université de BORDEAUX	**ANNÉE UNIVERSITAIRE 2014 / 2015** **S1 D'AUTOMNE** **PARCOURS : MA501 Code UE : N1MA5011** **Épreuve : Algèbre 4** **Date : 15/12/2014 Heure : 14h00 Durée : 3h** Documents non autorisés Épreuve de M. Yu. Bilu	**Collège Sciences et technologies**

Correction

Observations

— Tout anneau considéré ci-dessous est commutatif et unitaire.

— Si a et b sont des éléments d'un anneau A, on note $\langle a, b\rangle$ l'idéal engendré par a et b.

1. **Question de cours : anneaux euclidiens, principaux, factoriels**

   (a) Rappeler les définitions d'un anneau euclidien, d'un idéal principal et d'un anneau principal.

   Un anneau A est dit *euclidien* s'il existe une application $\delta : A \smallsetminus \{0\} \to \mathbb{N}$ (« stathme euclidien ») vérifiant la propriété suivante : pour tout $a \in A$ et tout $b \in A \smallsetminus \{0\}$ il existe $q, r \in A$ tels que $a = bq + r$ et soit $r = 0$, soit $\delta(r) < \delta(b)$.

   Un idéal I d'un anneau A est dit *principal* s'il est engendré par un seul élément : il existe $a \in I$ tel que $I = aA = \langle a\rangle$.

   Un anneau A est dit *principal* si tout idéal de A est principal.

   (b) Démontrer le théorème du cours : tout anneau euclidien est principal.

   Soit A un anneau euclidien et I un idéal de A. Montrons que I est principal. Si $I = \{0\}$ alors $I = 0A$, donc I est principal. Si $I \neq \{0\}$ alors l'ensemble non vide

   $$\{\delta(a) : a \in I,\ a \neq 0\} \subset \mathbb{N}$$

   admet un plus petit élément. Autrement dit, il existe $b \in I$ non nul tel que $\delta(b) \leq \delta(a)$ pour tout $a \in I$ non nul. Montrons que $I = bA$. On a $b \in I$ donc $bA \subset I$ car I est un idéal. Par ailleurs, tout $a \in I$ s'écrit comme $a = bq + r$ avec $q, r \in A$ et r vérifiant

   $$\text{soit } r = 0, \text{ soit } \delta(r) < \delta(b). \tag{1}$$

   Mais $r = a - bq \in I$. Donc si $r \neq 0$ alors $\delta(r) \geq \delta(b)$ par choix de b. La seconde option dans (1) est donc impossible. Ceci montre que tout $a \in I$ s'écrit $a = bq$ où $q \in A$. Autrement dit, $I \subset bA$ et finalement $I = bA$.

   (c) Rappeler les définitions d'un élément irréductible, de la factorisation unique et d'un anneau factoriel.

   Soit A un anneau. Un élément $a \in A$ non nul est dit irréductible s'il n'est pas inversible et s'il n'est pas produit de deux éléments non inversibles :

   $$a = bc \Rightarrow b \in A^\times \text{ ou } c \in A^\times.$$

   On dit que $a \in A$ non nul admet une *factorisation irréductible* si a s'écrit comme $a = \eta p_1 \cdots p_k$, où η est inversible et $p_1, \ldots, p_k$ sont irréductibles ($k \geq 0$ avec la convention selon laquelle un produit vide vaut 1).

   On dit que deux factorisations $a = \eta p_1 \cdots p_k = \theta q_1 \cdots q_\ell$ sont *équivalentes* si $k = \ell$ et si on peut re-numéroter $q_1, \ldots, q_k$ pour avoir $p_1 \sim q_1, \ldots, p_k \sim q_k$. (Ici « $\sim$ » signifie équivalence arithmétique : $x \sim y$ si $x \mid y$ et $y \mid x$.)

   On dit que $a \in A$ non nul admet une *factorisation unique* si a admet une factorisation irréductible, qui est unique à équivalence près.

   Un anneau intègre A est dit *factoriel* si tout élément non nul de A admet une factorisation unique.

   (d) Énoncer (sans démonstration) le théorème de factorisation unique pour les anneaux principaux intègres.

   Tout anneau principal intègre est factoriel.

2. **Les nombres gaussiens**

   On considère l'ensemble des *entiers gaussiens* $\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}\} \subset \mathbb{C}$.

(a) Montrer que $\mathbb{Z}[i]$ (muni des lois habituelles) est anneau intègre.
Une vérification immédiate montre que pour $z, w \in \mathbb{Z}[i]$ on $z \pm w, zw \in \mathbb{Z}[i]$. Ceci démontre que $\mathbb{Z}[i]$ est sous-anneau de $\mathbb{C}$. Puisque $\mathbb{C}$ est anneau intègre, $\mathbb{Z}[i]$ l'est aussi.

(b) Soit $\mathbb{Q}(i)$ le corps de décomposition du polynôme t^2+1 sur $\mathbb{Q}$. (On appelle $\mathbb{Q}(i)$ le corps des *nombres gaussiens*.) Est-il vrai que $\mathbb{Q}(i)$ est le corps des fractions de l'anneau $\mathbb{Z}[i]$?
Oui. Notons K le corps de fraction de $\mathbb{Z}[i]$:

$$K = \{z/w : z, w \in \mathbb{Z}[i], w \neq 0\}.$$

Si $Z = z/w \in K$ avec $z = x + yi \in \mathbb{Z}[i]$ et $0 \neq w = u + vi \in \mathbb{Z}[i]$ alors $Z = \frac{z\bar{w}}{w\bar{w}} = \frac{xu+yv}{u^2+v^2} + i\frac{-xv+yu}{u^2+v^2} \in \mathbb{Q}[i]$.

Réciproquement, tout $Z \in \mathbb{Q}[i]$ s'écrit comme $\frac{x+yi}{u}$ avec $x, y, u \in \mathbb{Z}$, $u \neq 0$, donc $Z = z/u$ avec $z = x + yi \in \mathbb{Z}[i]$ et $u \in \mathbb{Z}[i]$.

3. **Norme et divisibilité dans $\mathbb{Z}[i]$**

On définit la *norme* de $z = x + yi \in \mathbb{C}$ par $\mathcal{N}(z) = z\bar{z} = |z|^2 = x^2 + y^2$.

(a) Montrer que la norme est multiplicative : pour $z, w \in \mathbb{C}$ on a $\mathcal{N}(zw) = \mathcal{N}(z)\mathcal{N}(w)$.
On a $\mathcal{N}(zw) = zw\overline{zw} = z\bar{z}w\bar{w} = \mathcal{N}(z)\mathcal{N}(w)$.

(b) Soient $z, w \in \mathbb{Z}[i]$ tels que $z \mid w$ dans $\mathbb{Z}[i]$. Montrer que $\mathcal{N}(z) \mid \mathcal{N}(w)$ dans $\mathbb{Z}$.
Si $z \mid w$ alors $w = zz'$ avec $z' \in \mathbb{Z}[i]$. Par la question précédente $\mathcal{N}(w) = \mathcal{N}(z)\mathcal{N}(z')$ et $\mathcal{N}(w), \mathcal{N}(z), \mathcal{N}(z') \in \mathbb{Z}$.

(c) La réciproque ($\mathcal{N}(z) \mid \mathcal{N}(w) \Longrightarrow z \mid w$) est-elle vraie ?
Non. $\mathcal{N}(2+i) = \mathcal{N}(2-i) = 5$. Donc $\mathcal{N}(2+i) \mid \mathcal{N}(2-i)$, mais $2+i \nmid 2-i$, parce que $\frac{2-i}{2+i} = \frac{3}{5} - i\frac{4}{5} \notin \mathbb{Z}[i]$.

(d) Montrer que $z \in \mathbb{Z}[i]$ est inversible dans $\mathbb{Z}[i]$ si et seulement si $\mathcal{N}(z) = 1$.
On a $z \in \mathbb{Z}[i]^\times$ si et seulement si $z \mid 1$. Par la question 3b $z \mid 1$ implique $\mathcal{N}(z) \mid \mathcal{N}(1) = 1$; puisque $\mathcal{N}(z) \geq 0$, ceci signifie que $\mathcal{N}(z) = 1$.

Réciproquement, si $\mathcal{N}(z) = 1$ alors $z\bar{z} = 1$ ce qui signifie que $z \mid 1$.

(e) Déterminer le groupe $\mathbb{Z}[i]^\times$.
Par la question précédente, $z = x + yi \in \mathbb{Z}[i]^\times$ si et seulement si $x^2 + y^2 = 1$. Puisque $x, y \in \mathbb{Z}$, ceci n'est possible que si $x = \pm 1, y = 0$ ou si $x = 0, y = \pm 1$. Ceci montre que $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

(f) Soit $z \in \mathbb{Z}[i]$ tel que $\mathcal{N}(z)$ est un nombre premier. Montrer que z est irréductible dans $\mathbb{Z}[i]$.
Supposons que $z = w_1 w_2$, où $w_1, w_2 \in \mathbb{Z}[i]$, et montrons que w_1 ou w_2 est inversible. Par la question 3b,

$$\mathcal{N}(z) = \mathcal{N}(w_1)\mathcal{N}(w_2).$$

Puisque $\mathcal{N}(z)$ est premier, ceci implique que soit $\mathcal{N}(w_1) = 1$ soit $\mathcal{N}(w_2) = 1$, et on applique la question 3d pour conclure.

(g) La réciproque est-elle vraie ? Considérer $z = 3$.
Non : $\mathcal{N}(3) = 9$ n'est pas premier, mais 3 est irréductible dans $\mathbb{Z}[i]$. Pour le montrer, supposons le contraire : $3 = zw$ où $z, w \in \mathbb{Z}[i]$ et ne sont pas inversibles. En appliquant les questions 3b et 3d, on trouve $\mathcal{N}(z) = \mathcal{N}(w) = 3$. Écrivons $z = x + yi$; alors $x^2 + y^2 = 3$, d'où $x^2 \leq 3$ et $|x| \leq \sqrt{3}$. Nous obtenons $x = 0$ ou ± 1 ; mais si $x = 0$ alors $y^2 = 3$, ce qui est impossible, et si $x = \pm 1$ alors $y^2 = 2$ ce qui est également impossible.

4. **L'anneau $\mathbb{Z}[i]$ est euclidien**

(a) Montrer que pour tout $z \in \mathbb{C}$ il existe $q \in \mathbb{Z}[i]$ tel que $\mathcal{N}(z - q) \leq 1/2$.
Écrivons $z = x + yi$ et notons u et v les entiers les plus proches à x et à y, respectivement :

$$u, v \in \mathbb{Z}, \quad |u - x| \leq 1/2, \quad |v - y| \leq 1/2.$$

Alors pour $q = u + vi \in \mathbb{Z}[i]$ on a $\mathcal{N}(z - q) = (x-u)^2 + (y-v)^2 \leq (1/2)^2 + (1/2)^2 = 1/2$.

(b) Montrer que $\mathbb{Z}[i]$ est anneau euclidien.
Soient $a, b \in \mathbb{Z}[i]$, $b \neq 0$. Par la question précédente appliquée à $z = a/b$, nous trouvons $q \in \mathbb{Z}[i]$ tel que $\mathcal{N}(a/b - q) \leq 1/2$. Pour $r = a - bq$ on a $\mathcal{N}(r) = \mathcal{N}(a/b - q)\mathcal{N}(b) \leq (1/2)\mathcal{N}(b) < \mathcal{N}(b)$ car $\mathcal{N}(b) > 0$. Ceci montre que $\mathbb{Z}[i]$ est euclidien pour le « stathme » $\mathcal{N}$.

(c) **En déduire que $\mathbb{Z}[i]$ est un anneau principal et factoriel.**
Par les question 1d et 1b l'anneau $\mathbb{Z}[i]$ est principal et factoriel.

(d) Rappeler la définition d'un anneau noethérien.

Un anneau A est dit *noethérien* si tout idéal de A est engendré par un ensemble fini. En particulier, tout anneau principal est noethérien.

(e) L'anneau des polynômes $\mathbb{Z}[i][t]$ est-il principal ? factoriel ? noethérien ?

L'anneau $\mathbb{Z}[i]$ est noethérien (car principal) ; par le théorème de Hilbert l'anneau $\mathbb{Z}[i][t]$ est également noethérien.

Un autre théorème du cours affirme que l'anneau $A[t]$ est factoriel si A l'est. Ceci implique que $\mathbb{Z}[i][t]$ est factoriel.

Par contre, l'anneau $\mathbb{Z}[i][t]$ n'est pas principal. Montrons que l'idéal $I = \langle 3, t\rangle$ n'est pas principal. Supposons le contraire : $I = \langle f\rangle$ pour un certain $f \in I$. On a $f \mid 3$, d'où f est un polynôme constant et $f \sim 1$ ou $f \sim 3$ (rappelons que 3 est irréductible dans $\mathbb{Z}[i]$, voir question 3g). Mais $3 \nmid t$, d'où $f \sim 1$ et donc $1 \in I$. Ceci signifie qu'il existe des polynômes $u(t), v(t) \in \mathbb{Z}[i][t]$ tels que $1 = 3u(t) + tv(t)$. En particulier, $1 = 3u(0)$, et donc $3 \mid 1$, d'où une contradiction.

5. Théorème chinois

Soit A un anneau. Les idéaux I et J de A sont appelés *étrangers* si $I + J = A$.

(a) Montrer que pour les idéaux étrangers I, J on a $IJ = I \cap J$.

Il est clair que $IJ \subset I$ et $IJ \subset J$, d'où $IJ \subset I \cap J$.

Dans l'autre sens, puisque $I + J = A$, il existe $a \in I$ et $b \in J$ vérifiant $a + b = 1$. Si $x \in I \cap J$ alors $xa, xb \in IJ$, d'où $x = x(a + b) \in IJ$. Ceci montre que $I \cap J \subset IJ$.

(b) Démontrer le « théorème chinois » : si I et J sont des idéaux étrangers alors $A/IJ \cong A/I \times A/J$.

Soient φ_I et φ_J les morphismes canoniques $A \to A/I$ et $A \to A/J$, respectivement ; considérons le morphisme $\varphi : A \to A/I \times A/J$ défini par $\varphi(x) = (\varphi_I(x), \varphi_J(x))$. On a $\ker\varphi = \ker\varphi_I \cap \ker\varphi_J = I \cap J = IJ$ par la question précédente.

Montrons que φ est surjectif. (Attention : ceci n'est pas une conséquence immédiate de la surjectivité de φ_I et de φ_J !) Soit $(\bar{u}, \bar{v}) \in A/I \times A/J$; nous cherchons $x \in A$ tel que $\varphi(x) = (\bar{u}, \bar{v})$. Par la surjectivité de φ_I et de φ_J, il existe $u, v \in A$ tels que $\varphi_I(u) = \bar{u}$ et $\varphi_J(v) = \bar{v}$. Posons $x = ub + va$, où, comme dans la question précédente, $a \in I$ et $b \in J$ vérifient $a + b = 1$. Alors $\varphi_I(a) = 0$ et $\varphi_I(b) = \varphi_I(1) - \varphi_I(a) = 1 - 0 = 1$, ce qui implique $\varphi_I(x) = \varphi_I(u) = \bar{u}$. De la même façon on trouve que $\varphi_J(x) = \bar{v}$. Nous avons effectivement $\varphi(x) = (\bar{u}, \bar{v})$, ce qui démontre la surjectivité de φ.

Par la surjectivité de φ on a $A/I \times A/J \cong A/\ker\varphi = A/IJ$.

(c) On suppose que l'anneau A est principal. Soient $a, b \in A$. Montrer que les idéaux principaux $\langle a\rangle$ et $\langle b\rangle$ sont étrangers si et seulement si $\operatorname{pgcd}(a, b) = 1$.

Puisque A est principal, $\langle a, b\rangle = \langle d\rangle$ où $d = \operatorname{pgcd}(a, b)$. Mais $\langle a, b\rangle = \langle a\rangle + \langle b\rangle$, ce qui signifie que les idéaux $\langle a\rangle$ et $\langle b\rangle$ sont étrangers si et seulement si $\operatorname{pgcd}(a, b) = 1$.

6. L'anneau quotient

(a) Soit A un anneau fini intègre. Montrer que A est un corps.

Soit $a \in A$ non nul. Montrons que a est inversible. L'application $A \to A$, $x \mapsto xa$ est un morphisme de groupes abéliens (pour la loi $+$). Son noyau est l'ensemble des $x \in A$ tels que $xa = 0$. Puisque A est intègre, le noyau est réduit à $\{0\}$, et notre morphisme est injectif. Mais une application injective d'un ensemble fini dans lui-même est également surjective ; en particulier, il existe $x \in A$ tel que $xa = 1$.

Ceci montre que tout élément non nul de A est inversible. A est donc un corps.

(b) Soit $z \in \mathbb{Z}[i]$ un élément non nul. Montrer que l'anneau quotient $\mathbb{Z}[i]/\langle z\rangle$ est fini.

Remarquons tout d'abord que pour tout $C > 0$ il n'existe qu'un nombre fini d'éléments de $\mathbb{Z}[i]$ de norme inférieure à C.

Puisque $\mathbb{Z}[i]$ est euclidien pour le « stathme » $\mathcal{N}$, toute classe résiduelle modulo z contient un élément de norme inférieure à $\mathcal{N}(z)$. Ceci montre la finitude du nombre des classes résiduelles.

(c) Soit z un irréductible de $\mathbb{Z}[i]$. Montrer que l'anneau quotient $\mathbb{Z}[i]/\langle z\rangle$ est un corps.

Puisque z est irréductible et l'anneau $\mathbb{Z}[i]$ est principal, l'idéal $\langle z\rangle$ est premier et l'anneau quotient $\mathbb{Z}[i]/\langle z\rangle$ est intègre. Par les deux questions précédentes $\mathbb{Z}[i]/\langle z\rangle$ est un corps.

(d) Parmi les éléments $1 + i, 2 + i, 2, 3, 5 \in \mathbb{Z}[i]$ lesquels sont irréductibles dans $\mathbb{Z}[i]$?

On a vu dans la question 3g que 3 est irréductible. Les éléments $1 + i$ et $2 + i$ sont irréductibles par la question 3f. Par contre, 2 et 5 sont réductibles : $2 = (1 + i)(1 - i)$ et $5 = (2 + i)(2 - i)$.

(e) **Déterminer les anneaux quotients $\mathbb{Z}[i]/<2+i>$, $\mathbb{Z}[i]/<3>$ et $\mathbb{Z}[i]/<5>$.**

Soit $\varphi : \mathbb{Z}[i] \to \mathbb{Z}[i]/<2+i>$ le morphisme canonique et $\varphi_0 = \varphi|_{\mathbb{Z}}$, la restriction de φ à $\mathbb{Z}$. On a $\varphi(i) = \varphi_0(-2)$, d'où pour tout $z = x + yi$ nous avons $\varphi(z) = \varphi_0(x - 2y) \in \varphi_0(\mathbb{Z})$. Ceci implique que le morphisme φ_0 est surjectif, et donc $\mathbb{Z}[i]/<2+i> \cong \mathbb{Z}/\ker\varphi_0$. Puisque $5 = (2+i)(2-i) \in \ker\varphi_0$ et $1 \notin \ker\varphi_0$, le noyau de φ_0 est un idéal de $\mathbb{Z}$ contenant 5, mais pas 1. La seule possibilité est $\ker\varphi_0 = 5\mathbb{Z}$, ce qui montre que $\mathbb{Z}[i]/<2+i> \cong \mathbb{F}_5$. De la même façon $\mathbb{Z}[i]/<2-i> \cong \mathbb{F}_5$.

En tant que groupes additifs $\mathbb{Z}[i] \cong \mathbb{Z} \times \mathbb{Z}$ et $\mathbb{Z}[i]/<3> \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. En particulier, $|\mathbb{Z}[i]/<3>| = 9$. Puisque 3 est irréductible dans $\mathbb{Z}[i]$, l'anneau quotient $\mathbb{Z}[i]/<3>$ est un corps (voir la question 6c). Ceci montre que $\mathbb{Z}[i]/<3> \cong \mathbb{F}_9$.

Pour déterminer $\mathbb{Z}[i]/<5>$ écrivons $5 = (2+i)(2-i)$. Les éléments $2+i$ et $2-i$ sont irréductibles et non équivalents (voir la question 3c), donc $\mathrm{pgcd}(2+i, 2-i) = 1$. En utilisant l'exercice (5), nous trouvons

$$\mathbb{Z}[i]/\langle 5\rangle \cong \mathbb{Z}[i]/<2+i> \times \mathbb{Z}[i]/<2-i> \cong \mathbb{F}_5 \times \mathbb{F}_5.$$

7. Irréductibilité de certains polynômes

(a) Soit K un corps et soit L une extension de K de degré 2. Soit $f(t) \in K[t]$ un polynôme de degré 3. Montrer que $f(t)$ est irréductible dans $K[t]$ si et seulement si $f(t)$ est irréductible dans $L[t]$.

Si $f(t)$ est irréductible dans $L[t]$ alors il est clairement irréductible dans $K[t]$.

Réciproquement, supposons que le polynôme $f(t)$ soit réductible dans $L[t]$. Puisque $\deg f = 3$, il admet une racine dans L. Mais ceci signifie qu'il ne peut pas être irréductible dans $K[t]$: s'il l'est, alors toute racine de $f(t)$ engendre une extension de K de degré 3, et ne peut pas appartenir à une extension de degré 2.

(b) L'énoncé de la question précédente s'étend-il aux polynômes de degré 2 ? de degré 4 ? de degré 5 ?

Non pour le degré 2 : le polynôme $t^2 + 1$ est irréductible dans $\mathbb{R}[t]$ mais réductible dans $\mathbb{C}[t]$.

Non pour le degré 4 : le polynôme $t^4 + 1$ est irréductible dans $\mathbb{Q}[t]$ mais réductible dans $\mathbb{Q}(i)[t]$:

$$t^4 + 1 = (t^2 - i)(t^2 + i).$$

Oui pour le degré 5. Supposons que $f(t) \in K[t]$ de degré 5 soit réductible dans $L[t]$. Alors $f(t) = g(t)h(t)$ avec $g(t), h(t) \in L[t]$ et $\deg g \leq 2$. Toute racine de $g(t)$ est de degré au plus 4 sur K. Mais si $f(t)$ est irréductible dans $K[t]$ alors toute racine de $f(t)$ est de degré 5 sur K.

(c) Le polynôme $t^3 - t + 1$ est-il irréductible dans $\mathbb{F}_3[t]$? dans $\mathbb{F}_9[t]$?

Oui pour les deux questions. Ce polynôme n'a pas de racine dans $\mathbb{F}_3$, donc il est irréductible dans $\mathbb{F}_3[t]$. Par la question 7a il est également irréductible dans $\mathbb{F}_9[t]$.

(d) Le polynôme $2014t^3 + 2013t^2 + 2015t + 2014$ est-il irréductible dans $\mathbb{Z}[t]$? dans $\mathbb{Z}[i][t]$? dans $\mathbb{Q}[t]$? dans $\mathbb{Q}(i)[t]$?

Oui pour toutes les questions. Soit $\varphi : \mathbb{Z}[t] \to \mathbb{F}_3[t]$ la réduction modulo 3. Alors

$$\varphi(2014t^3 + 2013t^2 + 2015t + 2014) = t^3 - t + 1.$$

Ce dernier polynôme est irréductible dans $\mathbb{F}_3[t]$ et le polynôme $2014t^3 + 2013t^2 + 2015t + 2014$ est primitif ; ceci implique qu'il est irréductible dans $\mathbb{Z}[t]$. Par le lemme de Gauss il est également irréductible dans $\mathbb{Q}[t]$. Par la question 7a il est irréductible dans $\mathbb{Q}(i)[t]$. Puisqu'il est primitif, il est irréductible dans $\mathbb{Z}[i][t]$.

(e) Déterminer le corps de décomposition de $f(t) = t^3 - t + 1 \in \mathbb{F}_3[t]$.

Fixons une clôture algébrique $\bar{\mathbb{F}}_3$ de $\mathbb{F}_3$. Puisque $f(t)$ est irréductible dans $\mathbb{F}_3[t]$, chacune de ses racines dans $\bar{\mathbb{F}}_3$ engendre une extension de $\mathbb{F}_3$ de degré 3. Mais $\mathbb{F}_3$ n'admet qu'une seule extension de degré 3 dans $\bar{\mathbb{F}}_3$: c'est le corps $\mathbb{F}_{27}$. Ceci montre que toutes les racines de $f(t)$ appartiennent à $\mathbb{F}_{27}$, et chacune de ces racines engendre $\mathbb{F}_{27}$. Le corps $\mathbb{F}_{27}$ est donc le corps de décomposition de $f(t)$.

(f) Soient α, β, γ les racines de $f(t) = t^3 - t + 1 \in \mathbb{F}_3[t]$ dans son corps de décomposition.

i. Montrer que $\alpha^{13} = \beta^{13} = \gamma^{13} \in \{1, -1\}$.

Le groupe multiplicatif de $\mathbb{F}_{27}$ est cyclique d'ordre 26. Ceci implique que $\alpha^{26} = \beta^{26} = \gamma^{26} = 1$, et donc $\alpha^{13}, \beta^{13}, \gamma^{13} \in \{1, -1\}$.

Il nous reste à montrer que $\alpha^{13} = \beta^{13} = \gamma^{13}$. Posons $\theta = \alpha^{13}$. Alors α est une racine du polynôme $t^{13} - \theta \in \mathbb{F}_3[t]$. Mais l'ensemble $\{g(t) \in \mathbb{F}_3[t] : g(\alpha) = 0\}$ est un idéal dans l'anneau $\mathbb{F}_3[t]$ engendré par $f(t)$. Puisque le polynôme $t^{13} - \theta$ appartient à cet idéal, on a $t^{13} - \theta = f(t)h(t)$ pour un certain $h(t) \in \mathbb{F}_3[t]$. On obtient $\beta^{13} - \theta = f(\beta)h(\beta) = 0$, d'où $\beta^{13} = \theta$. De même, $\gamma^{13} = \theta$.

ii. **Déterminer $\alpha^4 + \beta^4 + \gamma^4$.**

Puisque $\alpha^3 - \alpha + 1 = 0$, on a $\alpha^4 = \alpha^2 - \alpha$, et de même pour β et γ. Nous avons donc

$$\alpha^4 + \beta^4 + \gamma^4 = \alpha^2 + \beta^2 + \gamma^2 - (\alpha + \beta + \gamma) = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma) - (\alpha + \beta + \gamma).$$

En regardant le coefficients du polynôme $f(t)$, nous trouvons

$$\alpha + \beta + \gamma = 0, \qquad \alpha\beta + \alpha\gamma + \beta\gamma = -1.$$

On a finalement $\alpha^4 + \beta^4 + \gamma^4 = 0^2 - 2 \cdot (-1) - 0 = 2 = -1$.