Chapitre 2 : Autres type de # et d'espaces

2.1 Les corps finis d'ordre premier

2.1.1 Arithmétique modulaire

Soient a et b deux nombres entier avec $b \neq 0$,

→ Division euclidienne : $a = qb + r$ avec $0 \leq r < |b|$.

- Nous disons que q est le quotient et r le reste de la division de a par b. Si $r = 0$, a est divisible par b.

2.2 ⊙ Fixons un entier $n > 0$. Nous disons que $a, b \in \mathbb{Z}$ sont congruents modulo n ⇔ a et b ont le même reste après division par n : $a \equiv b \pmod n$

2.3 ⊙ Soient $a, b, n \in \mathbb{Z}$ avec $n > 0$. Alors $a \equiv b \pmod n \Leftrightarrow$ $a - b$ est divisible par n.

DÉMO $a = qn + r$, $b = q'n + r'$

Alors, $a \equiv b \pmod n \Leftrightarrow r = r'$, et donc si $a - b = qn - q'n$

$= (q - q')n$

C'est à dire $a - b$ est divisible par n.

⊙ Congruence modulo n est une relation d'équivalence :

- $a \equiv b \pmod n \Leftrightarrow a - b = kn$, $k \in \mathbb{Z}$
- Réflexivité : $a \equiv a \pmod n \Leftrightarrow a - a = 0 = 0 \cdot n$, $0 \in \mathbb{Z}$
- Symétrie : $b \equiv a \pmod n \Leftrightarrow b - a = -kn$, $-k \in \mathbb{Z}$
- Transitivité : $b \equiv c \pmod n \Leftrightarrow b - c = \ell n$, $\ell \in \mathbb{Z}$

$a \equiv c \pmod n \Leftarrow a - c = a - b + b - c = kn + \ell n$

$= (k + \ell)n$, $k + n \in \mathbb{Z}$

⊙ Considérons le quotient de $\mathbb{Z}$ par rapport aux relations d'équivalence

↳ càd les classes d'équivalences

$\overline{0}, \overline{1}, \dots, \overline{n-1}$ où chaque $\overline{k}$ $(0 \leq k < n)$ est l'ensemble de tout les $a \in \mathbb{Z}$ tq le reste après a/n est egal à k !

$\overline{k} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a = qn + k\}$

→ Les classes d'eq. pour la congruence mod n $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$

2.6 ⊙ Soient $a, b, c, d, n \in \mathbb{Z}$ et $n > 1$. Supposons $a \equiv b \pmod n$ et $c \equiv d \pmod n$. Alors

① $a + c \equiv b + d \pmod n$

DEMO Par supposition $b - a = qn$, $q \in \mathbb{Z}$

$d - c = q'n$, $q \in \mathbb{Z}$

Alors $(b+d) - (a+c) = (b-a) + (d-c) = qn + q'n = (q+q')n$

② $ac \equiv bd \pmod n$

DEMO $bd - ac = bd - bc + bc - ac = b(d-c) + c(b-a)$

$= bq'n + cqn = (bq' + cq)n$, $bq' + cq \in \mathbb{Z}$

⊙ L'addition et la multiplication sont bien définie pour $\mathbb{Z}_n$ (classe d'équivalence sous congruence modulo n)

→ associative $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$ $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$

→ neutre $\bar{a} + \bar{0} = \bar{a}$ $\bar{a} \cdot \bar{1} = \bar{a}$

→ ∃ inverse $\bar{a} + -\bar{a} = \bar{0} = -\bar{a} + \bar{a}$ → distrib. $\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$

→ commutative $\bar{a} + \bar{b} = \bar{b} + \bar{a}$ $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$

→ $\mathbb{Z}_n$ est un anneau commutatif

2.1.2. Le corps $\mathbb{F}_p$ et ses espaces finis

Rappel: l'inverse multiplicatif de $a \in R_0$ est l'unique élément a^{-1} tq $a \cdot a^{-1} = 1$

• En arithmétique modulaire, ∄ d'inverse multiplicatif.

Supposons $n = mk$, $n, m, k \in \mathbb{N}$ et $k \neq 1 \neq m$.

Alors $\bar{m} \cdot \bar{k} = \bar{0}$ car $mk = 0 \pmod n$. Alors ∄ d'inverse multiplicatif pour $\bar{m}$ dans $\mathbb{Z}_n$.

DEMO Absurde: ∃ $\bar{a} \cdot \bar{m} = \bar{1}$. Alors $\bar{k} = \bar{1} \cdot \bar{k} = \bar{a} \cdot \bar{m} \cdot \bar{k} = \bar{a} \cdot \bar{0} = \bar{0}$

↯ car $0 < k < n$ donc k n'est pas divisible par n.

2.9 ⊙ Soit p un nombre premier. Alors $\forall \bar{a} \in \mathbb{Z}_p$ différent de $\bar{0}$ possède un inverse multiplicatif.

DÉMO • Soit $a \in \mathbb{Z}$ tq $a \not\equiv 0 \pmod p$. Soient $b, c \in \mathbb{Z}$ et $0 \leq b \leq c < p$.

• Supposons $ab = ac \pmod p$. Alors $a(c-b) = pq$, $q \in \mathbb{Z}$

Alors $pq = 0 \Leftrightarrow q = 0$ (absence de $p \Rightarrow$ "0") et $c - b = 0 \Leftrightarrow c = b$

→ La multiplication par $a \not\equiv 0 \pmod p$ est injective dans $\mathbb{Z}_p$.

L'application $\mu : \mathbb{Z}_p \to \mathbb{Z}_p$, $\overline{x} \mapsto \overline{a} \cdot \overline{x}$ est injective car

$\mu(b) = \mu(c) \Rightarrow ab \equiv ac \pmod p \Rightarrow b \equiv c \pmod p$

→ Puisque $\mathbb{Z}_p$ est fini, μ est bijective, donc $\exists\, \overline{a}^{-1} \in \mathbb{Z}_p$ tq $\mu(\overline{a}^{-1}) = 1 \Leftrightarrow \overline{a} \cdot \overline{a}^{-1} = 1$ ▨

⊙ Soit p un nombre premier, notons $\mathbb{Z}_p = \mathbb{F}_p$ = corps fini à p éléments. Considérons p et $n \in \mathbb{N}_0$. L'ensemble

$\mathbb{F}_p^{\,n} = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{F}_p\}$ est appelé l'espace n-dimensionnel sur $\mathbb{F}_p$.

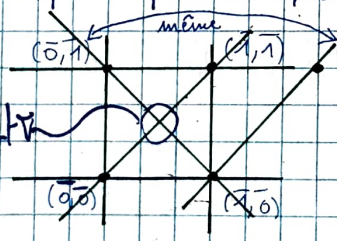
? → $\mathbb{F}_p^{\,n}$ contient p^n éléments.

⊙ Dans cet espace, nous pourrons considérer une addition et multiplicat° scalaire, en utilisant les même formules que dans $\mathbb{R}^n$.

⊙ Dans cet espace, nous pourrons aussi considérer des droites, des plans et des hyperplans (dans $\mathbb{F}_p^{\,n}$).

→ exemple : $p = 2$ → $\mathbb{F}_p = \{\overline{0}, \overline{1}\}$

$\mathbb{F}_p^{\,2} = \{(\overline{0},\overline{1}), (\overline{0},\overline{0}), (\overline{1},\overline{0}), (\overline{1},\overline{1})\}$



ne se croisent pas !

→ Les droites "diagonales" ne se croisent pas dans ce plan

↳ $(\overline{0},\overline{1})$ peut se représenter par le point $(\overline{2},\overline{1})$

2.2. Les nombres complexes

2.2.1 Motivation et définition

→ Prenons l'équation $x^2 + 1 = 0$. Elle n'a pas de solution dans $\mathbb{R}$, car le carré d'un nombre est tjs positif.

↳ notons i un nombre non-réel qui satisfait $i^2 = -1$.

↳ grâce à i, nous pouvons résoudre bcp d'équations :

$$x^2 + 1 = 0 \iff x^2 = -1$$

$$x = \sqrt{-1} = \sqrt{1 \cdot i^2} = \sqrt{1}\sqrt{i^2} = 1 \cdot i = i$$

2.11 ⊙ L'ensemble des nombres complexes est défini par :

$$\mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \}$$

- a est la partie réelle et b la partie imaginaire.
- $0 + bi$ est un imaginaire pur.
- Si $z = a + bi$, alors $\overline{z} = a - bi$ est le conjugé de z.

⊙ Addition : $(a + bi) + (c + di) = (a + c) + (b + d)i$

⊙ Multiplication : $(a + bi) + (c + di) = (ac - bd) + (ad + bc)i$

→ $\mathbb{C}$ est un anneau et même un champ

→ $z \cdot \overline{z} = a^2 + b^2$

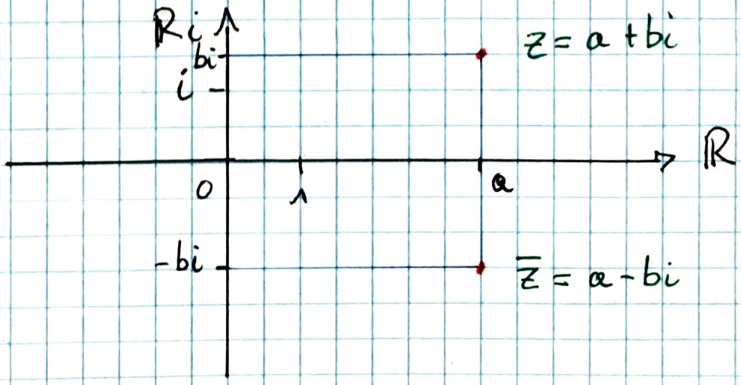
→ $(a + bi)^{-1} = \frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} \Rightarrow z^{-1} = \frac{1}{z} = \frac{\overline{z}}{z\overline{z}}$

2.2.2 Plan de Gauss

- Muni de deux axes : l'axe des réels $\mathbb{R} = \{ a + 0i \mid a \in \mathbb{R} \}$

  l'axe des imaginaire $\mathbb{R}i = \{ 0 + bi \mid b \in \mathbb{R} \}$

- Le module : $|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$



2.2.3 Forme polaire

• Posons $\rho = |z| = \sqrt{a^2+b^2}$

$\rightarrow \frac{z}{\rho} = \frac{a+bi}{\sqrt{a^2+b^2}} = \frac{a}{\sqrt{a^2+b^2}} + \frac{b}{\sqrt{a^2+b^2}} i$

$\rightarrow \left(\frac{a}{\sqrt{a^2+b^2}}\right)^2 + \left(\frac{b}{\sqrt{a^2+b^2}}\right)^2 = 1$

$e^{i\pi}+1=0$

$\rightarrow \frac{z}{\rho} = \cos\theta + i\sin\theta \Leftrightarrow z = \rho(\cos\theta + i\sin\theta)$

↳ forme polaire de z.

$\rightarrow$ L'angle $\theta = \text{Arg}(z)$: argument de z.

⊙ Multiplication : $zz' = \rho(\cos\theta + i\sin\theta).\rho'(\cos\theta' + i\sin\theta')$

$= \underline{\rho\rho'(\cos(\theta+\theta') + i\sin(\theta+\theta'))}$.

⊙ Formule d'Euler : $e^{i\theta} = \cos\theta + i\sin\theta$

$\rightarrow \underline{z = \rho e^{i\theta}}$

$\rightarrow zz' = \rho\rho' e^{i(\theta+\theta')}$

2.13 ⊙ Si $z = \rho(\cos\theta + i\sin\theta) = \rho e^{i\theta}$ avec $\rho, \theta \in \mathbb{R}$, $n \in \mathbb{Z}$, alors

$z^n = \rho^n(\cos n\theta + i\sin n\theta) = \rho^n e^{in\theta}$

2.3 Les polynômes

2.3.1 L'anneau des polynômes

⊙ Un polynome sur $\mathbb{R}$ en une variable X est une expression de la forme $\sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$

avec $n \in \mathbb{N}$, $a_i \in \mathbb{R}$, $i = 0, 1, \ldots, n$

$\rightarrow$ X est une indéterminée ou variable sur $\mathbb{R}$.

$\rightarrow$ $a_i \in \mathbb{R}$ sont les coefficients.

$\rightarrow$ Un polynome peut être nommé $f(X)$ et l'ensemble de tout les polynomes sur $\mathbb{R}$ dans la variable $X = \mathbb{R}[X]$

⊙ Definissons les additions et les multiplications (où $n \leq m$)

$$\rightarrow \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i = \sum_{i=0}^{n} (a_i + b_i) X^i + \sum_{i=n+1}^{m} b_i X^i$$

$$\rightarrow \left(\sum_{i=0}^{n} a_i X^i \right) \cdot \left(\sum_{i=0}^{m} b_i X^i \right) = \sum_{i=0}^{n+m} \left(\sum_{k+\ell=i} a_k b_\ell \right) X^i$$

→ addition est associative et la multiplicat° est commutative

⊙ $\mathbb{R}[X]$ est un anneau commutatif.

⊙ Multiplication scalaire :

$$r \cdot \left(\sum_{i=0}^{n} a_i X^i \right) = \sum_{i=0}^{n} r\, a_i X^i$$

⊙ Polynome à deux variables X et Y : $\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} X^i Y^j$

Deg 2.14 | Soit $f(X) = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X^1 + a_2 X^2 + \dots + a_n X^n$ un polynome avec $a_n \neq 0$. Alors le degrée de $f(X)$ est :

$$\deg(f) = n.$$

→ $\forall r \in \mathbb{R}_0$, $\deg(r) = 0$

→ Par def, $\deg(0) = -\infty$

⊙ Un polynome est unitaire si $a_{\deg f(X)} = 1$

Le 2.15 | Considerons $f, g \in \mathbb{R}[X]$. Alors

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$$

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

2.3.2. La division euclidienne

Prop 2.16 | (Division euclidienne pour polynome) Soient $f(X), g(X) \in \mathbb{R}[X]$ deux polynome réels tq $n = \deg f \geq m = \deg g$. Alors $\exists!$ $q(X)$ et $r(X) \in \mathbb{R}[X]$ qui satisfont les prop. suivantes :

① $\deg q = \deg f - \deg g$

② $\deg r < \deg g$

③ $f(X) = q(X) g(X) + r(X)$

→ Nous appelons $q(X)$ le quotient et $r(X)$ le reste de la division de $f(X)$ par $g(X)$

DEMO

Ecrivons $f(X) = \sum_{i=0}^{n} a_i X^i$ et $g(X) = \sum_{i=0}^{m} b_i X^i$

- Alors le polynome $f(X) - \frac{a_n}{b_m} X^{n-m} g(X)$ est donné par

$$h(X) = \sum_{i=n-m}^{n-1} \left(a_i - \frac{a_n}{b_m} b_{i-n+m}\right) X^i + \sum_{i=0}^{n-m-1} a_i X^i \quad \text{et} \quad \deg h < n.$$

- Nous obtenons $f(X) = \frac{a_n}{b_m} X^{n-m} g(X) + h(X)$

- Si $\deg h(X) \geq m$, on répète la construction (en remplaçant f par h).

- On arrive à $f(X) = q(X) g(X) + r(X)$ où $\deg r(X) < \deg g(X)$

(2) Montrons que q et f sont uniques.

Supposons qu'$\exists$ $q'(X)$ et $r'(X)$ tq $f(X) = q'(X) g(X) + r'(X)$ et $\deg r'(X) < \deg g'(X)$. Alors on trouve :

$$(q(X) - q'(X)) g(X) = r'(X) - r(X)$$

- A droite, le degré du polynome est $< m = \deg g$
- A gauche, le polynome doit être de degré $< \deg g$

Alors, $q(X) - q'(X) = 0$ et $r'(X) - r(X) = 0$

Def 2.17 Nous disons qu'un polynome $f(X)$ est divisible par $g(X)$ si $\exists$ $h(X)$ tq $f(X) = g(X) h(X)$

2.3.3 Racines d'un polynome

Def 2.19 Soit $f(X) = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \in \mathbb{R}[X]$ un polynome réel. Une racine de $f(X)$ est un nombre $r \in \mathbb{R}$ tq

$$f(r) = a_0 + a_1 r + a_2 r^2 + \dots + a_n r^n = 0$$

Prop 2.20 Soit $f(X) \in \mathbb{R}[X]$ un polynome avec $\deg f \geq 1$. Alors $\alpha \in \mathbb{R}$ est une racine de $f \Leftrightarrow \exists$ $g(X) \in \mathbb{R}[X]$ avec $\deg g = \deg f - 1$ tq

$$f(X) = (X - \alpha) g(X), \text{ c.à.d } f(X) \text{ divisible par } X - \alpha.$$

DEMO

Par la division euclidienne de $X - \alpha$, nous trouvons un polynome $g(X) \in \mathbb{R}$ et $r \in \mathbb{R}$ tq $\deg g = \deg f - 1$ et

$$f(X) = (X - \alpha) g(X) + r$$

Evaluons en $X = \alpha$: $0 = f(\alpha) = 0 \cdot g(\alpha) + r$

Donc $r = 0$ et $g(X)$ satisfait les propriétés.

Def 2.21 Soit $f(X) \in \mathbb{R}[X]$ un polynome. $\alpha \in \mathbb{R}$ est une racine de multiplicité m si $f(X)$ est divisible par $(X-\alpha)^m$ mais pas par $(X-\alpha)^{m+1}$. Alors $\exists\, g(X) \in \mathbb{R}[X]$ tq:

$$f(X) = (X-\alpha)^m g(X) \text{ et } \alpha \text{ n'est pas racine de } g(X)$$

→ Si la multiplicité d'une racine > 1, nous disons que α est une racine multiple

Co 2.22 Pour un polynome $f(X)$ de degré n, Σ multiplicité de toutes les racines de $f \leq n$

DEMO

- Soit α_1 une racine de $f(X)$ de multiplicité m_1.
  Alors $\exists !\ g(X)$ tq $f(X) = (X-\alpha_1)^{m_1} g(X)$
- Si $\alpha_2 \neq \alpha_1$ est une autre racine de $f(X)$, nous trouvons
  $$0 = f(\alpha_2) = (\alpha_2 - \alpha_1)^{m_1} g(\alpha_2)$$
- Comme $\alpha_2 \neq \alpha_1$, $g(\alpha_2) = 0$. Donc $g(X) = (X-\alpha_2)h(X)$ et $f(X) = (X-\alpha_1)^{m_1}(X-\alpha_2)h(X)$ pour un unique $h(X) \in \mathbb{R}[X]$
- Après un nombre fini d'étapes, nous trouvons:
  $f(X) = (X-\alpha_1)^{m_1} \dots (X-\alpha_p)^{m_p} \ell(X)$ où $\alpha_1, \dots, \alpha_n$ sont toutes les racines de f et $\ell(X)$ n'a pas de racines.
- En comparant les degrés, on trouve:
  $$n \geq \sum_{i=1}^{p} m_p$$

2.3.4 Racines de polynomes complexes et réels

⊙ Le théorème fondamental de l'algèbre affirme que pour chaque polynome de degré positif à coefficient dans $\mathbb{C}$, possède une racine dans $\mathbb{C}$.

→ Tout polynome $f(X) \in \mathbb{C}$ de degré positif a $\deg(f(x))$ racines

⊙ Soit un polynome complexe $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$
On définit $\overline{f(x)} = \overline{a_n} x^n + \overline{a_{n-1}} x^{n-1} + \dots + \overline{a_0}$ aussi complexe.

Prop 2.23 Considérons $f(x) \in \mathbb{R}[X]$ à coefficients réel et degré > 0. Si z_0 est une racine $\in \mathbb{C}$ de $f(x)$, alors $\overline{z_0}$ est aussi une racine de $f(X)$

DEMO

- Comme tout les coefficients sont réels, $\overline{a} = a \ \forall a \in \mathbb{R}$, on a $\overline{f(x)} = f(x)$
- Soit z_0 une racine complexe de $f(x)$. Donc $f(z_0) = 0$
- Alors $\overline{f(z_0)} = 0 = \overline{f}(\overline{z_0}) = f(\overline{z_0})$, donc $\overline{z_0}$ est racine de $f(x)$

Co 2.24 Chaque polynôme réel $f(x)$ se factorise en un produit de polynômes de degré 2 avec racines purements complexes conjuguées $(x - z_0)(x - \overline{z_0})$ avec $\mathrm{Im}\, z_0 \neq 0$ et de polynome de degré 1, correspondant aux racines réelles

DEMO

- Si z_0 est une racine purement complexe, $\overline{z_0}$ est egalement racine de $f(x)$.
- Alors $(x - z_0)(x - \overline{z_0}) \in \mathbb{R}$, car $= x^2 - (z_0 + \overline{z_0})x + z_0\overline{z_0}$
  $= x^2 - 2\,\mathrm{Re}(z_0)\,x + |z_0|^2 \in \mathbb{R}[X]$.
- Par division euclidienne, $\exists\, q(x)$ et $r(x)$ avec
  $\deg(r(x)) \lneq \deg((x - z_0)(x - \overline{z_0})) = 2$ tel que
  $f(x) = q(x)(x + z_0)(x - \overline{z_0}) + r(x)$
- Si $\deg(r(x)) = 1$, alors $r(x) = ax + b$, $a, b \in \mathbb{R}$, $a \neq 0$
- Pour $x = z_0$, $0 = r(z_0) = a z_0 + b$ ✗ car $\mathrm{Im}(a z_0 + b)$
  $= a\,\mathrm{Im}(z_0) \neq 0$ car $a \neq 0$ et $\mathrm{Im}(z_0) \neq 0$

$\rightarrow \deg(r(x)) = 0$, càd $r(x)$ est constant.

- En $x = z_0$, $r(x) = r(z_0) = 0 \Rightarrow (x - z_0)(x - \overline{z_0})$ divise $f(x)$ dans $\mathbb{R}[X]$
- Si $f(x)$ a d'autres racines purement complexe, c'est aussi une racine de $q(x)$, il faut répéter l'argument jusqu'à ce qu'il n'y ai plus que des racines réelles.

⊙ Si le polynome réel $f(x) \in \mathbb{R}[X]$ est de degré impair, alors $\exists$ une racine réelle

2.3.5. Le plus grand commun diviseur

⊙ Le GCD(f,g) est l'unique polynome monique (unitaire) de degré max qui divise les deux polynomes $f(x)$ et $g(x)$

Voici un algorithme pour le calculer :

[A] Soient deux polynomes $\in \mathbb{R}[X]$ ou tout autre corps commutatif ($\mathbb{F}_p[X]$, $\mathbb{C}[X]$, $\mathbb{Q}[X]$, ...)

- Nous avons $r_{-1}(X) := f(x)$ et $r_0 := g(x) \neq 0$.
- Soient $q_1(x)$ et $r_1(x)$ les uniques polynomes complexes tq :

$$r_{-1}(x) = q_1(x)\, r_0(x) + r_1(x) \text{ avec } \deg(r_1(x)) \lneq \deg(r_0(x))$$

[B] ① Si $r_1(x) = 0$, nous nous arrêtons ici.

② Si $r_1(x) \neq 0$, soient $q_2(x)$ et $r_2(x)$ les uniques polynomes tq : $r_0(x) = q_2(x)\, r_1(x) + r_2(x)$ avec $\deg(r_2(x)) \lneq \deg(r_1(x))$

[C] ① Si $r_2(x) = 0$, nous nous arretons ici

② Si $r_2(x) \neq 0$, on recommence jusqu'à obtenir

$$r_{k-1}(x) = q_{k+1}(x)\, r_k(x) + r_{k+1}(x) \text{ avec } \deg(r_{k+1}(x)) \lneq \deg(r_k(x))$$

puis $r_k(x) = q_{k+2}(x)\, r_{k+1}(x) + r_{k+2}(x)$ avec $\deg(r_{k+2}(x)) \lneq \deg(r_{k+1}(x))$

[D] A chaque étape, on diminue d'un degré, jusqu'à ce que $r_{k+2}(x) = 0$, alors $r_{k+1}(x)$ est un pgcd de $f(x)$ et $g(x)$.

car r_{k+1} divise $r_k(x)$ et $r_{k+1}(x)$, et donc aussi $r_k(x)$.

Par itérance, $r_{k+1}(x)$ divise $r_0(x)$ et $r_{-1}(x)$

[E] Pour trouver le plus grand commun diviseur, il faut multiplier par l'inverse du coefficient du degré principal.

[F] On peut réécrire le GCD(f,g) comme

$$\text{PGCD}(f,g) = y(x) f(x) + z(x) g(x)$$