Retour d'oral : Algèbre

Mohamed NASSIRI

Tirage :

☐ 161 - Distances et isométries d'un espace affine euclidien.
☒ 141 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Développements :

☐ Existence et unicité des corps finis.
☒ Critère d'Eisenstein.

Spectateurs :

1

Préparation :

J'ai fait le plan suivant :

I) Irréductibilité
II) Adjonction de racines
    1) Corps de rupture
    2) Corps de décomposition
    3) Corps algébriquement clos
III) Application : Corps finis

J'avais 29 items. J'ai pu, pendant la préparation, regarder la démonstration de chaque item et noter quelques éléments de démonstration. J'ai seulement admis l'unicité des corps de rupture et de décomposition. Il me restait une bonne heure pour faire mes développements.

Défense de plan :

Alors, au départ, quand on est au lycée, on a notre bonne vieille équation polynômiale $ax^2 + bx + c = 0$. Quand on est en seconde, on ne sait pas résoudre ça, donc on passe par une "forme canonique". En première, on a un outil, le discriminant mais on dit qu'on n'a pas de solutions dans $\mathbb{R}$. En fait, on na pas encore $\mathbb{C}$ qui est, sans vouloir spoiler la suite, algébriquement clos. Et puis, en terminale, on a $\mathbb{C}$ et donc on sait résoudre. (*Je vois un membre du jury qui fait une tête bizarre genre "Il va nous parler de ça pendant 6 minutes ..." Il se trouve que j'avais fini ma partie "Nostalgie"*)

Mais maintenant, on a des anneaux, des corps, etc. Donc on va donner une bonne définition de l'irréductibilité. Et l'un des premiers critères qui arrive et qui fera l'objet de mon premier développement, c'est le critère d'Eisentein. Il demande quand même quelques hypothèses mais il est très fort ! Il faut prendre un polynôme

sur un anneau factoriel A et considérer aussi K son corps des fractions. Et si par exemple, notre polynôme a un contenu, que je défini dans le plan, qui vaut 1. Alors il est aussi irréductible sur A. C'est une proposition qu'il y a juste avant le critère d'Eisentein dans mon plan.

Une autre fois de voir, c'est de ne plus vraiment regarder les "élements" mais les "ensembles". On va chercher le plus petit corps, et il faut encore définir ce qu'on entend par "plus petit", où notre polynôme a une racine. Ce sera la notion de corps de rupture. Par exemple, Le polynôme $P(X) = X^3 - 2$ a pour racines $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $\overline{j}\sqrt[3]{2}$, et un corps de rupture est par exemple $\mathbb{Q}(\sqrt[3]{2})$. Dans ce corps, la racine $\sqrt[3]{2}$ est bien dedans. Le problème c'est qu'on n'a pas les racines complexes. Mais bon, la notion n'est pas à jeter à la poubelle. Loin de là ! Elle permet notamment d'avoir deux nouveaux critères d'irréductibilité avec les degrés des extensions. Ah oui ! J'ai mis une astérisque devant chaque critère d'irréductibilité (*Il y en avait une petite dizaine*).

Maintenant, l'idée ça va être de chercher le corps où il y a toutes les racines du polynômes. On appelera le corps de décomposition. Notre polynôme sera scindé. En reprenant mon exemple, on peut voir que le corps $\mathbb{Q}(j, \sqrt[3]{2})$ est un corps de décomposition de P.

Pour finir, on va chercher des corps où cette fois-ci, tous nos polynômes sont scindés. Ça sera en quelque sorte les "meilleurs" corps qu'on puisse avoir. On dira qu'ils sont algébriquement clos. Par exemple, on retrouve le célèbre théorème de D'Alembert-Gauss qui nous dit que $\mathbb{C}$ est algébriquement clos. Et retrouve un nouveau critère d'irréductibilité que l'on connaissait au lycée sur les polynômes de degré 2 sans racines réelles.

Comme application, je vous propose les corps finis. En fait, pour prouver l'existence et l'unicité des corps finis, qui fera l'objet de mon deuxième développement... Ah pardon, je ne l'ai pas précisé par écrit sur mon plan (*Je n'avais pas mis "DEV 2" à côté...*). Donc je disais, pour prouver l'existence et l'unicité des corps finis, ça nous sera donner par les corps de décomposition. L'unicité vient de l'unicité des corps de décomposition, qui est le seul résultat que j'ai admis avec l'unicité des corps de rupture. Ça utilise également, dans la construction, les polynômes irréductibles.
Et je veux ajouter un résultat remarquable ! On a vu tout à l'heure que le corps de rupture et le corps de décomposition sont différents a priori. En effet, les corps $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(j, \sqrt[3]{2})$ ne sont pas égaux, même à isomorphisme près ! Mais dans les corps finis, cette notion coïncide : corps de rupture et corps de décomposition, c'est la même chose. Et mon dernier item, il s'agit de la construction de $\mathbb{F}_4$ et $\mathbb{F}_8$ à partir de polynômes irréductibles. (*Je ne sais pas pourquoi j'ai fini par ça alors que c'était mieux de terminer sur les corps de rupture et corps de décomposition dans les corps finis.*)

Développement :

Il a duré 14 minutes il me semble ... Mais le jury m'a posé une question d'un air étonné : "Vous avez fini ?" Donc je me suis demandé si j'ai pas fait plus court ...
J'ai fait aucune erreur.

Questions du jury :

- Jury 1 : Vous utilisez le contenu et des propriétés de celui-ci. C'est quoi ?
- Moi : Le contenu, c'est le *pgcd* des coefficients.
- Jury 3 : D'accord. Ah un moment, vous utilisez $c(PQ) = c(P)c(Q)$.
- Moi : Oui c'est dans mon plan.
- Jury 3 : Vous pouvez nous le démontrer ?
- Moi : Euh oui ! Il faut d'abord démontrer pour des polynômes primitifs, ça reprend le morphisme dans

---

mon développement. Alors, on prend $P, Q \in A[X]$ avec $c(P) = c(Q) = 1$, et on va supposer, par l'absurde, que $c(PQ) \neq 1$. Donc il existe un nombre premier p tel que $c \mid c(PQ)$. Alors, on va regarder $B = A/pA$ car B a la bonne propriété d'être intègre, et on a le morphisme

$$\widehat{\psi} : A[X] \to B[X]$$
$$\sum a_i X^i \mapsto \sum \psi(a_i) X^i$$

(*Dans le développement, j'avais ce morphsime et le morphisme* $\psi : A \to B,\ a \mapsto \psi(a)$)
Comme c'est un morphisme, on a

$$0 = \widehat{\psi}(PQ) = \widehat{\psi}(P)\widehat{\psi}(Q)$$

et comme on a un anneau intègre, on a soit $\widehat{\psi}(P) = 0$, soit $\widehat{\psi}(Q) = 0$, mais c'est absurde car $c(P) = c(Q) = 1$.

- Jury 3 : Est-ce que si P est irréductible dans $K[X]$ il est irréductible dans $A[X]$?
- Moi : Non ! Il faut un contenu 1 en plus. Je l'ai mis dans mon plan.
- Jury 3 : Oui c'est pour ça que je vous le demande. Mais alors, est-ce que votre critère d'Eisenstein, on ne pourrait pas le simplifier pour avoir un résultat d'irréductibilité sur A ?
- Moi : Le changer dans quel sens ?
- Jury 3 : Votre polynôme, on peut pas faire quelque chose dessus ?
- Moi : Ah ! Bah on peut prendre un polynôme unitaire X^n et le contenu va valoir 1, en faisant ça

$$X^n + \sum_{i=0}^{n-1} a_i X^i$$

- Jury 3 : Non mais vous ne changez pas le polynôme, il est donné !
- Moi : (*Ouais bah c'est très clair comme question ...*) Euh ...
- Jury 3 : Avec le contenu ?
- Moi : Ah ! On peut mettre le contenu en facteur !
- Jury 3 : Et ?
- Moi : Et et et ... Alors on a $P(X) = a_n X^n + ... + a_1 X + a_0$
- Jury 3 : Voilà ! Mettez le contenu en facteur, vous aurez des nouveaux coefficients a'_1, etc.
- Moi : Oui oui. Alors $P(X) = c(P)(a'_n X^n + ... + a'_1 X + a'_0)$. A priori, rien ne garantit que p divise encore les a'_i
- Jury 3 : C'est pas acceptable comme réponse ça !
- Moi : (*Oula ... A ce moment, je suis un peu destabilisé par le changement de ton ...*) C'est peut-être évident mais je ne vois pas ...
- Jury 3 : Bah est-ce que je mettre p en facteur de ce polynôme ?
- Moi : Ah ! C'était ça ! Bah non car $p \nmid a_n$!
- Jury 3 : Oui voilà ! Donc non, le critère d'Eisenstein, on ne peut pas faire mieux.

- Jury 3 : Vous avez parlé de corps de rupture. Est-ce que vous pourriez démontrer l'existence d'un corps de rupture ?
- Moi : Euh oui ... Alors attendez, je sais que je dois considérer $K[X]/(f)$ ...
- Jury 1 : Prenez un polynôme P.
- Moi : D'accord. Soit $P \in K[X]$ ...
- Jury 2 : Vous le prenez quelconque le corps ?
- Moi : Euh au moins commutatif, intègre et unitaire ... (J'avais en tête un anneau ...)
- Jury 3 : Bah c'est un corps ...
- Moi : Euh oui ... Ah oui ! Désolé, j'avais un anneau en tête ... Désolé. Bon donc, je prend un facteur irréductible f de P, et donc $P = fQ$ (*Comme Jury 1 m'a dit de prendre un polynôme P, je l'ai pris quelconque, oubliant qu'un corps de rupture c'est défini à partir d'un polynôme irréductible ...*). Donc je considère

$K[X]/(f)$ ...
- Jury 1 : C'est quoi comme objet $K[X]/(f)$?
- Moi : Euh ... C'est un anneau, ça c'est sûr ... Je ne pense pas que ce soit un corps ... (*Gros débile que je suis ...*) Est-ce que je peux regarder mes notes ? Il me manque un argument et je ne vois plus ...
- Jury 3 : (*Le jury au complet n'avait pas l'air trop pour*) Euh ... Allez-y ...
- Moi : (Du coup, je vois qu'il faut considérer un morphisme) Ah voilà ! Il faut considérer le morphisme :

$$\begin{aligned} \varphi : K[X] &\to K[X]/(f) \\ X &\mapsto \sum \varphi(X) := \alpha \end{aligned}$$

Où l'on a noté α l'image (ou la classe) de X. Du coup, on a

$$f(\alpha) = f(\overline{X}) = \overline{f(X))} = 0$$

Donc α c'est une racine de f, donc de P, et $K[X]/(f)$ est un corps de rupture de f.
- Jury 3 : Vous avez parlé de l'unicité des corps de rupture. Vous pensez que c'est unique là avec la façon dont vous l'avez construit ?
- Moi : Bah oui c'est unique à isomrphisme près ...
- Jury 3 : Euh vous êtes sûrs ...
- Moi : Je ne vois pas le problème ...
- Jury 3 : Votre facteur irréductible, vous l'avez pris quelconque !
- Moi : Ah oui ...
- Jury 3 : Les corps de rupture c'est défini à partir des polynômes irréductibles
- Moi : Ah mais je suis bête ...

- Jury 1 : Vous avez parlé d'irréductible et de premier, c'est quoi le lien entre les deux ?
- Moi : Je sais que premier implique toujours irréductible, il faut juste de l'intégrité et dans l'autre sens de la factorialité. Mais attendez, le lien ? Entre les éléments ou les idéaux ?
- Jury 1 : Donnez nous la définition d'idéal premier et d'éléments irréductibles.
- Moi : I est un idéal premier si : $I \neq A$, mais ça j'ai un doute, et si $\forall a, b \in A$ tel que $ab \in I$, alors soit $a \in I$, soit $b \in I$.
Et un élément $x \in A$ est irréductible si $x = pq$, alors $p \in A^*$ ou $q \in A^*$, où A^* ce sont les inversibles.
- Jury 1 : Vous ne supposez rien de plus sur x ?
- Moi : Non nul ?
- Jury 1 : Il peut être inversible ?
- Moi : Alors est-ce que c'est si grave ... Ah bah, non il ne peut pas être inversible ... Si on prend l'exemple des entiers, ça revient au problème de 1 n'est pas un nombre premier. Donc il faut supposer que x n'est pas inversible.
- Jury 1 : D'accord ! Du coup, c'est quoi le lien entre irréductible et premier ?
- Moi : (*Je me rends compte que la question n'est pas très clair ...*) Le lien entre les éléments ou les idéaux ?
- Jury 3 : Les éléments par exemple.
- Moi : On a $I = (p)$. Et vous le lien entre p quand il est irréductible et/ou premier ?
- Jury 3 : Oui voilà ! Vous avez défini p comme le générateur de I apparemment, donc allez-y.
- Moi : (*Elle commence à durer cette question alors que j'ai l'impression d'y avoir répondu dès le début ...*) Donc premier implique toujours irréductible, il faut de l'intégrité et dans l'autre sens de la factorialité. Car dans la démonstration, on va décomposer nos éléments en produit d'irréductibles et montre que p fait parti de ces irréductibles.
- Jury 1 : La factorisation en irréductibles, elle est unique ?
- Moi : Euh non ... (*Abruti un jour, abruti toujours ... Je le sais en plus qu'elle est unique ! Grrrr !!*)
- Jury 3 : Après ça dépend ce que vous appelez unique ?
- Moi : (*Ouf ! Sauvé ! Je peux me rattraper !*) Elle est unique à inversible près ! On peut écrire nos éléments sous la forme $u \prod q_i^{\alpha_i}$ où u est inversible et du coup, on pourrait avoir $v \prod q_i^{\alpha_i}$ qui est le même nombre mais

avec un autre inversible v.
- Jury 1 : Seulement à inversible près ?
- Moi : (*Ah ! Je vois où tu veux m'emmener !*) Non, il faut aussi ajouter des valuations nulles pour pouvoir comparer nos éléments. Par exemple, si on veut comparer deux entiers, on peut écrire $2^0 3^2$ et $2^2 3^0$.
- Jury 2 : D'accord.

- Jury 1 : A quel moment sert la factorialité dans votre développement ?
- Moi : (*Je ne l'ai pas vu venir celle-là ...*) Dès le début, quand on quotiente $B = A/pA$ pour pouvoir avoir de l'intégrité.
- Jury 1 : Mouais ... Pas que ...
- Moi : Euh ... (*Je réfléchis un petit moment ... Oui, ça m'arrive ...*) Ah ! Le contenu ! Pour pouvoir parler de *pgcd*.
- Jury 1 : Et alors, pourquoi la factorialité est utile ?
- Moi : (*Je bloque parce que j'ai l'impression d'avoir dit la réponse mais qu'il veut autre chose ... Et je ne vois pas...*)
- Jury 1 : Oui voilà ! Il existe partout le *pgcd* ?
- Moi : Ah ! Je viens de comprendre ce que vous vouliez : l'existence du *pgcd* ! Alors, non, il n'existe pas partout. Dans les anneaux euclidiens, oui. On n'a même un algorithme pour le construire. Dans les anneaux principaux, c'est par presque par définition, et dans les anneaux factoriels, c'est donné par la décomposition en irréductibles justement.
- Jury 1 : D'accord.
(*Un peu déçu car je sais que l'on a même une formule du pgcd avec le min sur les valuations ... Je le savais mais je ne l'ai pas dit ...*)

- Jury 2 : Moi j'aimerais qu'on parle de corps finis.
- Moi : D'accord ! *Bah allez... Histoire de finir en beauté...*
- Jury 2 : Qu'est-ce que vous pouvez dire du cardinal d'un corps fini ?
- Moi : C'est la puissance d'un nombre premier.
- Jury 2 : Pourquoi ?
- Moi : Ça vient de la caractéristique.
- Jury 2 : Expliquez nous.
- Moi : Alors on prend un anneau A (*Vous sentez arriver la connerie...*)

$$\begin{aligned} c : \mathbb{Z} &\to A \\ n &\mapsto n.1_A \end{aligned}$$

Et on va regarder Ker$c$. Soit il n'existe pas de n tel que $n.1_A = 0$ et on dira que la caractéristique est infini. Soit il existe un entier p tel que ça vaut 0, et comme le noyau c'est un idéal, on a ... (*Et là je bug un peu... Ne me demandez pas pourquoi ...*)
- Jury 3 : Notez le $d\mathbb{Z}$ si vous voulez.
- Moi : Oui voilà ! On a Ker$c = d\mathbb{Z}$. Et d est un nombre premier.
- Jury 3 : Euh attendez. Pourquoi ça serait premier ?
- Moi : Ah oui pardon... Il faut la définir sur un corps ici... On a

$$\begin{aligned} c : \mathbb{Z} &\to K \\ n &\mapsto n.1_A \end{aligned}$$

Et donc là, $\mathbb{Z}/d\mathbb{Z}$ est isomorphe à Imc, qui est un sous-corps de K, donc d est premier.
- Jury 3 : Vous utilisez quoi pour dire que $\mathbb{Z}/d\mathbb{Z}$ est isomorphe à Imc ?
- Moi : (*Étonné de la question quand même...*) Le premier théorème d'isomorphisme.
- Jury 3 : Ok d'accord.
- Jury 2 : Oui mais vous avez dit une puissance d'un nombre premier.

- Moi : Ah oui, c'est vrai ! Ca vient des sous-corps premiers. Par exemple, $\mathbb{F}_p$ est un sous-corps premier d'un corps fini F. On peut donc voir F comme un $\mathbb{F}_p$-espace vectoriel.
- Jury 3 : Et ?
- Moi : Et quoi ?
- Jury 3 : Et $\mathbb{F}_p$-espace vectoriel ?
- Moi : Ah ! De dimension fini !
- Jury 3 : (*En souriant*) Oui voilà !
- Jury 2 : Vous avez parlé de clôture algébrique. Est-ce qu'un corps fini peut-être algébriquement clos ?
- Moi : Non. Un corps algébriquement clos est forcément infini ?
- Jury 2 : Vous êtes sûr ?
- Moi : (*Un peu dérouté et pourtant je sais que c'est vrai*) Je peux vous le démontrer si vous voulez ?
- Jury 2 : Oui allez-y !
- Moi : Je prends un corps fini K et je voudrais prendre une extension L ...
- Jury 3 : Attendez ! Il ne faut qu'avec K.
- Moi : Ah bah oui ... En fait, j'aimerais écrire $K = k(\alpha_1, ..., \alpha_n)$ et dire que le polynôme $(X - \alpha_1)...(X - \alpha_n) + 1$ n'a pas de racines dans K.
- Jury 3 : C'est pas toujours possible d'écrire K ainsi ? C'est qui k ?
- Moi : Ah bah oui ! k c'est le sous-corps premier !
- Jury 3 : Et les α_i ?
- Moi : Les éléments du corps K.
- Jury 3 : Oui voilà.
- Jury 2 : Est-ce que vous connaissez une clotûre algébrique pour les $\mathbb{F}_{p^n}$?
- Jury 3 : C'est quoi les relations d'inclusions pour les corps finis ?
- Moi : (*Oula ... Nouvelle épreuve : répondre à deux questions en même temos ...*) Alors

$$\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \qquad n \mid m$$

Dans le sens direct, on peut voir $\mathbb{F}_{p^m}$ comme un $\mathbb{F}_{p^n}$-espace vectoriel, et donc au aura $p^m = |p^n|^d$, et donc $m = pd$.
- Jury 3 : Et le sens réciproque ?
- Moi : J'ai jamais dit que c'était équivalent (*Oui je fais des petites vannes comme ça pour détendre l'atmosphère*). Mais je sais que c'est équivalent ... Alors sinon, pour répondre à l'autre question, la clôture algébrique c'est un truc succulent comme une union de $\mathbb{F}_{p^{n!}}$. Mais je suis désolé, pour le sens réciproque, je n'ai pas l'argument là ...
- Jury 2 : On va s'arrêter là.

Ressenti :

Jury pas trop agréable, avec des visages très fermés même si j'ai réussi à décrocher un sourire à un des trois sur l'histoire d'un $\mathbb{F}_p$ espace-vectoriel de dimension fini. Pas beaucoup d'aide pour répondre, j'ai du tout chercher tout seul. Des fois, ça allait vite, des fois un peu moins.
Sur le coup, ça ne m'a pas marqué, mais avec le recul, je me suis rendu compte que je n'ai pas eu beaucoup de questions sur les polynômes irréductibles, mais surtout sur de la factorialité, le *pgcd*, les éléments/ideaux irréductibles et premiers, corps finis, etc.

Note :	**14/20**

Commentaire du jury :
Algèbre et géométrie : polynômes irréductibles, 56/80. Développement solide. Bonne réactivité. Bonne culture mathématique, qui demande à être confortée par une prise de recul plus importante.