Université Claude Bernard Lyon 1 — Algèbre et Géométrie
Semestre d'automne 2020-21 — L3 MGA

Examen 3 – Durée 75 min – le lundi 10 mai 2021

Les documents, les téléphones et les calculatrices ne sont pas autorisés.
La notation tiendra compte du soin apporté à la rédaction des réponses.
Les **réponses mal justifiées** ne permettront pas d'obtenir tous les points.

Exercice 1.

a) Résoudre l'équation $X^2 - 6X + 5 = 0$ dans $\mathbb{Z}/13\mathbb{Z}$.
Comme $\mathbb{Z}/13\mathbb{Z}$ est un corps, on peut utiliser le discrinant. Celui-ci vaut $\Delta = 36 - 20 = 16 = 4^2$. Donc les solutions de l'équation sont

$$x = \frac{\pm 4 + 6}{2} = 5 \text{ et } 1.$$

On vérifie sans peine que $X^2 - 6X + 5 = (X - 5)(X - 1)$.

b) On veut résoudre la même équation dans $\mathbb{Z}/15\mathbb{Z}$.

i) Calculer a^2 pour $a \in \{\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},\ \bar{4},\ \bar{5},\ \bar{6},\ \bar{7}\}$.
Les carrés sont 0, 1, 4, -6, 1, -5, 6, 4.

ii) En déduire les solutions de l'équation $X^2 = 4$ dans $\mathbb{Z}/15\mathbb{Z}$.
D'après le calcul précédent (exhaustif au signe près) : $\{\pm 2, \pm 7\}$.

iii) Déduire des deux questions précédentes les solutions de $X^2 - 6X + 5 = 0$ dans $\mathbb{Z}/15\mathbb{Z}$.
On a

$$\Delta = 16 = 1 = (\pm 1)^2 = (\pm 4)^2$$

et $1/2 = 8$ (car $8x2 = 16 = 1$). Donc $X^2 - 6X + 5 = (X + 5)(X + 4) = (X - 5)(X - 1)$. On a donc au moins 4 solution $\{1, \pm 5, -4\}$.
Réciproquement, on utilise la forme canonique.

$$X^2 - 6X + 5 = (X - 3)^2 - 4$$

Donc l'équation devient $(X - 3)^2 = 4$. D'après le calcul des carrés on sait que cela revient à $X - 3 \in \{\pm 2, \pm 7\}$ qui donnent les 4 solutions trouvées.

Exercice 2. Zéros des polynômes à plusieurs variables

Soit $n \neq 1$ et P un polynôme en les n variables $X_1, \ldots, X_n$ à coefficients complexes. On pose

$$V(P) = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \ :\ P(x_1, \ldots, x_n) = 0\}.$$

a) On suppose qu'il existe des ensembles infinies $S_1, \ldots, S_n$ de $\mathbb{C}$ tels que

$$S_1 \times \cdots \times S_n \subset V(P).$$

On va montrer que P est nul.

i) Montrer que si $n = 1$ alors P est nul.
Le polynôme P a une infinité de racines. Il est nul.

ii) Justifier que P peut s'écrire sous la forme

$$P = Q_d X_n^d + \cdots + Q_1 X_n + Q_0,$$

avec $d \in \mathbb{N}$ et $Q_d, \ldots, Q_0$ dans $\mathbb{C}[X_1, \ldots, X_{n-1}]$.
On écrit chaque monome comme $aX_1^{\alpha_1} \ldots X_n^{\alpha_n} = (aX_1^{\alpha_1} \ldots X_{n-1}^{\alpha_{n-1}})X_n^{\alpha_n}$ *et on trouve la forme voulue.*

iii) Montrer que pour tout $0 \leq i \leq d$ et tout $(x_1, \ldots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$, on a

$$Q_i(x_1, \ldots, x_{n-1}) = 0.$$

Une fois $(x_1, \ldots, x_{n-1}) \in S_1 \times \cdots \times S_{n-1}$ *fixé, le polynôme en* X_n, $Q_d(x_1, \ldots, x_{n-1})X_n^d + \cdots + Q_1(x_1, \ldots, x_{n-1})X_n + Q_0(x_1, \ldots, x_{n-1})$ *a une infinité de racines. Donc tous ces coefficients sont nuls. CQFD.*

iv) Montrer que $P = 0$.
Il s'agit d'une récurrence. La première question étant l'initialisation et la précédente l'hérédité.

b) Montrer que, si P est non nul alors $\mathbb{C}^n - V(P)$ est dense dans $\mathbb{C}^n$.
Le plus simple est de choisir comme norme sur $\mathbb{C}^n$ *le max des* $|z_i|$ *(la norme infinie). Si par l'absurde* $\mathbb{C}^n - V(P)$ *n'est pas dense,* $V(P)$ *est d'intérieur non vide et contient une boule. Cette boule est un produit de n boules de* $\mathbb{C}$. *La question précédente montre alors que* P *est nul. Contradiction.*

c) Soit maintenant $H_1, \ldots, H_s$ des hyperplans de $\mathbb{C}^n$. Montrer que $\mathbb{C}^n - \bigcup_{i=1}^s H_i$ est dense dans $\mathbb{C}^n$.
Soit φ_i *une équation de* H_i *(forme linéaire). La question découle de la précédente avec* $P = \prod_i \varphi_i$.

Exercice 3. Résultant de deux polynômes

Soit P et Q deux polynômes à coefficients complexes de degrés p et q et de coefficients dominants a et b, respectivement.
Considérons l'application suivante

$$\begin{array}{rccc} \varphi : & \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X] & \longrightarrow & \mathbb{C}_{p+q-1}[X] \\ & (U, V) & \longmapsto & UP + VQ. \end{array}$$

a) Montrer que φ est une application linéaire.
Avec des notations évidentes, on a

$$\varphi(\lambda(U_1, V_1) + (U_2, V_2)) = \lambda U_1 P + V_1 Q + U_2 P + V_2 Q = \lambda\varphi(U_1, V_1) + \varphi(U_2, V_2).$$

Donc φ *est linéaire.*

b) Montrer que φ est inversible si et seulement si elle est injective si et seulement si P et Q sont premiers entre eux.
La première équivalence provient de l'égalité des dimensions $(p+q)$ *des espaces de départ et d'arrivée de l'application linéaire* φ.
Par ailleurs, supposons $P \wedge Q = 1$. *Alors* $UP = -VQ$ *impose* P *divise* VQ *et donc par Gauss* P *divise* V. *Vu les dégré cela ne peut arriver que si* $V = 0$. *De même* $U = 0$. *Et* φ *est injective.*
supposons $D := P \wedge Q \neq 1$. *Alors* $P = DA$ *et* $Q = DB$. *Mais alors* $BP - AQ = 0$ *et* (B, A) *est un élément non nul du noyau de* φ.
Indication : Ne pas utiliser Bezout !

On munit l'espace de départ de la base $\mathcal{B} = ((1,0), \ldots, (X^{q-1}, 0), (0,1), \ldots, (0, X^{p-1}))$ et celui d'arrivée de la base canonique $\mathcal{C}$. Posons

$$M = \mathrm{M}at_{\mathcal{C}\,\mathcal{B}}(\varphi) \qquad \text{et} \qquad \mathrm{Res}(P, Q) = \det(M).$$

c) Pour $1 \leq i \leq q$, déterminer le coefficient (i,i) de M.

A la colone i, on a les coordonnées de $\varphi((X^{i-1},0)) = X^{i-1}P$. A la i-ème ligne de cette colonne on a donc le coef en X^{i-1} de $X^{i-1}P$, c'est-à-dire $P(0)$.
Ecrivons

$$P(X) = a\prod_i X - \alpha_i \qquad Q(X) = b\prod_j X - \beta_j.$$

Considérons la fonction

$$\Gamma : \mathbb{C} \longrightarrow \mathbb{C},\ t \longmapsto \mathrm{Res}(P(X+t), Q(X)).$$

On admettra que Γ est un polynôme de degré pq dont le coefficent directeur est $(-1)^{pq}a^q b^p$ (cela peut se montrer sans trop de peine en examinant la matrice M).

d) Montrer que, pour tout i et j, $\Gamma(\alpha_i - \beta_j) = 0$.
Les polynômes $P(X + \alpha_i - \beta_i)$ et $Q(X)$ ont une racine commune qui est β_i. Donc il ne sont pas premier entre eux. Donc le résultant est nul : $\Gamma(\alpha_i - \beta_j) = 0$.

e) En déduire que, si les $\alpha_i - \beta_j$ sont deux à deux distincts, on a

$$\mathrm{Res}(P,Q) = a^q b^p \prod_{i,j} \alpha_i - \beta_j.$$

Le polynôme Γ a pq racines distinctes, il est de degré pq et son coef directeur est $a^q b^p$. Donc

$$\Gamma = a^q b^p \prod_{i,j} (X - \alpha_i - \beta_j).$$

En évaluant en 0 on obtient le formule voulue.

f) Sous ces mêmes hypothèses en déduire que

$$\mathrm{Res}(P,Q) = a^q \prod_i Q(\alpha_i).$$

Pour i fixé on a

$$\prod_j b(\alpha_i - \beta_j) = Q(\alpha_i).$$

Donc la formule voulue découle de celle obtenue à la question précédente.

g) En utilisant la dernière question de l'exercice 2, montrer que cette formule est toujours valable.
On considère l'application

$$\mathbb{C}^{p+q} \longrightarrow \mathbb{C}, (\alpha_i, \beta_j) \longmapsto \mathrm{Res}(\prod_i (X - \alpha_i), \prod_j (X - \beta_j) - \prod_{i,j} \alpha_i - \beta_j.$$

D'après l'expression comme déterminant, cette application est continue. D'après la question précédente elle est nulle dès que $\forall i,j,k,l \alpha_i - \beta_j \neq \alpha_k - \beta_l$. D'après l'exercice précédent cet ensemble est dense. Donc la fonction est nulle.

Exercice 4. Entiers algébriques

a) Soit $P = X^4 - 5X^2 + 1$. Déterminer les racines complexes de P.
C'est une équation bicarré. On a $\Delta = 25 - 4 = 21$. Donc les racines complexes de $Y^2 - 5Y + 1$ qui sont

$$\frac{\pm\sqrt{21} + 5}{2}$$

sont réelles et positives. Les racines de P sont donc

$$\pm\sqrt{\pm\frac{\sqrt{21}+5}{2}}.$$

b) Montrer que P est irréductible dans $\mathbb{Q}[X]$.

Comme P est de contenu 1, d'après le cours il suffit de montrer qu'il est irréductible dans $\mathbb{Z}[X]$. Si $P = AB$ avec A et B dans $\mathbb{Z}[X]$, alors quitte à multiplier par -1, on peut supposer que A et B sont unitaires (car P l'est).

Si $\deg(A) = 1$ ou $\deg(B) = 1$, alors P a une racine dans $\mathbb{Z}$. Il est facile de voir qu'aucune des 4 racines complexes trouvées à la question 1 n'est entière. Contradiction.

Supposons à présent que $\deg(A) = \deg(B) = 2$. On écrit $A = X^2 + aX + b$ et $B = X^2 + a'X + b'$. Alors $AB = P$ équivaut à

$$\begin{cases} a' + a = 0 \\ b' + aa' + b = -5 \\ ab' + a'b = 0 \\ bb' = 1 \end{cases}$$

Donc $b = b' = \pm 1$ (les nombres a, a', b, b' étant des entiers). Donc $aa' = -a^2 = -7$ ou -3. Contradiction (car $\sqrt{7}$ et $\sqrt{3}$ ne sont pas entiers).

Un nombre complexe α est appelé *entier algébrique* s'il existe un polynôme unitaire Q à coefficients entiers tel que $Q(\alpha) = 0$.

c) Donner trois exemples d'entiers algébriques. *La notation tiendra compte de la variété des exemples.*

i convient puisque il annule $X^2 + 1$.

1 (ou tout entier) convient car il annule $X - 1$.

Les 4 racines de P trouvées à la question 1 conviennent aussi.

d) Soit α un nombre complexe algébrique et $P \in \mathbb{Q}[X]$ son polynôme minimal unitaire.
Montrer que α est un entier algébrique si et seulement si $P \in \mathbb{Z}[X]$.

Si P est à coefficient entier, il est clair que α est un entier algébrique.

Réciproquement supposons que α annule $Q \in \mathbb{Z}[X]$ unitaire. Comme P est minimal, P divise Q. Donc $Q = AP$. Soit a et b les ppcm des dénominateurs des coefficients de A et P respectivement. On a alors

$$abQ = aA.bP.$$

En prenant le contenu, on obtient

$$ab = ab\, c(Q) = c(abQ) = c(aA)\, c(bP) \in \mathbb{Z}.$$

Mais alors, en divisant la première égalité par cet entier, on obtient

$$Q = \frac{abQ}{ab} = \frac{aA.bP}{c(aA)\, c(bP)} = \frac{aA}{c(aA)} . \frac{bP}{c(bP)}.$$

Posons $\tilde{P} = \frac{bP}{c(bP)}$. Evidemment $\tilde{P} \in \mathbb{Z}[X]$, $\tilde{P}(\alpha) = 0$. On finit la preuve en remarquant que la dernière égalité montre que le coefficient dominant de $\tilde{P}(\alpha)$ vaut ± 1.

e) En déduire un exemple de nombre algébrique qui ne soit pas un entier algébrique.

Le polynôme $X^2 - \frac{1}{2}$ est irréductible dans $\mathbb{Q}[X]$. C'est donc le polynôme minimal de $\frac{\sqrt{2}}{2}$ qui est un nombre algébrique. La question précédente montre que ce n'est pas un entier algébrique.

f) Soit α et β deux entiers algébriques. Notons P_α et P_β leurs polynômes minimaux unitaires. Soient $\alpha = \alpha_1, \ldots, \alpha_p$ les racines complexes (répétées avec multiplicité) de P_α. Posons $R = \prod_i P_\beta(X - \alpha_i)$. Justifier que $R(\alpha + \beta) = 0$.

Le polynôme R contient comme facteur $P_\beta(X - \alpha)$. Donc $R(\alpha + \beta)$ a pour facteur $P_\beta(\alpha + \beta - \alpha) = P_\beta(\beta) = 0$, donc est nul.

g) Déduire de l'exercice précédent que $\alpha + \beta$ est un entier algébrique.

L'exercice précédent assure que $R(t) = \mathrm{Res}(P(X + t), Q)$. Mais alors son expression comme un déterminant montre qu'il est à coefficients entiers. Or $R(\alpha + \beta) = 0$. Donc $\alpha + \beta$ est un entier algébrique.