Exercices d'algèbre – Fiche 1: Exemples de formes quadratiques

Responsable: Isar Stubbe

---

1. Déterminer les formes quadratiques parmi les applications suivantes. Le cas échéant, donner la forme bilinéaire symétrique associée, ainsi qu'une matrice symétrique (pour une base au choix).

   (a) $q\colon \mathbb{R}^6 \to \mathbb{R}\colon (x_1, ..., x_6) \mapsto x_1x_2 + 2x_2x_3 - x_3^2 + x_5(x_5 + x_6)$

   (b) $q\colon \mathbb{R}^{n\times n} \to \mathbb{R}\colon M \mapsto \det(M)$ (Donner une réponse en fonction de n.)

   (c) $q\colon \mathbb{R}[X]_{\leq n} \to \mathbb{R}\colon p \mapsto \int_0^1 p(x)dx$

   (d) $q\colon \mathbb{C} \to \mathbb{R}\colon z \mapsto z\bar{z}$

   (e) $q\colon \mathbb{C} \to \mathbb{C}\colon z \mapsto z\bar{z}$

2. Parmi les applications ci-dessous, déterminer les formes bilinéaires. Pour chaque forme bilinéaire, donner la forme quadratique associée, la forme bilinéaire *symétrique* associée à cette forme quadratique, et une matrice symétrique de cette forme bilinéaire symétrique (pour une base au choix).

   (a) $b\colon \mathbb{R}^5 \times \mathbb{R}^5 \to \mathbb{R}\colon ((x_1, ..., x_5), (y_1, ..., y_5)) \mapsto x_1y_2 - (3x_3 + x_2)y_5$

   (b) $b\colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}\colon (z_1, z_2) \mapsto i \cdot |z_1| \cdot \overline{z_2}$

   (c) $b\colon \mathbb{C} \times \mathbb{C} \to \mathbb{R}\colon (z_1, z_2) \mapsto \Re(z_1 + z_2)$

   (d) $b\colon \mathbb{Q}^{3\times 3} \times \mathbb{Q}^{3\times 3} \to \mathbb{Q}\colon (A, B) \mapsto \mathrm{tr}(A^tB)$

   (e) $b\colon \mathbb{R}[X]_{\leq 3} \times \mathbb{R}[X]_{\leq 3} \to \mathbb{R}\colon (P, Q) \mapsto \int_0^1 tP(t)Q'(t)dt$

3. Soit la forme quadratique $q\colon \mathbb{R}^3 \to \mathbb{R}\colon (x_1, x_2, x_3) \mapsto -2(x_1x_2 + x_2x_3) + 2x_2(x_2 + x_3) + 3x_3^2$.

   (a) Donner sa matrice par rapport à la base canonique.

   (b) Expliquer pourquoi il n'est pas possible de construire une base q-orthogonale par le procédé de Gram-Schmidt partant de la base canonique.

4. Soit la forme quadratique $q\colon \mathbb{R}^3 \to \mathbb{R}\colon (x_1, x_2, x_3) \mapsto -2x_1^2 - 2x_2^2 - 5x_3^2 + 2x_1x_2 - 2x_1x_3 - 4x_2x_3$.

   (a) Donner sa matrice par rapport à la base canonique.

   (b) Trouver une base q-orthogonale par le procédé de Gram-Schmidt partant de la base canonique. Est-il possible d'en déduire une base q-ortho*normale* de $\mathbb{R}^3$?

   (c) Ecrire la matrice de q par rapport à cette base orthogonale.

   (d) Exprimer le lien entre les deux matrices trouvées ci-dessus.

5. Notons $\mathrm{Bilin}(V)$ l'espace des formes bilinéaires sur V. Une forme bilinéaire $b\colon V \times V \to K$ est *symétrique* si $b(\underline{x}, \underline{y}) = b(\underline{y}, \underline{x})$ et *alternée* si $b(\underline{x}, \underline{y}) = -b(\underline{y}, \underline{x})$.

   (a) Montrer que les formes symétriques forment un sous-espace $\mathrm{Sym}(V) \subseteq \mathrm{Bilin}(V)$.

   (b) Montrer que les formes alternées forment un sous-espace $\mathrm{Alt}(V) \subseteq \mathrm{Bilin}(V)$.

   (c) Montrer que $\mathrm{Bilin}(V) = \mathrm{Sym}(V) \oplus \mathrm{Alt}(V)$.

   (d) Vérifier que $\mathrm{Sym}(V)$ et $\mathrm{Alt}(V)$ sont exactement les espaces propres de l'application linéaire $\tau\colon \mathrm{Bilin}(V) \to \mathrm{Bilin}(V)$ définie par $\tau(b)(\underline{x}, \underline{y}) = b(\underline{y}, \underline{x})$.

   (e) Comment traduire ces résultats en language matriciel?

Exercices d'algèbre – Fiche 2: Réduction de formes quadatiques sur $\mathbb{R}^n$

Responsable: Isar Stubbe

---

1. Démontrer que n formes linéaires $\phi_i\colon \mathbb{R}^n \to \mathbb{R}\colon (x_1,...,x_n) \mapsto \sum_j a_{ij}x_j$ forment une base de $(\mathbb{R}^n)^*$ si et seulement si la matrice $A = (a_{ij})_{ij}$ est inversible; dans ce cas, $(\phi_1,...,\phi_n)$ est la base duale de la base formée par les colonnes de A^{-1}. Appliquer cette méthode à:

   (a) $\phi_1(x,y) = 3x + 2y$, $\phi_2(x,y) = -x + 4y$

   (b) $\phi_1(x,y,z) = 3x - y + z$, $\phi_2(x,y,z) = -x + z$, $\phi_3(x,y,z) = x + y + z$

   (c) $\phi_1(x_1,...,x_4) = x_1 + x_2 + x_3 + x_4$, $\phi_2(x_1,...,x_4) = -x_1 + x_2 + x_3 + x_4$,
   $\phi_3(x_1,...,x_4) = -x_1 - x_2 + x_3 + x_4$, $\phi_4(x_1,...,x_4) = -x_1 - x_2 - x_3 + x_4$

2. Ecrire chaque forme quadratique $q\colon \mathbb{R}^n \to \mathbb{R}$ comme une somme pondérée de carrés de formes linéaires indépendantes par la méthode de réduction de Gauss, en déduire une base q-orthogonale de $\mathbb{R}^n$, puis le rang et la signature de q:

   (a) $q(x,y) = x^2 + xy$

   (b) $q(x,y,z) = 3x^2 + 4xy - 5y^2 - xz + \frac{13}{3}yz$

   (c) $q(x,y,z) = 3x^2 + 11y^2 - z^2 + 2xy - 2xz - 6yz$

   (d) $q(x,y,z) = x^2 + 3xy$

   (e) $q(x,y,z,t) = xy + yz + zt + tx$

3. Pour chaque matrice réelle symétrique donnée, faire la réduction de Gauss d'une forme quadratique associée pour trouver une matrice diagonale congruente, et préciser la matrice de passage:

$$A = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 3 \\ 0 & 3 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

4. Soit une forme quadratique réelle $q\colon \mathbb{R}^n \to \mathbb{R}$ de rang complet, et b la forme bilinéaire symétrique associée. Montrer l'équivalence de:

   (a) pour tout $t \in \mathbb{R}$ il existe un $\underline{x} \in \mathbb{R}^n$ tel que $q(\underline{x}) = t$ (q est une forme *universelle*).

   (b) il existe un $\underline{x} \in \mathbb{R}^n \setminus \{\underline{0}\}$ tel que $q(\underline{x}) = 0$ ($\underline{x}$ est un vecteur *isotrope*),

   (c) il existe $\underline{x}, \underline{y} \in \mathbb{R}^n$ tels que $q(\underline{x}) = 0 = q(\underline{y})$ et $b(\underline{x}, \underline{y}) = 1$ ($(\underline{x}, \underline{y})$ est une *paire hyperbolique*).

   Indication: (a⇒b) Utiliser une base orthogonale. (b⇒c) Utiliser que le rang de q est complet pour montrer qu'il existe un $\underline{y}_0 \neq \underline{0}$ tel que $b(\underline{x}, \underline{y}_0) \neq 0$. Déterminer $\underline{y} = r\underline{x} + s\underline{y}_0$ par les conditions $b(\underline{x}, \underline{y}) = 1$ et $b(\underline{y}, \underline{y}) = 0$. (c⇒a) Calculer $q(r\underline{x} + s\underline{y})$.

5. Par le Théorème Spectral de l'algèbre linéaire, pour toute matrice symétrique réelle A on peut trouver une matrice orthogonale B telle que B^tAB soit diagonale. Expliquer comment on peut s'en servir pour réduire des formes quadratiques réelles. Quels sont les avantages et/ou les inconvénients de cette méthode de réduction (comparée avec la méthode de Gauss et le procédé de Gram-Schmidt)?

Exercices d'algèbre – Fiche 3: Lemme de Zorn

Responsable: Isar Stubbe

---

1. *Reformulations du lemme de Zorn.* Montrer l'équivalence des assertions suivantes:

   (a) Dans tout ensemble ordonné, toute chaîne est contenue dans une chaîne maximale.

   (b) Tout ensemble ordonné contient une chaîne maximale.

   (c) Tout ensemble ordonné dont toute chaîne est majorée, a un élément maximal.

   (d) Tout ensemble ordonné non-vide dont toute chaîne non-vide est majorée, a un élément maximal.

   Indication. (a⇒b) Considérer la chaîne vide. (b⇒c) Considérer un majorant d'une chaîne maximale. (c⇒a) Soit une chaîne C dans un ensemble ordonné $(P, \leq)$. L'ensemble des chaînes dans $(P, \leq)$ contenant C est ordonné par inclusion, et toute chaîne $\mathcal{C}$ dans cet ensemble ordonné (une chaîne de chaînes, donc) est majorée par $\bigcup \mathcal{C}$. Conclure. (c⇔d) Etudier la chaîne vide.

2. *Le lemme de Zorn implique le théorème de Bernstein.* Pour tous ensembles X et Y, il existe une injection $X \to Y$ ou une injection $Y \to X$.

   (a) Observer que le théorème est trivial lorsque $X = \emptyset$ ou $Y = \emptyset$. Dans la suite on supposera que $X \neq \emptyset \neq Y$.

   (b) Montrer qu'une relation $R \subseteq X \times Y$ entre X et Y satisfait à

   $$\text{si } (x, y) \in R \text{ et } (x', y) \in R \text{ alors } x = x', \text{ et si } (x, y) \in R \text{ et } (x, y') \in R \text{ alors } y = y'$$

   si et seulement si R est le graphe d'une *bijection partielle* entre X et Y.

   (c) Montrer que l'ensemble de ces relations est non-vide et ordonné par l'inclusion de relations.

   (d) Soit une chaîne non-vide $\mathcal{C}$ dans cet ensemble ordonné. Montrer que $\bigcup \mathcal{C}$ en est un majorant.

   (e) Par le lemme de Zorn il existe un élément maximal $P_{\mathsf{max}} \subseteq X \times Y$. Montrer que la relation P_{max} est le graphe d'une injection $X \to Y$ ou que la relation opposée $P_{\mathsf{max}}^{\mathsf{op}}$ est le graphe d'une injection $Y \to X$.

3. *Le lemme de Zorn implique le principe de bon ordre.* Tout ensemble peut être bien ordonné.

   (a) Observer que tout est trivial pour l'ensemble vide; considérons donc un ensemble $A \neq \emptyset$.

   (b) Notons $(B, \leq_B)$ pour un sous-ensemble $B \subseteq A$ muni d'un bon ordre $\leq_B$. Montrer qu'il existe au moins une telle paire $(B, \leq_B)$.

   (c) Ecrivons $(B, \leq_B) \preccurlyeq (C, \leq_C)$ lorsque $(B, \leq_B)$ est un *segment initial* de $(C, \leq_C)$: cela veut dire que $B \subseteq C$, $\leq_C$ coïncide avec $\leq_B$ sur B, et $x \leq_C y$ pour tout $x \in B$ et $y \in C \setminus B$. Montrer qu'il s'agit d'une relation d'ordre.

   (d) Soit une chaîne non-vide $\mathcal{C}$ dans cet ensemble ordonné. Poser $C := \bigcup \{B \mid (B, \leq_B) \in \mathcal{C}\}$ et définir un <u>bon</u> ordre $\leq_C$ adéquat pour montrer que $\mathcal{C}$ est majorée par $(C, \leq_C)$.

   (e) Par le lemme de Zorn il existe un élément maximal $(B, \leq_B)$. Montrer que $B = A$ et conclure. Indication: s'il existe $a \in A \setminus B$ alors on peut définir $(B', \leq_{B'})$ par $B' = B \cup \{a\}$ et $b \leq_{B'} a$ pour tout $b \in B$.

Exercices d'algèbre – Fiche 4: Axiome du choix

Responsable: Isar Stubbe

---

1. *Reformulations de l'axiome du choix.* Démontrer l'équivalence des assertions suivantes:

   (a) Pour toute famille d'ensembles non-vides $(A_i)_{i\in I}$, le produit cartésien $\prod_{i\in I} A_i$ est non-vide.

   (b) Pour toute surjection $f\colon A \to B$ il existe $g\colon B \to A$ tel que $f \circ g = \mathsf{id}_B$.

   (c) Toute relation entière $R \subseteq A \times B$ contient une fonction $f\colon A \to B$. (Une relation $R \subseteq A \times B$ est *entière* si pour tout $a \in A$ il existe $b \in B$ tel que $(a, b) \in R$.)

   (d) Pour tout ensemble A il existe une *fonction de choix*, i.e. $f\colon \mathcal{P}(A) \setminus \{\emptyset\} \to A$ telle que $f(X) \in X$ pour tout $\emptyset \neq X \subseteq A$.

2. *Axiome du choix dénombrable.* Par définition, un ensemble D est *dénombrable* lorsqu'il existe une injection $D \to \mathbb{N}$.

   (a) Montrer: un ensemble dénombrable est soit fini, soit en bijection avec $\mathbb{N}$.

   (b) Démontrer sans utiliser l'axiome du choix que, pour toute famille *finie* d'ensembles non-vides $(A_i)_{i\in I}$, le produit cartésien est non-vide.

   (c) En déduire l'équivalence des assertions suivantes:

      (i) Pour toute famille *dénombrable* d'ensembles non-vides $(A_i)_{i\in I}$, le produit cartésien $\prod_{i\in I} A_i$ est non-vide.

      (ii) Pour toute famille d'ensembles non-vides $(A_n)_{n\in\mathbb{N}}$, le produit cartésien $\prod_{n\in\mathbb{N}} A_n$ est non-vide.

      Ce sont deux formulations équivalentes de l'*axiome du choix dénombrable*. L'axiome du choix est strictement plus fort que l'axiome du choix dénombrable.

   (d) Utiliser l'axiome du choix dénombrable pour démontrer que toute réunion dénombrable d'ensembles dénombrables est un ensemble dénombrable.
   Indication. Notons $(A_i)_{i\in I}$ pour une famille dénombrable d'ensembles dénombrables A_i. Par hypothèse on a une injection $f\colon I \to \mathbb{N}$. Si on pose $B_i = \{f\colon A_i \to \mathbb{N} \mid f \text{ est injective}\}$ alors par hypothèse tout B_i est non-vide, et *par l'axiome du choix dénombrable* on peut trouver des injections $(f_i\colon A_i \to \mathbb{N})_{i\in I}$. Combiner ces ingrédients pour trouver une injection $\bigcup_{i\in I} A_i \to \mathbb{N}$.

   (e) Où utilise-t-on l'axiome du choix dénombrable lorsqu'on démontre qu'une fonction $f\colon \mathbb{R} \to \mathbb{R}$ est continue en $x \in \mathbb{R}$ (selon la "définition ε-δ") si et seulement si l'image par f de toute suite de limite x est une suite de limite $f(x)$?

3. *Le principe de bon ordre implique l'axiome du choix.* Pour tout bon ordre $(A, \leq)$, montrer que $f : \mathcal{P}(A) \setminus \emptyset \to A\colon X \mapsto \min(X)$ est (bien définie et) une fonction de choix.

4. *L'axiome du choix implique le lemme de Zorn.* Pour une démonstation élégante et élémentaire, voir [Jonathan Lewin, *A Simple Proof of Zorn's Lemma*, The American Mathematical Monthly **98** pp. 353–354, 1991].

   "Disasters happen without the axiom of choice, disasters happen with the axiom of choice", peut-on lire dans le livre Axiom of Choice *de H. Herrlich [Springer Lecture Notes Math., 2006], entièrement dédié à "the most controversial axiom in mathematics".*

Exercices d'algèbre – Fiche 5: Anneaux, homomorphismes, idéaux

Responsable: Isar Stubbe

Dans la suite, tout anneau $A = (A, +, 0, \cdot, 1)$ est supposé commutatif et unitaire, et tout homomorphisme d'anneaux $f\colon A \to B$ préserve $+$, 0, $\cdot$ et 1.

1. Pour E un ensemble quelconque, montrer que $\mathcal{P}(E)$ un anneau pour les opérations $X+Y = X \triangle Y$ (différence symétrique) et $XY = X \cap Y$ (intersection). Montrer que $\mathcal{A} \subseteq \mathcal{P}(E)$ en est un sous-anneau si et seulement si $\mathcal{A}$ contient $\emptyset$ et est stable pour le complémentaire et l'intersection finie.

2. Montrer que $A = \{\frac{a}{b} \mid a, b \in \mathbb{Z} \text{ avec } b \text{ impair}\}$ est un anneau contenant $\mathbb{Z}$ et contenu dans $\mathbb{Q}$. Déterminer les éléments inversibles dans cet anneau. Monter que, si $x \in A$ n'est pas inversible, alors $1 - x$ l'est.

3. Montrer que le produit cartésien de deux anneaux est toujours un anneau (les opérations étant définies 'composante par composante') mais que le produit cartésien de deux corps n'est jamais un corps.

4. Pour un anneau quelconque A, donner tous les homomorphismes de $\mathbb{Z}$ à A. Montrer que les homomorphismes de $\mathbb{Z}[X]$ à A sont en bijection avec les éléments de A.

5. Montrer qu'un sous-ensemble $I \subseteq A$ d'un anneau en est un idéal si et seulement si I est le noyau d'un homomorphisme partant de A, si et seulement si I est le noyau d'un homomorphisme surjectif partant de A.

6. Montrer que, pour deux entiers $m, n \in \mathbb{Z}$, n divise m si et seulement si $(m) \subseteq (n)$, si et seulement le quotient $p\colon \mathbb{Z} \to \mathbb{Z}/(n)$ factorise à travers le quotient $q\colon \mathbb{Z} \to \mathbb{Z}/(m)$ (cela veut dire qu'il existe un homomorphisme $h\colon \mathbb{Z}/(m) \to \mathbb{Z}/(n)$ tel que $h \circ q = p$).

7. Pour un homomorphisme $f\colon A \to B$, prouver que $\mathrm{im}(f)$ est un sous-anneau de B, isomorphe au quotient $A/\ker(f)$. Préciser cette propriété lorsque f est une surjection ou une injection.

8. Montrer que $A = \{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a, b \in \mathbb{R}\}$ est un anneau (commutatif!) pour le produit et la somme matriciels. Déterminer les éléments (non-)inversibles de A. Montrer que les éléments non-inversibles forment un idéal I tel que $A/I \cong \mathbb{R}$.

9. Montrer qu'un anneau non-nul A est un corps si et seulement si A n'admet que les idéaux triviaux, si et seulement si tout homomorphisme de A vers un anneau non-nul est injectif.

Exercices d'algèbre – Fiche 6: Idéaux premiers, idéaux maximaux

Responsable: Isar Stubbe

---

1. Déterminer s'il s'agit d'un idéal ou d'un sous-anneau (ou aucun des deux) lorsqu'on considère:
   (a) l'ensemble des nombres pairs dans $\mathbb{Z}$,
   (b) l'ensemble des nombres impairs dans $\mathbb{Z}$,
   (c) l'ensemble des polynômes de degré pair dans $\mathbb{Q}[X]$,
   (d) l'ensemble des matrices diagonales dans $A = \{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a, b \in \mathbb{R}\}$,
   (e) l'ensemble des polynômes dont 3 est une racine dans $\mathbb{R}[X]$,
   (f) l'ensemble des points de la droite d'équation $3x + 2y = 1$ dans $\mathbb{R} \times \mathbb{R}$,
   (g) l'ensemble $\{\frac{a}{3^k} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$ dans $A = \{\frac{a}{b} \mid a, b \in \mathbb{Z} \text{ avec } b \text{ impair}\}$,
   (h) l'ensemble des sous-ensembles finis dans $\mathcal{P}(\mathbb{N})$.

   (A propos d'un sous-ensemble d'un anneau: quand est-il à la fois un sous-anneau et un idéal?)

2. Un élément $a \in A$ d'un anneau est *nilpotent* s'il existe un $n \in \mathbb{N} \setminus \{0\}$ tel que $a^n = 0$. Montrer que l'ensemble $N(A)$ des nilpotents dans A est un idéal; c'est le *nilradical* de A. Montrer que, pour tout $a \in N(A)$ et tout $b \in A$, $1 + ab$ est inversible. Montrer que le nilradical de $A/N(A)$ est nul.

3. Montrer qu'un quotient A/I est un anneau intègre si et seulement si I est un idéal premier de A, et que ce quotient est un corps si et seulement si I est maximal. (Qu'est-ce que cela dit si on pose $I = (0)$?) En déduire que tout idéal maximal est premier.

4. Soit un homomorphisme d'anneaux $f\colon A \to B$. Montrer que l'image réciproque d'un idéal de B est un idéal de A. Montrer que l'image réciproque d'un idéal premier est un idéal premier. Par contre, pour l'unique homomorphisme $\mathbb{Z} \to \mathbb{Q}$, montrer que l'image réciproque de l'unique idéal maximal de $\mathbb{Q}$ n'est pas maximal dans $\mathbb{Z}$.

5. Utiliser le lemme de Zorn pour montrer que tout idéal propre d'un anneau A est contenu dans un idéal maximal. En déduire que tout élément non-inversible d'un anneau est contenu dans un idéal maximal, et que donc la réunion de tous les idéaux maximaux est l'ensemble des éléments non-inversibles de A. Est-ce un idéal?

6. Soit A un anneau non-trivial. Montrer l'équivalence des assertions suivantes:
   (a) A admet un unique idéal maximal,
   (b) les éléments non-inversibles de A forment un idéal (nécessairement maximal),
   (c) pour tout $x \in A$, soit x est inversible, soit $1 - x$ est inversible.

   Dans ce cas, on dit que A est un *anneau local*, et le quotient de A par son unique idéal maximal est son *corps résiduel*.

7. Montrer que $A = \{\frac{a}{b} \mid a, b \in \mathbb{Z} \text{ avec } b \text{ impair}\}$ est un anneau local, dont le corps résiduel est un corps à deux éléments.

8. Montrer que $A = \{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a, b \in \mathbb{R}\}$ est un anneau local, et calculer son corps résiduel.

Exercices d'algèbre – Fiche 7: Anneaux de polynômes

Responsable: Isar Stubbe

Pour $f = f_n X_n + ... + f_1 X + f_0 \in A[X]$ et $a \in A$, on note $f(a) := f_n a^n + ... + f_1 a + f_0$ et on dit que a est une *racine* de f si $f(a) = 0$. Rappellons qu'un élément d'un anneau est *irréductible* s'il est non-nul, non-inversible, et sans diviseurs propres; un élément est *premier* s'il est non-nul et engendre un idéal premier.

1. Quelque soit l'anneau A, montrer que $A[X]$ n'est jamais un corps.

2. Diviser (avec reste) ou expliquer pourquoi ce n'est pas possible:

   (a) $-X^4 + 3X^3 + X^2 - X + 5$ par $2X^2 + X + 1$ dans $\mathbb{Z}[X]$,
   (b) $-X^4 + 3X^3 + X^2 - X + 5$ par $2X^2 + X + 1$ dans $(\mathbb{Z}/(6))[X]$,
   (c) $-X^4 + 3X^3 + X^2 - X + 5$ par $5X^2 + X + 1$ dans $(\mathbb{Z}/(6))[X]$,
   (d) $-X^4 + 3X^3 + X^2 - X + 5$ par $X^2 + X + 1$ dans $\mathbb{Z}[X]$,
   (e) $-X^4 + 3X^3 + X^2 - X + 5$ par $2X^2 + X + 1$ dans $\mathbb{Q}[X]$.

3. Montrer qu'un anneau A est intègre si et seulement si $A[X]$ est intègre. Dans ce cas, observer que $\deg(fg) = \deg(f) + \deg(g)$ pour tous $f, g \in A[X]$. (Par convention, le degré du polynôme zéro est $-\infty$.)

4. Soit A un anneau quelconque. Montrer que, dans $A[X]$, on peut toujours diviser (avec reste) par les polynômes $f = f_n X^n + ... f_1 X + f_0$ avec f_n inversible. En déduire que $a \in A$ est une racine de f si et seulement si $X - a$ divise f dans $A[X]$. Pour $A = \mathbb{Z}/(4)$, donner toutes les racines de $2X^2 + 2X$ et calculer toutes les factorisations obtenues. Montrer que A est intègre si et seulement si tout $0 \neq f \in A[X]$ admet au plus $\deg(f)$ racines.

5. Pour A un anneau quelconque et $a \in A$, montrer que $\gamma \colon A[X] \to A \colon f \mapsto f(a)$ est un homomorphisme surjectif. Quel isomorphisme détermine-t-il? Pour $p, n \in \mathbb{Z}$ avec p premier, montrer que $I = \{f \in \mathbb{Z}[X] \mid p \text{ divise } f(n)\}$ est un idéal premier non-principal de $\mathbb{Z}[X]$.

6. Montrer qu'un anneau A est un corps si et seulement si $A[X]$ est principal.
   Indication. Si A est un corps, alors la division euclidienne de polynômes sert à démontrer que $A[X]$ est principal. Réciproquement, pour $a \neq 0$ dans A on considère l'idéal $(a, X) \subseteq A[X]$. Par hypothèse on a $(a, X) = (f)$ pour un $f \in A[X]$. Ecrire en toutes lettres que $f = f_n X^n + ... + f_1 X + f_0$ divise à la fois a et X, et conclure à l'aide de l'intégralité de ($A[X]$ et de) A que $(a, X) = (f_0) = A[X]$. En déduire que a est inversible.

7. Soit K un corps. Montrer que $K[X, Y]$ est intègre mais pas principal.

   Le Théorème de la base *de D. Hilbert dit que, si A est un anneau noetherien, alors $A[X]$ l'est aussi. Ainsi $K[X, Y]$ est un anneau noetherien qui n'est pas principal. C'est aussi le cas de $\mathbb{Z}[X]$.*

8. Soit A un anneau principal. Montrer que $a \in A$ est irréductible si et seulement si a est premier. Montrer que les idéaux premiers non-nuls coïncident avec les idéaux maximaux non-nuls. En déduire, pour K un corps, que $f \in K[X]$ est irréductible si et seulement si $K[X]/(f)$ est un corps.

9. Soit K un corps. Montrer que tout $f \in K[X]$ de degré 1 est irréductible. Montrer que $f \in K[X]$ de degré 2 ou 3 est irréductible si et seulement si f n'a pas de racine dans K. Qu'en est-il pour f de degré 4 ou plus? Qu'en est-il pour $K = \mathbb{C}$? Qu'en est-il si K n'est pas un corps?

Exercices d'algèbre – Fiche 8: Entiers de Gauss

Responsable: Isar Stubbe

---

1. Vérifier que l'ensemble $\mathbb{Z}[\sqrt{-3}] = \{m + n\sqrt{-3} \mid m, n \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$ contenant l'anneau $\mathbb{Z}$. On va montrer que $\mathbb{Z}[\sqrt{-3}]$ n'est pas à factorisation unique (et donc pas non plus principal ou euclidien). Dans la suite on note $N(z) = z\overline{z}$ pour la *norme* de $z \in \mathbb{C}$.
   (a) Vérifier que $N(z_1 z_2) = N(z_1)N(z_2)$ pour tout $z_1, z_2 \in \mathbb{C}$.
   (b) En déduire les éléments inversibles de $\mathbb{Z}[\sqrt{-3}]$.
   (c) Trouver deux factorisations ("non-associées") de 4 dans $\mathbb{Z}[\sqrt{-3}]$.
   (d) Montrer que 2 est irréductible mais pas premier dans $\mathbb{Z}[\sqrt{-3}]$.

2. Vérifier que l'ensemble $\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\}$ des *entiers de Gauss* est un sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$. On va montrer que cet anneau est euclidien pour la norme $N(z) = z\overline{z}$. Pour $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$, on calcule $z = \frac{a}{b}$ dans $\mathbb{C}$. Soit $z = x + yi$ avec $x, y \in \mathbb{R}$, et notons $m \in \mathbb{Z}$ l'arrondi entier de x, et $n \in \mathbb{Z}$ l'arrondi entier de y. (Faire un dessin dans le plan complexe pour montrer que $m + ni$ est l'entier de Gauss "le plus près" de $x + yi$.)
   (a) Observer que $|x - m| \leq \frac{1}{2}$ et $|y - n| \leq \frac{1}{2}$.
   (b) En déduire que $N\Big(b((x - m) + (y - n)i)\Big) < N(b)$.
   (c) Poser $q = m + ni$, $r = a - bq$, et conclure.
   (d) Diviser (avec reste) $15 + 9i$ par $2 - i$ dans $\mathbb{Z}[i]$.

   On va déterminer les éléments irréductibles de $\mathbb{Z}[i]$. Puisque *irréductible* est synonyme de *premier* dans cet anneau (pourquoi?), on parle de *nombres premiers de Gauss*.
   (e) Déterminer les éléments inversibles de $\mathbb{Z}[i]$.
   (f) En déduire que, si z divise $z' \neq 0$ dans $\mathbb{Z}[i]$, alors z est un diviseur propre si et seulement si $1 < N(z) < N(z')$.
   (g) Montrer que, si z est premier dans $\mathbb{Z}[i]$, alors aussi $\overline{z}$ l'est. Conclure que, dans le plan complexe, les nombres premiers de Gauss présentent une symétrie *par octant*: l'axe réelle, l'axe imaginaire, et leur deux bissectrices, sont des axes de symétrie.
   (h) Montrer que toute somme de carrés d'entiers est un produit dans $\mathbb{Z}[i]$.
   (i) Soit $p = m^2 + n^2 \in \mathbb{Z}$ un nombre premier qui est une somme de carrés non-nuls ($2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, $17 = 1^2 + 4^2$, ...). Montrer que p n'est pas premier dans $\mathbb{Z}[i]$, mais que $m + ni$ l'est (avec $m \neq 0 \neq n$ donc).
   Indication. $N(m + ni) = p$ n'a pas de diviseurs propres dans $\mathbb{N}$.
   (j) Soit $z = m + in$ un élément premier dans $\mathbb{Z}[i]$, avec $m \neq 0 \neq n$. Montrer que $N(z)$ est premier dans $\mathbb{Z}$ (et donc une somme de deux carrés non-nuls).
   Indication. Si $N(z) = rs$ dans $\mathbb{N}$, alors les facteurs premiers de r et s dans $\mathbb{Z}[i]$ donnent des facteurs premiers de $N(z)$ dans $\mathbb{Z}[i]$. Mais $N(z) = z\overline{z}$ est déja une factorisation en facteurs premiers dans $\mathbb{Z}[i]$. Conclure par l'unicité d'une telle factorisation.
   (k) Soit $p \in \mathbb{Z}$ un nombre premier qui n'est pas somme de deux carrés non-nuls (3, 7, 11, ...). Montrer que p est aussi premier dans $\mathbb{Z}[i]$.
   Indication. Si $z = m + ni$ est un diviseur propre de p dans $\mathbb{Z}[i]$, alors $N(z) = m^2 + n^2$ divise $N(p) = p^2$ dans $\mathbb{N}$, et $1 < N(z) < p^2$.
   (l) Finalement, montrer aussi: si $p \in \mathbb{Z}$ est premier dans $\mathbb{Z}[i]$, alors p est premier dans $\mathbb{Z}$ (et n'est pas une somme de carrés non-nuls).

Exercices d'algèbre – Fiche 9: Illustration des nombres premiers de Gauss

Responsable: Isar Stubbe

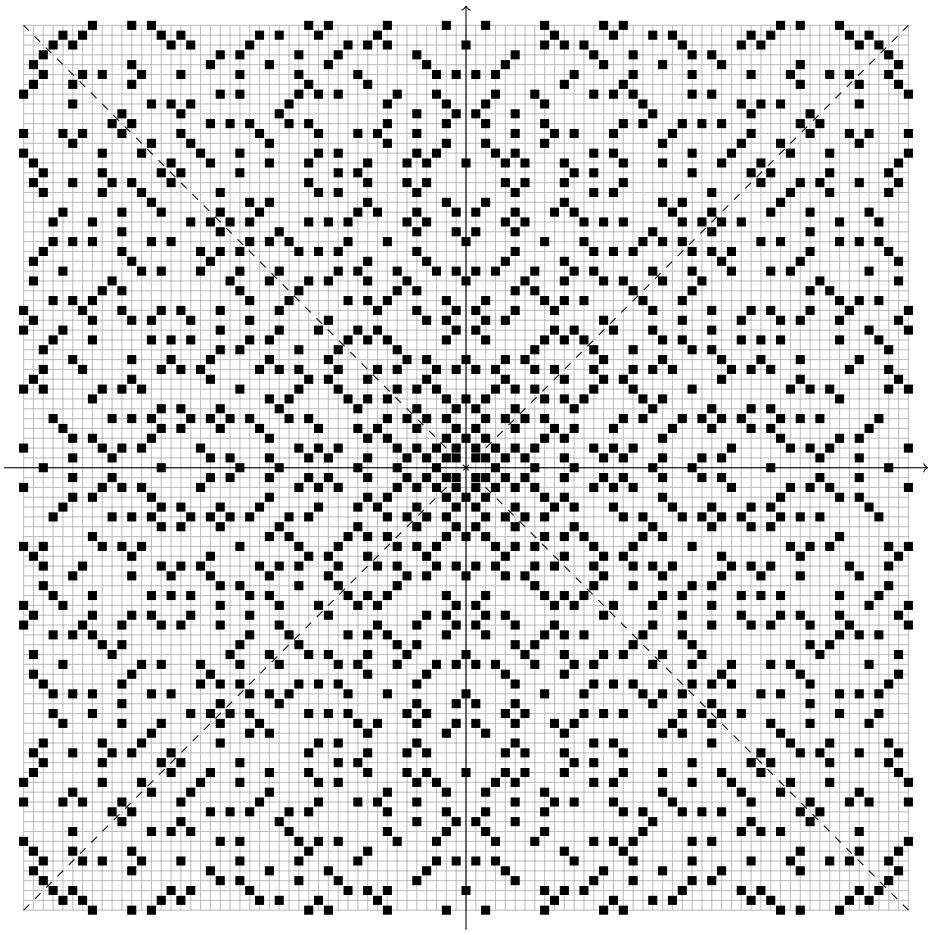
Nous avons démontré que $m + ni$ est un *nombre premier de Gauss* si et seulement si:

- soit $m \neq 0 \neq n$ et $m^2 + n^2$ est un nombre premier,
- soit $m = 0$ et $|n|$ est un nombre premier qui n'est pas une somme de carrés non-nuls,
- soit $n = 0$, et $|m|$ est un nombre premier qui n'est pas une somme de carrés non-nuls.

Il est facile de voir que, pour tout nombre premier $p \neq 2 \in \mathbb{Z}$, soit $p \equiv 1 \bmod 4$, soit $p \equiv 3 \bmod 4$ (et $p = 2$ est le seul nombre premier tel que $p \equiv 2 \bmod 4$). De plus, on vérifie aussi facilement $m^2 + n^2 \not\equiv 3 \bmod 4$ pour tout $m, n \in \mathbb{Z}$. Ainsi, si un nombre premier $p \neq 2$ est une somme de carrés non-nuls, alors $p \equiv 1 \bmod 4$. Par le *Théorème des deux carrés* de P. Fermat (en réalité déjà publié par A. Girard dans sa traduction d'un livre d'arithmétique de S. Stevin en 1625), aussi la réciproque est vraie: si $p \equiv 1 \bmod 4$ alors p est une somme de carrés (et bien sûr aussi 2 est une somme de carrés). Ainsi, pour tout nombre premier $p \in \mathbb{Z}$, on a $p \equiv 3 \bmod 4$ si et seulement si p n'est pas une somme de carrés non-nuls. Il suit que $m + ni$ est un nombre premier de Gauss si et seulement si:

- soit $m \neq 0 \neq n$ et $m^2 + n^2$ est un nombre premier,
- soit $m = 0$ et $|n|$ est un nombre premier tel que $|n| \equiv 3 \bmod 4$,
- soit $n = 0$ et $|m|$ est un nombre premier tel que $|m| \equiv 3 \bmod 4$.

Voici une illustration de quelques nombres premiers de Gauss dans le plan complexe:



Exercices d'algèbre – Fiche 10: Corps finis et infinis

Responsable: Isar Stubbe

Rappellons que la *caracteristique* d'un corps K est l'entier positif engendrant le noyau de l'unique homomorphisme d'anneaux $\mathbb{Z} \to K$; ainsi $\mathrm{car}(K) \in \mathbb{N}$ est nul ou un nombre premier. Le *corps premier* de K est son plus petit sous-corps; c'est le corps de fractions de l'image de $\mathbb{Z} \to K$.

1. Montrer qu'un corps de caractéristique nul est infini (de manière équivalente: un corps fini est de caractéristique non-nul). Donner un exemple de corps infini de caractéristique non-nul.

2. Soit $p \in \mathbb{Z}$ premier et K un corps. Montrer que $|K| = p$ si et seulement s'il existe un (nécessairement unique) isomorphisme $\mathbb{Z}/(p) \cong K$. Ainsi on peut noter $\mathbb{F}_p$ pour "le" corps à p éléments.
   Indication. Etudier l'isomorphisme induite par $\mathbb{Z} \to K$.
   Plus généralement, on peut montrer que deux corps finis avec le même nombre d'éléments (nécessairement p^m éléments) sont toujours isomorphes (mais l'isomorphisme n'est pas unique).

3. Montrer qu'aucun homomorphisme $f\colon K \to L$ n'existe entre corps de caractéristiques différentes, et que tout homomorphisme $f\colon K \to L$ fixe le corps premier (commun à K et L).

4. Montrer que $f = X^2 + X + 1$ est un polynôme irréductible dans $\mathbb{F}_2[X]$, et donner les tables d'addition et de multiplication du corps à 4 éléments $\mathbb{F}_2[X]/(f)$. Quels sont les autres anneaux (commutatifs et unitaires) à 4 éléments?

5. Donner les tables d'addition et de multiplication d'un corps à 9 éléments.

6. Montrer que $f = X^2 + X + 1$ est irréductible sur $\mathbb{Q}$. En déduire que $K = \mathbb{Q}[X]/(f)$ est une extension de $\mathbb{Q}$ dans laquelle (la classe latérale de) X est une racine de f. Factoriser f sur K.

7. Montrer que tout corps K algébriquement clos est infini.
   Indication. Identifier les polynômes irreductibles à coefficients dans K et montrer qu'il y en a une infinité (par le *théorème d'Euclide* pour l'anneau $K[X]$).

8. (a) Pour K un corps, montrer que tout sous-groupe fini de $(K^\times, \cdot, 1)$ est cyclique.
   Indication. Soit $G \subseteq K^\times$ un sous-groupe tel que $|G| = n$. Si aucun élément de G est d'ordre n, alors il existe $m < n$ tel que $x^m = 1$ pour tout $x \in G$. En déduire une contradiction.
   (b) En déduire que $X^p - X = \prod_{a \in \mathbb{F}_p}(X - a)$ dans $\mathbb{F}_p[X]$.
   (c) Conclure par le *théorème de Wilson*: $(p-1)! \equiv -1 \bmod p$.

9. Soit K un corps de caractéristique $p \neq 0$.
   (a) Montrer que $(a+b)^p = a^p + b^p$ pour tous $a, b \in F$.
   Indication. Montrer que p divise $\binom{p}{k}$ si $0 < k < p$.
   (b) En déduire que $\Phi\colon K \to K\colon a \mapsto a^p$ est un homomorphisme.
   (c) Pour K un corps fini, conclure que $\Phi\colon K \to K$ est un isomorphisme; c'est l'*automorphisme de Frobenius* de K.

   On peut montrer que Φ engendre le groupe des automorphismes du corps fini K; cela fait partie de la théorie de Galois.

   Pour la petite histoire: le terme Körper *a été introduit par R. Dedekind en 1871, dans un supplément aux* Vorlesungen über Zahlentheorie von P.G. Lejeune Dirichlet. *Ce livre, rédigé par Dedekind, est disponible ici:* `https://publikationsserver.tu-braunschweig.de`.

Exercices d'algèbre – Fiche 11: Extensions de $\mathbb{Q}$

Responsable: Isar Stubbe

Rappel: pour $a \in L \supseteq K$, soit l'homomorphisme $\gamma\colon K[X] \to L\colon f \mapsto f(a)$. Si $\ker(\gamma) \neq (0)$, on dit que a est *algébrique* sur K, et son *polynôme minimal* $\min(a, K)$ est l'unique générateur unitaire de $\ker(\gamma)$. Autrement dit, $\min(a, K)$ est l'unique polynôme unitaire irréductible à coefficients dans K ayant $a \in L$ pour racine.

Pour établir l'irréductibilité de polynômes unitaires à coefficients dans $\mathbb{Q}$, on pourra utiliser le *critère d'Eisenstein*: si $f = X^n + f_{n-1}X^{n-1} ... + f_1X + f_0$ est dans $\mathbb{Z}[X]$ et p est un nombre premier divisant chaque f_i mais p^2 ne divisant pas f_0, alors f est irréductible dans $\mathbb{Q}[X]$.

1. (a) Calculer $\min(\sqrt{2}, \mathbb{Q})$.
   (b) Posons $\alpha = 1 + \sqrt{2}$. Montrer que $\min(\alpha, \mathbb{Q}) = X^2 - 2X - 1$.
   (c) Pour $\beta = \sqrt{\alpha}$, montrer que $\beta \notin \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\alpha)$.
   (d) Calculer $\min(\beta, \mathbb{Q})$.
2. Soit K une extension de degré 2 de $\mathbb{Q}$. Montrer qu'il existe $a \in \mathbb{Q}$ tel que $K = \mathbb{Q}(\sqrt{a})$.
3. Pour tout $n \geq 1$, montrer qu'il existe une extension de degré n de $\mathbb{Q}$.
4. Soient $a, b \in \mathbb{C}$ des éléments algébriques sur $\mathbb{Q}$. Montrer que:
   (a) $[\mathbb{Q}(a, b) : \mathbb{Q}] \leq [\mathbb{Q}(a) : \mathbb{Q}] \cdot [\mathbb{Q}(b) : \mathbb{Q}]$.

   Supposons maintenant que $[\mathbb{Q}(a) : \mathbb{Q}]$ et $[\mathbb{Q}(b) : \mathbb{Q}]$ sont premiers entre-eux. Montrer que:
   (b) $[\mathbb{Q}(a, b) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}] \cdot [\mathbb{Q}(b) : \mathbb{Q}]$,
   (c) $\mathbb{Q}(a) \cap \mathbb{Q}(b) = \mathbb{Q}$,
   (d) $\min(a, \mathbb{Q}) = \min(a, \mathbb{Q}(b))$.
5. Déterminer le corps de racines de $X^5 + X^4 - 2X - 2$ sur $\mathbb{Q}$. Même question pour $X^3 - 1$.
6. Démontrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
7. Rappellons qu'un *nombre constructible* est un nombre réel qui peut être obtenu par une suite finie d'opérations parmi $\{+, -, \times, \div, \sqrt{\ }\}$ de 0 et 1 (voir mon cours de Géométrie, notamment pour le lien avec les constructions avec règle et compas). Notons $\mathbb{Q} \subseteq K \subseteq \mathbb{R}$ le corps des nombres constructibles.
   (a) Montrer, pour tout $a \in K$, qu'il existe une suite d'extensions $\mathbb{Q} \subseteq K_1 \subseteq ... \subseteq K_r$ telles que $a \in K_r$ et $[K_{i+1} : K_i] \leq 2$ pour tout i.
   Indication. Lorsqu'on exécute une operations parmi $\{+, -, \times, \div, \sqrt{\ }\}$, on doit "au pire" ajouter une racine carrée.
   (b) En déduire que tout $a \in K$ est algébrique sur $\mathbb{Q}$, et formuler une condition nécessaire sur le degré de $\min(a, \mathbb{Q})$.
   (c) Montrer que $\sqrt[3]{2}$ n'est pas constructible. *Ainsi, la duplication du cube unité est impossible avec règle et compas.*
   (d) Démontrer la formule $\cos(3\alpha) = 4\cos^3(\alpha) - 3\cos(\alpha)$ et en déduire que $\cos(\frac{\pi}{9})$ est racine du polynôme irréductible $f = 8X^3 - 6X - 1$. Conclure que $\cos(\frac{\pi}{9})$ n'est pas constructible, bien que $\cos(\frac{\pi}{3})$ l'est. *Ainsi, il existe un angle non-trisectable avec règle et compas.*
   (e) Sachant que π n'est pas algébrique, montrer que $\sqrt{\pi}$ ne l'est pas non plus. *Ainsi, la quadrature du cercle est impossible avec règle et compas.*

Exercices d'algèbre – Fiche 12: Extensions cyclotomiques

Responsable: Isar Stubbe

---

1. Montrer que les solutions de $X^n = 1$ dans $\mathbb{C}$ forment un groupe cyclique.

   Un $\omega \in \mathbb{C}$ tel que $\omega^n = 1$ est une *racine n-ième de l'unité*. Si l'ordre de ω est n, alors c'est une *racine primitive n-ième de l'unité*. Une extension $\mathbb{Q}(\omega)$ de $\mathbb{Q}$ par une racine primitive n-ième de l'unité ω, est appelée une *extension cyclotomique*.

2. Pour $n \geq 3$, on note $\alpha = \frac{2\pi}{n}$; ainsi le polygone régulier à n côtés est constructible avec règle et compas si et seulement si $\cos\alpha$ est un nombre constructible (voir mon cours de Géométrie).

   (a) Utiliser l'identité $e^{i\alpha} = \cos\alpha + i\sin\alpha$ dans $\mathbb{C}$ pour montrer que $\cos\alpha = \frac{1}{2}(e^{i\alpha} + e^{-i\alpha})$, puis en déduire que $\mathbb{Q}(e^{i\alpha}) \supseteq \mathbb{Q}(\cos\alpha) \supseteq \mathbb{Q}$.

   (b) Montrer que $e^{i\alpha}$ est racine d'un polynôme de degré 2 sur $\mathbb{Q}(\cos\alpha)$ et en déduire $[\mathbb{Q}(e^{i\alpha}) : \mathbb{Q}(\cos\alpha)]$.

   (c) Donner $[\mathbb{Q}(\cos\alpha) : \mathbb{Q}]$ en fonction du degré du polynome minimal de $e^{i\alpha}$ sur $\mathbb{Q}$.

   (d) Formuler une condition nécessaire pour la constructibilité du polygone régulier à n côtés en fonction du degré du polynome minimal d'une racine primitive n-ième de l'unité sur $\mathbb{Q}$.

3. Pour tout $n \geq 1$, le *polynôme cyclotomique* est défini par $\Phi_n(X) = \prod_{i=1}^{k}(X - \omega_i) \in \mathbb{C}[X]$ avec $\omega_1, ..., \omega_k$ les racines *primitives* n-ièmes de l'unité.

   (a) En titre d'exemple, calculer Φ_1, Φ_2, Φ_2 et Φ_4. En général, montrer que $\deg(\Phi_n) = \varphi(n)$ (la *fonction indicatrice d'Euler*).

   (b) Pour p un nombre premier, montrer que $\Phi_p(X) = X^{p-1} + ... + X + 1 \in \mathbb{Q}[X]$.
   Indication. Expliquer pourquoi $X^p - 1 = \prod_{i=1}^{p}(X - \omega_i)$ avec $\omega_1, ..., \omega_p$ *toutes* les racines p-ièmes de l'unité, puis diviser ce polynôme par $X - 1$.

   (c) Montrer que Φ_p est irréductible dans $\mathbb{Q}[X]$. Quel est donc le degré d'une extension cyclotomique de $\mathbb{Q}$ par une racine primitive p-ième de l'unité?
   Indication. Simplifier $\Phi_p(X + 1)$ à l'aide de (b) et appliquer le critère d'Eisenstein.

   (d) Donner une condition nécessaire pour la constructibilité du polygone régulier à p côtés.

   (e) Prouver que, si $p = 2^m + 1$ est un nombre premier impair, alors m est une puissance de 2. Indication: Par l'absurde, si $m = 2^k l$ avec l impair, montrer que $X + 1$ divise $X^l + 1$ et poser $X = 2^k$.

   Les nombres $F_n = 2^{2^n} + 1$ sont les *nombres de Fermat*. Nous avons donc établi une condition nécessaire pour la constructibilité d'un polygone régulier à p côtés: il faut que p soit un nombre premier de Fermat. Il est facile de voir que $F_0, ..., F_4$ sont des nombres premiers—et à ce jour ce sont les seuls nombres premiers de Fermat connus!

   En fait, il est possible de montrer que chaque polynôme cyclotomique $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$. Cela implique, comme dans l'exercice précédent, une condition nécessaire pour la constructibilité d'un polygone régulier à n côtés. De plus, il est possible de montrer que cette condition nécessaire est aussi suffisante, donnant le résultat suivant: Un polygone régulier à n côtés est constructible si et seulement si $\varphi(n)$ est une puissance de 2, si et seulement si $n = 2^r p_1 ... p_k$ où $r \geq 0$ et les p_i sont des nombres premiers de Fermat distincts.