TD n°1. Solutions

Exercice 1. Montrer que dans $\mathbb{Z}[\sqrt{-5}]$, 3, 7, $2+\sqrt{-5}$, $4+\sqrt{-5}$ sont irréductibles.
Montrer que la décomposition de 21 en facteurs irréductibles dans $\mathbb{Z}[\sqrt{-5}]$ n'est pas unique ($\mathbb{Z}[\sqrt{-5}]$ n'est pas *factoriel*).

Solution. Les équations $a^2+5b^2)=3$ et $a^2+5b^2=7$ n'ont pas de solutions, donc il n'y a pas d'élément de $\mathbb{Z}[\sqrt{-5}]$ de norme 3 ou 7. En particulier, si z est de norme 9, 21 ou 49, un diviseur propre non inversible de z devrait être de norme 3 ou 7 : z est donc irréductible. Ici $N(3)=N(2+\sqrt{-5})=9$, $N(7)=49$ et $N(4+\sqrt{-5})=21$.
On a $21=3\cdot 7=(4+\sqrt{-5})\cdot(4-\sqrt{-5})$ et l'on obtient deux décompositions en facteurs irréductibles.

Exercice 2. Montrer que, si z est un élément irréductible de $\mathbb{Z}[i]$, alors $N(z)$ est un nombre premier ou le carré d'un nombre premier.

Solution. Comme z est irréductible, $barz$ aussi (l'irréductibilité est invariante par automorphisme d'anneau, en particulier par conjugaison complexe). On a $z\bar{z}=N(z)$ et z et $\bar{z}$ sont irréductibles. Par unicité de la décomposition en facteur irréductibles, la décomposition en facteur premiers de $N(z)$ contient au plus deux éléments. Si elle n'en contient qu'un, alors $N(z)$ est premier. Si elle en contient deux, $N(z)=pq$, et p et q doivent être associés à z et $\bar{z}$. Comme $p^2=N(z)=N(\bar{z})=q^2$, on obtient $p=q$ et $N(z)=p^2$ comme voulu.

Exercice 3. Donner un polynôme unitaire de $\mathbb{Z}[X]$ annulant $\sqrt{2}+\sqrt{3}$.

Solution. On pose $x=\sqrt{2}+\sqrt{3}$. On a alors

$$x^2=5+2\sqrt{6}$$

$$(x^2-5)^2=24$$

Le polynôme $(X^2-5)^2-24$ convient donc.

On peut aussi appliquer l'algorithme donné dans la preuve du théorème disant que la somme de deux entiers algébriques est encore un entier algébrique, ce qui nous donne que $x=\sqrt{2}+\sqrt{3}$ vérifient

$$M\begin{pmatrix}1\\ \sqrt{2}\\ \sqrt{3}\\ \sqrt{6}\end{pmatrix}=x\begin{pmatrix}1\\ \sqrt{2}\\ \sqrt{3}\\ \sqrt{6}\end{pmatrix}$$

où

$$M=\begin{pmatrix}0&2&3&0\\ 1&0&0&3\\ 1&0&0&2\\ 0&1&1&0\end{pmatrix}.$$

En particulier le polynôme caractéristique de M convient.

Exercice 4. Montrer qu'un nombre rationnel est un entier algébrique si et seulement si il appartient à $\mathbb{Z}$.

Solution. Soit $x\in\mathbb{Q}$, qu'on peut supposer non nul, zéro d'un polynôme unitaire $P=X^N+\sum_{0\leq n<N}a_nX^n$ de $\mathbb{Z}[X]$. Ecrivons x sous la forme p/q avec p et $q>0$ entiers premiers entre eux et multiplions par q^N l'égalité $P(p/q)=0$. On obtient

$$p^n=\sum_{0\leq n<N}a_np^nq^{N-n}.$$

Le membre de gauche étant divisible par q, on en déduit que p^n est divisible par q. Or comme p et q sont premiers entre eux, $q=1$ et donc $x\in\mathbb{Z}$.

Exercice 5. Soit $d\neq 1$ un entier impair sans facteur carré. Montrer que, si $a,b\in\mathbb{Q}$, $a+b\sqrt{d}$ est un entier algébrique si et seulement si $2a$ et a^2-db^2 sont entiers. Montrer que l'anneau des entiers algébriques de $\mathbb{Q}\left[\sqrt{d}\right]$ est :

a) $\mathbb{Z}[\sqrt{d}]$ si $d \equiv 3 \bmod 4$;

b) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \bmod 4$.

Solution. Soit $z = a + b\sqrt{d}$ et soit $z' = a - b\sqrt{d}$. Si $P \in \mathbb{Q}[X]$, alors $P(z) \in \mathbb{Q}[\sqrt{d}]$ et s'écrit donc sous la forme $c + d\sqrt{d}$ avec $c, e \in \mathbb{Q}$. On vérifie facilement que $P(z') = c - e\sqrt{d}$ (l'application $c + d\sqrt{d} \mapsto c - e\sqrt{d}$ est un automorphisme d'anneau de $\mathbb{Q}[\sqrt{d}]$). En particulier z annule P si et seulement si z' annule P. Donc si z est un entier algébrique z' aussi. Comme les entier algébriques forment un anneau, $z + z' = 2a$ et $zz' = a^2 - db^2$ doivent aussi être des entiers algébriques, donc des entiers d'après l'exercice précédent.
Réciproquement si $2a$ et $a^2 - db^2$ sont entiers, le polynôme $X^2 - 2aX + a^2 - db^2$ est un polynome unitaire de $\mathbb{Z}[X]$ annulant z, et z est donc entier algébrique.
Donc si z est entier algébrique $a \in \frac{1}{2}\mathbb{Z}$ et l'on déduit de $a^2 - db^2 \in \mathbb{Z}$ que $db^2 \in \frac{1}{4}\mathbb{Z}$. Comme d est sans facteur carré, on obtient $b \in \frac{1}{2}\mathbb{Z}$. En posant $a' = 2a$ et $b' = 2b$, il suffit pour conclure de vérifier que $a'^2 - db'^2 \equiv 0 \bmod 4$ si et seulement si a' et b' sont pairs dans le cas $d \equiv 3 \bmod 4$ et si et seulement si a' et b' sont de même parité dans le cas $d \equiv 1 \bmod 4$.

Exercice 6. Parmi les nombres algébriques suivants, lesquels sont des entiers algébriques ?

a) $\alpha = \frac{1+\sqrt[4]{17}}{2}$

b) $\beta = \frac{\sqrt{11}+\sqrt{13}}{2}$,

c) $\gamma = \frac{\sqrt{5}+\sqrt{13}}{2}$,

d) $\delta = \frac{i+\sqrt{11}+\sqrt{13}}{2}$,

Solution. a) On vérifie comme dans l'exercice précédent que si α était entier $\alpha' = \frac{1-\sqrt[4]{17}}{2}$ le serait aussi. Or $\alpha\alpha' = \frac{1-\sqrt{17}}{4}$, qui n'est pas entier d'après l'exercice précédent, donc α n'est pas entier.

b) On a $\beta^2 = 6 + \frac{\sqrt{143}}{2}$, qui n'est pas entier d'après l'exercice précédent donc, β n'est pas entier.

c) $\gamma = \frac{\sqrt{5}+1}{2} + \frac{-1+\sqrt{13}}{2}$ est entier comme somme de deux entiers.

d) Si δ était entier, $\delta\bar{\delta} = \frac{25+2\sqrt{143}}{4}$ le serait aussi, or ce n'est pas le cas d'après l'exercice précédent.

Exercice 7. a) Soit R un anneau euclidien. Montrer qu'il existe $x \in R$ non inversible tel que $R^* \cup \{0\} \to R/(x)$ soit surjective.

b) Soit $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. Déterminer A^* et montrer que A n'est pas euclidien.

c) Si $a, b \in A\backslash 0$, montrer qu'il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et qui vérifient, soit $a = bq + r$, soit $2a = bq + r$.

d) Montrer que (2) n'est pas un idéal maximal de A.

e) Montrer que A est principal.

Exercice 8. Montrer que pour tout corps K, il existe une infinité de polynômes unitaires irréductibles. En déduire que tout corps algébriquement clos est infini.

Exercice 9. a) Montrer que toute extension K/k de degré premier est monogène.

b) Soient K/k une extension et P un polynôme irréductible sur k. Montrer que si le degré de P est premier au degré de K/k, alors P est irréductible sur K.

c) Soient k un corps et x un élément algébrique sur k de degré impair. Montrer que $k(x^2) = k(x)$.

Solution. a) Soit $x \in K\backslash k$. Alors $[k(x) : k]$ est strictement supérieur à 1 et doit diviser le degré p de K/k d'après la multiplcativité des degrés. Donc $[k(x) : k] = p$ et donc $k(x) = K$.

b) Soit Q un facteur irréductible de P dans $K[X]$ et $L = K[X]/P$. Soit n le degré de P et m le degré de Q et $d = [K : k]$. On note α l'image de X dans L. Le corps $k(\alpha)$ est engendré sur k par une racine de P qui est irréductible sur k, donc $[k(\alpha) : k] = n$. De même $[L : K] = m$. Donc $[L : k] = [L : K][K : k] = md$ mais $md = [L : k] = [L : k(\alpha)][k(\alpha) : k]$ est divisible par n. Comme d et n sont premier entre eux, n divise m, a fortiori $n \leq m$, ce qui implique que P et Q sont associés : P est donc irréductible sur K.

c) Comme x est zéro de $X^2 - x^2 \in k(x^2)[X]$, $[k(x) : k(x^2)] \leq 2$. Or $[k(x) : k(x^2)]$ divise $[k(x) : k]$ par multiplicativité des degrés et $[k(x) : k]$ est impair, donc $[k(x) : k(x^2)] \neq 2$. Donc $[k(x) : k(x^2)] = 1$, comme voulu.

Exercice 10. Déterminer le degré des extensions suivantes de $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2},\sqrt{18},\sqrt{-7}),\qquad \mathbb{Q}(i,\sqrt[4]{2}),\qquad \mathbb{Q}(\sqrt{3},\sqrt[3]{2}),\qquad \mathbb{Q}(\sqrt{2+\sqrt{2}}),\qquad \mathbb{Q}(i,\sqrt{2+\sqrt{2}}).$$

Solution. On a $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ car $\sqrt{2}$ est racine de X^2-2 qui est irréductible (sinon on aurait $\sqrt{2}\in\mathbb{Q}$). Remarquons que $\sqrt{18}=3\sqrt{2}$ est dans $\mathbb{Q}(\sqrt{2})$. Comme $\sqrt{-7})$ est racine de X^2+7, on a $[\mathbb{Q}(\sqrt{2},\sqrt{18},\sqrt{-7}):\mathbb{Q}(\sqrt{2})]\leq 2$. Or, comme $\sqrt{-7}\notin\mathbb{R}$ et $[\mathbb{Q}(\sqrt{2})\subset\mathbb{R}$, on a donc $\mathbb{Q}(\sqrt{2},\sqrt{18},\sqrt{-7})\neq\mathbb{Q}(\sqrt{2})$. Donc $[\mathbb{Q}(\sqrt{2},\sqrt{18},\sqrt{-7}):\mathbb{Q}(\sqrt{2})]=2$ et $[\mathbb{Q}(\sqrt{2},\sqrt{18},\sqrt{-7}):\mathbb{Q}]=4$ par multiplicativité.

On a $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt[4]{2})\subset\mathbb{Q}(i,\sqrt[4]{2})$.

On a $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ comme précédemment.

On a $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})]\leq 2$ car $\sqrt[4]{2}$ est racine de $X^2-\sqrt{2}$. Si $\sqrt[4]{2}\in\mathbb{Q}(\sqrt{2})$, on aurait $(a+b\sqrt{2})^2=\sqrt{2}$ avec $a,b\in\mathbb{Q}$, on obtient, en décomposant dans la base $1,\sqrt{2}$, $a^2+2b^2=0$ et $2ab=1$, on obtient $a^4=-1/2$ dans $\mathbb{Q}$ ce qui n'est pas possible. Donc $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})]=2$.

De même $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}(\sqrt[4]{2})]\leq 2$, car i est solution de X^2-1. Comme $\mathbb{Q}(\sqrt[4]{2})\subset\mathbb{R}$ mais $i\notin\mathbb{R}$, $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}(\sqrt[4]{2})]\leq 2$.

Par multiplicativité, $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}]=8$.

Le polynome X^3-2 est irréductible sur $\mathbb{Q}$ car sinon il aurait un facteur de degré 1, et donc aurait une racine dans $\mathbb{Q}$ ce qui n'est pas le cas. Donc $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$. De même X^2-3 est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Q}(\sqrt[3]{2})$ d'après exo 9.b. Donc $[\mathbb{Q}(\sqrt{3},\sqrt[3]{2}):\mathbb{Q}(\sqrt[3]{2})]=2$, et donc le degré cherché est 6 par multiplicativité

On a $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt{2+\sqrt{2}})$. L'important est de savoir si $2+\sqrt{2}$ est un carré dans $\mathbb{Q}(\sqrt{2})$. Or $N(2+\sqrt{2})=2$, qui n'est pas un carré dans $\mathbb{Q}$, donc $2+\sqrt{2}$ est un carré dans $\mathbb{Q}(\sqrt{2})$. Donc $[\mathbb{Q}(\sqrt{2+\sqrt{2}}):\mathbb{Q}(\sqrt{2})]=2$, et $[\mathbb{Q}(\sqrt{2+\sqrt{2}}):\mathbb{Q}]=4$ par multiplicativité.

On a $\mathbb{Q}(\sqrt{2+\sqrt{2}})\subset\mathbb{R}$ et $i\notin\mathbb{R}$, donc comme précédemment $[\mathbb{Q}(i,\sqrt{2+\sqrt{2}}):\mathbb{Q}]=2[\mathbb{Q}(\sqrt{2+\sqrt{2}}):\mathbb{Q}]=8$.

Exercice 11. Soit K une extension de k de degré 2.

a) On suppose que la caractéristique de k est différente de 2. Montrer qu'il existe $a\in k$ tel que K soit isomorphe à $k[X]/(X^2-a)$. A quelle condition deux extensions de cette forme sont-elles isomorphe ? Décrire les automorpohismes de K fixant k.

b) On suppose que k est de caractéristque 2. Montrer qu'il existe $a\in k$ tel que K soit isomorphe à $K[X]/(X^2-a)$ ou à $K[X]/(X^2-X-a)$. A quelle condition deux extensions de cette forme sont-elles isomorphe ? Décrire les automorpohismes de K.

Solution. Soit $x\in K\backslash k$. La famille $1,x$ est libre sur k donc $x^2=bx+c$. En caractéristique différente de 2, on obtient $(x+b/2)^2=c+b^2/4$. En posant $a=c+b^2/4$ et en envoyant X sur $x+b/2$, on obtient un morphisme $k[X]/(X^2-a)\to K$, qui est un isomorphisme car $1,x+b/2$ forment une base de K sur k. Si $b\in k$ est un carré dans $k[X]/(X^2-a)$, alors $b=(c+d\sqrt{a})^2$, et donc $2cd=0$ et $b=c^2+ad^2$. Donc soit b soit b/a est un carré dans k. Or si b est un carré $k[X]/(X^2-a)$ n'est pas un corps. Donc $k[X]/(X^2-a)$ et $k[X]/(X^2-b)$ sont isomorphes si et seulement si b/a est un carré.

Notons y une racine de a dans K. Si σ est un automorphisme de K fixant k. On a $\sigma(y)^2=\sigma(y^2)=\sigma(a)=a$ donc $\sigma(y)$ est y ou $-y$. Comme y engendre K, on obtient au plus deux automorphismes possibles. On vérifie facilement que $\sigma(e+fy)=e-fy$ définit bien un automorphisme

Exercice 12. On dit qu'un nombre algébrique x est constructible à la règle et au compas si il existe une tour d'extensions de corps

$$k_0=\mathbb{Q}\subset k_1\subset\cdots\subset k_n$$

avec $[k_{i+1}:k_i]=2$ et $x\in k_n$.

a) Justifier géométriquement la terminologie.

b) Montrer que $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas.

c) Montrer que $\cos(\frac{\pi}{9})$ n'est pas constructible à la règle et au compas.

Solution. Supposons qu'il existe $k_1,\ldots,k_n$ comme dans l'énoncé avec $\sqrt[3]{2}\in k_n$. Alors $[k_n:\mathbb{Q}]=2^n$ et $[\sqrt[3]{2}:\mathbb{Q}]$ divise 2^n donc doit être une puissance de 2. Or on a déjà dans l'exercice 11 que $[\sqrt[3]{2}:\mathbb{Q}]=3$, donc $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas.

On a $(e^{it}+e^{-it})^3=e^{3it}+e^{-3it}+3(e^{it}+e^{-it})$. Donc $2\cos(\frac{\pi}{9})$ est racine de $P=X^3-3X-2cos(\pi/3)=X^3-3X-1$. On vérifie que $\mathbb{Q}$ est irréductible sur $\mathbb{Q}$ en vérifiant qu'il n'a pas de racine : une telle racine a serait un entier algébrique, donc un entier. Donc $1=a^3-3a$ est divisible par a ce qui montre que $a=1$ ou -1. On vérifie que 1 et -1 ne sont pas solutions.

Donc $[\mathbb{Q}(cos(\frac{\pi}{9})):\mathbb{Q}]$ est divisible par 3, ce qui prouve la non constructibilité de $\cos(\frac{\pi}{9})$

Exercice 13. Soit L/K une extension de corps de degré 3 et soient $\alpha, \beta \in L$ tels que $L = K[\alpha] = K[\beta]$. Montrer qu'il existe $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ tel que $\beta = g \cdot \alpha = \frac{a\alpha+b}{c\alpha+d}$. Discuter l'unicité de g.

Exercice 14. Montrer que tout automorphisme de corps de $\mathbb{R}$ est l'identité (on pourra montrer qu'un tel automorphisme est nécessairement croissant).

Solution. Un tel automorphisme s conserve la propriété d'être un carré, donc la propriété d'être positif. Donc si $a \leq b$, $s(b) - s(a) = s(b-a) \leq 0$, donc s est croissant. De plus s est l'identité sur $\mathbb{Q}$ comme tout morphisme de corps. Soit $x \in \mathbb{R}$. Soit (a_n) (resp. (b_n)) une suite de rationnels tendants vers x par valeurs inférieures (par valeurs supérieurs). Alors, comme s est croissante, $a_n = s(a_n) \leq s(x) \leq s(b_n) = b_n$. En prenant la limite quand n tend vers l'infini, on obtient $s(x) = x$.