SEMAINE 1

ALGÈBRE GÉNÉRALE

EXERCICE 1 :

1. Soit G un groupe fini, soient x et y deux éléments de G qui commutent. On note $m = \omega(x)$, $n = \omega(y)$ les ordres respectifs des éléments x et y.

a. On suppose m et n premiers entre eux. Montrer que $\omega(xy) = mn$.

b. On ne suppose plus m et n premiers entre eux. A-t-on $\omega(mn) = m \vee n$?

2. Soit G un groupe commutatif fini. Montrer qu'il existe un élément z de G dont l'ordre est l'*exposant* du groupe G (c'est-à-dire le p.p.c.m. des ordres des éléments de G).

3. Soit K un corps (commutatif), soit G un sous-groupe fini du groupe multiplicatif K^*. Montrer que G est cyclique.

Sources : nombreuses (c'est archi-classique), parmi lesquelles Michel DEMAZURE, Cours d'Algèbre, éditions Cassini, ISBN 2-84225-000-1.

- -

1.a. Posons $z = xy$. On a $z^{mn} = (xy)^{mn} = (x^m)^n (y^n)^m = e$, donc $\omega(z) \mid mn$.

D'autre part, comme $m \wedge n = 1$, il existe deux entiers relatifs u et v tels que $um + vn = 1$ (relation de Bézout). Alors

$$z^{um} = x^{um} y^{um} = x^{um} y^{1-vn} = (x^m)^u \, y \, (y^n)^{-v} = eye = y$$

et, de même, $z^{vn} = x$. Donc x et y appartiennent au sous-groupe $<z>$ engendré par z, mais ce sous-groupe est cyclique d'ordre $\omega(z)$. On en déduit que les ordres de x et de y divisent l'ordre de z, donc leur p.p.c.m. divise aussi l'ordre de z, soit $mn \mid \omega(z)$.

Finalement, $\omega(z) = mn$.

b. Si $m \wedge n \neq 1$, on n'a plus $\omega(xy) = m \vee n$ en général. En effet, dans le groupe $\mathcal{U}_3 = \{1, j, j^2\}$, on a $\omega(j) = \omega(j^2) = 3$, mais $\omega(j\, j^2) = \omega(1) = 1$.

2. Soit n l'exposant du groupe G. Décomposons n en produit de facteurs premiers : $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

Alors, pour tout i, il existe dans G un élément x_i d'ordre $p_i^{\alpha_i}$: en effet, il existe au moins un élément y_i de G tel que la p_i-valuation de $\omega(y_i)$ soit α_i, c'est-à-dire $\omega(y_i) = p_i^{\alpha_i} m_i$ avec $m_i \wedge p_i = 1$. Alors $(y_i^{m_i})^{p_i^{\alpha_i}} = e$. L'ordre de l'élément $y_i^{m_i}$ divise $p_i^{\alpha_i}$, donc est de la forme p_i^{β} avec $\beta \leq \alpha_i$; si on avait $\beta < \alpha_i$, alors on aurait $(y_i^{m_i})^{p_i^{\beta}} = y_i^{p_i^{\beta} m_i} = e$, ce qui contredit $\omega(y_i) = p_i^{\alpha_i} m_i$. On a donc bien $\omega(y_i^{m_i}) = p_i^{\alpha_i}$.

En utilisant la question **1.a.**, par une récurrence immédiate sur k, on déduit que l'élément $y = \prod_{i=1}^{k} y_i^{m_i}$ est d'ordre n.

3. Soit N l'ordre du groupe G, soit n son exposant (*cf.* ci-dessus), soit z un élément de G d'ordre n. Par le théorème de Lagrange, on a $n \mid N$.

Par ailleurs, le polynôme $P = X^n - 1$ de $K[X]$ admet au plus n racines dans K et, tout élément de G étant racine de P, on a $N \leq n$.

En conclusion, $n = N$, donc G est cyclique (G est engendré par z).

EXERCICE 2 :

Soit p un nombre premier, $p \geq 3$.

1. Combien y a-t-il de carrés dans le corps $K = \mathbf{Z}/p\mathbf{Z}$?

2. Montrer qu'un élément x de $\left(\mathbf{Z}/p\mathbf{Z}\right)^*$ est un carré si et seulement si $x^{\frac{p-1}{2}} = \overline{1}$.

3. Quels sont les nombres premiers p pour lesquels $-\overline{1}$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$?

4. En déduire qu'il existe une infinité de nombres premiers de la forme $4k+1$, $k \in \mathbb{N}$.

Source : Daniel PERRIN, Cours d'Algèbre, éditions Ellipses, ISBN 2-7298-5552-1.

- -

1. Soit $G = \left(\mathbf{Z}/p\mathbf{Z}\right)^*$ le groupe multiplicatif des éléments non nuls du corps $K = \mathbf{Z}/p\mathbf{Z}$. L'application $q : x \mapsto x^2$ est un endomorphisme de ce groupe G et $\operatorname{Ker} q = \{-\overline{1}, \overline{1}\}$: en effet, $\{-\overline{1}, \overline{1}\} \subset \operatorname{Ker} q$, $-\overline{1} \neq \overline{1}$ car $p > 2$ et le polynôme $X^2 - \overline{1}$, à coefficients dans le corps K, admet au plus deux racines dans ce corps.

On a donc $|\operatorname{Ker} q| = 2$, d'où $|\operatorname{Im} q| = \dfrac{|G|}{|\operatorname{Ker} q|} = \dfrac{p-1}{2}$. En rajoutant l'élément $\overline{0}$ qui est son propre carré, on dénombre $\dfrac{p+1}{2}$ carrés dans $\mathbf{Z}/p\mathbf{Z}$.

2. Si $x = y^2$ avec $y \in G = \left(\mathbf{Z}/p\mathbf{Z}\right)^*$, alors $x^{\frac{p-1}{2}} = y^{p-1} = \overline{1}$ car $|G| = p-1$ (théorème de Lagrange).

Les carrés de G (qui sont au nombre de $\dfrac{p-1}{2}$ d'après la question **1.**) sont racines de l'équation **(E)** : $x^{\frac{p-1}{2}} - \overline{1} = \overline{0}$; mais cette équation admet au plus $\dfrac{p-1}{2}$ racines dans le corps K. L'équation **(E)** admet donc exactement $\dfrac{p-1}{2}$ racines dans K qui sont les carrés de $\left(\mathbf{Z}/p\mathbf{Z}\right)^*$.

3. Etant donné que $p > 2$ (donc $-\overline{1} \neq \overline{1}$ dans $\mathbf{Z}/p\mathbf{Z}$), on a les équivalences

$$-\overline{1} \text{ carré} \iff (-\overline{1})^{\frac{p-1}{2}} = \overline{1} \iff (-1)^{\frac{p-1}{2}} = 1 \iff \frac{p-1}{2} \text{ pair} \iff p \equiv 1 \text{ modulo } 4\,.$$

4. Soit $n \in \mathbb{N}^*$, montrons qu'il existe des nombres premiers congrus à 1 modulo 4 qui sont plus grands que n.

Pour cela, posons $A = (n!)^2 + 1$.

Tout diviseur premier p de A vérifie $p > n$ (les nombres premiers p tels que $p \leq n$ divisent $(n!)^2 = A - 1$). Soit p un tel diviseur (il en existe au moins un) ; on a $(n!)^2 \equiv -1$ modulo p, donc $-\overline{1}$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$, donc $p \equiv 1$ modulo 4. CQFD

EXERCICE 3 :

1. Soit A un anneau principal, soit K son corps des fractions. Pour tout polynôme P non nul de $A[X]$, on note $c(P)$ **-contenu** de P- le pgcd des coefficients du polynôme P (c'est un élément de A défini "à association près", c'est-à-dire à multiplication près par un élément inversible de l'anneau A). Le polynôme P de $A[X]$ est dit **primitif** si $c(P) = 1$ (ses coefficients sont premiers entre eux dans leur ensemble).

a. Montrer que le produit de deux polynômes primitifs de $A[X]$ est primitif. Que vaut $c(PQ)$ si P et Q sont deux polynômes non nuls de $A[X]$?

b. Soient P et Q deux polynômes de $A[X]$, premiers entre eux dans $A[X]$ (leurs seuls diviseurs communs sont les éléments inversibles de l'anneau $A[X]$, c'est-à-dire...?). Montrer qu'ils sont premiers entre eux dans l'anneau $K[X]$.

2. Soient P et Q deux polynômes de $\mathbb{C}[X,Y] = \mathbb{C}[X][Y]$, premiers entre eux dans $\mathbb{C}[X,Y]$.

a. Démontrer l'existence d'un polynôme D non nul de $\mathbb{C}[X]$ et de deux polynômes A et B de $\mathbb{C}[X,Y]$ tels que

$$D(X) = A(X,Y)\,P(X,Y) + B(X,Y)\,Q(X,Y)\ .$$

b. Montrer que le système **(S)** : $\begin{cases} P(x,y) &= 0 \\ Q(x,y) &= 0 \end{cases}$ a un nombre fini de solutions dans $\mathbb{C}^2$.

Sources :

- *Daniel PERRIN, Cours d'Algèbre, Éditions Ellipses, ISBN 2-7298-5552-1 ;*
- *FRANCINOU et GIANELLA, Exercices de Mathématiques pour l'Agrégation, Algèbre 1, Éditions Masson, ISBN 2-225-84366-X.*
- *ENS Lyon/Cachan, épreuve du concours MP*, session 2000.*

- -

1.a. Posons $P = \displaystyle\sum_{i=0}^{m} a_i X^i$ et $Q = \displaystyle\sum_{j=0}^{n} b_j X^j$, supposons-les tous les deux primitifs. Si le produit PQ n'était pas primitif, il existerait un élément irréductible (ou "premier") p de l'anneau A divisant tous les coefficients de PQ, à savoir tous les $c_k = \displaystyle\sum_{i+j=k} a_i b_j$. Comme p ne divise pas tous les coefficients de A, soit i_0 le plus petit indice i pour lequel p ne divise pas a_i, soit de même $j_0 = \min\{j \in [\![1,n]\!]\ ;\ b_j \notin pA\}$. On a alors

$$c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{i<i_0} a_i b_{i_0+j_0-i} + \sum_{j<j_0} a_{i_0+j_0-j} b_j \ .$$

L'élément irréductible p divise les deux dernières sommes et divise $c_{i_0+j_0}$, il divise donc aussi le produit $a_{i_0} b_{j_0}$, donc il divise l'un des facteurs, ce qui est absurde.

On a utilisé ici le lemme d'Euclide, valable dans tout anneau principal (ou, plus généralement, factoriel) : si p est irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Il est clair que, si $a \in A$ et $P \in A[X]$, alors $c(aP) = a\, c(P)$.

Si P et Q sont deux polynômes quelconques, on peut écrire $P = c(P) \cdot P_0$ et $Q = c(Q) \cdot Q_0$, où P_0 et Q_0 sont primitifs ; alors $P_0 Q_0$ est primitif et

$$c(PQ) = c\big(c(P)\, c(Q) \cdot P_0 Q_0\big) = c(P) c(Q)\, c(P_0 Q_0) = c(P) c(Q) \ .$$

b. Soient P et Q deux polynômes de $A[X]$, premiers entre eux dans $A[X]$ (leurs seuls diviseurs communs dans $A[X]$ sont les éléments inversibles de l'anneau A). Il s'agit de montrer qu'ils sont premiers entre eux dans $K[X]$, c'est-à-dire que leurs seuls diviseurs communs dans $K[X]$ sont les constantes (éléments de K). Écrivons $P = c(P) \cdot P_0$ et $Q = c(Q) \cdot Q_0$ avec P_0 et Q_0 primitifs. Soit D un diviseur commun à P et Q dans $K[X]$: il existe R et S dans $K[X]$ tels que $\left\{\begin{array}{rcl} P & = & DR \\ Q & = & DS \end{array}\right.$ **(*)**.

On peut écrire $D = \dfrac{d_1}{d_2} D_0$ avec $d_1 \in A$, $d_2 \in A$ premiers entre eux, et $D_0 \in A[X]$ primitif : pour cela, on réduit au même dénominateur les coefficients de D, ce qui donne $D = \dfrac{\Delta}{b}$ avec $\Delta \in A[X]$ et $b \in A \setminus \{0\}$, puis $D = \dfrac{c(\Delta)}{b}\, D_0$ avec D_0 primitif, et on simplifie éventuellement la fraction $\dfrac{c(\Delta)}{b}$:

Par exemple, avec $A = \mathbf{Z}$ et $K = \mathbb{Q}$, on a $\dfrac{6}{7} + \dfrac{3}{8} X + \dfrac{15}{4} X^2 = \dfrac{3}{56}(16 + 7X + 70X^2)$ et le polynôme entre parenthèses est primitif dans $\mathbf{Z}[X]$.

De même, $R = \dfrac{r_1}{r_2} R_0$ et $S = \dfrac{s_1}{s_2} S_0$ avec R_0 et S_0 dans $A[X]$, primitifs. Le système **(*)** se réécrit alors sous la forme d'égalités dans $A[X]$:

$$\left\{\begin{array}{rcl} d_2 r_2\, c(P) \cdot P_0 & = & d_1 r_1\, D_0 R_0 \\ d_2 s_2\, c(Q) \cdot Q_0 & = & d_1 s_1\, D_0 S_0 \end{array}\right. . \qquad (**)$$

Les polynômes $D_0 R_0$ et $D_0 S_0$ étant primitifs d'après **a.**, en égalant les contenus dans **(**)**, on obtient $\left\{\begin{array}{rcl} u\, d_2 r_2\, c(P) & = & d_1 r_1 \\ v\, d_2 s_2\, c(Q) & = & d_1 s_1 \end{array}\right.$, où u et v sont deux éléments inversibles de l'anneau A. En réinjectant dans **(**)**, cela donne $\left\{\begin{array}{rcl} P_0 & = & u\, D_0 R_0 \\ Q_0 & = & v\, D_0 S_0 \end{array}\right.$, donc le polynôme $D_0 \in A[X]$ divise, dans $A[X]$, les polynômes P_0 et Q_0 ; il divise donc aussi les polynômes $P = c(P) \cdot P_0$ et $Q = c(Q) \cdot Q_0$, donc D_0 est une constante (inversible dans A) et $D = \dfrac{d_1}{d_2} D_0$ est une constante (élément de K), ce qu'il fallait démontrer.

Si P et Q sont deux polynômes de $A[X]$, le lecteur montrera facilement (le plus dur a été fait) l'équivalence entre les assertions :

(i) *: P et Q sont premiers entre eux dans $A[X]$;*

(ii) *:* $\begin{cases} c(P) \text{ et } c(Q) \textit{ sont premiers entre eux dans } A \\ P \text{ et } Q \textit{ sont premiers entre eux dans } K[X] \end{cases}$.

2.a. Appliquons la question **1.b.** avec $A = \mathbb{C}[X]$ et $K = \mathbb{C}(X)$. Les polynômes P et Q, premiers entre eux dans $A[Y] = \mathbb{C}[X,Y]$, sont aussi premiers entre eux dans $K[Y] = \mathbb{C}(X)[Y]$. Comme $K = \mathbb{C}(X)$ est un corps, l'anneau $K[Y]$ est principal et on peut appliquer l'identité de Bézout : il existe des polynômes U et V dans $\mathbb{C}(X)[Y]$ tels que $UP + VQ = 1$. On peut écrire $U(X,Y) = \displaystyle\sum_{i=0}^{m} U_i(X)Y^i$ et $V(X,Y) = \displaystyle\sum_{j=0}^{n} V_j(X)Y^j$, les U_i et les V_j étant des éléments de $\mathbb{C}(X)$; si on note $D(X)$ le ppcm des dénominateurs de ces fractions rationnelles U_i et V_j, on peut écrire $U(X,Y) = \dfrac{A(X,Y)}{D(X)}$ et $V(X,Y) = \dfrac{B(X,Y)}{D(X)}$, où A et B sont des polynômes de $\mathbb{C}[X,Y]$, et on a ainsi

$$A(X,Y)P(X,Y) + B(X,Y)Q(X,Y) = D(X)\ .$$

b. Si le couple $(x,y) \in \mathbb{C}^2$ vérifie le système **(S)**, alors x est racine du polynôme D (il y en a un nombre fini). Les indéterminées X et Y jouant le même rôle, il y a aussi un nombre fini de valeurs possibles de y, donc de couples (x,y).

EXERCICE 4 : Un théorème de Sylow

Soit G un groupe fini, d'ordre $n = p^\alpha m$ avec p premier et $p \wedge m = 1$.

On note X l'ensemble des parties de G de cardinal p^α, et Y l'ensemble des sous-groupes de G d'ordre p^α.Le but du jeu est de montrer que $Y \neq \emptyset$, et plus précisément que le nombre de sous-groupes de G d'ordre p^α (*les p-Sylow de G*) est congru à 1 modulo p.

Pour cela, on fait opérer G sur X par translation à gauche : si $g \in G$ et $E \in X$, on pose

$$g \cdot E = gE = \{ga\ ;\ a \in E\}\ .$$

1. Soit $E \in X$. Montrer que son stabilisateur $\mathcal{S}_E = \{g \in G \mid g \cdot E = E\}$ est de cardinal au plus égal à p^α.

2. Soit $E \in X$. Montrer que le cardinal du stabilisateur $\mathcal{S}_E$ est égal à p^α si et seulement si E est une classe à droite modulo un sous-groupe d'ordre p^α (c'est-à-dire $E = H \cdot x$ avec $x \in G$ et $H \in Y$).

3. Montrer que $|X|$ est congru à $m|Y|$ modulo p.

4. Montrer que $|X|$ est congru à m modulo p.

5. Conclure.

Source : Daniel PERRIN, Cours d'Algèbre, éditions Ellipses, ISBN 2-7298-5552-1.

- -

1. Les translations étant des permutations de G, si $E \in X$, on a bien $g \cdot E \in X$, c'est-à-dire $|g \cdot E| = |E| = p^\alpha$. De plus, avec $E \in X$, les égalités $e \cdot E = E$ et $(gh) \cdot E = g \cdot (h \cdot E)$ sont immédiates, on a donc bien une action du groupe G sur l'ensemble X.

Soit $E \in X$, soit $a \in E$ donné ; si $g \in \mathcal{S}_E$, alors $ga \in g \cdot E = E$, donc $g \in Ea^{-1}$. On a donc $\mathcal{S}_E \subset Ea^{-1}$, où a est un élément quelconque de E, d'où $|\mathcal{S}_E| \leq |Ea^{-1}| = |E| = p^\alpha$.

Rappelons que le stabilisateur $\mathcal{S}_E$ d'un élément E de X est un sous-groupe de G (vérification immédiate).

2. • Si $E = Hx$ avec $H \in Y$, alors

$$g \in \mathcal{S}_E \iff gE = E \iff gHx = Hx \iff gH = H$$

mais, H étant un sous-groupe, cette dernière condition équivaut à $g \in H$. On a alors $\mathcal{S}_E = H$, d'où $|\mathcal{S}_E| = p^\alpha$.

• Si $|\mathcal{S}_E| = p^\alpha$, alors $\mathcal{S}_E$ est un sous-groupe d'ordre p^α, posons $H = \mathcal{S}_E \in Y$. Si on se donne $a \in E$, on a $H \subset Ea^{-1}$ d'après la question **1.**, d'où $H = Ea^{-1}$ (égalité des cardinaux), donc $E = Ha$: E est une classe à droite modulo a.

3. Les éléments de X de la forme Hx avec $H \in Y$ et $x \in G$ sont au nombre de $m|Y|$: chaque sous-groupe d'ordre p^α, s'il en existe, définit m classes à droite distinctes et deux sous-groupes distincts ne peuvent engendrer une même classe à droite (supposons $H_1x_1 = H_2x_2$, alors $x_1 = ex_1 \in H_2x_2$, donc $x_1x_2^{-1} \in H_2$ puis $x_2x_1^{-1} = (x_1x_2^{-1})^{-1} \in H_2$ et enfin $H_1 = H_2x_2x_1^{-1} = H_2$).

Les autres éléments E de X ont un stabilisateur $\mathcal{S}_E$ dont le cardinal est strictement inférieur à p^α, mais divise $p^\alpha m$ (car les stabilisateurs sont des sous-groupes de G), donc $|\mathcal{S}_E|$ est de la forme $p^k d$, avec $0 \leq k \leq \alpha - 1$ et $d \mid m$. Ils ont donc une orbite dont le cardinal (qui est l'indice du stabilisateur), $[G : \mathcal{S}_E] = p^{\alpha-k}\dfrac{m}{d}$, est multiple de p.

Les orbites de X sous l'action de G par translation à gauche étant deux à deux disjointes, on déduit $|X| \equiv m|Y|$ modulo p.

4. Le cardinal de X ne dépend que de l'ordre du groupe G et non de sa structure : c'est le nombre de parties à p^α éléments d'un ensemble à $n = p^\alpha m$ éléments. On peut donc supposer ici que $G = \mathbf{Z} / _{n\mathbf{Z}}$. Dans ce cas, G, cyclique d'ordre $p^\alpha m$, admet un unique sous-groupe d'ordre p^α, donc $|Y| = 1$ et $|X| \equiv m$ modulo p.

Cette question est d'ordre purement combinatoire : il s'agit de prouver que, pour p premier, $\alpha \in \mathbb{N}$ et $m \wedge p = 1$, on a $C_{p^\alpha m}^{p^\alpha} \equiv m$ modulo p. Si quelqu'un a une démonstration élémentaire de ce résultat, je suis preneur...

5. On a $m|Y| \equiv m$ modulo p d'après les questions **3.** et **4.** Comme m et p sont premiers entre eux, on peut simplifier cette congruence : il reste $|Y| \equiv 1$ modulo p, ce que l'on voulait prouver et, en particulier, $|Y| \neq 0$.

EXERCICE 5 :

Soient A et B deux polynômes non nuls de $\mathbb{C}[X]$, d'écriture factorisée

$$A = a\prod_{i=1}^{m}(X-\alpha_i) \qquad ; \qquad B = b\prod_{j=1}^{n}(X-\beta_j)\ .$$

On appelle **résultant** des polynômes A et B le nombre

$$\mathrm{Res}(A,B) = a^n\, b^m \prod_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} (\alpha_i-\beta_j)\ .$$

Si $A=0$ ou $B=0$, on pose $\mathrm{Res}(A,B)=0$.

1. On suppose $B\neq 0$, soit R le reste de la division euclidienne de A par B. Montrer que

$$\mathrm{Res}(A,B) = (-1)^{mn}\, b^{m-\deg(R)}\,\mathrm{Res}(B,R)\ .$$

2. Que vaut $\mathrm{Res}(A,A')$? Dans quel cas est-il nul ?

3. Ecrire une condition nécessaire et suffisante pour que le polynôme $A=X^5+pX+q$ (avec p et q réels) admette trois racines réelles distinctes.

Source : Jean-Pierre ESCOFIER, Théorie de Galois, éditions Masson, ISBN 2-225-82948-9.

- -

1. Notons d'abord que $\mathrm{Res}(A,B) = (-1)^{mn}\,\mathrm{Res}(B,A) = (-1)^{\deg(A)\cdot\deg(B)}\,\mathrm{Res}(B,A)$, puis que $\mathrm{Res}(B,A) = b^m\, a^n \prod_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} (\beta_j-\alpha_i) = b^{\deg(A)}\cdot\prod_{j=1}^{n} A(\beta_j)$. Or, de $A=BQ+R$, on déduit que $A(\beta_j)=R(\beta_j)$ pour tout $j\in[\![1,n]\!]$, donc

$$\begin{aligned}
\mathrm{Res}(A,B) &= (-1)^{mn}\,\mathrm{Res}(B,A)\\
&= (-1)^{mn}\, b^{\deg(A)}\cdot\prod_{j=1}^{n} A(\beta_j)\\
&= (-1)^{mn}\, b^{\deg(A)}\cdot\prod_{j=1}^{n} R(\beta_j)\\
&= (-1)^{mn}\, b^{\deg(A)-\deg(R)}\cdot\left[b^{\deg(R)}\cdot\prod_{j=1}^{n} R(\beta_j)\right]\\
&= (-1)^{mn}\, b^{\deg(A)-\deg(R)}\cdot\mathrm{Res}(B,R)\ .
\end{aligned}$$

Le résultant de deux polynômes peut ainsi se calculer par l'algorithme d'Euclide ; c'est l'algorithme le plus efficace.

Remarque. Si $B=\lambda$ (constant), alors $\mathrm{Res}(A,B)=\lambda^m=\lambda^{\deg(A)}$.

2. On a vu $\operatorname{Res}(A,B) = (-1)^{\deg(A)\cdot\deg(B)}\operatorname{Res}(B,A) = a^{\deg(B)}\prod_{i=1}^{m} B(\alpha_i)$, où les α_i sont les racines de A.

Ainsi,

$$\operatorname{Res}(A,A') = a^{m-1}\cdot\prod_{i=1}^{m} A'(\alpha_i)\ .$$

Or, $A' = a\cdot\sum_{i=1}^{m}\left(\prod_{j\neq i}(X-\alpha_j)\right)$ et, pour tout $i\in[\![1,m]\!]$, $A'(\alpha_i) = a\cdot\prod_{j\neq i}(\alpha_i-\alpha_j)$, donc

$$\operatorname{Res}(A,A') = a^{2m-1}\prod_{i=1}^{m}\left(\prod_{j\neq i}(\alpha_i-\alpha_j)\right) = (-1)^{\frac{m(m-1)}{2}}\,a^{2m-1}\prod_{i<j}(\alpha_i-\alpha_j)^2\ .$$

Le résultant de A et A' (aussi appelé **discriminant** du polynôme A) est nul si et seulement si A admet une racine double, c'est-à-dire si et seulement si $A\wedge A'\neq 1$.

La définition exacte du discriminant du polynôme A est $D(A) = \frac{1}{a}\,(-1)^{\frac{m(m-1)}{2}}\operatorname{Res}(A,A')$.

3. On a $\operatorname{Res}(A,A') = \prod_{i<j}(\alpha_i-\alpha_j)^2$, où les α_i $(1\leq i\leq 5)$ sont les racines de A.

D'autre part, $A' = 5X^4+p$, le reste de la division euclidienne de A par A' est $R = \frac{4}{5}pX+q$, celui de la division de A' par R est une constante λ que l'on détermine en posant $X = -\frac{5q}{4p}$ dans l'identité $A' = RQ+\lambda$ donc $\lambda = A'\left(-\frac{5q}{4p}\right) = \frac{3125q^4+256p^5}{256p^4}$. Finalement,

$$\operatorname{Res}(A,A') = 5^4\operatorname{Res}(A',R) = 5^4\left(\frac{4p}{5}\right)^4\operatorname{Res}(R,\lambda) = 5^4\left(\frac{4p}{5}\right)^4\lambda^{\deg(R)} = 256p^5+3125q^4\ .$$

On en déduit déjà que A admet une racine double si et seulement si

$$256\,p^5+3125\,q^4 = 0\ .$$

Par ailleurs,

- si A admet cinq racines réelles (non nécessairement distinctes), alors
$$\operatorname{Res}(A,A') = \prod_{i<j}(\alpha_i-\alpha_j)^2\geq 0\ ;$$
- si A admet une racine réelle a et deux couples $(b,\overline{b})$, $(c,\overline{c})$ de racines conjuguées, alors

$$\begin{aligned}\operatorname{Res}(A,A') &= (b-a)^2(\overline{b}-a)^2(c-a)^2(\overline{c}-a)^2(\overline{b}-b)^2(c-b)^2(\overline{c}-b)^2(c-\overline{b})^2(\overline{c}-\overline{b})^2(\overline{c}-c)^2\\ &= 16\,(\operatorname{Im}b)^2\,(\operatorname{Im}c)^2\,|b-a|^4\,|c-a|^4\,|c-b|^4\,|\overline{c}-b|^4\geq 0\ .\end{aligned}$$

- si A admet trois racines réelles a, b, c et un couple $(d,\overline{d})$ de racines conjuguées, alors

$$\begin{aligned}\mathrm{Res}(A,A') &= (b-a)^2(c-a)^2(d-a)^2(\overline{d}-a)^2(c-b)^2(d-b)^2(\overline{d}-b)^2(d-c)^2(\overline{d}-c)^2(\overline{d}-d)^2 \\ &= -4\,(\mathrm{Im}\,d)^2\,(b-a)^2\,(c-a)^2\,(d-a)^2\,|d-a|^4\,|d-b|^4\,|d-c|^4 \leq 0\,,\end{aligned}$$

l'inégalité étant stricte lorsque les racines réelles a, b, c sont distinctes.

La condition recherchée est donc

$$256\,p^5 + 3125\,q^4 < 0\,.$$

EXERCICE 6 :

Dans cet exercice, on admet que, pour tout p premier, le groupe multiplicatif $\left(\mathbf{Z}/p\mathbf{Z}\right)^*$ *des éléments non nuls du corps* $\mathbf{Z}/p\mathbf{Z}$ *est cyclique* (*cf. exercice* 1).

Soit n un entier, $n \geq 2$. On dira que n vérifie la propriété **(F)** si, pour tout entier relatif a, a^n est congru à a modulo n.

1. Montrer le **petit théorème de Fermat** : tout nombre premier p vérifie la propriété **(F)**.

On appelle **nombre de Carmichael** tout entier n composé vérifiant la propriété **(F)**.

2. Soit n un entier sans facteur carré, $n \geq 2$. Soit m un entier ($m \geq 2$) tel que, pour tout diviseur premier p de n, $p-1$ divise $m-1$. Montrer que a^m est congru à a modulo n pour tout entier relatif a.

3. Soit $n = p^2 m$ avec p premier et $m \in \mathbb{N}^*$; vérifier $(1+p\,m)^n \equiv 1$ modulo n.

4. Montrer qu'un entier $n \geq 2$ vérifie la propriété **(F)** si et seulement si n est sans facteur carré et $p-1$ divise $n-1$ pour tout diviseur premier p de n.

Source : Michel DEMAZURE, Cours d'Algèbre, éditions Cassini, ISBN 2-84225-000-1.

- -

1. Si $a \in \mathbf{Z}$ n'est pas multiple de p, alors sa classe de congruence modulo p (notons-la $\overline{a}$) est un élément du groupe multiplicatif $\left(\mathbf{Z}/p\mathbf{Z}\right)^*$ d'ordre $p-1$, donc $\overline{a}^{\,p-1} = \overline{1}$, c'est-à-dire $a^{p-1} \equiv 1$ modulo p, d'où $a^p \equiv a$ modulo p.

Si a est multiple de p, on a évidemment $a^p \equiv a \equiv 0$ modulo p.

2. Il faut montrer que $n \mid a^m - a$; mais, par hypothèse, n est le produit de ses facteurs premiers, qui sont deux à deux premiers entre eux. Il suffit donc de prouver que tout diviseur premier p de n divise $a^m - a$ (n est le p.p.c.m. de ses diviseurs premiers).

Soit donc p un diviseur premier de n.

▷ si a est multiple de p, $a^m - a$ est multiple de p (évident)

$\triangleright$ si a n'est pas multiple de p, on a $a^{p-1} \equiv 1$ modulo p d'après la question **1.**. Comme $m-1 = (p-1)k$ avec k entier naturel, $a^{m-1} = (a^{p-1})^k$ est aussi congru à 1 modulo p, donc $a^m \equiv a$ modulo p.

Le lecteur en déduira par exemple que $a^{13} \equiv a$ modulo 35 pour tout entier relatif a, et donc $a^{12} \equiv 1$ modulo 35 pour tout entier a premier avec 35. L'exposant du groupe $\left(\mathbf{Z}/_{35\,\mathbf{Z}}\right)^*$, d'ordre $\varphi(35) = 24$, des éléments inversibles de l'anneau $\mathbf{Z}/_{35\,\mathbf{Z}}$ est 12, puisqu'on peut voir qu'il existe des éléments d'ordre 12 exactement, par exemple la classe de 2.

3. Si $n = p^2 m$, alors

$$(1 + p\,m)^n = 1 + np\,m + \sum_{k=2}^{n} C_n^k (p\,m)^k \ .$$

Chaque terme de cette dernière somme est divisible par $p^2 m^2$ donc *a fortiori* par $n = p^2 m$, donc $(1 + p\,m)^n \equiv 1$ modulo n.

4. • Supposons n sans facteur carré tel que $\forall p \in \mathcal{P}_n \quad p - 1 \mid n - 1$ ($\mathcal{P}_n$: support premier de n). Alors n vérifie la propriété **(F)** d'après la question **2.**

• Soit n vérifiant la propriété **(F)**.

Alors n est sans facteur carré : par l'absurde, si on avait $n = p^2 m$ avec p premier, l'entier $a = 1 + p\,m$ vérifierait $a^n \equiv 1$ modulo n d'après la question **3.**, ce qui contredit $a^n \equiv a$ modulo n.

Ecrivons $n = p_1 \dots p_m$ (produit de nombres premiers distincts). Pour tout $i \in [\![1, m]\!]$, soit a_i un entier dont la classe modulo p_i est un générateur du groupe cyclique $\left(\mathbf{Z}/_{p_i\,\mathbf{Z}}\right)^*$. D'après le théorème chinois, il existe un entier a tel que $a \equiv a_i$ modulo p_i pour tout i. Par hypothèse, $a^n \equiv a$ modulo n ; comme $a \wedge n = 1$ (a n'est divisible par aucun des p_i), on peut "simplifier cette congruence par a" et $a^{n-1} \equiv 1$ modulo n d'où, *a fortiori*, $a^{n-1} \equiv 1$ modulo p_i pour tout i, donc $a_i^{n-1} \equiv 1$ modulo p_i.
Cela implique que $n - 1$ est multiple de l'ordre de a_i modulo p_i, c'est-à-dire $p_i - 1 \mid n - 1$, ce qu'il fallait démontrer.