TD n°1.

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*).

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.

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

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

Exercice 5. Soit d un nombre 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 $\mathbb{Q}\,[\sqrt{d}]$ est :

a) $\mathbb{Z}[\sqrt{d}]$ si $d \equiv 3 \bmod 4$;
b) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \bmod 4$.

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

a) $\beta = \frac{\sqrt{11}+\sqrt{13}}{2}$,
b) $\gamma = \frac{\sqrt{5}+\sqrt{13}}{2}$,
c) $\delta = \frac{i+\sqrt{11}+\sqrt{13}}{2}$,
d) $\frac{1+\sqrt[4]{17}}{2}$.

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) est 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 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 $k(x^2) = k(x)$.

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

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

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

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.

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).