *groupe des classes d'idéaux*, qui mesure justement le défaut de principalité de l'anneau $\mathcal{O}_K$).

Pour montrer qu'ils forment un anneau, on adopte la même stratégie que pour le corps des nombres algébriques, avec néanmoins une complication du fait que l'on ne puisse pas utiliser la théorie de la dimension lorsqu'on remplace le corps $\mathbb{Q}$ par l'anneau $\mathbb{Z}$. C'est l'objet de la partie I (*Généralités*).

Étude des carrés modulo un nombre premier impair. On donne comme application arithmétique des anneaux $\mathcal{O}_K$ **la loi de réciprocité quadratique** (identité $(*)$ de l'énoncé). C'est l'un des résultats les plus importants de l'arithmétique moderne, même s'il est hélas difficile d'expliquer pourquoi dans le programme des classes préparatoires. Contentons-nous de l'observation quasiment triviale qu'il permet de déterminer extrêmement rapidement si un élément est un carré modulo p. Or c'est une préoccupation qui revient très souvent dans l'étude des équations diophantiennes, comme vous pouvez le voir en inspectant le regroupement thématique des exercices de travaux dirigés.

Cette loi de réciprocité quadratique nous dit quelque chose d'étonnant : si p ou q est congru à 1 modulo 4, alors p est un carré modulo q si et seulement si q est un carré modulo p. Si p et q sont congrus à 3 modulo 4, alors p est un carré modulo q si et seulement si q ne l'est pas modulo p. C'est étonnant parce qu'en principe, on n'a pas lieu de penser qu'il existe des interactions entre les classes modulo p et celles modulo q (c'est justement la difficulté de passer de $\mathbb{Z}/p\mathbb{Z}$ à $\mathbb{Z}/q\mathbb{Z}$ qui fait tout le sel des cent quatre-vingt-seize démonstrations recensées de cette identité).

Autre façon de comprendre pourquoi elle est étonnante : prenez un nombre premier p fixé. Notons $\left(\frac{p}{q}\right)$ l'entier valant 1 si p est un carré modulo q, et -1 si p n'est pas un carré modulo q (si $p = q$ alors il vaut 0). C'est le **symbole de Legendre**, qu'on distingue comme étant **l'unique caractère de** $(\mathbb{Z}/p\mathbb{Z})^\times$ **d'ordre** 2 (conséquence de la cyclicité du groupe par exemple). Alors on ne devrait pas s'attendre à ce que la suite $q \mapsto \left(\frac{p}{q}\right)$ soit spécialement régulière. Et pourtant il s'avère qu'elle a un comportement très prévisible d'après la loi de réciprocité quadratique : cela dépend exclusivement de la congruence de q modulo un certain entier. Par exemple, pour $q \mapsto \left(\frac{-1}{q}\right)$ et $q \mapsto \left(\frac{2}{q}\right)$, cela dépend exclusivement de la congruence de q modulo 4 et 8 respectivement : cela fait partie de ce qui est démontré dans le sujet.

Pour la démontrer, sans aller dans les détails de la philosophie de la démonstration, remarquons que ce qui fait la difficulté de la démonstration de $(*)$, c'est qu'on doit raisonner à la fois dans $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$, pour corréler les propriétés de p modulo q et q modulo p. Pour passer outre cette difficulté, on utilise un isomorphisme dont j'ai déjà parlé à quelques reprises, en précisant son intérêt : si G est un groupe commutatif fini, alors le groupe $\widehat{G}$ des caractères est isomorphe à G (on rappelle qu'un caractère de G est un morphisme de G dans $\mathbb{C}^*$). Ainsi il revient au même d'étudier G et $\widehat{G}$. Appliqué à $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$, l'intérêt est qu'en travaillant avec les caractères de $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$, et plus précisément leurs images, on se retrouve dans $\mathbb{C}$: dans cet ensemble, on peut volontiers faire interagir (par multiplication, somme, etc.), des caractères provenant de groupes différents. L'obstruction ci-dessus disparaît.

Les caractères semblent ne jamais apparaître dans ce problème. Et pourtant, ils apparaissent implicitement lorsqu'on étudie l'espace des fonctions de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}$ (il est engendré sur $\mathbb{C}$ par les caractères de $\mathbb{Z}/n\mathbb{Z}$, l'orthogonalité des caractères assurant même que c'en est une base orthogonale). Ils apparaissent dans la définition de φ, qui est la **transformation de Fourier** sur le groupe $\mathbb{Z}/n\mathbb{Z}$. En effet, quand x parcourt $\mathbb{Z}/n\mathbb{Z}$, les fonctions $y \mapsto (\zeta_n)^{xy}$ parcourent l'ensemble des caractères de $\mathbb{Z}/n\mathbb{Z}$ (explicités dans le devoir maison n^o 4).

Le calcul de ces sommes sur $\mathbb{Z}/n\mathbb{Z}$, et de la **somme de Gauß** $\tau_n = \sum_{k\in\mathbb{Z}/n\mathbb{Z}} \zeta^{k^2}$, est l'occasion d'illustrer l'emploi de différentes **permutations** de $\mathbb{Z}/n\mathbb{Z}$ pour permettre des simplifications qu'une indexation par $k \in [\![0, n-1]\!]$ ne permettrait pas aussi agréablement. Si vous avez buté là-dessus, vous vous devez d'accorder une attention toute particulière à la résolution des questions où elles apparaissent. C'est incontournable car de telles sommes apparaissent dans bien des considérations arithmétiques (comme la formule d'orthogonalité qui permet de dénombrer des solutions à des équations modulo p). Elles permettent de démontrer un cas particulier du **théorème de Kronecker-Weber** dans la question 21 : toute racine carrée d'entier est somme de racines de l'unité.

Un commentaire sur le calcul de $\left(\frac{2}{q}\right)$, qui est l'occasion de digressions riches sur l'importance des corps finis et de l'arithmétique hors de $\mathbb{Z}$. Une démonstration classique que 2 est un carré modulo q si et seulement si $q \equiv \pm 1 \bmod 8$ repose sur l'observation suivante : dans $\mathbb{C}$, une racine carrée de 2 s'écrit : $\sqrt{2} = 2\cos\left(\frac{\pi}{4}\right) = \omega + \omega^{-1}$, où ω est une racine huitième de l'unité. Cette identité peut se démontrer par des méthodes purement algébriques, sans passer par le cosinus ni l'exponentielle (essayer de le faire !). Comme je l'ai quelques fois dit dans les exercices de travaux dirigés : **quand une identité se démontre dans $\mathbb{R}$ ou $\mathbb{C}$ par des manipulations purement algébriques, on peut espérer qu'elle reste valable dans tout corps voire tout anneau** (éventuellement avec de bonnes hypothèses : commutativité, intégrité). Ainsi, pour fabriquer une racine carrée de 2 dans $\mathbb{Z}/p\mathbb{Z}$: on introduit ω tel que : $\omega^8 = 1$ (et d'ordre exactement 8). Comment être sûr qu'il en existe dans $\mathbb{Z}/p\mathbb{Z}$? Ce n'est pas forcément le cas, mais au pire on en crée une par adjonction de racine, de la

même manière qu'on construit $\mathbb{C}$ à partir de $\mathbb{R}$ par adjonction de racine. Ainsi ω vit dans un corps fini K contenant $\mathbb{Z}/p\mathbb{Z}$. Ceci étant dit, on vérifie que $z = \omega + \omega^{-1} \in K$ est effectivement une racine carrée de 2. Ensuite, il reste à se demander : est-ce que cette racine carrée est dans $\mathbb{Z}/p\mathbb{Z}$?

Pour cela : de la même manière qu'on vérifie qu'un nombre complexe est un réel en regardant s'il est égal à son conjugué, ou qu'on vérifie qu'un élément de $\mathbb{Q}[\sqrt{D}] = \left\{a + b\sqrt{D} \mid (a,b) \in \mathbb{Q}^2\right\}$ est rationnel en regardant s'il est fixé par l'automorphisme de conjugaison $a+b\sqrt{D} \mapsto a-b\sqrt{D}$ (voir la remarque de la question 8 puis celle de la question 11) : on montre qu'un élément $x \in K$ est dans $\mathbb{Z}/p\mathbb{Z}$ en regardant s'il est un point fixe de l'automorphisme de Frobenius $x \mapsto x^p$. C'est-à-dire, ici : on regarde si $z^p = z$. Pour simplifier $z^p = \omega^p + \omega^{-p}$, on utilise le fait que ω soit d'ordre 8, et on en déduit que 2 est un carré modulo p si et seulement si : $z^p = z$, si et seulement si : $p \equiv \pm 1 \bmod 8$. C'est effectivement ce que démontre la question 27 du sujet. C'est le calcul de z^p qui justifie la pertinence de vouloir écrire z en fonction de racines de l'unité.

Les corps finis n'étant pas au programme des classes préparatoires, le concepteur du sujet a trouvé un moyen ingénieux de contourner la difficulté. On l'a dit, on le reformule un peu autrement : l'idée est de raisonner par analogie avec la formule valable dans $\mathbb{C}$: on a $2i = (1+i)^2$, donc $\sqrt{2}$ s'exprime en fonction de $1+i$ (et d'une racine carrée de i). D'après ce qu'on raconte plus haut, il y a donc espoir qu'une racine carrée de 2 modulo q s'exprime aussi en fonction d'une racine carrée de -1, qui vit *a priori* dans un corps fini K contenant $\mathbb{Z}/q\mathbb{Z}$. Pour construire un corps fini K dans lequel il existe une racine carrée de -1, s'il n'en existe pas dans $\mathbb{Z}/q\mathbb{Z}$ (ce qui est le cas si et seulement si $q \equiv 3 \bmod 4$) on peut prendre : $K = \frac{\mathbb{Z}/q\mathbb{Z}[X]}{(X^2+1)\mathbb{Z}/q\mathbb{Z}[X]}$ (construction par analogie avec $\mathbb{C}$). Or le théorème d'isomorphisme permet de montrer que K est isomorphe à $\frac{\mathbb{Z}[X]/(X^2+1)\mathbb{Z}[X]}{q\mathbb{Z}[X]/(X^2+1)\mathbb{Z}[X]}$, c'est-à-dire à $\mathbb{Z}[i]/q\mathbb{Z}[i]$ (avec $i = \overline{X}$, qui vérifie bien : $i^2 + 1 = \overline{X^2+1} = \bar{0}$). Par conséquent : raisonner dans ce corps fini K, c'est comme raisonner dans $\mathbb{Z}[i]/q\mathbb{Z}[i]$, or toute égalité dans $\mathbb{Z}[i]/q\mathbb{Z}[i]$ provient d'une égalité dans $\mathbb{Z}[i]$: parfait, cet anneau rentre bien dans le cadre du programme ! Le calcul qu'on comptait faire initialement dans K n'a qu'à être fait dans $\mathbb{Z}[i]$ (en mettant de côté les multiples de q, de sorte que ce soit « la même chose que dans $\mathbb{Z}[i]/q\mathbb{Z}[i]$ »), et il devrait donner exactement la même chose (c'est le principe d'un isomorphisme). C'est l'idée des questions 26 et 27.

Je ne me lasse pas d'observer à quelles points les identités peuvent être universelles, tant qu'elles sont démontrées par des moyens purement algébriques. Finalement, le i complexe n'est guère différent d'une racine carrée de -1 dans une extension de $\mathbb{Z}/p\mathbb{Z}$, et $\sqrt{2}$ est intimement relié à une racine carrée de 2 modulo p (puisqu'on passe de l'un à l'autre *via* l'isomorphisme décrit ci-dessus), alors qu'*a priori* ce sont des objets de nature différente. Cet étonnement vient aussi de notre formation qui est d'abord analytique avant d'être algébrique : quand on voit $\sqrt{2}$ comme un zéro de $x \mapsto x^2 - 2$ ou un nombre approximativement égal à 1,4, et quand on voit les nombres complexes sous forme trigonométrique ou exponentielle, on en oublie qu'ils sont aussi des entités abstraites (presque) entièrement caractérisées par les équations qu'ils vérifient, et que ces équations ont un sens ailleurs que dans $\mathbb{R}$ ou $\mathbb{C}$.

Après ces développements très éthérés, revenons sur le plancher des vaches. Toute étude des carrés modulo p doit passer par les résultats suivants, vus dans ce devoir et que tout élève de MP* se doit IMPÉRATIVEMENT de savoir démontrer les yeux fermés :

- il y a $\dfrac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$;
- ils sont caractérisés par l'égalité : $x^{\frac{p-1}{2}} \equiv 1 \bmod p$, tandis que les non carrés vérifient : $x^{\frac{p-1}{2}} \equiv -1 \bmod p$;
- on en déduit que -1 est un carré modulo p si et seulement si : $p \equiv 1 \bmod 4$;
- comme : $\left(\dfrac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \bmod p$, et que le membre de droite est un morphisme de $(\mathbb{Z}/p\mathbb{Z})^\times$, il en est de même du symbole de Legendre (ce qui ne va pas de soi sinon) ; on en déduit notamment que **le produit de deux non carrés est un carré** (comme dans $\mathbb{R}$, mais pas comme dans $\mathbb{Q}$ par

exemple : cela n'est donc pas toujours valable et n'allait pas de soi), et **le produit d'un carré et d'un non carré est un non carré**.

Automorphismes de corps. La seconde partie du problème explicite les anneaux d'entiers algébriques les plus simples (hormis $\mathbb{Z}$), à savoir ceux d'un corps de dimension 2 sur $\mathbb{Q}$. Ce sont les entiers algébriques des **corps quadratiques**. Leur étude passe par l'explicitation des automorphismes de corps de $\mathbb{Q}[\sqrt{D}]$. Vous retiendrez du traitement de cette section :

— comment on explicite les automorphismes d'un corps (TRÈS IMPORTANT) ;

— l'identité $P(\sigma(x)) = \sigma(P(x))$ (avec P polynôme), et à quoi elle sert ;

— le fait que **les points fixes d'un automorphisme de corps caractérisent les éléments d'un sous-corps** (c'est proche de leur motivation historique, formulé en termes modernes).

Ce problème a ceci d'intéressant qu'il vous fait *utiliser* les automorphismes de corps (questions 8 et 11). On ne se contente pas de vous les faire expliciter comme si c'était une fin en soi. On s'étonnera qu'ils soient la clé pour expliciter les entiers algébriques d'un corps. C'est un enseignement de la **théorie de Galois**, qui généralise tout cela : quand on connaît tous les automorphismes d'un corps de nombres, on en connaît toute la substance arithmétique.

Ce qu'on retiendra en bref. Condition nécessaire et suffisante pour être un carré modulo p. Nombre de carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Condition nécessaire et suffisante pour que $\mathbb{Q}[\zeta]$ soit un corps, soit de dimension finie sur $\mathbb{Q}$. Construction des automorphismes de corps de $\mathbb{Q}[\sqrt{D}]$. Caractérisation des points fixes d'un automorphisme de corps. Image d'une racine d'un polynôme par un automorphisme de corps. Calculs de sommes indexées par un groupe fini par changement d'indice. Transformation et inversion de Fourier sur $\mathbb{Z}/n\mathbb{Z}$. Initiation à la réduction des endomorphismes. Loi de réciprocité quadratique.

Questions faciles ou classiques à retravailler

— GÉNÉRALITÉS : toutes les questions ;

— PREMIÈRE PARTIE : questions 3 et 6 ;

— DEUXIÈME PARTIE : questions 7 et 11 ;

— TROISIÈME PARTIE : questions 13 et 15, questions 16 et 17 (à refaire après avoir vu la réduction des endomorphismes) ;

— QUATRIÈME PARTIE : questions 22 à 24.

2 Corrigé

Préliminaires

1. Soit π le produit à calculer. On nous indique de regrouper les termes x et yx^{-1} dans le produit. Mais pour cela, encore faut-il qu'ils soient distincts. On a : $x \neq yx^{-1}$, si et seulement si : $x^2 \neq y$. Par conséquent, si y n'est pas un carré, on peut toujours regrouper les termes x et yx^{-1}. Dans le cas contraire, il faut faire un peu attention :

   — si y n'est pas un carré : les $p-1$ facteurs du produit se regroupent en $(p-1)/2$ couples $x \cdot (yx^{-1}) = y$ et on a : $\pi = y^{(p-1)/2}$;

   — si y est un carré, alors il existe $a \in \mathbb{Z}/p\mathbb{Z}$ tel que : $y = a^2 = (-a)^2$, et seuls a et $-a$ sont racines carrées de y par intégrité de $\mathbb{Z}/p\mathbb{Z}$; en effet, pour tout $x \neq \pm a$ on a : $x^2 - y = x^2 - a^2 = (x-a)(x+a) \neq \bar{0}$; de plus : $a \neq -a$, car a est non nul et p est impair, donc les $p-3$ facteurs de π autres que a et $-a$ se regroupent deux par deux en couples dont le produit égale y, et on obtient : $\pi = y^{(p-3)/2}a(-a) = -y^{(p-1)/2}$.

   D'où le résultat.

Questions à se poser, réflexes à acquérir. Pourquoi, au moment d'affirmer que $a \neq -a$, préciser que p est impair ?

2. En appliquant la question précédente avec $y = \bar{1} = \bar{1}^2$, qui est un carré, on a : $\bar{1} = \bar{1}^{(p-1)/2} = -\pi$. Maintenant, pour y quelconque, on sait d'après la question précédente que : $y^{(p-1)/2} = -\pi = \bar{1}$ si y est un carré, et $y^{(p-1)/2} = \pi = -\bar{1}$ sinon : d'où le résultat.

Remarque. Comme : $\pi = \overline{(p-1)!}$, on a implicitement démontré le théorème de Wilson.

Remarque. Cette égalité permet de démontrer qu'il y a exactement $\frac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$ (et donc $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$). En effet, les carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$ sont exactement les racines de $X^{\frac{p-1}{2}} - \bar{1}$. Or ce polynôme est scindé à racines simples, puisqu'il divise le polynôme $X^{p-1} - \bar{1}$ (en vertu de l'identité remarquable : $X^{p-1} - \bar{1} = (X^{\frac{p-1}{2}} - \bar{1})(X^{\frac{p-1}{2}} + \bar{1})$) qui est lui-même scindé à racines simples. En effet, par le petit théorème de Fermat, toute classe de $(\mathbb{Z}/p\mathbb{Z})^\times$ est racine de ce polynôme, ce qui lui fait exactement $p-1$ racines.

En résumé : $X^{\frac{p-1}{2}} - \bar{1}$ est scindé et à racines simples, donc il admet exactement $\frac{p-1}{2}$ racines, qui s'avèrent être les carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ d'après le résultat de cette question : il y a donc $\frac{p-1}{2}$ carrés.

On peut aussi montrer qu'il y a $\frac{p-1}{2}$ solutions de l'équation $y^{\frac{p-1}{2}} = \bar{1}$ grâce à la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$: ce sont exactement les éléments de l'unique sous-groupe de cardinal $\frac{p-1}{2}$.

Remarque. Le résultat de cette question se démontre souvent autrement : on montre que l'ensemble des carrés est inclus dans l'ensemble des racines de $X^{\frac{p-1}{2}} - \bar{1}$, en écrivant que si : $y = x^2$, avec $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, alors par le petit théorème de Fermat on a : $y^{\frac{p-1}{2}} = x^{p-1} = \bar{1}$. C'est ensuite un argument de cardinalité qui permet d'avoir l'égalité entre ces deux ensembles (et donc l'équivalence : $y^{\frac{p-1}{2}} = \bar{1} \iff y$ est un carré ; dans le cas contraire, l'égalité $y^{p-1} = \bar{1}$ et l'intégrité de $\mathbb{Z}/p\mathbb{Z}$ impliquent $y^{\frac{p-1}{2}} = -\bar{1}$). Pour estimer le cardinal de l'ensemble des carrés, on utilise le théorème d'isomorphisme pour avoir le cardinal de l'image du morphisme $x \mapsto x^2$, dont le noyau a deux éléments : $\bar{1}$ et $-\bar{1}$. On en déduit qu'il y a $\frac{p-1}{2}$ carrés. Pour le cardinal de l'ensemble des racines de $X^{\frac{p-1}{2}} - \bar{1}$: on utilise le fait qu'il soit borné par le degré du polynôme, d'où le résultat.

Questions à se poser, réflexes à acquérir. Retenir votre démonstration préférée de ce résultat classique, ainsi que du nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$ (qui est déjà apparu dans votre devoir précédent !).

Première partie – Généralités

3. Supposons (i). Soit $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{Q}[X]$ un polynôme unitaire annulant ζ. Nous allons montrer que $\mathbb{Q}[\zeta]$ est engendré par la famille $(\zeta^0, \dots, \zeta^{n-1})$. Soit $z \in \mathbb{Q}[\zeta]$. Il existe $A \in \mathbb{Q}[X]$ tel que : $z = A(\zeta)$. Effectuons la division euclidienne de A par P : il existe $(Q, R) \in \mathbb{Q}[X]^2$ tel que : $A = PQ + R$, avec : $\deg(R) < \deg(P)$, c'est-à-dire : $\deg(R) \leqslant n-1$. Alors, en évaluant cette égalité en ζ, on a : $A(\zeta) = R(\zeta) \in \mathrm{Vect}_{\mathbb{Q}}(\zeta^0, \dots, \zeta^{n-1})$. D'où : $\mathbb{Q}[\zeta] \subseteq \mathrm{Vect}_{\mathbb{Q}}(\zeta^0, \dots, \zeta^{n-1})$. Puisque $\mathbb{Q}[\zeta]$ est inclus dans un $\mathbb{Q}$-espace vectoriel de dimension finie, il est lui-même de dimension finie (et d'ailleurs, l'inclusion réciproque est triviale).

Il reste à prouver que tout élément z non nul de $\mathbb{Q}[\zeta]$ admet un inverse multiplicatif dans $\mathbb{Q}[\zeta]$. Or l'application $y \mapsto zy$ est un endomorphisme de $\mathbb{Q}[\zeta]$ (puisque $\mathbb{Q}[\zeta]$ est un anneau contenant z), injectif par intégrité de $\mathbb{Q}[\zeta]$, donc surjectif puisque c'est un endomorphisme d'un espace vectoriel de dimension finie. Par conséquent il existe $y \in \mathbb{Q}[\zeta]$ tel que : $zy = 1$, c'est-à-dire : $z^{-1} = y \in \mathbb{Q}[\zeta]$. Ainsi $\mathbb{Q}[\zeta]$ est un sous-corps de $\mathbb{C}$ de dimension finie sur $\mathbb{Q}$: c'est un corps de nombres. On a montré que (i) implique (ii).

Réciproquement, supposons (ii). Si d est la dimension de $\mathbb{Q}[\zeta]$, alors la famille $(1, \zeta, \dots, \zeta^d)$ est $\mathbb{Q}$-liée puisqu'elle possède $d+1$ éléments : il existe donc $(a_0, \dots, a_d) \in \mathbb{Q}^{d+1}$ non nul tel que : $\sum_{i=0}^{d} a_i \zeta^i = 0$. Par conséquent $P = \sum_{i=0}^{d} a_i X^i$ est non nul et admet ζ pour racine ; quitte à le diviser

par son coefficient dominant (qui n'est *a priori* pas a_d, mais ce n'est pas gênant), il est unitaire et annule toujours ζ : d'où le résultat, (ii) implique (i).

On a bien démontré l'équivalence.

Remarque. Si on veut obtenir la dimension de $\mathbb{Q}[\zeta]$, il nous faut une base dans la construction ci-dessus. On y parvient si l'on remplace P par le polynôme minimal de ζ sur $\mathbb{Q}$.

Autre démonstration que $\mathbb{Q}[\zeta]$ est un corps si l'on a (i). Une autre démonstration que $\mathbb{Q}[\zeta]$ est un corps de nombres passe par le polynôme minimal et une relation de Bézout. Vous remarquerez l'analogie avec le calcul d'inverse dans $\mathbb{Z}/p\mathbb{Z}$. Soit π_ζ le polynôme minimal de ζ sur $\mathbb{Q}$. Il existe par hypothèse. Soit $z \in \mathbb{Q}[\zeta]$ non nul. Il existe $A \in \mathbb{Q}[X]$ tel que : $z = A(\zeta)$. Comme z est supposé non nul, A n'admet pas ζ pour racine, donc π_ζ ne divise pas A. Comme π_ζ est irréductible, cela assure que π_ζ et A n'ont pas de diviseur irréductible en commun, donc ils sont premiers entre eux : par le théorème de Bézout, il existe $(U, V) \in \mathbb{Q}[X]^2$ tel que : $U\pi_\zeta + VA = 1$. En évaluant en ζ, on obtient : $V(\zeta)A(\zeta) = 1$, d'où : $z^{-1} = A(\zeta)^{-1} = V(\zeta) \in \mathbb{Q}[\zeta]$. Ce qu'il fallait démontrer.

Autre démonstration du sens réciproque. Le cas $\zeta = 0$ est trivial, puisque le polynôme $P = X$ est un annulateur unitaire à coefficients rationnels qui annule 0 (et $\mathbb{Q}[0] = \mathbb{Q}$ est un corps de nombres). Supposons donc : $\zeta \neq 0$. Alors : $\zeta^{-1} \in \mathbb{Q}[\zeta]$, donc il existe $n \in \mathbb{N}$ et $(a_0, \dots, a_n) \in \mathbb{Q}^{n+1}$ tels que : $\zeta^{-1} = a_0\zeta^0 + \cdots + a_n\zeta^n$. Quitte à diminuer n on peut supposer : $a_n \neq 0$, car : $\zeta^{-1} \neq 0$. Alors $P = X^{n+1} + \dfrac{a_{n-1}}{a_n}X^n + \cdots + \dfrac{a_0}{a_n}X - \dfrac{1}{a_n}$ est un polynôme annulateur de ζ, unitaire et à coefficients rationnels.

Questions à se poser, réflexes à acquérir.

- Lorsque je démontre l'inversibilité par le théorème de Bézout, pourquoi dois-je prendre π_z et ne peux pas me contenter du P introduit en début de résolution ?
- Quel intérêt a la démonstration de l'inversibilité *via* le théorème de Bézout ?
- Pourquoi faut-il remplacer P par le polynôme minimal si l'on veut obtenir une base de $\mathbb{Q}[\zeta]$? Quelle est alors sa dimension ?
- La démonstration de l'inversibilité *via* l'étude de $y \mapsto yz$ ne vous rappelle-t-elle pas des souvenirs ? Peut-elle se généraliser à d'autres circonstances ?
- Je propose deux démonstrations du sens réciproque : qu'apporte l'une par rapport à l'autre ?
- Dans la démonstration du sens réciproque : le polynôme proposé peut-il être de degré $d-1$?

4. On a aisément, par récurrence : $\forall k \in \mathbb{N}$, $m_{x^k} = (m_x)^k$, or la famille $\left(X^k\right)_{k\in\mathbb{N}}$ engendre $\mathbb{Q}[X]$ sur $\mathbb{Q}$ et l'application $x \mapsto m_x$ est $\mathbb{Q}$-linéaire, donc : $\forall P \in \mathbb{Q}[X]$, $m_{P(x)} = P(m_x)$. Il est alors évident que (i) équivaut à (ii) (en effet m_x est l'endomorphisme nul si et seulement si $x = 0$, par intégrité de K).

Montrons que (ii) implique (iii). Supposons que m_x admet un annulateur unitaire à coefficients entiers. On peut alors écrire, en isolant le coefficient dominant dans une relation de dépendance algébrique : $(m_x)^k = \sum_{i=0}^{k-1} a_i(m_x)^i$, avec $(a_i)_{0\leqslant i\leqslant k-1} \in \mathbb{Z}^k$. Soient $(u_1, \dots, u_p)$ une famille $\mathbb{Q}$-génératrice de K, et $u_{i,j} = (m_x)^j(u_i)$ pour tous $i \in [\![1, p]\!]$ et $j \in [\![0, k-1]\!]$. Justifions que $W = \sum_{i=1}^{p}\sum_{j=0}^{k-1} \mathbb{Z}u_{i,j}$ est stable par m_x : comme c'est un morphisme de groupes, il suffit de vérifier la stabilité sur la partie génératrice $(u_{i,j})_{\substack{1\leqslant i\leqslant p\\ 0\leqslant j\leqslant k-1}}$, et c'est alors immédiat :

$$\forall i \in [\![1, p]\!],\ \forall j \in [\![0, k-2]\!],\ m_x\left(u_{i,j}\right) = (m_x)^{j+1}(u_i) = u_{i,j+1} \in W,$$

et pour $j = k-1$ on a :

$$\forall i \in [\![1, p]\!],\ m_x\left(u_{i,k-1}\right) = (m_x)^k(u_i) = \sum_{\ell=0}^{k-1} a_\ell(m_x)^\ell(u_i) = \sum_{i=0}^{k-1} a_\ell u_{i,\ell} \in W.$$

D'où le résultat : W est stable par m_x et la famille $(u_{i,j})_{\substack{1\leqslant i\leqslant p\\ 0\leqslant j\leqslant k-1}}$ engendre K car elle contient $(u_1,\dots,u_p)$, donc (ii) implique (iii).
Enfin, montrons que (iii) implique (i). Soit $(v_1,\dots,v_n)$ une famille $\mathbb{Q}$-génératrice de K telle que : $m_x\left(\sum_{i=1}^n \mathbb{Z}v_i\right)\subseteq\sum_{i=1}^n \mathbb{Z}v_i$. En particulier, pour tout $i\in[\![1,n]\!]$, on a : $v_ix=m_x(v_i)\in\sum_{i=1}^n\mathbb{Z}v_i$, donc pour tout $i\in[\![1,n]\!]$ il existe $(a_{i,j})_{1\leqslant j\leqslant n}\in\mathbb{Z}^n$ tel que : $v_ix=\sum_{j=1}^n a_{i,j}v_j$. On a donc :

$$\begin{cases} 0 &= (x-a_{1,1})v_1 - a_{1,2}v_2 - \cdots - a_{1,n}v_n,\\ 0 &= -a_{2,1}v_1 + (x-a_{2,2})v_2 - \cdots - a_{2,n}v_n,\\ \vdots & \vdots \qquad\qquad \vdots\\ 0 &= -a_{n,1}v_1 - a_{n,2}v_2 - \cdots + (x-a_{n,n})v_n, \end{cases}$$

ou encore, en posant : $A=((a_{i,j}))_{1\leqslant i,j\leqslant n}$ et : $V=\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}$, on a : $(x\mathrm{I}_n-A)V=0_{\mathrm{M}_{n,1}(\mathbb{Q})}$.
C'est un système linéaire admettant une solution non triviale V (elle est non triviale puisque $(v_1,\dots,v_n)$ engendre K sur $\mathbb{Q}$). Son déterminant est donc nul. Or, si l'on note $a'_{i,j}=x\delta_{i,j}-a_{i,j}$, alors :

$$\det(x\mathrm{I}_n-A)=\sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{i=1}^n a'_{i,\sigma(i)}$$

est une somme d'éléments de $\mathbb{Z}[x]$, donc c'est un polynôme en x, unitaire puisque son terme de plus haut degré (qui vaut n) correspond au produit des coefficients diagonaux, c'est-à-dire à $\sigma=\mathrm{id}$, et vaut : $\prod_{i=1}^n(x-a_{i,i})$, qui est bien unitaire ; les autres permutations donnent un terme de degré au plus $n-2$ (puisqu'une permutation non triviale ne peut pas fixer exactement $n-1$ points) et cela n'affecte pas le coefficient en facteur de x^n.
D'où le résultat : si l'on pose $P=\det(X\mathrm{I}_n-A)$, alors $P\in\mathbb{Z}[X]$ est unitaire, et on a : $P(x)=0$. Donc (iii) implique (i).
Puisque (i) implique (ii), (ii) implique (iii) et (iii) implique (i), on a montré l'équivalence des trois propositions.

Remarque. J'ai implicitement calculé un polynôme caractéristique et utilisé le théorème de Cayley-Hamilton (ou plutôt : je l'ai démontré dans un cas particulier). Son usage ne se borne donc pas à la réduction des endomorphismes, et c'est normal : son application la plus évidente est qu'elle fournit des polynômes annulateurs explicites pour tout endomorphisme de dimension finie. C'est là qu'on comprend pourquoi on vous fait reformuler la propriété d'être un entier algébrique à l'aide d'un endomorphisme.

Questions à se poser, réflexes à acquérir.

- Vérifier si besoin ce que je n'ai pas détaillé, pour l'équivalence entre (i) et (ii). Bien noter, comme souvent, l'économie rédactionnelle à raisonner sur une base ou une famille génératrice.
- Comprendre comment fut construite la famille lorsqu'on voulut montrer que (ii) implique (iii). Une façon de le comprendre : si $(v_1,\dots,v_n)$ convient, ce doit être stable par m_x et donc aussi par $(m_x)^k$ pour tout k ; songer à une famille qui assure cela.
- Se convaincre que la stabilité se résume à une vérification sur une partie génératrice.
- Pourquoi une famille génératrice doit être non nulle ici ?
- Songer, plus tard, à un autre contexte d'algèbre linéaire où l'on vous fait étudier des polynômes et leurs racines *via* le polynôme caractéristique de matrices adéquates. Ce n'est donc pas une idée neuve.
- Vérifier ce que j'ai omis concernant $\det(x\mathrm{I}_n-A)$.
- Pourquoi la notation $\det(X\mathrm{I}_n-A)$, avec l'indéterminée dans le déterminant, est-elle licite ?

5. On choisit une famille $(v_1, \dots, v_n)$ adaptée à m_x (c'est-à-dire telle que $(v_1, \dots, v_n)$ engendre le $\mathbb{Q}$-espace vectoriel K et tel que $\sum_{i=1}^{n} v_i\mathbb{Z}$ soit stable par m_x ; une telle famille existe par la question précédente). Soit par ailleurs : $y^p = \sum_{i=0}^{p-1} a_i y^i$ une relation de dépendance entre les puissances de y à coefficients entiers. On note $v_{i,j} = v_i y^j$ pour tous $i \in [\![1, n]\!]$ et $j \in [\![0, p-1]\!]$ et on considère la famille $(v_{i,j})_{\substack{1\leqslant i\leqslant n\\ 0\leqslant j\leqslant p-1}}$ qui engendre K sur $\mathbb{Q}$ (puisqu'elle contient la famille génératrice $(v_i)_{1\leqslant i\leqslant n}$). Notons : $W = \sum_{i=1}^{n} \mathbb{Z}v_i$. Le sous-groupe que $(v_{i,j})_{\substack{1\leqslant i\leqslant n\\ 0\leqslant j\leqslant p-1}}$ engendre est :

$$X = \sum_{j=0}^{p-1}\sum_{i=1}^{n} \mathbb{Z}v_i y^j = \sum_{j=0}^{p-1} (m_y)^j(W).$$

On va montrer que X est stable par m_x et m_y. Le sous-groupe W est stable par m_x par construction, et donc :

$$m_x(X) = \sum_{j=0}^{p-1} m_x \circ (m_y)^j(W) = \sum_{j=0}^{p-1} m_{xy^j}(W) = \sum_{j=0}^{p-1} (m_y)^j \circ m_x(W) \subseteq \sum_{j=0}^{p-1} (m_y)^j(W) = X,$$

donc X est stable par m_x. Par ailleurs on a : $(m_y)^p = \sum_{i=0}^{p-1} a_i (m_y)^i$, donc : $(m_y)^p(W) \subseteq \sum_{i=0}^{p-1} a_i (m_y)^i(W)$, et on en déduit :

$$m_y(X) = \sum_{j=1}^{p-1} (m_y)^j(W) + (m_y)^p(W) \subseteq \sum_{j=0}^{p-1} (m_y)^j(W) = X,$$

Donc X est stable par m_y aussi. La famille $(v_{i,j})_{\substack{1\leqslant i\leqslant n\\ 0\leqslant j\leqslant p-1}}$ est donc adaptée à la fois à m_x et à m_y. On alors :

$$m_{x+y}(X) = (m_x + m_y)(X) \subseteq X, \quad \text{et :} \quad m_{xy}(X) = (m_x \circ m_y)(X) \subseteq X,$$

ce qui prouve que $x + y$ et xy sont des entiers algébriques.

Questions à se poser, réflexes à acquérir.

— Comme dans la question 4, pouvait-on montrer la stabilité de X en raisonnant uniquement sur une partie génératrice ?

— Comprendre ce qui a motivé la définition de la famille $(v_{i,j})_{i,j}$ qui convient à la fois pour m_x et m_y. Une piste potentielle : revoir comment on démontre que l'ensemble des *nombres* algébriques est un corps. On rappelle que dans les grandes lignes, cela revient à inclure $\mathbb{Q}[x + y]$ et $\mathbb{Q}[xy]$, pour x et y algébriques, dans $\mathbb{Q}[x][y]$ qui est de dimension finie sur $\mathbb{Q}$; mais comment construit-on une partie génératrice de $\mathbb{Q}[x][y]$?

6. L'inclusion $\mathbb{Z} \subseteq \mathcal{O}_K \cap \mathbb{Q}$ est facile : il suffit de montrer que $\mathbb{Z}$ est inclus dans $\mathcal{O}_K$, ce qui est le cas puisqu'un entier n est annulé par le polynôme unitaire à coefficients entiers $X - n$ (on peut aussi utiliser le fait qu'un sous-anneau de $\mathbb{C}$ doive contenir $\mathbb{Z}$ qui est son plus petit sous-anneau). Justifions donc l'inclusion réciproque : soit $x \in \mathcal{O}_K \cap \mathbb{Q}$. Comme $x \in \mathbb{Q}$, il existe p et q premiers entre eux tels que : $x = \frac{p}{q}$, et comme $x \in \mathcal{O}_K$ il existe $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{Z}[X]$ tel que : $P(x) = 0$. En multipliant cette égalité par q^n, on obtient :

$$p^n + \sum_{i=0}^{n-1} a_i p^i q^{n-i} = 0.$$

En réduisant modulo q, on a : $p^n \equiv 0 \bmod q$, donc q divise p^n. Or q et p sont premiers entre eux, donc : $q \in \{1, -1\}$, et : $x = \pm p \in \mathbb{Z}$. D'où : $\mathcal{O}_K \cap \mathbb{Q} \subseteq \mathbb{Z}$, ce qui démontre l'égalité voulue.

Questions à se poser, réflexes à acquérir.

— J'affirme ci-dessus qu'un sous-anneau de $\mathbb{C}$ doit contenir $\mathbb{Z}$. Pourquoi ? Et si ce n'est pas un sous-anneau de $\mathbb{C}$, quelles sont les possibilités pour le plus petit sous-anneau ?

— Pourquoi cette idée de multiplier l'égalité $P(x) = 0$ par q^n ? Quel raisonnement aurait été impossible sans cela ?

— Cette démonstration a un intérêt *pratique* : pourquoi permet-elle de déterminer les racines rationnelles de P (même non unitaire), ou de démontrer qu'il n'y en a pas ?

Deuxième partie – Entiers des corps quadratiques

7. On vérifie sans peine que σ ainsi défini est bien un isomorphisme de corps. En effet, soit $(a, b, a', b') \in \mathbb{Q}^4$. On a :

$$\sigma((a + b\sqrt{d})(a' + b'\sqrt{d})) = \sigma\left(aa' + bb'd + (ab' + a'b)\sqrt{d}\right) = (aa' + bb'd) - (ab' + a'b)\sqrt{d},$$

et :

$$\sigma(a+b\sqrt{d})\sigma(a'+b'\sqrt{d}) = (a-b\sqrt{d})(a'-b'\sqrt{d}) = aa'+bb'd-(ab'+a'b)\sqrt{d} = \sigma((a+b\sqrt{d})(a'+b'\sqrt{d})),$$

donc σ commute avec la multiplication et sa $\mathbb{Q}$-linéarité ne pose aucune difficulté. C'est un automorphisme, de réciproque lui-même, puisque : $\sigma^2 = \mathrm{Id}_{\mathbb{Q}[\sqrt{D}]}$. Encore plus trivialement, $\mathrm{Id}_{\mathbb{Q}[\sqrt{D}]}$ est aussi un automorphisme de corps.

Il s'agit de montrer qu'il n'y en a pas d'autre. Considérons un isomorphisme quelconque f du corps $\mathbb{Q}[\sqrt{D}]$. Alors l'ensemble des $x \in K$ tels que $f(x) = x$ est un sous-corps de K, donc il contient $\mathbb{Q}$ et on en déduit : $\forall a \in \mathbb{Q}$, $f(a) = a$, ce qui assure que f est $\mathbb{Q}$-linéaire.

On a aussi : $f(\sqrt{D})^2 = f(\sqrt{D}^2) = f(D) = D$, donc : $f(\sqrt{D}) \in \{\sqrt{D}, -\sqrt{D}\}$. Ainsi f coïncide soit avec Id, soit avec σ, sur la $\mathbb{Q}$-base $(1, \sqrt{D})$ et donc, par $\mathbb{Q}$-linéarité : $f = \mathrm{Id}_{\mathbb{Q}[\sqrt{D}]}$, ou : $f = \sigma$. D'où le résultat.

Remarque. En vérité, après avoir montré qu'il s'agit d'un morphisme de corps, vérifier qu'il s'agit d'un automorphisme est superflu : un morphisme de corps est toujours injectif, et puisqu'il est en plus $\mathbb{Q}$-linéaire entre deux espaces vectoriels de même dimension finie, il est bijectif.

Remarque. En utilisant le fait que $\mathbb{Q}[\sqrt{D}] = \left\{P(\sqrt{D}) \mid P \in \mathbb{Q}[X]\right\}$, on peut démontrer que $\sigma : P(\sqrt{D}) \mapsto P(-\sqrt{D})$ est un morphisme sans le moindre effort, en écrivant par exemple : $\sigma(P(\sqrt{D}))\sigma(Q(\sqrt{D})) = P(-\sqrt{D})Q(-\sqrt{D}) = (PQ)(-\sqrt{D})$. C'est surtout avantageux lorsqu'on est dans un corps de dimension plus grande que 2 (imaginez faire les mêmes calculs que ci-dessus avec une combinaison linéaire de n puissances de ζ à la place de $a + b\sqrt{d}$). Il y a cependant une subtilité à vérifier : le fait que l'image de $\sigma(z)$, avec $z \in \mathbb{Q}[\sqrt{D}]$, ne dépende pas de la façon d'écrire z comme un polynôme en $\sqrt{D}$.

Questions à se poser, réflexes à acquérir.

— Comprendre pourquoi l'identité : $\forall a \in \mathbb{Q}$, $f(a) = a$, implique la $\mathbb{Q}$-linéarité de f.

— Vous remarquerez que je justifie très rapidement que f fixe les rationnels. Comprendre l'argument : pourquoi $\{x \in K \mid f(x) = x\}$ est un sous-corps de K ? Pourquoi cela implique qu'il contient $\mathbb{Q}$? Je fais une observation analogue à la question 5 mais avec $\mathbb{Z}$. Comparer avec la démonstration « naïve » que $f(a) = a$ pour tout $a \in \mathbb{Q}$, afin d'apprécier l'économie.

— Généraliser la méthode de construction des morphismes d'un sous-corps de $\mathbb{C}$, où l'on montre qu'ils fixent $\mathbb{Q}$ et utilise ensuite le fait qu'ils préservent les racines des équations polynomiales. On l'a fait avec $\sqrt{D}$ ici, avec i pour les automorphismes de $\mathbb{C}$ fixant $\mathbb{R}$ en travaux dirigés : plus généralement, si on veut déterminer les automorphismes de $\mathbb{Q}[\zeta]$, que fait-on, qu'obtient-on ?
La méthode doit devenir un RÉFLEXE.

— Pourquoi un morphisme de corps est toujours injectif ? Proposer deux démonstrations : avec ou sans les idéaux.

— Faire la vérification en fin de remarque ci-dessus. Vous aurez recours au polynôme minimal.

8. S'il existe $r \in \mathbb{Q}^*$ tel que : $D = r^2 D'$, alors D' est non carré. De plus :

$$\sqrt{D'} = \pm(\sqrt{D})/r \in \mathbb{Q}[\sqrt{D}], \quad \text{et :} \quad \sqrt{D} = \pm r\sqrt{D'} \in \mathbb{Q}[\sqrt{D'}],$$

d'où : $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$.
Si D' est non carré et $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}] = K$, alors K admet trois isomorphismes de corps : Id, σ et σ' associé au changement de signe de $\sqrt{D'}$. D'après la question précédente on a donc : $\sigma = \sigma'$, puis : $\sigma(\sqrt{D'}) = -\sqrt{D'}$, ce qui implique : $\sqrt{D'} = b\sqrt{D}$ avec $b \in \mathbb{Q}$ (il est facile de montrer que si $x \in \mathbb{Q}[\sqrt{D}]$, alors $\sigma(x) = -x$ si et seulement si x est proportionnel à $\sqrt{D}$: faites-le), d'où : $D = \dfrac{1}{b^2} D'$. D'où le résultat.

Remarque. On a dit plus haut que : $\sigma(x) = -x \iff x \in \mathbb{Q}\sqrt{D}$. Il est tout aussi facile de vérifier que :

$$\forall x \in K, \quad (\sigma(x) = x \iff x \in \mathbb{Q}).$$

Notez qu'on a déterminé là les caractéristiques géométriques de la symétrie σ. Cette équivalence très facile à démontrer est peut-être la propriété la plus importante vérifiée par σ : voir son usage à la question 11.

Questions à se poser, réflexes à acquérir.

- Pourquoi l'appartenance de $\sqrt{D'}$ à $\mathbb{Q}[\sqrt{D}]$ (et de même en inversant les rôles de D et D') suffit à avoir l'égalité ensembliste voulue ? C'est l'occasion, peut-être, de remarquer que $\mathbb{Q}[\zeta]$ peut être défini par une propriété de minimalité, à l'instar des sous-groupes, idéaux et sous-espaces vectoriels engendrés par une partie, qui peut servir à montrer des inclusions très rapidement.
- Vérifier l'équivalence sur les éléments fixés par σ ou transformés en leur opposé. Faire un parallèle avec la conjugaison complexe, et noter que c'est un phénomène déjà observé en mathématiques.
- Trouver une autre démonstration, plus naïve, que $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$ implique $D = r^2 D'$ avec $r \in \mathbb{Q}$.
- Apprécier, dans cette résolution, cette illustration d'un principe que je reformule çà et là de différentes manières : quand on connaît tous les automorphismes d'un corps de nombres, on en connaît toute la substance arithmétique (ici : les racines carrées qu'il possède).

9. Décomposons D en facteurs premiers : $D = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n}$, où les p_i sont des nombres premiers distincts et les α_i des entiers *relatifs*. Posons alors :

$$\forall i \in [\![1, n]\!],\ \beta_i = \alpha_i \bmod 2 \in \{0,1\}, \quad \text{et :} \quad d = \pm p_1^{\beta_1} \dots p_n^{\beta_n} \in \mathbb{Z}.$$

Alors d est sans facteurs carrés et $\frac{D}{d}$ est un carré par construction, donc par la question précédente : $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{d}]$. D'où l'existence.
Montrons l'unicité de d. Soient d et d' deux entiers relatifs sans facteurs carrés tels que : $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{d'}]$. Par la question précédente, il existe $r \in \mathbb{Q}^*$ tel que : $d = r^2 d'$. Posons : $r = \frac{p}{q}$, où p et q sont deux entiers premiers entre eux. L'équation précédente donne alors : $p^2 d' = q^2 d$. Comme p^2 est premier à q^2, on en déduit que p^2 divise d, mais d est sans facteur carré donc : $p^2 = 1$, et de même : $q^2 = 1$, d'où finalement : $d = d'$. Ce qu'il fallait démontrer.

Questions à se poser, réflexes à acquérir.

- Comprendre ce qui a motivé la définition de β_i et d. Éventuellement réfléchir sur des exemples de D concrets.
- Peut-on décomposer tout nombre rationnel comme produit de nombres premiers, comme on l'a fait ci-dessus ? Y a-t-il toujours unicité de la décomposition ? Pourquoi ne fait-on jamais d'arithmétique avec des nombres rationnels malgré cette décomposition apparemment possible ? Justifier.

10. Soit $(1, x)$ une $\mathbb{Q}$-base de K sur $\mathbb{Q}$. L'objectif est de se ramener à la racine carrée d'un rationnel. Pour ce faire : on montre que x est solution d'une équation polynomiale du second degré, et on sait qu'une telle solution s'écrit en fonction de la racine carrée du discriminant. C'est l'idée sous-jacente aux manipulations ci-dessous.

On a : $x^2 \in K = \mathrm{Vect}_{\mathbb{Q}}(1, x)$, donc il existe $(\alpha, \beta) \in \mathbb{Q}^2$ tel que : $x^2 = \alpha + \beta x$, soit :

$$\left(x - \frac{\beta}{2}\right)^2 = \alpha + \frac{\beta^2}{4} = D.$$

Si D est le carré d'un rationnel, alors il existe $r \in \mathbb{Q}$ tel que : $D = r^2$, et on obtient : $x - \frac{\beta}{2} \in \{r, -r\} \subseteq \mathbb{Q}$, donc : $x \in \mathbb{Q}$, ce qui est absurde puisque $(1, x)$ est $\mathbb{Q}$-libre. On en déduit que D n'est pas un carré de rationnel, et alors : $\sqrt{D} = \pm\left(x - \frac{\beta}{2}\right) \in K$, d'où : $\mathbb{Q}[\sqrt{D}] \subseteq K$, puis $\mathbb{Q}[\sqrt{D}] = K$ par comparaison des dimensions.

Questions à se poser, réflexes à acquérir.

— Se convaincre que x n'est *a priori* pas une racine carrée de rationnel, et qu'il fallait bien ces manipulations pour s'y ramener.

— J'ai motivé la résolution en parlant du discriminant, et pourtant il semble n'apparaître nulle part dans ma démonstration. Où est-il caché ? Pourquoi la résolution est bien l'illustration de ce que j'ai motivé ?

— Comparer cette résolution avec ce que j'ai fait dans le devoir sur table n^o 3, dernière partie, pour construire un isomorphisme entre $\mathbb{R}[x] = \mathbb{R} + \mathbb{R}x$ et $\mathbb{C}$. Quel rapport avec ce qui est fait ici ?

11. Si $x \in \mathcal{O}_K$, alors x annule un polynôme $P \in \mathbb{Z}[X]$ unitaire. Comme P est à coefficients entiers, donc rationnels, et que σ est un morphisme de corps, on a :

$$P(\sigma(x)) = \sigma(P(x)) = \sigma(0) = 0,$$

donc : $\sigma(x) \in \mathcal{O}_K$. Or $\mathcal{O}_K$ est un anneau, donc $u = x + \sigma(x)$ et $v = x\sigma(x)$ appartiennent aussi à $\mathcal{O}_K$. Ils sont de plus invariants par σ du fait que : $\sigma^2 = \mathrm{Id}_K$:

$$\sigma(u) = \sigma(x) + \sigma^2(x) = \sigma(x) + x = u, \quad \sigma(v) = \sigma(x)\sigma^2(x) = \sigma(x)x = v,$$

donc d'après la remarque de la question 8, les éléments u et v appartiennent à $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$: ce qu'il fallait démontrer.

Réciproquement, supposons que $u = x + \sigma(x)$ et $v = x\sigma(x)$ sont entiers. Alors x (et $\sigma(x)$) est racine du polynôme $X^2 - uX + v \in \mathbb{Z}[X]$, donc : $x \in \mathcal{O}_K$.

Remarque. Les quantités $x+\sigma(x)$ et $x\sigma(x)$ sont respectivement appelées la *trace* et la *norme* de x. La première quantité est la trace de l'endomorphisme m_x, d'où le nom. La norme est son déterminant (si vous avez fait des exercices sur l'anneau $\mathbb{Z}[i]$, vous l'avez probablement déjà croisée). Cela ne va pas de soi. Vous pourrez éventuellement essayer de le démontrer après le traitement du chapitre de réduction des endomorphismes, et proposer une généralisation en dimension supérieure.

Remarque. On remarque que les points fixes de σ sont exactement les rationnels, au même titre que les points fixes de la conjugaison complexe sont exactement les nombres réels, et dans un corps fini contenant $\mathbb{Z}/p\mathbb{Z}$: les points fixes de l'automorphisme de Frobenius $x \mapsto x^p$ sont exactement les éléments de $\mathbb{Z}/p\mathbb{Z}$. La généralisation de ce phénomène est un des résultats préliminaires de la théorie de Galois (un corollaire du *lemme d'Artin*), et c'est un des emplois privilégiés des automorphismes de corps : montrer qu'un nombre est dans un certain corps en vérifiant qu'il est laissé invariant par des automorphismes. Appréciez l'efficacité de l'approche (vous l'aviez déjà constatée pour la caractérisation des réels *via* la conjugaison complexe).

Questions à se poser, réflexes à acquérir.

— Comprendre l'égalité : $P(\sigma(x)) = \sigma(P(x))$ et, dans chaque exercice où l'on a manipulé des morphismes de corps : noter qu'on a utilisé une telle relation immanquablement. Elle est vraiment centrale ! Comprendre pourquoi ! (On peut presque dire que c'est ce qui a historiquement motivé leur étude, et explique pourquoi les morphismes de corps ne sont jamais loin quand on étudie des équations polynomiales.) Remarquer qu'on l'a implicitement utilisée plus tôt dans ce sujet : où ?

Cette propriété, et celle sur les points fixes de σ, sont les deux seules à retenir s'il fallait résumer les automorphismes de corps à peu de choses.

— Je parle de $\mathbb{Z}[i]$ ci-dessus : voir comment on utilise la « norme » dans les exercices sur cet anneau (et observer qu'effectivement, c'est aussi un entier dans ce contexte). Cela vous donnera deux exemples d'utilisation de cet outil apprécié des arithméticiens.

— J'affirme que l'idée d'introduire le polynôme $X^2 - uX + v$ va complètement de soi, si on a bien en tête la propriété $P \circ \sigma = \sigma \circ P$ pour tout P, et plus généralement si l'on a bien suivi l'emploi fait de σ dans ce problème : pourquoi ?

12. L'égalité $\{x + y\omega \mid (x, y) \in \mathbb{Z}^2\} = \mathbb{Z}[\omega]$ découle simplement du fait que ω vérifie une équation de degré 2 (nous allons le montrer ci-dessous en passant). Ne nous attardons donc pas là-dessus, et montrons que $\mathcal{O}_K$ est le groupe engendré par 1 et ω.

Montrons d'abord que $\omega \in \mathcal{O}_K$ en montrant qu'il est annulé par un polynôme unitaire à coefficients entiers :

— si : $d \equiv 1 \bmod 4$, alors $\omega^2 = \dfrac{1+d}{4} + \dfrac{\sqrt{d}}{2} = \dfrac{d-1}{4} + \omega$ et $\dfrac{d-1}{4} \in \mathbb{Z}$ donc $X^2 - X - \frac{d-1}{4}$ est à coefficients entiers et annule ω ;

— si : $d \not\equiv 1 \bmod 4$, alors $\omega^2 = d$ donc $X^2 - d$ est à coefficients entiers et annule ω.

Dans tous les cas, on a : $\omega \in \mathcal{O}_K$. De plus, évidemment : $1 \in \mathcal{O}_K$, donc la stabilité par somme permet de conclure : $\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$.

Réciproquement, soit $x = a + b\sqrt{d} \in \mathcal{O}_K$ avec $(a, b) \in \mathbb{Q}^2$. On a, par la question précédente :

$$x + \sigma(x) = 2a \in \mathbb{Z}, \quad x\sigma(x) = a^2 - db^2 = q \in \mathbb{Z},$$

donc : $a = \frac{p}{2}$ avec $p \in \mathbb{Z}$, et : $4db^2 = p^2 - 4q$.

Pour démontrer : $x \in \mathbb{Z}[\omega]$, selon la congruence de d modulo 4, la clé est de déterminer si a et b sont entiers ou demi-entiers. Cela incite à étudier $2b \in \mathbb{Q}$, afin de savoir si c'est un entier ou non. Posons donc : $2b = \frac{u}{v}$ où u et v sont des entiers premiers entre eux. Il ne coûte rien de supposer que v est positif. On a, d'après ce qui précède :

$$du^2 = v^2(p^2 - 4q),$$

donc v^2 divise du^2, et comme u et v sont premiers entre eux, u^2 et v^2 le sont aussi, donc par le théorème de Gauß on sait que v^2 divise d. Or d est sans facteur carré, donc : $v = 1$. Ainsi : $b = \frac{u}{2}$, ce qui prouve déjà une partie de ce qu'on voulait (b est un entier ou demi-entier). Pour conclure, remarquons la congruence : $du^2 \equiv p^2 \bmod 4$. Ensuite :

— si : $d \equiv 1 \bmod 4$, alors : $u^2 \equiv p^2 \bmod 4$, donc u et p ont même parité, et on en déduit :

$$x = a + b\sqrt{d} = \frac{p-u}{2} + u\omega \in \mathbb{Z}[\omega] ;$$

— si : $d \equiv 2 \bmod 4$, alors p est pair, donc u l'est également (par la congruence ci-dessus : $2u^2 \equiv 0 \bmod 4$, qui implique : $u^2 \equiv 0 \bmod 2$), donc :

$$x = a + b\sqrt{d} = \frac{p}{2} + \frac{u}{2}\omega \in \mathbb{Z}[\omega] ;$$

— si : $d \equiv 3 \bmod 4$ et p est impair, alors : $p^2 \equiv 1 \bmod 4$, ce qui n'est pas le cas de du^2 quel que soit la parité de u, donc ce cas est impossible ;

— si : $d \equiv 3 \bmod 4$ et p est pair, alors u est aussi pair et :

$$x = \frac{p}{2} + \frac{u}{2}\omega \in \mathbb{Z}[\omega]\,;$$

— le cas $d \equiv 0 \bmod 4$ est impossible puisque d est sans facteur carré.

Dans tous les cas possibles on a bien : $x \in \mathbb{Z}[\omega]$, donc : $\mathcal{O}_K \subseteq \mathbb{Z}[\omega]$, ce qui achève la démonstration.

Questions à se poser, réflexes à acquérir.

— Vérifier ce que j'ai admis en amont de la résolution.

— On est passé plusieurs fois, dans ce sujet, d'une égalité dans $\mathbb{Q}$ à une égalité dans $\mathbb{Z}$ pour y faire de l'arithmétique : bien observer l'intérêt et l'efficacité de la stratégie.

— Pourquoi, si u et v sont premiers entre eux, alors u^2 et v^2 aussi ? C'est très facile si l'on prend l'affaire par le bon bout (dans l'aide à la révision du cours du chapitre IV, je fais une remarque à ce sujet).

— Expliquer le passage de : $2u^2 \equiv 0 \bmod 4$, à : $u^2 \equiv 0 \bmod 2$. Quand est-il licite de « tout diviser par un même entier » (y compris le module), dans une relation de congruence $a \equiv b \bmod n$?

Troisième partie – Calcul de τ_n

13. On a :

$$|\tau_n|^2 = \tau_n\overline{\tau_n} = \sum_{x\in\mathbb{Z}/n\mathbb{Z}}\sum_{y\in\mathbb{Z}/n\mathbb{Z}}(\zeta_n)^{x^2-y^2} = \sum_{x\in\mathbb{Z}/n\mathbb{Z}}\sum_{y\in\mathbb{Z}/n\mathbb{Z}}(\zeta_n)^{(x-y)(x+y)}.$$

En vue de nous ramener à une somme géométrique, faisons le changement d'indice $z = x + y$. Comme $y \mapsto x + y$ est une permutation de $\mathbb{Z}/n\mathbb{Z}$, cela donne :

$$|\tau_n|^2 = \sum_{x\in\mathbb{Z}/n\mathbb{Z}}\sum_{z\in\mathbb{Z}/n\mathbb{Z}}(\zeta_n)^{(2x-z)z} = \sum_{z\in\mathbb{Z}/n\mathbb{Z}}\sum_{x\in\mathbb{Z}/n\mathbb{Z}}(\zeta_n)^{(2x-z)z} = \sum_{z\in\mathbb{Z}/n\mathbb{Z}}(\zeta_n)^{-z^2}\sum_{x\in\mathbb{Z}/n\mathbb{Z}}(\zeta_n)^{2xz}$$
$$= \sum_{z\in\mathbb{Z}/n\mathbb{Z}}(\zeta_n)^{-z^2}\sum_{x=0}^{n-1}\left((\zeta_n)^{2z}\right)^x.$$

On reconnaît une somme géométrique de raison $(\zeta_n)^{2z}$. Si $2z \equiv 0 \bmod n$ (ce qui équivaut à $z \equiv 0 \bmod n$ vu que, par hypothèse, 2 et n sont premiers entre eux), alors cette somme égale n. Sinon, elle est égale à :

$$\sum_{x=0}^{n-1}\left((\zeta_n)^{2z}\right)^x = \frac{1-(\zeta_n)^{2zn}}{1-(\zeta_n)^{2z}} = 0,$$

car ζ_n est une racine n^{e} de l'unité. Finalement seul le terme correspondant à $z = \bar{0}$ est non nul. On en déduit :

$$|\tau_n|^2 = n(\zeta_n)^{-0^2} = n,$$

d'où le résultat.

Questions à se poser, réflexes à acquérir.

— Ce raisonnement montre bien l'intérêt d'interpréter une somme indexée par les entiers de 0 à $n-1$ comme une somme indexée par $\mathbb{Z}/n\mathbb{Z}$: les changements d'indice sont plus agréables à faire (s'en convaincre si vous êtes perplexes). Mais sous quelle condition est-il possible d'écrire : $\sum_{k=0}^{n-1}\bigstar = \sum_{\bar{k}\in\mathbb{Z}/n\mathbb{Z}}\bigstar$, sans problème de bonne définition ? Dans ces circonstances, je vous recommande de *toujours* avoir dans un coin de la tête l'expression de droite.

— Plus généralement, dans toutes les circonstances (ou presque : la première question de ce devoir est le seul contre-exemple qui me vient à l'esprit) où nous avons croisé une somme ou un produit indexé par un groupe fini, remarquer que le calcul passe toujours par un changement d'indice convenable, très souvent par translation (donc $x \mapsto x+y$ dans un groupe additif et $x \mapsto xy$ dans le cas multiplicatif).

14. Pour abréger, posons : $\forall k \in \mathbb{Z}/n\mathbb{Z}$, $\delta_k = \mathbb{1}_{\{k\}}$. Cela définit évidemment des éléments de V.
Soit $f \in V$. On a clairement : $f = \sum_{k\in\mathbb{Z}/n\mathbb{Z}} f(k)\delta_k$, ce qui montre que la famille $\mathcal{F} = (\delta_k)_{k\in\mathbb{Z}/n\mathbb{Z}}$ est $\mathbb{C}$-génératrice. Montrons qu'elle est libre : soit $(a_k)_{k\in\mathbb{Z}/n\mathbb{Z}} \in \mathbb{C}^{\mathbb{Z}/n\mathbb{Z}}$ tel que : $0 = \sum_{k\in\mathbb{Z}/n\mathbb{Z}} a_k\delta_k$. En évaluant cette égalité en $\ell \in \mathbb{Z}/n\mathbb{Z}$, on a : $\forall \ell \in \mathbb{Z}/n\mathbb{Z}$, $0 = \sum_{k\in\mathbb{Z}/n\mathbb{Z}} a_k\delta_k(\ell) = a_\ell$, ce qui démontre que la seule relation de dépendance linéaire est la relation triviale, donc $\mathcal{F}$ est une famille $\mathbb{C}$-libre.
Étant à la fois libre et génératrice, $\mathcal{F}$ est une $\mathbb{C}$-base de V, d'où : $\dim_{\mathbb{C}}(V) = n$. On a de plus :

$$\begin{aligned}\forall k \in \mathbb{Z}/n\mathbb{Z}, \quad \varphi(\delta_k) &= \sum_{\ell\in\mathbb{Z}/n\mathbb{Z}} \varphi(\delta_k)(\ell)\delta_\ell \\ &= \sum_{\ell\in\mathbb{Z}/n\mathbb{Z}} \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \delta_k(y)(\zeta_n)^{\ell y}\delta_\ell \\ &= \sum_{\ell\in\mathbb{Z}/n\mathbb{Z}} (\zeta_n)^{\ell k}\delta_\ell \qquad (1) \\ &= (\zeta_n)^{k^2}\delta_k + \sum_{\ell\neq k} (\zeta_n)^{\ell k}\delta_\ell,\end{aligned}$$

donc : $\mathrm{tr}(\varphi) = \sum_{k\in\mathbb{Z}/n\mathbb{Z}} (\zeta_n)^{k^2} = \tau_n$, d'où le résultat.

Questions à se poser, réflexes à acquérir.
- Généraliser : si G est un ensemble fini, donner la dimension et une base de $\mathcal{F}(G, \mathbb{C})$. Noter que G n'a pas besoin d'avoir une structure.
- Comprendre le rapport entre mon calcul de $\varphi(\delta_k)$ et de la trace. Si besoin : écrire la matrice de φ dans la base $\mathcal{F}$.
- Il est parfois pénible d'écrire une trace, lorsque le calcul s'effectue dans une base qui n'est pas indexée par $[\![1, n]\!]$. Vous avez peut-être déjà rencontré cette difficulté avec la trace d'endomorphismes de $\mathrm{M}_n(K)$. Comment proposer une expression de la trace d'un endomorphisme maniable peu importe l'indexation de la base ?

15. Soient $f \in V$ et $x \in K$. On a :

$$\varphi\circ\varphi(f)(x) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \varphi(f)(y)(\zeta_n)^{xy} = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)(\zeta_n)^{yz}(\zeta_n)^{xy} = \sum_{z\in\mathbb{Z}/n\mathbb{Z}} \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(z)(\zeta_n)^{y(x+z)}.$$

Par un calcul analogue à celui de la question 13 : si $x + z \neq \bar{0}$, alors : $(\zeta_n)^{x+z} \neq 1$, et donc :

$$\sum_{y\in\mathbb{Z}/n\mathbb{Z}} (\zeta_n)^{y(x+z)} = \frac{(\zeta_n)^{n(x+z)} - 1}{(\zeta_n)^{x+z} - 1} = 0.$$

Autrement, si $x + z = \bar{0}$, alors : $\sum_{y\in\mathbb{Z}/n\mathbb{Z}} (\zeta_n)^{y(x+z)} = n$, d'où le résultat :

$$\varphi\circ\varphi(f)(x) = f(-x)\sum_{y\in\mathbb{Z}/n\mathbb{Z}} (\zeta_n)^0 + \sum_{z\neq -x} \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(z)(\zeta_n)^{y(x+z)} = nf(-x).$$

Remarque. L'application φ est la transformation de Fourier sur $\mathbb{Z}/n\mathbb{Z}$ (dont je parle dans les commentaires du devoir maison n^o 4), et nous avons démontré dans cette question la formule d'inversion de Fourier.
Remarque. Comme $f \mapsto nf(-x)$ et $\varphi\circ\varphi$ sont linéaires, il suffisait de démontrer cette égalité sur la base $\mathcal{F} = (\delta_k)_{k\in\mathbb{Z}/n\mathbb{Z}}$ de la question 14.

16. Notons ι l'application $f \mapsto (x \mapsto f(-x))$. Elle vérifie clairement : $\iota^2 = \mathrm{Id}_V$, et comme c'est une application $\mathbb{C}$-linéaire on en déduit que c'est une symétrie de V. En particulier :

$$V = \ker(\iota - \mathrm{Id}_V) \oplus \ker(\iota + \mathrm{Id}_V).$$

Or on a, d'après la question précédente : $\dfrac{1}{n}\varphi^2 = \iota$, d'où le résultat.

> **Questions à se poser, réflexes à acquérir.** Revoir comment on a démontré en 1re année que les projecteurs et les symétries induisent de telles décompositions en sous-espaces supplémentaires, et surtout : à quoi elles servent (cela peut aussi servir à étudier ces endomorphismes qu'à expliciter l'espace vectoriel ambiant). Sans aucune exagération, elles sont la préoccupation centrale de l'algèbre linéaire et nous y recourrons régulièrement.

17. Notons : $E_1 = \ker\left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right)$, et Φ_1 la restriction $\frac{1}{\sqrt{n}}\varphi$ à E_1. Elle induit un endomorphisme de E_1, puisque l'on a par définition de ce noyau :

$$\begin{aligned}\forall f \in E_1, \quad \left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right)(\Phi_1(f)) = \left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right)\left(\frac{1}{\sqrt{n}}\varphi(f)\right) &= \frac{1}{\sqrt{n}}\left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right) \circ \varphi(f) \\ &= \frac{1}{\sqrt{n}}\varphi \circ \left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right)(f) \\ &= \frac{1}{\sqrt{n}}\varphi(0) \\ &= 0,\end{aligned}$$

de sorte que : $\forall f \in E_1$, $\Phi_1(f) \in E_1$. De plus, toujours par définition de ce noyau :

$$\forall f \in E_1, \quad \Phi_1^2(f) = \frac{1}{\sqrt{n}}\varphi\left(\frac{1}{\sqrt{n}}\varphi(f)\right) = \frac{1}{n}\varphi^2(f) = f,$$

donc : $\Phi_1^2 = \mathrm{Id}_{E_1}$. Ainsi Φ_1 est une symétrie de E_1, donc :

$$E_1 = \ker\left(\Phi_1 - \mathrm{Id}_{E_1}\right) \oplus \ker\left(\Phi_1 + \mathrm{Id}_{E_1}\right).$$

C'est-à-dire, avec quelques abus de notation apparents (on confond φ et sa restriction, de même avec l'identité), dont on démontrerait aisément la justesse mais que j'omets, car ils rallongeraient bêtement le raisonnement en nous détournant de sa préoccupation première :

$$\begin{aligned}\ker\left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right) &= \ker\left(\frac{1}{\sqrt{n}}\varphi - \mathrm{Id}_V\right) \oplus \ker\left(\frac{1}{\sqrt{n}}\varphi + \mathrm{Id}_V\right) \\ &= \ker\left(\varphi - \sqrt{n}\mathrm{Id}_V\right) \oplus \ker\left(\varphi + \sqrt{n}\mathrm{Id}_V\right). \qquad (2)\end{aligned}$$

En faisant le même raisonnement sur $\ker\left(\frac{1}{n}\varphi^2 + \mathrm{Id}_V\right)$ avec la restriction de $\dfrac{1}{i\sqrt{n}}\varphi$, on obtient :

$$\ker\left(\frac{1}{n}\varphi^2 + \mathrm{Id}_V\right) = \ker\left(\varphi - i\sqrt{n}\mathrm{Id}_V\right) \oplus \ker\left(\varphi + i\sqrt{n}\mathrm{Id}_V\right). \qquad (3)$$

De plus, par la question précédente, les noyaux $\ker\left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right)$ et $\ker\left(\frac{1}{n}\varphi^2 + \mathrm{Id}_V\right)$ sont supplémentaires dans V. On en déduit que si l'on concatène une base de $\ker\left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right)$ adaptée à la somme directe (2), avec une base de $\ker\left(\frac{1}{n}\varphi^2 + \mathrm{Id}_V\right)$ adaptée à la somme directe (3), alors la famille $\mathcal{B}$ ainsi obtenue est une base de V, et la matrice représentative de φ dans cette base est :

$$\mathrm{M}_{\mathcal{B}}(\varphi) = \begin{pmatrix} \sqrt{n}\mathrm{I}_a & & & \mathbf{0} \\ & -\sqrt{n}\mathrm{I}_b & & \\ & & i\sqrt{n}\mathrm{I}_c & \\ \mathbf{0} & & & -i\sqrt{n}\mathrm{I}_d \end{pmatrix} = \mathrm{Diag}\left(\sqrt{n}\mathrm{I}_a, -\sqrt{n}\mathrm{I}_b, i\sqrt{n}\mathrm{I}_c, -i\sqrt{n}\mathrm{I}_d\right), \qquad (4)$$

avec :

$$\begin{array}{ll} a = \dim\left(\ker\left(\varphi - \sqrt{n}\mathrm{Id}_V\right)\right), & b = \dim\left(\ker\left(\varphi + \sqrt{n}\mathrm{Id}_V\right)\right), \\ c = \dim\left(\ker\left(\varphi - i\sqrt{n}\mathrm{Id}_V\right)\right), & d = \dim\left(\ker\left(\varphi + i\sqrt{n}\mathrm{Id}_V\right)\right). \end{array} \tag{5}$$

D'où le résultat.

Remarque. Avec les outils du chapitre V, cette question et la précédente seront complètement caduques : nous nous contenterons de dire que $\varphi^4 = n^2\mathrm{Id}_V$, de sorte que $X^4 - n^2$ soit un polynôme annulateur de φ. Comme il est scindé et à racines simples sur $\mathbb{C}$, l'endomorphisme φ est diagonalisable et son spectre est inclus dans l'ensemble de ces racines (qui sont justement $\sqrt{n}$, $-\sqrt{n}$, $i\sqrt{n}$ et $-i\sqrt{n}$).

Questions à se poser, réflexes à acquérir.

- Être certain d'avoir compris le rapport entre les deux décompositions en sous-espaces supplémentaires, et la matrice diagonale obtenue. Réciproquement, si la matrice d'un endomorphisme f dans une base est diagonale, vérifier qu'on a une décomposition analogue en sous-espaces supplémentaires. Ce sens réciproque vous permettra de comprendre la philosophie de ces deux questions et les décompositions des projecteurs et symétries sous un autre angle, peut-être.
- Se convaincre de la justesse de l'identité $\left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right) \circ \varphi = \varphi \circ \left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right)$, et remarquer que j'ai déjà utilisé une telle relation de commutation quelque part dans ce sujet, afin d'obtenir un résultat de stabilité. Où ? Retenir que la commutation intervient souvent dans ce genre de vérification.
- Pourquoi $\ker(\Phi_1 - \mathrm{Id}_{E_1}) = \ker\left(\frac{1}{\sqrt{n}}\varphi - \mathrm{Id}_V\right)$ alors que, *a priori*, les endomorphismes ne sont pas définis sur les mêmes espaces ? Quelle est la clé qui rend cette égalité valable ?
- Se convaincre de ma « multiplication » par $\sqrt{n}$ dans (2).
- Pourquoi avoir divisé par $i\sqrt{n}$, et non $\sqrt{n}$ ou $-\sqrt{n}$, pour l'étude sur $\ker\left(\frac{1}{n}\varphi^2 + \mathrm{Id}_V\right)$?
- Reconnaître là une illustration de la motivation de la réduction des endomorphismes, présente dans *Présentation des chapitres en MP* et développée très amplement au chapitre V.

18. D'après les relations (2) et (5) de la question précédente, on a :

$$a + b = \dim\left(\ker\left(\frac{1}{n}\varphi^2 - \mathrm{Id}_V\right)\right) = \dim\left(\ker\left(\varphi^2 - n\mathrm{Id}_V\right)\right),$$

or on peut expliciter ce noyau, puisque par la question 15 on a : $\forall f \in V$, $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $\varphi^2(f)(x) = nf(-x)$, de sorte que :

$$\forall f \in V, \quad f \in \ker\left(\varphi^2 - n\mathrm{Id}_V\right) \iff \varphi^2(f) = nf \iff \forall x \in \mathbb{Z}/n\mathbb{Z},\ f(-x) = f(x).$$

Autrement dit : $\ker(\varphi^2 - n\mathrm{Id}_V)$ est l'espace vectoriel des fonctions *paires* de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}$. On sait en proposer une base. En effet, si l'on reprend les notations de la question 14, alors pour toute fonction paire $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ on a :

$$f = \sum_{k \in \mathbb{Z}/n\mathbb{Z}} f(k)\delta_k = f(0)\delta_0 + \sum_{k=1}^{\frac{n-1}{2}} f(\bar{k})\delta_{\bar{k}} + \sum_{k=1}^{\frac{n-1}{2}} f(-\bar{k})\delta_{-\bar{k}} = f(\bar{0})\delta_{\bar{0}} + \sum_{k=1}^{\frac{n-1}{2}} f(\bar{k})\left(\delta_{\bar{k}} + \delta_{-\bar{k}}\right),$$

en prenant $[\![-\frac{n-1}{2}, \frac{n-1}{2}]\!]$ comme système complet de représentants de $\mathbb{Z}/n\mathbb{Z}$. On en déduit que la famille $(\delta_{\bar{0}}) \cup \left(\delta_{\bar{k}} + \delta_{-\bar{k}}\right)_{1 \leqslant k \leqslant \frac{n-1}{2}}$ engendre $\ker(\varphi^2 - n\mathrm{Id}_V)$. On démontre sa liberté comme dans la question 14. C'est donc une base, et on en déduit : $\dim\left(\ker(\varphi^2 - n\mathrm{Id}_V)\right) = \frac{n+1}{2}$. Donc, d'après l'identité en début de résolution, on a :

$$a + b = \frac{n+1}{2}.$$

De même, $c + d$ est égal à la dimension de l'espace vectoriel des fonctions *impaires* de $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, dont une base est la famille $\left(\delta_{\bar{k}} - \delta_{-\bar{k}}\right)_{1 \leqslant k \leqslant \frac{n-1}{2}}$. Donc :

$$c + d = \frac{n-1}{2}.$$

Enfin, par la question 14 on a : $\tau_n = \mathrm{tr}(\varphi)$, mais d'après l'identité (4) de la question précédente on a aussi : $\mathrm{tr}(\varphi) = ((a-b)+i(c-d))\sqrt{n}$, donc : $\tau_n = ((a-b)+i(c-d))\sqrt{n}$, et par la question 13 on a : $|\tau_n|^2 = n$, ce qui permet de conclure :

$$(a-b)^2 + (c-d)^2 = 1.$$

Remarque. Comme une somme de carrés d'entiers ne vaut 1 que si l'un des termes est nul, l'autre égal à 1, on peut déjà déduire de cette identité que a et b sont distants de 1 et $c = d$, ou inversement. Combiné aux deux autres égalités, on voit qu'il n'y a que peu de possibilités pour leurs valeurs respectives, par exemple : $a = \frac{n+3}{4}$, $b = \frac{n-1}{4}$ et $c = d = \frac{n-1}{4}$, etc. La congruence de n modulo 4 permet en plus d'écarter des possibilités. Par exemple, les égalités que nous venons d'écrire nécessitent $n \equiv 1 \bmod 4$, parce que a, b, c et d doivent être des entiers. L'objectif de la dernière question est d'éliminer toutes les possibilités sauf une afin d'avoir la valeur de a, b, c et d. On a utilisé la trace et la dimension des espaces pour avoir les informations plus haut : il est naturel d'utiliser le déterminant comme ultime contrainte.

Questions à se poser, réflexes à acquérir.

- Vérifier la justesse des bases proposées pour les espaces des fonctions paires et des fonctions impaires.
- Peut-on obtenir la liberté de $\left(\delta_{\bar{k}} \pm \delta_{-\bar{k}}\right)_{1 \leqslant k \leqslant \frac{n-1}{2}}$ par un argument matriciel simple, qui utiliserait la donnée que $(\delta_k)_{k \in \mathbb{Z}/n\mathbb{Z}}$ est une base par la question 14 ?
- Ne pouvait-on pas déduire les bases obtenues plus rapidement, en utilisant ce que l'on connaît comme propriété des symétries (on a en effet vu que $\frac{1}{n}\varphi^2$ en est une), et plus précisément en utilisant la décomposition de tout vecteur selon leurs caractéristiques géométriques ?)

19. Soit $\mathcal{F}$ la base explicitée à la question 14. D'après le calcul (1) de cette même question, la matrice de φ dans cette base est :

$$M = \left(\left((\zeta_n)^{(k-1)(\ell-1)}\right)\right)_{0 \leqslant k,\ell \leqslant n-1}.$$

C'est la matrice de Vandermonde associée à la famille $(1, (\zeta_n), \ldots, (\zeta_n)^{n-1})$. Donc :

$$\det(\varphi) = \prod_{k=1}^{n-1} \prod_{\ell=0}^{k-1} ((\zeta_n)^k - (\zeta_n)^\ell),$$

En utilisant la technique de l'angle moitié et en notant $\xi = \exp\left(\frac{i\pi}{n}\right)$, on obtient :

$$\det(\varphi) = \prod_{k=1}^{n-1} \prod_{\ell=0}^{k-1} ((\zeta_n)^k - (\zeta_n)^\ell) = \prod_{k=1}^{n-1} \prod_{\ell=0}^{k-1} \xi^{k+\ell}(\xi^{k-\ell} - \xi^{\ell-k}) = \prod_{k=1}^{n-1} \prod_{\ell=0}^{k-1} \xi^{k+\ell} \left(2i \sin\left((k-\ell)\frac{\pi}{n}\right)\right).$$

Comme : $\displaystyle\prod_{\ell=0}^{k-1} \xi^{k+\ell} = \xi^{k^2} \xi^{\sum_{\ell=0}^{k-1} \ell} = \xi^{k^2} \xi^{\frac{(k-1)k}{2}}$, on en déduit :

$$\det(\varphi) = \prod_{k=1}^{n-1} \xi^{\frac{k(3k-1)}{2}} (2i)^k \prod_{\ell=0}^{k-1} \sin\left((k-\ell)\frac{\pi}{n}\right) = \xi^{\frac{n(n-1)^2}{2}} (2i)^{\frac{n(n-1)}{2}} \prod_{k=1}^{n-1} \prod_{\ell=0}^{k-1} \sin\left((k-\ell)\frac{\pi}{n}\right).$$

Comme les sinus sont tous positifs, on en déduit :

$$\arg(\det(\varphi)) \equiv \frac{\pi}{4}(n-1)(3n-2) \bmod 2\pi.$$

Mais on a aussi, en calculant le déterminant de la matrice de l'identité (4) :

$$\det(\varphi) = \sqrt{n}^{\,n}(-1)^b i^c (-i)^d = \sqrt{n}^{\,n} i^{2b+c-d} = \sqrt{n}^{\,n} e^{\frac{i\pi(2b+c-d)}{2}},$$

d'où, en comparant les arguments :

$$2b + c - d \equiv \frac{(n-1)(3n-2)}{2} \bmod 4. \tag{6}$$

D'après la relation $(a-b)^2 + (c-d)^2 = 1$, qui implique $a - b = 0$ et $c - d = \pm 1$, ou $a - b = \pm 1$ et $c - d = 0$ (ce sont les seuls couples d'entiers dont la somme au carré peut donner 1), on a quatre cas à considérer (bien noter que les valeurs de a, b, c et d proposées n'utilisent pas la relation de congruence ci-dessus : c'est une très bête résolution de système ; on utilise la relation de congruence pour déterminer si ces solutions sont impossibles ou non) :

— si $a = b$ et $c - d = 1$, alors :

$$a = b = c = \frac{n+1}{4}, \quad d = \frac{n-3}{4}, \quad (\text{et } : n = 4d + 3 \equiv 3 \bmod 4)$$

et dans ce cas (6) équivaut à : $2d + 3 \equiv (2d+1)(12d+7) \bmod 4$, ce qui est vérifié puisque : $(2d+1)(12d+7) \equiv -(2d+1) \equiv 2d + 3 \bmod 4$;

— si $a = b$ et $d - c = 1$, alors :

$$a = b = d = \frac{n+1}{4}, \quad c = \frac{n-3}{4}, \quad (\text{et } : n = 4c + 3 \equiv 3 \bmod 4),$$

et dans ce cas (6) équivaut à : $2c+1 \equiv (2c+1)(12c+7) \bmod 4$, ce qui est impossible puisque : $(2c+1)(12c+7) \equiv -(2c+1) \equiv 2c + 3 \bmod 4$;

— si $a - b = 1$ et $c = d$, alors :

$$a = \frac{n+3}{4}, \quad b = c = d = \frac{n-1}{4}, \quad (\text{et } : n = 4d + 1 \equiv 1 \bmod 4),$$

et dans ce cas (6) équivaut à : $2d \equiv 2d(12d+1) \bmod 4$, ce qui est vérifié puisque : $12d \equiv 0 \bmod 4$;

— si $b - a = 1$ et $c = d$, alors :

$$b = \frac{n+3}{4}, \quad a = c = d = \frac{n-1}{4}, \quad (\text{et } : n = 4d + 1 \equiv 1 \bmod 4),$$

et dans ce cas (6) équivaut à : $2d + 2 \equiv 2d(12d+1) \bmod 4$, ce qui est impossible puisque : $12d \equiv 0 \bmod 4$.

Conclusion :

— si $n \equiv 3 \bmod 4$, alors : $a = b = c = \dfrac{n+1}{4}$, $d = \dfrac{n-3}{4}$;

— si $n \equiv 1 \bmod 4$, alors : $a = \dfrac{n+3}{4}$, $b = c = d = \dfrac{n-1}{4}$.

Questions à se poser, réflexes à acquérir.

— Je n'ai pas détaillé le calcul de $\prod_{k=1}^{n-1} \xi^{\frac{k(3k-1)}{2}}$: le faire.

— Se demander pourquoi l'expression exacte du déterminant de Vandermonde ne m'intéressait pas, et pourquoi on savait que l'argument modulo 2π suffirait pour conclure. C'est peut-être plus clair si on calcule d'abord $\det(\varphi)$ avec l'expression de l'identité (4). Une fois qu'on a compris pourquoi, remarquer que je pouvais (légèrement) alléger le calcul : où ?

— Pourquoi, après avoir vérifié que le premier cas donne une congruence vraie, ai-je malgré tout voulu traiter le cas suivant, au lieu de tout de suite conclure : « donc, lorsque $n \equiv 3 \bmod 4$, on a $a = b = c = \frac{n+1}{4}$ et $d = \frac{n-3}{4}$? »

20. On a $\tau_n = ((a-b) + i(c-d))\sqrt{n}$. Donc, d'après le résultat de la question précédente :

— si : $n \equiv 3 \bmod 4$, alors : $a - b = 0$, et : $c - d = 1$, donc : $\tau_n = i\sqrt{n}$;
— si : $n \equiv 1 \bmod 4$, alors : $a - b = 1$, et : $c - d = 0$, donc : $\tau_n = \sqrt{n}$;

d'où le résultat.

Remarque. J'affirme que, ayant démontré que $|\tau_n| = \sqrt{n}$, un bon usage de la conjugaison complexe permettait de démontrer que si $n \equiv 1 \bmod 4$ alors $\tau_n = \pm\sqrt{n}$, tandis que si $n \equiv 3 \bmod 4$ alors $\tau_n = \pm i\sqrt{n}$. C'est donc lever l'indétermination du signe qui est difficile et nécessita autant d'efforts dans cette partie (pour une somme si simple à définir, et dont le calcul serait trivial sans la présence du carré ! !). On peut d'ailleurs expliquer pourquoi le signe est *impossible* à déterminer sans recourir à des outils hors de la théorie des groupes, des anneaux et des corps. J'en discute brièvement en note à la fin de ce document :

`http://mathem-all.fr/bw/ENS/Algebre2016/cosconstructible.pdf`

Cette même note permettra de remarquer que cette condition de congruence modulo 4 est intimement liée à la condition nécessaire et suffisante pour que -1 soit un carré modulo p (conséquence facile de la question 2).

Questions à se poser, réflexes à acquérir.
— Finalement, où est-il intervenu que n est impair, dans tout ce raisonnement ? Ne peut-on pas obtenir la valeur de τ_n pour n pair semblablement ?
— Méditer sur la remarque.

21. On note $K = \mathbb{Q}[\sqrt{n}]$ où n est un entier sans facteur carré. La question précédente montre que si $n \equiv 1 \bmod 4$, alors : $\sqrt{n} = \tau_n \in \mathbb{Q}[\zeta_n]$. Si $n \equiv 3 \bmod 4$, alors :

$$\sqrt{n} = -i\tau_n = \sum_{k\in\mathbb{Z}/n\mathbb{Z}} -e^{\frac{i\pi}{2}}(\zeta_n)^{k^2} = \sum_{k\in\mathbb{Z}/n\mathbb{Z}} -e^{\frac{2i\pi n}{4n}}(\zeta_n)^{k^2} = -\sum_{k\in\mathbb{Z}/n\mathbb{Z}} (\zeta_{4n})^{k^2+n} \in \mathbb{Q}\left[\zeta_{4n}\right],$$

donc $K \subseteq \mathbb{Q}[\zeta_n]$ ou $K \subseteq \mathbb{Q}[\zeta_{4n}]$ selon la congruence de n modulo 4 : d'où le résultat.

Remarque. Auriez-vous réussi à montrer que $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{5}$ sont des combinaisons linéaires de racines de l'unité sans passer par ce calcul très savant de τ_n ?

Questions à se poser, réflexes à acquérir. Encore une fois, pourquoi vérifier $\sqrt{n} \in \mathbb{Q}[\zeta_n]$ suffit pour avoir $K \subseteq \mathbb{Q}[\zeta_n]$?

Quatrième partie – Réciprocité quadratique

22. On doit montrer que si q est un carré modulo p, alors : $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\zeta_p)^{qx^2} = \sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\zeta_p)^{x^2}$: cette « disparition » de q laisse entendre qu'on a fait un changement d'indice. En effet, l'application $y \mapsto qy$ est une permutation de l'ensemble des carrés comme on le vérifie aisément (sa réciproque est $y \mapsto q^{-1}y$), donc : $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\zeta_p)^{qx^2} = \sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\zeta_p)^{x^2} = \tau_p = \left(\frac{q}{p}\right)\tau_p$.

Supposons à présent que q n'est pas un carré modulo p. La remarque de la question 2 assure que le sous-groupe H des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ (pourquoi est-ce un groupe ?) est de cardinal $\frac{p-1}{2}$, donc l'ensemble quotient $(\mathbb{Z}/p\mathbb{Z})^\times/H$ est de cardinal 2 : il admet deux classes ; la classe de l'élément neutre et une autre classe qui contient tous les non carrés. Comme q n'est pas un carré modulo p, il est dans la seconde classe, donc : $(\mathbb{Z}/p\mathbb{Z})^\times = H \sqcup qH$. On en déduit :

$$\sum_{y\in(\mathbb{Z}/p\mathbb{Z})^\times} (\zeta_p)^y = \sum_{y\in H} (\zeta_p)^y + \sum_{y\in qH} (\zeta_p)^{qy} \overset{(*)}{=} \frac{1}{2}\left(\sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\times} (\zeta_p)^{x^2} + \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\times} (\zeta_p)^{qx^2}\right).$$

L'égalité $(*)$ vient du fait que $x^2 = (-x)^2$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$: il faut éviter les doublons pour bien avoir la somme sur tous les carrés. Or :

$$\sum_{y\in(\mathbb{Z}/p\mathbb{Z})^\times} (\zeta_p)^y = \sum_{y\in\mathbb{Z}/p\mathbb{Z}} (\zeta_p)^y - 1 = -1,$$

suivant un calcul classique déjà effectué à la question 13 sous une forme légèrement différente (c'est une somme géométrique). Donc :

$$\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\zeta_p)^{qx^2} = \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\times} (\zeta_p)^{qx^2} + 1 = -2 - \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\times} (\zeta_p)^{x^2} + 1 = -\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\zeta_p)^{x^2},$$

c'est-à-dire : $\displaystyle\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\zeta_p)^{qx^2} = -\tau_p = \left(\frac{q}{p}\right)\tau_p$, d'où le résultat.

Questions à se poser, réflexes à acquérir. Vérifier ce que j'ai omis (que $y \mapsto qy$ permute l'ensemble des carrés : pourquoi est-ce bien à valeurs dans l'ensemble des carrés, en premier lieu ?).

23. Considérons $\varphi : \begin{cases} \mathbb{Z}^2 & \to & \mathbb{Z}/pq\mathbb{Z} \\ (x,y) & \mapsto & (xp+yq) \bmod pq. \end{cases}$. C'est un morphisme de groupes. Soit $(x,y) \in \mathbb{Z}^2$. On a :

$$\varphi(x,y) = 0 \bmod pq \iff pq \mid xp+yq \overset{(1)}{\iff} \begin{cases} p \mid xp+yq \\ q \mid xp+yq \end{cases} \iff \begin{cases} p \mid yq \\ q \mid xp \end{cases} \overset{(2)}{\iff} \begin{cases} p \mid y \\ q \mid x \end{cases},$$

car p et q sont premiers entre eux (on l'utilise pour l'implication réciproque de (1), puis pour le lemme d'Euclide dans l'implication directe de (2)). On en déduit : $\ker(\varphi) = q\mathbb{Z} \times p\mathbb{Z}$, et par le théorème de factorisation des morphismes l'application suivante :

$$\phi : \begin{cases} \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/pq\mathbb{Z} \\ (x \bmod q, y \bmod p) & \mapsto & \varphi(x,y) \end{cases}$$

est bien définie et est injective. Les ensembles de départ et d'arrivée ayant même cardinal fini, ϕ est bijective : d'où le résultat.

Remarque. Le théorème de factorisation des morphismes étant hors programme, vous deviez normalement expliquer pourquoi, si $x \equiv x' \bmod q$ et $y \equiv y' \bmod p$, on a : $\varphi(x,y) = \varphi(x',y')$. Cela ne rallonge pas la rédaction : il suffit de reprendre ce qui a été écrit plus haut en remplaçant x et y par $x - x'$ et $y - y'$ dans les relations de divisibilité. L'injectivité est immédiate quand cette vérification est faite : si $\phi(x \bmod q, y \bmod p) \equiv 0 \bmod pq$, alors par le raisonnement ci-dessus p divise y et q divise x, donc $(x \bmod q, y \bmod p) = (0 \bmod q, 0 \bmod p)$ et le noyau est trivial.

Questions à se poser, réflexes à acquérir.

— Le théorème de factorisation des morphismes devrait plutôt impliquer que $\phi : \mathbb{Z}^2/(q\mathbb{Z}\times p\mathbb{Z}) \to \mathbb{Z}/pq\mathbb{Z}$ est bien définie, pourtant ce n'est pas ce que j'ai écrit. Se convaincre que cela donne bien la même chose que $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

— Aurait-on pu montrer la surjectivité de ϕ autrement ? Peut-on expliciter la bijection réciproque ?

24. On a, par la formule du changement de variable avec la bijection $(x \bmod q, y \bmod p) \mapsto (xp + yq) \bmod pq$ de la question précédente :

$$\tau_{pq} = \sum_{z\in\mathbb{Z}/pq\mathbb{Z}} (\zeta_{pq})^{z^2} = \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \sum_{y\in\mathbb{Z}/p\mathbb{Z}} (\zeta_{pq})^{(xp+yq)^2} = \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \sum_{y\in\mathbb{Z}/p\mathbb{Z}} (\zeta_{pq})^{x^2p^2+y^2q^2+2xypq}.$$

Or : $(\zeta_{pq})^{pq} = 1$, donc :

$$\tau_{pq} = \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \sum_{y\in\mathbb{Z}/p\mathbb{Z}} (\zeta_{pq})^{x^2p^2+y^2q^2} = \left(\sum_{x\in\mathbb{Z}/q\mathbb{Z}} (\zeta_{pq})^{x^2p^2}\right)\left(\sum_{y\in\mathbb{Z}/p\mathbb{Z}} (\zeta_{pq})^{y^2q^2}\right).$$

Enfin : $(\zeta_{pq})^p = \zeta_q$, et de même en inversant les rôles de p et q, donc :

$$\tau_{pq} = \left(\sum_{x\in\mathbb{Z}/q\mathbb{Z}} \zeta_q^{px^2}\right)\left(\sum_{y\in\mathbb{Z}/p\mathbb{Z}} \zeta_p^{qy^2}\right).$$

Or, d'après la question 22, on a : $\displaystyle\sum_{y\in\mathbb{Z}/p\mathbb{Z}} \zeta_p^{qy^2} = \left(\frac{q}{p}\right)\tau_p$, et et on a de même : $\displaystyle\sum_{x\in\mathbb{Z}/q\mathbb{Z}} \zeta_q^{px^2} = \left(\frac{p}{q}\right)\tau_q$,

d'où le résultat : $\tau_{pq} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\tau_p\tau_q$.

25. Remarquons d'abord :

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1 \bmod 4 \text{ ou } q \equiv 1 \bmod 4, \\ -1 & \text{sinon.} \end{cases} \tag{7}$$

Faisons donc une distinction de cas. D'après la question 20 :

— si $p \equiv 3 \bmod 4$ et $q \equiv 3 \bmod 4$, alors : $pq \equiv 1 \bmod 4$, donc : $\tau_{pq} = \sqrt{pq}$, $\tau_p = i\sqrt{p}$ et $\tau_q = i\sqrt{q}$, donc :

$$\tau_{pq} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\tau_p\tau_q \iff \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = -1 \overset{(7)}{=} (-1)^{\frac{p-1}{2}\frac{q-1}{2}};$$

— si $p \equiv 1 \bmod 4$ et $q \equiv 1 \bmod 4$, alors : $pq \equiv 1 \bmod 4$, donc : $\tau_{pq} = \sqrt{pq}$, $\tau_p = \sqrt{p}$ et $\tau_q = \sqrt{q}$, donc :

$$\tau_{pq} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\tau_p\tau_q \iff \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = 1 \overset{(7)}{=} (-1)^{\frac{p-1}{2}\frac{q-1}{2}};$$

— si $p \equiv 1 \bmod 4$ et $q \equiv 3 \bmod 4$, alors : $pq \equiv 3 \bmod 4$, donc : $\tau_{pq} = i\sqrt{pq}$, $\tau_p = \sqrt{p}$ et $\tau_q = i\sqrt{q}$, donc :

$$\tau_{pq} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\tau_p\tau_q \iff \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = 1 \overset{(7)}{=} (-1)^{\frac{p-1}{2}\frac{q-1}{2}};$$

et de même si on inverse les rôles de p et q.

Dans tous les cas, on a bien : $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, ce qu'on voulait démontrer.

Remarque. Cette identité est ce qu'on appelle la *loi de réciprocité quadratique*.

Questions à se poser, réflexes à acquérir.

— Vérifier les valeurs de $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ annoncées.

— Était-il possible d'alléger la rédaction en proposant une expression de τ_n valable pour tout n ?

26. Notons que d'après la question 12, on a : $\mathcal{O}_K = \mathbb{Z}[i]$ (on a en effet, avec la notation de l'énoncé : $i = \sqrt{-1}$, et : $-1 \equiv 3 \bmod 4$).

D'après la formule du binôme de Newton, on a :

$$(1+i)^q = \sum_{k=0}^{q} \binom{q}{k} i^k = 1 + i^q + \sum_{k=1}^{q} \binom{q}{k} i^k \equiv 1 + i^q \bmod q.$$

Montrons alors que pour tout $k \in [\![1, q-1]\!]$, le nombre premier q divise $\binom{q}{k}$. Nous proposons une autre démonstration, plus classique, que celle vue en travaux dirigés. Soit $k \in [\![1, q-1]\!]$. On a :

$$k!(q-k)!\binom{q}{k} = q! = q \cdot (q-1)!.$$

On en déduit que q divise $k!(q-k)!\binom{q}{k}$. Cependant il ne divise pas les entiers entre 1 et k (puisqu'ils lui sont tous strictement inférieurs par hypothèse sur k), donc par le lemme d'Euclide q ne divise pas $k!$. Par le même raisonnement, q ne divise pas $(q-k)!$. Toujours par le lemme d'Euclide, on en déduit que q divise $\binom{q}{k}$, ce qu'on voulait démontrer. On peut alors écrire, pour tout $k \in [\![1, q-1]\!]$, le coefficient binomial sous la forme : $\binom{q}{k} = q \cdot n_k$, avec $n_k \in \mathbb{N}$. Ensuite, en reprenant le calcul ci-dessus :

$$(1+i)^q = 1 + i^q + q\sum_{k=1}^{q} n_k i^k.$$

En posant : $x = \sum_{k=1}^{q} n_k i^k$ (qui appartient bien à $\mathcal{O}_K$ en tant que somme d'éléments de cet anneau), on a bien : $(1+i)^q = 1 + i^q + qx$, ce qu'il fallait démontrer.

Questions à se poser, réflexes à acquérir.

- Comprendre en quoi c'est le lemme d'Euclide qui permet d'affirmer que p ne divise pas $k!$ ni $(p-k)!$. Vérifier qu'il est en général faux de penser que n ne divise pas $k!$ pour tout $k < n$.
- On avait démontré : $(X + \bar{1})^p = X^p + \bar{1}$, en travaux dirigés, par une autre méthode. Comparer avec l'identité de cette question.
- J'avais aussi dit, en travaux dirigés, que dans tout *corps* K contenant $\mathbb{Z}/p\mathbb{Z}$, on a : $\forall (x,y) \in K^2$, $(x+y)^p = x^p + y^p$. Pouvait-on s'en servir dans cette question ? Que dire de $\mathcal{O}_K/q\mathcal{O}_K$?
- La démonstration de la divisibilité de $\binom{p}{k}$ par p étant très classique : retenir sa démonstration préférée, parmi celles abordées.

27. Comme q est impair, on peut écrire :

$$(1+i)^q = \left((1+i)^2\right)^{\frac{q-1}{2}}(1+i) = (2i)^{\frac{q-1}{2}}(1+i).$$

Or, d'après la question 2, on a : $2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) \bmod q$. Considérons donc $k \in \mathbb{Z}$ tel que : $2^{\frac{q-1}{2}} = \left(\frac{2}{q}\right) + kq$. D'après le calcul ci-dessus, on a :

$$(1+i)^q = \left(\frac{2}{q}\right) i^{\frac{q-1}{2}}(1+i) + kqi^{\frac{q-1}{2}}(1+i).$$

En posant : $x' = ki^{\frac{q-1}{2}}(1+i) \in \mathcal{O}_K$, on a donc : $(1+i)^q = \left(\frac{2}{q}\right) i^{\frac{q-1}{2}}(1+i) + qx'$. En combinant cette égalité avec celle de la question précédente, on a donc :

$$(1+i^q) - \left(\left(\frac{2}{q}\right) i^{\frac{q-1}{2}}(1+i)\right) = q(x'-x). \tag{8}$$

On voudrait en déduire : $(1+i^q) = \left(\frac{2}{q}\right) i^{\frac{q-1}{2}}(1+i)$ (ce qui revient à dire que $x = x'$). En effet, une fois cette égalité prouvée, il suffit d'isoler $\left(\frac{2}{q}\right)$ pour en avoir une valeur explicite, et partant de là il n'est plus difficile de vérifier que cela coïncide avec l'expression de l'énoncé. C'est donc

l'objectif de ce qui suit. On raisonne par l'absurde en comparant le module de chaque membre de l'égalité.
Si $x \neq x'$, alors : $|x'-x| \geqslant 1$. En effet, $x'-x$ est un élément de $\mathbb{Z}[i] = \{a+bi \mid (a,b) \in \mathbb{Z}^2\}$, et le module au carré d'un élément de $\mathbb{Z}[i]$ est donc la somme de deux entiers au carré : dès que l'un des deux est non nul, cela donne une quantité supérieure ou égale à 1. Comme q est un nombre premier impair, cela implique : $|q(x'-x)| \geqslant 3$, or par l'inégalité triangulaire on a :

$$\left|(1+i^q) - \left(\left(\frac{2}{q}\right) i^{\frac{q-1}{2}}(1+i)\right)\right| \leqslant |1+i^q| + \left|\left(\frac{2}{q}\right) i^{\frac{q-1}{2}}(1+i)\right| = |1+i^q| + |1+i|$$

Ces deux nombres sont de module $\sqrt{2}$. Pour $1+i$ c'est un calcul facile, et pour $1+i^q$ on peut par exemple noter que si q est impair, alors : $1+i^q = 1 \pm i = \sqrt{2}e^{\pm\frac{i\pi}{4}}$. Donc :

$$\left|(1+i^q) - \left(\left(\frac{2}{q}\right) i^{\frac{q-1}{2}}(1+i)\right)\right| \leqslant 2\sqrt{2} < 3, \quad (\text{car } 8 < 9)$$

ce qui contredit l'égalité (8).
Par l'absurde, on a donc : $x = x'$, puis :

$$\left(\frac{2}{q}\right) = i^{\frac{1-q}{2}} \frac{1+i^q}{1+i} = e^{\frac{i\pi(1-q)}{4} - \frac{i\pi}{4} + \frac{iq\pi}{4}} \frac{2\cos\left(\frac{q\pi}{4}\right)}{\sqrt{2}} = \sqrt{2}\cos\left(\frac{q\pi}{4}\right),$$

et on vérifie pour chaque valeur possible de q mod 8 que cette expression est égale à $(-1)^{\frac{q^2-1}{8}}$: dans les deux cas, cela vaut 1 si et seulement si $q \equiv \pm 1 \bmod 8$, et -1 sinon. D'où le résultat.

Questions à se poser, réflexes à acquérir.
- Comprendre ce qui put motiver mon idée de comparer les modules pour avoir l'égalité finale. Pour cela : éventuellement se demander comment on aurait fait si l'égalité avait été modulo q, mais dans $\mathbb{Z}$.
- Au vu du membre de gauche, le membre de droite de l'égalité finale doit être un réel : pouvait-on le voir sans la moindre simplification ?
- Vérifier ce que j'eus la paresse de vérifier en fin de raisonnement.

28. Notons d'abord que par définition du symbole $\left(\frac{\cdot}{p}\right)$ et par la question 2, on a pour tout nombre premier impair p et tout entier x premier avec p :

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \bmod p.$$

Cette égalité implique en particulier :

$$\forall (\bar{x},\bar{y}) \in \left((\mathbb{Z}/p\mathbb{Z})^\times\right)^2, \left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right), \text{ et : } \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1 \bmod 4, \\ -1 & \text{si } p \equiv -1 \bmod 4. \end{cases}$$

Ces deux égalités, ainsi que la loi de réciprocité quadratique (l'identité $(*)$ de l'énoncé, qu'on peut réinterpréter ainsi : $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ si p ou q est congru à 1 modulo 4, et $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ sinon), vont permettre de calculer $\left(\frac{101}{691}\right)$ très rapidement :

$$\left(\frac{101}{691}\right) = \left(\frac{691}{101}\right) = \left(\frac{85}{101}\right) = \left(\frac{5}{101}\right)\left(\frac{17}{101}\right) = \left(\frac{101}{5}\right)\left(\frac{101}{17}\right) = \left(\frac{1}{5}\right)\left(\frac{-1}{17}\right) = 1,$$

donc 101 est un carré modulo 691.

Questions à se poser, réflexes à acquérir.

— J'utilise allègrement le fait que le symbole $\left(\frac{x}{p}\right)$ ne dépende pas du représentant de x mod p : pourquoi est-ce vrai ?

— Vérifier la justesse de la simplification de $(-1)^{\frac{p-1}{2}}$ proposée. Remarquer que cette égalité donne aisément la condition nécessaire et suffisante pour que -1 soit un carré, comme si de rien n'était.

— J'ai comparé $\left(\frac{x}{p}\right)$ et $x^{\frac{p-1}{2}}$ MODULO p dans un premier temps, puis j'ai écrit une égalité dans $\mathbb{Z}$ dans le cas $x = -1$. Négligence de ma part ?

— Plus généralement, sauriez-vous donner un algorithme de calcul de $\left(\frac{a}{p}\right)$ ainsi que sa complexité informatique, en fonction de la taille de p ?

29. Soit $n \in \mathbb{Z}$ non carré, montrons qu'il existe une infinité de nombres premiers ℓ tels que n mod ℓ ne soit pas un carré dans $\mathbb{Z}/\ell\mathbb{Z}$. Décomposons n en facteurs premiers : $n = (-1)^{\alpha_0} 2^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ où les p_i sont des nombres premiers impairs distincts et les α_i sont des entiers naturels non nul. Puisque n n'est pas un carré, l'un des α_i est impair.

Premier cas. S'il existe $i \geqslant 2$ tel que α_i soit impair, par exemple si α_2 est impair : soit $x \in \mathbb{Z}$ non carré modulo p_2 (un tel entier existe car le nombre de carrés distincts dans $\mathbb{Z}/p_2\mathbb{Z}$ est $\frac{p_2+1}{2} < p_2$, d'après la remarque de la question 2). D'après le théorème de la progression arithmétique et le théorème chinois, il existe une infinité de nombres ℓ premiers vérifiant les congruences simultanées :

$$\ell \equiv 1 \bmod 8, \qquad \ell \equiv x \bmod p_2, \qquad \forall i \in [\![3, k]\!],\ \ell \equiv 1 \bmod p_i,$$

donc -1 et 2 sont des carrés modulo ℓ (pour -1 c'est conséquence du fait que $(-1)^{\frac{\ell-1}{2}} = 1$ si ℓ est congru à 1 modulo 4, et pour 2 c'est conséquence de la question 27 : d'après cette question, 2 est un carré modulo ℓ si et seulement si $\ell \equiv \pm 1 \bmod 8$ ou $\ell = 2$), et ℓ est un carré modulo $p_3, \dots, p_k$. Or : $\ell \equiv 1$ mod 4, donc par la loi de réciprocité quadratique $(*)$ les nombres premiers $p_3, \dots, p_k$ sont des carrés modulo ℓ.

Par contre ℓ n'est pas un carré modulo p_2 et donc, par l'identité $(*)$, le nombre premier p_2 n'est pas un carré modulo ℓ. Ainsi, n est congru modulo ℓ au produit d'un carré par une puissance impaire d'un non carré, c'est un non carré modulo ℓ.

Deuxième cas. Si α_1 est impair : on considère de même les nombres premiers ℓ vérifiant :

$$\ell \equiv 5 \bmod 8, \qquad \forall i \in [\![3, k]\!],\ \ell \equiv 1 \bmod p_i.$$

Pour un tel ℓ, les entiers $-1, p_2, \dots, p_k$ sont des carrés modulo ℓ tandis que 2 n'en est pas un et donc n non plus (raisonnement analogue).

Troisième cas. Si α_0 est impair et tous les autres α_i sont pairs : alors tout nombre premier ℓ tel que $\ell \equiv 3$ mod 4 convient car $-n$ est un carré modulo ℓ et -1 n'en est pas un.

D'où le résultat dans tous les cas.

Questions à se poser, réflexes à acquérir.

— Noter là une très belle application du théorème chinois : fabriquer des entiers vérifiant LES RELATIONS DE CONGRUENCE QUE L'ON VEUT ! C'est aussi ainsi qu'on peut l'utiliser dans le critère de Korselt (feuille d'exercices).

— Pourquoi c'est le théorème de la progression arithmétique qui permet d'avoir une infinité de nombres premiers vérifiant les congruences proposées ? On ne reconnaît pas vraiment l'énoncé du devoir.