Irréductibilité de polynômes et applications

Gourdon, p. 58
Perrin, p. 76
Caldero, Algèbre, p. 279

Lemme des contenus : Soit $P, Q \in \mathbb{Z}[X]$. Alors $c(PQ) = c(P)c(Q)$.

On considère $P_1 = \frac{P}{c(P)}$, $Q_1 = \frac{Q}{c(Q)} \in \mathbb{Z}[X]$ et $c(P_1) = c(Q_1) = 1$.
Si $c(P_1Q_1) > 1$, alors il existe p premier tel que $p \mid c(P_1Q_1)$ i.e. $\overline{P_1Q_1} = \bar{0}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. → se généralise à A factoriel en utilisant p irréductible ⟺ (p) premier par le lemme d'Euclide
D'où, par intégrité, $\overline{P_1} = \bar{0}$ ou $\overline{Q_1} = \bar{0}$ i.e. $p \mid c(P_1) = 1$ ou $p \mid c(Q_1) = 1$ ⇒⟸
⇒ Donc $c(P_1Q_1) = 1$ et $c(PQ) = c\left(c(P)c(Q)\frac{P}{c(P)}\frac{Q}{c(Q)}\right) = c(P)c(Q)\underbrace{c(P_1Q_1)}_{=1} = c(P)c(Q)$.

Proposition : Soit A anneau factoriel et $P \in A[X]$.
Si P est irréductible sur A, il l'est sur $\mathrm{Frac}(A)$.

Soit $Q, R \in \mathbb{K}[X] = \mathrm{Frac}(A)[X]$ tels que $P = QR$. Soit $q, r \in A$ tels que $\underbrace{qQ}_{=:Q_1}, \underbrace{rR}_{=:R_1} \in A[X]$. D'où $qrP = Q_1R_1$.
Par le lemme des contenus, $qrc(P) = c(Q_1)c(R_1)$. De plus, $qrP = c(Q_1)c(R_1)\underbrace{\frac{Q_1}{c(Q_1)}}_{=:Q_2}\underbrace{\frac{R_1}{c(R_1)}}_{=:R_2} = qrc(P)Q_2R_2$.
Puisque $q, r \neq 0$, par intégrité de A, $P = \underbrace{c(P)Q_2}_{\in A[X]}\underbrace{R_2}_{\in A[X]}$.
Or, P est irréductible dans $A[X]$, donc $\deg Q_2 = 0$ ou $\deg R_2 = 0$ i.e. $\deg Q = 0$ ou $\deg R = 0$ i.e. P est irréductible dans $\mathbb{K}[X]$.

Proposition (Critère d'Eisenstein) : Soit A anneau factoriel et $\mathbb{K} = \mathrm{Frac}(A)$.
Soit $P = a_nX^n + \cdots + a_1X + a_0 \in A[X]$ et $p \in A$ irréductible.
On suppose : 1) $p \nmid a_n$
2) $\forall 0 \leq i \leq n-1,\ p \mid a_i$
3) $p^2 \nmid a_0$
Alors P est irréductible dans $\mathbb{K}[X]$.

Par la proposition précédente, si P est réductible dans $\mathbb{K}[X]$, il l'est dans $A[X]$. Soit $Q, R \in A[X]$ tels que $P = QR$ avec $1 \leq \underbrace{\deg Q}_{=q}, \underbrace{\deg R}_{=r} < \deg P$. Écrivons $Q = b_qX^q + \cdots + b_0$, $R = c_rX^r + \cdots + c_0$.
Puisque A est factoriel et p irréductible, (p) est premier donc $B := A/(p)$ est intègre.
Dans $B[X]$, on a alors : $\overline{P} = \bar{a}_nX^n = \bar{Q}\bar{R}$. Puisque $\bar{0} \neq \bar{a}_n = \bar{b}_q\bar{c}_r$, par intégrité de B, $\bar{b}_q, \bar{c}_r \neq \bar{0}$. → car L est un corps
Soit $L = \mathrm{Frac}(B)$. Alors l'égalité $\bar{Q}\bar{R}$ est toujours valable dans $L[X]$. Comme $L[X]$ est principal et X est irréductible, par unicité de la décomposition en irréductibles dans $L[X]$, X divise $\bar{Q}$ et $\bar{R}$.
D'où $\bar{b}_0 = \bar{c}_0 = \bar{0}$ dans B i.e. $p \mid b_0$ et $p \mid c_0$. Donc $p^2 \mid b_0c_0 = a_0$ ⇒⟸ Donc P est irréductible dans $\mathbb{K}[X]$.

Corollaire : Soit p premier et $\Phi_p = \prod_{\zeta \in \mu_p^*}(X - \zeta) = \frac{\prod_{\zeta \in \mu_p}(X-\zeta)}{X-1} = \frac{X^p-1}{X-1} = X^{p-1} + \cdots + X + 1$.
Alors Φ_p est irréductible dans $\mathbb{Q}[X]$.

On a : $(X-1)\Phi_p(X) = X^p - 1$ donc $X\Phi_p(X+1) = (X+1)^p - 1 = \sum_{k=1}^{p}\binom{p}{k}X^k$. D'où $\Phi_p(X+1) = \sum_{k=1}^{p}\binom{p}{k}X^{k-1}$.
Or, $\forall 1 \leq k \leq p-1$, $p \mid \binom{p}{k}$, $p \nmid \binom{p}{p} = 1$ et $p^2 \nmid \binom{p}{1} = p$. Par Eisenstein, $\Phi_p(X+1)$ est irréductible dans $\mathbb{Q}[X]$.
Donc $\Phi_p(X)$ l'est aussi.

Corollaire : $\mathbb{R}$ est un $\mathbb{Q}$-espace vectoriel de dimension infinie.

Par Eisenstein, $\forall n \in \mathbb{N}^*$, $X^n - 2$ est irréductible sur $\mathbb{Q}$. La famille $(1, \sqrt[n]{2}, \ldots, (\sqrt[n]{2})^{n-1})$ est donc $\mathbb{Q}$-libre dans $\mathbb{R}$.
En effet, s'il existait $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ tels que $a_{n-1}\sqrt[n]{2}^{n-1} + \cdots + a_0 = 0$, alors $X^n - 2 \mid a_{n-1}X^{n-1} + \cdots + a_0$ car $X^n - 2$ est le polynôme minimal de $\sqrt[n]{2}$ sur $\mathbb{Q}$. D'où, par degré, $a_{n-1} = \cdots = a_0 = 0$.