Polynômes irréductibles

Exercice 1. *Factorisation sur $\mathbb{R}$ de X^8+X^4+1*
Factoriser X^8+X^4+1 sur $\mathbb{R}$.

Exercice 2. *Polynôme irréductible sur $\mathbb{Q}$*
Démontrer que $1+(X-1)^2(X-3)^2$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 3. *Polynômes positifs sur $\mathbb{R}$*
Soit $\mathcal{E}=\{P\in\mathbb{R}[X] \text{ tq } \exists\, Q,R\in\mathbb{R}[X] \text{ tq } P=Q^2+R^2\}$.
1) Montrer que $\mathcal{E}$ est stable par multiplication.
2) Montrer que $\mathcal{E}=\{P\in\mathbb{R}[X] \text{ tq } \forall\, x\in\mathbb{R},\ P(x)\geqslant 0\}$.
3) (Centrale MP 2000, avec Maple) $P=65X^4-134X^3+190X^2-70X+29$. Trouver A et B dans $\mathbb{Z}[X]$ tels que $P=A^2+B^2$.

Exercice 4. *Lemme de Gauss*
Soit $P\in\mathbb{Z}[X]$. On appelle *contenu de P* le pgcd des coefficients de P (notation : $\text{cont}(P)$).
1) Soient $P,Q\in\mathbb{Z}[X]$ avec $\text{cont}(P)=1$, et $R=PQ$. Soit p un facteur premier de $\text{cont}(R)$.
a) Si p est premier avec le coefficient constant de P, Démontrer que p divise tous les coefficients de Q.
b) Si p divise le coefficient constant de P, se ramener au cas précédent.
c) En déduire que $\text{cont}(Q)=\text{cont}(R)$.
2) Lorsque $\text{cont}(P)\neq 1$, trouver $\text{cont}(PQ)$.
3) Application : Soit $R\in\mathbb{Z}[X]$, et $P,Q\in\mathbb{Q}[X]$ tels que $R=PQ$. Montrer qu'il existe $P_1,Q_1\in\mathbb{Z}[X]$ proportionnels à P et Q et tels que $R=P_1Q_1$ (*cad : un polynôme à coefficients entiers réductible sur $\mathbb{Q}$ est aussi réductible sur $\mathbb{Z}$.*)

Exercice 5. *Polynômes irréductibles sur $\mathbb{Z}$*
Démontrer que X^4+X+1 et X^6+X^2+1 sont irréductibles dans $\mathbb{Z}[X]$.

Exercice 6. *Polynômes irréductibles sur $\mathbb{Z}$*
Soient $a_1,\dots,a_n\in\mathbb{Z}$ distincts.
1) Montrer que $(X-a_1)\dots(X-a_n)-1$ est irréductible dans $\mathbb{Z}[X]$.
2) Même question avec $(X-a_1)\dots(X-a_n)+1$, n impair.

Exercice 7. *Critère d'irréductibilité d'Eisenstein*
Soit $P\in\mathbb{Z}[X]$, $P=X^n+a_{n-1}X^{n-1}+\dots+a_0X^0$ et p un nombre premier tel que : $a_0\equiv 0\,(\text{mod}\,p)$, $\dots$, $a_{n-1}\equiv 0\,(\text{mod}\,p)$, $a_0\not\equiv 0\,(\text{mod}\,p^2)$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.

Exercice 8. *Irréductibilité de X^p-a*
Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$, $a\in\mathbb{K}$ et $p\in\mathbb{N}$ premier. Montrer que le polynôme X^p-a est irréductible sur $\mathbb{K}$ si et seulement s'il n'a pas de racine dans $\mathbb{K}$. Indication : si $X^p-a=PQ$ avec $P,Q\in\mathbb{K}[X]$ unitaires non constants, factoriser P dans $\mathbb{C}$ et considérer $P(0)$.

Exercice 9. *Polynômes sans facteur carré*
Soit $\mathbb{K}$ un corps fini de cardinal k et $d\in\mathbb{N}^*$. On note U_d l'ensemble des polynômes de $\mathbb{K}[X]$ unitaires de degré d et V_d le sous-ensemble des ces polynômes sans facteur carré (il n'existe pas $Q\in\mathbb{K}[X]$ non constant tel que Q^2 divise le polynôme considéré). Soient u_d, v_d les cardinaux de ces ensembles.
1) Montrer : $u_d=\sum_{2q+r=d}u_qv_r$.
2) Calculer u_d puis v_d.

solutions

Exercice 1.
$(X^2-X+1)(X^2+X+1)(X^2-X\sqrt{3}+1)(X^2+X\sqrt{3}+1)$.

Exercice 2.
racines : $\alpha = 2+\sqrt{\frac{\sqrt{2}+1}{2}}+i\sqrt{\frac{\sqrt{2}-1}{2}}$, $\beta = 2-\sqrt{\frac{\sqrt{2}+1}{2}}-i\sqrt{\frac{\sqrt{2}-1}{2}}$, $\bar{\alpha}, \bar{\beta}$.
Factorisation de P sur $\mathbb{R}$: $P = (X^2-2\Re(\alpha)X+|\alpha|^2)(X^2-2\Re(\beta)X+|\beta|^2)$ et les facteurs sont irrationnels.

Exercice 3.
1) $P = |Q+iR|^2$.
2) Factoriser P.
3) Avec Maple : $P = \frac{1}{65}Q\overline{Q}$ avec $Q = 65X^2+(49i-67)X+(42+11i)$ et Q est irréductible sur $\mathbb{Q}[i]$. Donc si $P = A^2+B^2 = (A+iB)(A-iB)$ avec A, B polynômes à coefficients entiers alors, quitte à changer B en $-B$, il existe $\lambda \in \mathbb{Q}[i]$ tel que : $A+iB = \lambda Q$ et $A-iB = \bar{\lambda}\overline{Q}$ d'où :

$$2A = 65(\lambda+\bar{\lambda})X^2+((49i-67)\lambda-(49i+67)\bar{\lambda})X+((42+11i)\lambda+(42-11i)\bar{\lambda})$$
$$2iB = 65(\lambda-\bar{\lambda})X^2+((49i-67)\lambda+(49i+67)\bar{\lambda})X+((42+11i)\lambda-(42-11i)\bar{\lambda})$$
$$\lambda\bar{\lambda} = 65.$$

En particulier $65\lambda \in \mathbb{Z}[i]$, écrivons $\lambda = \frac{u+iv}{65}$ avec $u, v \in \mathbb{Z}$:

$$A = uX^2-\frac{67u+49v}{65}X+\frac{42u-11v}{65}$$
$$B = vX^2+\frac{49u-67v}{65}X+\frac{11u+42v}{65}$$
$$u^2+v^2 = 65.$$

$67u+49v$ est divisible par 65 si et seulement si $u \equiv 8v \pmod{65}$ et dans ce cas les autres numérateurs sont aussi multiples de 65. La condition $u^2+v^2 = 65$ donne alors $v = \pm 1, u = \pm 8$ d'où :

$$A = \pm(8X^2-9X+5), \qquad B = \pm(X^2+5X+2).$$

Exercice 6.
1) Si $P = QR$ alors $Q(a_i)R(a_i) = -1 \Rightarrow Q(a_i) = -R(a_i) = \pm 1$, donc $Q+R$ a n racines, donc est nul, et $P = -Q^2$: contradiction pour $x \to \infty$.
2) Même raisonnement : $P = Q^2$, donc $Q^2-1 = (Q-1)(Q+1) = (X-a_1)\dots(X-a_n)$.
On répartit les facteurs entre $Q-1$ et $Q+1$: $n = 2p$, contradiction.

Exercice 7.
Soit $P = QR$ avec $Q = X^{n_1}+b_{n_1-1}X^{n_1-1}+\dots+b_0X^0$ et $R = X^{n_2}+c_{n_2-1}X^{n_2-1}+\dots+c_0X^0$.
Par hypothèse sur $a_0 = b_0c_0$, p divise un et un seul des entiers b_0, c_0. Supposons que p divise $b_0, b_1, \dots, b_{k-1}$: alors $a_k \equiv b_kc_0 \pmod{p}$ donc p divise b_k. On aboutit à «p divise le coefficient dominant de Q», ce qui est absurde.

Exercice 8.
On suppose $a \neq 0$ et $X^p-a = PQ$ avec $P, Q \in \mathbb{K}[X]$ unitaires non constants. Soit $n = \deg(P) \in [\![1, p-1]\!]$ et $b = (-1)^nP(0) \in \mathbb{K}$. b est le produit de certaines racines p-èmes de a, donc $b^p = a^n$. De plus $n \wedge p = 1$; soit $nu+pv = 1$ une relation de Bézout. On a alors $b^{pu} = a^{nu} = a^{1-pv}$ d'où $a = (b^u/a^v)^p$ donc $b^u/a^v \in \mathbb{K}$ est racine de X^p-a.

Exercice 9.
1) Tout polynôme P unitaire de degré d se décompose de manière unique en $P = Q^2R$ avec Q, R unitaires et R sans facteur carré.
2) On a $u_d = k^d$ et $u_{d+2} = ku_d+v_{d+2}$, d'où $v_0 = 1$, $v_1 = k$, $v_d = k^d-k^{d-1}$ si $d \geqslant 2$.