TD du cours[1] d'Algèbre 2, 2004

Gaëtan CHENEVIER

[1]Cours de Maitrise de l'ENS, enseigné par Marc ROSSO.

Table des matières

CHAPITRE 1

Algèbre linéaire, algèbres sur un corps

23 Février 2004

T.D. n^o 1 du cours d'Algèbre II

Tous les anneaux dans ce TD sont supposés unitaires.

Exercice 1 Soient A un anneau commutatif, M et N deux A-modules.

(a) Montrer que les tenseurs purs de $M \otimes_A N$ engendrent ce dernier comme A-module.

(b) Montrer que si $x \in M$, $y \in N$, $x \otimes 0 = 0 = 0 \otimes y$. Réciproquement, montrer que si A est un corps et $x \otimes y = 0$, alors x ou y est nul.

Fixons des familles A-génératrices respectives (e_i) et (f_j) de M et N.

(c) Montrer que la famille des $e_i \otimes f_j$ est une famille A-génératrice du A-module $M \otimes_A N$.

(b) Montrer que si (e_i) et (f_j) sont de plus des A-bases de M et N, alors la famille du (c) est une A-base de $M \otimes_A N$.

Remarques: (i) En général, il existe des éléments de $M \otimes_A N$ qui ne sont pas des tenseurs purs (cf. exercice 2). De plus, si A n'est pas un corps, il est possible que $x \otimes y = 0$ et que ni x, ni y, ne soit nul (cf. exercice 3. (b)).

(ii) Du (d) se déduit en particulier que si M et N sont A-libres de rangs finis respectifs m et n, alors $M \otimes_A N$ est A-libre de rang mn.

Exercice 2 Soient k un corps, V, W des k-espaces vectoriels de dimension finie, $V^* := \mathrm{Hom}_k(V, k)$.

(a) Montrer qu'il existe une unique application k-linéaire $\iota : V^* \otimes_k W \to \mathrm{Hom}_k(V, W)$, telle que $\iota(\varphi \otimes v) = (x \mapsto v\varphi(x))$, puis que ι est un isomorphisme.

(b) Montrer que les tenseurs purs de $V^* \otimes_k W$ coïncident via ι avec les applications linéaires $V \to W$ de rang ≤ 1. Plus généralement, montrer que le nombre minimal de tenseurs purs nécessaires à l'écriture d'un élément $x \in V^* \otimes_k W$ comme somme de tenseur purs est exactement le rang de l'application linéaire $\iota(x)$.

Posons $n := \inf(\dim_k(V), \dim_k(W))$ et, pour $0 \leq r \leq n$, $X_r \subset V \otimes_k V$ le sous-ensemble des éléments pouvant s'écrire comme somme d'au plus r tenseurs purs. Ainsi, $X_n = V \otimes_k W$, et si $r < r'$ alors $X_r \subsetneq X_{r'}$ (justifier).

(c) (*Exemple*) Supposons $\dim_k(V) = \dim_k(W) = 2$, montrer que l'ensemble X_1 des tenseurs purs de $V \otimes_k W$ est une quadrique non dégénérée, de la forme $xy + zt = 0$ dans une base bien choisie.

(d) Montrer que X_r est un fermé algébrique[1] de $V \otimes_k W$, qui est un cône centré en 0. Si $k = \mathbb{R}$ ou $\mathbb{C}$ et $V \otimes_k W$ est muni de sa topologie d'espace vectoriel normé, montrer que X_{n-1} est un fermé d'intérieur vide de $V \otimes_k W$.

---

[1] Soient W un k-espace vectoriel de dimension finie et (x_i) une k-base de W^*. Un *fermé algébrique* de W est un sous-ensemble de V qui est exactement l'ensemble des zéros communs d'un ensemble de polynômes en les x_i. On vérifie facilement que cette dernière propriété ne dépend pas de la base (x_i) choisie, et que les fermés algébriques sont exactement les fermés d'une topologie sur W : la *topologie de Zariski*. Si $k = \mathbb{R}$ ou $\mathbb{C}$, cette topologie est moins fine que la topologie d'espace vectoriel normé.

Exercice 3 Soient A un anneau commutatif, I et J des idéaux de A.

(a) Montrer qu'il existe une unique application A-linéaire $(A/I) \otimes_A (A/J) \to A/(I+J)$ envoyant $(a \bmod I) \otimes (a' \bmod J)$ sur $(aa' \bmod (I+J))$, et que c'est un isomorphisme.

(b) En déduire la structure du groupe abélien $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z})$ pour $m, n \in \mathbb{Z}$.

(c) On suppose que A est un *anneau principal*, et que M et N sont des A-modules de type fini. Décrire la structure de $M \otimes_A N$ en fonction de celles de M et N.

Exercice 4 (Quelques produits tensoriels sur $\mathbb{Z}$)

(a) Montrer que l'application canonique $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}$ (justifier) est un isomorphisme de groupes abéliens.

(b) Calculer les produits tensoriels sur $\mathbb{Z}$ de deux groupes abéliens quelconques parmi les suivants : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$.

(c) Montrer que le morphisme naturel (préciser) de groupes abéliens

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^{\mathbb{N}} \to \mathbb{Q}^{\mathbb{N}}$$

est une injection d'image le sous-groupe des suites de rationnels à dénominateurs bornés, qui est un sous-groupe strict de $\mathbb{Q}^{\mathbb{N}}$.

(d) Vérifier cependant que les groupes abéliens $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^{\mathbb{N}}$ et $\mathbb{Q}^{\mathbb{N}}$ sont isomorphes entre eux, ainsi qu'à $\mathbb{Q}^{(\mathbb{R})}$.

Exercice 5* Soient k un corps, $A := k[X,Y]$, m l'idéal (X,Y) de A. On va montrer qu'en tant que A-modules,

$$m \otimes_A m \simeq m^2 \oplus (A/m)$$

Ici, m^2 désigne l'idéal $m.m$ de A, *i.e.* (X^2, XY, Y^2).

(a) Montrer que le A-module m/m^2 admet une structure naturelle de A/m-espace vectoriel de dimension 2. En déduire l'existence d'une forme A-bilinéaire alternée non nulle : $m \times m \to A/m$.

(b) Montrer que le sous-A-module de $m \otimes_A m$ engendré par l'élément $v := X \otimes Y - Y \otimes X$ est isomorphe à A/m, et qu'il admet un supplémentaire.

(c) Montrer que la suite de A-modules

$$0 \longrightarrow A \xrightarrow{f} A^2 \xrightarrow{g} m \longrightarrow 0,$$

définie par $f(a) = (-Ya, Xa)$ et $g((a,b)) = Xa + Yb$, est une suite exacte courte. En déduire le noyau de la surjection A-linéaire induite par $g : m \oplus m \to m^2$.

(d) Conclure.

Exercice 6 Soient k un corps, W un k-espace vectoriel, et $0 \to V' \to V \to V'' \to 0$ une suite exacte de k-espaces vectoriels. Montrer que la suite induite (préciser) :

$$0 \to V' \otimes_k W \to V \otimes_k W \to V'' \otimes_k W \to 0,$$

est aussi une suite exacte.

Les exercices suivant concernent les algèbres de quaternions sur un corps. Un *corps* sera toujours supposé commutatif, une *algèbre à division* est une algèbre associative unitaire telle que tout élément non nul admet un inverse des deux côtés.

Exercice 7* (Algèbres de quaternions sur un corps) Soit K un corps de caractéristique $\neq 2$, on fixe a et b dans K^*. On considère, sur le K-espace vectoriel

$$V := Ke_1 \oplus Ke_2 \oplus Ke_3 \oplus Ke_4,$$

l'application K-bilinéaire $V \times V \to V$, $(x, y) \mapsto x.y$ définie sur la base des e_i par :

$$e_1.e_i = e_i.e_1 = e_i,\ e_2.e_2 = a,\ e_3.e_3 = b,\ e_2.e_3 = -e_3.e_2 = e_4$$

$$e_4.e_4 = -ab,\ e_2.e_4 = -e_4.e_2 = ae_3,\ e_3.e_4 = -e_4.e_3 = -be_2$$

(a) Montrer que $(x, y) \mapsto x.y$ munit V d'une structure de K-algèbre associative, non commutative, de neutre e_1 et de centre Ke_1.

On note $(\frac{a,b}{K})$ cette K-algèbre. Ainsi, $(\frac{-1,-1}{\mathbb{R}})$ coïncide avec l'algèbre des quaternions usuels. Par habitude, on note 1, i, j et k les éléments respectifs e_1, e_2, e_3 et e_4. On considère l'ensemble $C_{a,b}$ des solutions dans $\mathbb{P}^2(K)$ de la conique d'équation $aX^2 + bY^2 = Z^2$.

(b) Vérifier que le K-endomorphisme de $(\frac{a,b}{K})$ défini par

$$\tau(u + vi + wj + tk) := u - vi - wj - tk$$

est une involution de satisfaisant $\tau(x.y) = \tau(y).\tau(x)$ pour tout $x, y \in V$. De plus, si $x \in V$, montrer que $\chi_x := T^2 - (x + \tau(x))T + x\tau(x)$ est dans $K[T]$ et annule x.

(c) Montrer que $(\frac{1,1}{K})$ est isomorphe comme K-algèbre à $M_2(K)$. Identifier les χ_x. Indication: On pourra chercher des matrices I et J dans $M_2(K)$ telles que $I^2 = J^2 = 1$ et $IJ = -JI$.

(d) Montrer que si $C_{a,b} \neq \emptyset$, $(\frac{a,b}{K})$ est K-isomorphe à $M_2(K)$. Qu'en déduire si K est algébriquement clos ? si K est un corps fini ? si $K = \mathbb{R}$?

(e) Soit f une forme quadratique non dégénérée sur un K-espace vectoriel de dimension 4 dont le discriminant est un carré dans K^*. Montrer que la dimension maximale d'un sous-espace totalement isotrope pour f est 0 ou 2.

(f) Montrer que si $C_{a,b} = \emptyset$, alors $(\frac{a,b}{K})$ est une algèbre à division.

(g*) Montrer que si p est un nombre premier $\equiv 3 \bmod 4$, $(\frac{-1,p}{\mathbb{Q}})$ est une algèbre à division, et qu'elle contient un sous-corps isomorphe à $\mathbb{Q}(\sqrt{p})$. En déduire qu'il existe une infinité d'algèbres à division de dimension 4 sur $\mathbb{Q}$ deux à deux non isomorphes.

Exercice 8 Soit D une $\mathbb{R}$-algèbre à division de dimension finie sur $\mathbb{R}$. On va montrer qu'en tant que $\mathbb{R}$-algèbre, D est isomorphe à $\mathbb{R}$, $\mathbb{C}$ ou à l'algèbre des quaternions réels $\mathbb{H}$.

(a) Soit $x \in D \backslash \mathbb{R}$, montrer que $\mathbb{R}[x]$ est isomorphe à $\mathbb{C}$ comme $\mathbb{R}$-algèbre. Quel est le centralisateur de x dans D ?

On suppose $[D : \mathbb{R}] > 2$. On choisit $i \in D$ tel que $i^2 = -1$ (justifier).

(b) Si $j \in D\backslash\mathbb{R}[i]$, montrer que $ij - ji$ est non nul et anticommute avec i (*i.e.* $zi = -iz$). En déduire l'existence d'un $j \in D\backslash\mathbb{R}[i]$ tel que $ji = -ij$ et $j^2 = -1$.

(c) Soit $x \in D\backslash\mathbb{R}[i]$ tel que $xi = -ix$, montrer que $x \in j\mathbb{R}[i]$.

(d) Conclure[2].

[2]En procédant comme dans cet exercice, et avec les notations de l'exercice 7, vous pouvez montrer que si K est un corps de caractéristique $\neq 2$, toute K-algèbre à division de centre K et de dimension 4 sur K est K-isomorphe à $(\frac{a,b}{K})$ pour certains a et b dans K^*.

1 Mars 2004

T.D. n^o 2 du cours d'Algèbre II

Tous les anneaux dans ce TD sont supposés unitaires. On pourra commencer par les questions : ex. 1 a) et b), ex. 2 a)-d) et g), et ex. 3.

Exercice 1

(a) Soit $k \subset K$ une extension de corps, $P \in k[X]$, montrer que l'application naturelle $k[X]/(P) \otimes_k K \longrightarrow K[X]/(P)$ est un isomorphisme de K-algèbres.

(b) En déduire la structure des $\mathbb{R}$-algèbres suivantes :

$$\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{R},\ \mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{R},\ \mathbb{Q}(\sqrt[3]{2}) \otimes_{\mathbb{Q}} \mathbb{R}.$$

Décrire de même la $\mathbb{C}$-algèbre $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$, et les $\mathbb{Q}$-algèbres $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3})$.

(c) À quelle condition sur une extension de corps $k \subset K$, l'anneau $K \otimes_k K$ est-il un corps ?

Exercice 2 (Algèbres diagonalisables) Soient k un corps et A une k-algèbre de dimension finie sur k.

(a) Montrer que A est k-isomorphe[3] à une sous-k-algèbre de $\mathrm{M}_n(k)$, et que l'on peut choisir $n = \dim_k(A)$.
Indication: Considérer la représentation régulière gauche : $A \to \mathrm{End}_k(A),\ a \mapsto (x \mapsto ax)$.

(a') Donner par exemple explicitement un morphisme injectif de $\mathbb{Q}$-algèbres $\mathbb{Q}(\sqrt{2}) \to \mathrm{M}_2(\mathbb{Q})$, ou encore $\mathbb{Q}[X]/(X^n) \to \mathrm{M}_n(\mathbb{Q})$.

On supposera donc dans ce qui suit que $A \subset \mathrm{M}_n(k)$ est une sous-k-algèbre, et ce sans perte de généralité. On fixe $k \subset K$ une extension de corps et on verra $\mathrm{M}_n(k)$ comme étant inclus dans $\mathrm{M}_n(K)$.

(b) Montrer que l'application naturelle $A \otimes_k K \to \mathrm{M}_n(K)$ induit un K-isomorphisme de $A \otimes_k K$ sur la sous-K-algèbre de $\mathrm{M}_n(K)$ engendrée par $K.1$ et A.

Ainsi, on dispose d'une description concrète de l'extension des scalaires pour les sous-k-algèbres de $\mathrm{M}_n(k)$.

(c) Soit $D_n(k) \subset \mathrm{M}_n(k)$ la sous-k-algèbre des matrices diagonales. Vérifier que $D_n(k)$ est k-isomorphe à la k-algèbre produit k^n.

Une k-algèbre k-isomorphe à k^n est dite *diagonale* pour cette raison. Fixons $K \supset k$ une clôture algébrique de k. Une k-algèbre A est dite diagonalisable si $A \otimes_k K$ est une K-algèbre diagonale, i.e. $A \otimes_k K \simeq K^{\dim_k(A)}$.

(d) On suppose de plus que A est un corps commutatif de caractéristique nulle, montrer que A est diagonalisable.

[3]Entendons par là "isomorphe en tant que k-algèbre".

Indication: Si $P \in k[X]$ est irréductible, alors P a des racines *distinctes* dans K. En effet, P' est non nul (cela utilise que car(k)=0) et premier à P dans $k[X]$. On n'utilisera pas le théorème de l'élément primitif dans cette question, qui concluerait en vertue de l'exercice 1.(a).

(e*) (Généralisation du (d)) On suppose que k est de caractéristique nulle. Montrer que A est diagonalisable si, et seulement si, elle est commutative et sans élément nilpotent non nul.

Indication: Pour la condition suffisante, on montrera d'abord que le polynôme minimal de tout élément de A est sans facteur carré.

(f) Soient p premier, $k := \mathbb{F}_p(T)$ et $A := k[X]/(X^p - T)$. Montrer que A est un corps, puis que $A \otimes_k K \simeq K[u]/(u^p)$. En déduire que A n'est pas diagonalisable[4].

On termine par deux applications.

(g) Donner une condition nécessaire et suffisante sur $x \in k^n$ pour que $k[x] = k^n$. Déduire de cela et du (d) que si k est un corps de caractéristique nulle et L/k une extension finie, alors il existe $x \in L$ tel que $L = k[x]$ (théorème de l'élément primitif).

(h) Soit $L \supset k$ une extension finie de corps de caractéristique nulle, montrer que $\mathrm{Hom}_{k-\mathrm{alg}}(L, K)$ a exactement $[L : K]$ éléments.

Exercice 3 (Retour sur les quaternions de Hamilton) Soit $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ la $\mathbb{R}$-algèbre des quaternions usuels de Hamilton.

(a) Montrer que $\mathbb{H}$ est $\mathbb{R}$-isomorphe à une sous-$\mathbb{R}$-algèbre de $\mathrm{M}_4(\mathbb{R})$, mais pas de $\mathrm{M}_n(\mathbb{R})$ si n n'est pas divisible par 4.

(b) Montrer que $\mathrm{M}_2(\mathbb{H})$ n'est pas $\mathbb{R}$-isomorphe à $\mathrm{M}_4(\mathbb{R})$, et plus généralement que $\mathrm{M}_n(\mathbb{H})$ n'est jamais $\mathbb{R}$-isomorphe à $\mathrm{M}_m(\mathbb{R})$.

(c) Montrer que $\mathbb{H}$ est $\mathbb{R}$-isomorphe à une sous-$\mathbb{R}$-algèbre de $\mathrm{M}_2(\mathbb{C})$, puis que $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$ est $\mathbb{C}$-isomorphe à $\mathrm{M}_2(\mathbb{C})$.

Si A est une k-algèbre, l'anneau A^{opp} opposé[5] de A est aussi une k-algèbre de manière naturelle. En particulier, A et A^{opp} sont k-isomorphes si, et seulement si, il existe $u \in \mathrm{Aut}_k(A)$ tel que $u(xy) = u(y)u(x)$ pour tout $x, y \in A$.

(d) Montrer que $\mathrm{M}_n(k) \simeq \mathrm{M}_n(k)^{\mathrm{opp}}$ et que $\mathbb{H} \simeq \mathbb{H}^{\mathrm{opp}}$.

(e) Montrer qu'il existe un unique morphisme de k-algèbres $A \otimes_k A^{\mathrm{opp}} \to \mathrm{End}_k(A)$ tel que $a \otimes b \mapsto (x \mapsto axb)$. Vérifier que c'est un isomorphisme si $A = \mathrm{M}_n(k)$.

(f) Montrer que $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \simeq \mathrm{M}_4(\mathbb{R})$.

Dans les exercices qui suivent, on s'intéresse aux algèbres centrales simples sur un corps. Si k est un corps et A une k-algèbre, on dit que A est *centrale* si son centre est réduit à $k.1$, *simple* si A n'a pas d'idéaux bilatères autres que $\{0\}$ et A, *à division* ou *un corps gauche*

[4]En fait, (d), (e) et (h) sont valables plus généralement si le corps k est parfait, i.e. satisfaisant la première phrase de l'indication du (c). Les même démonstration doivent marcher.

[5]Si $(A, +, \times)$ est un anneau, l'anneau opposé est $(A, +, \times^{\mathrm{opp}})$, où $a \times^{\mathrm{opp}} a' := a' \times a$.

si tout élément de A est inversible des deux côtés. Ayant en vue de classifier les k-algèbres, il est naturel de commencer par celles qui sont simples.

Exercice 4 (Formes tordues de $\mathrm{M}_n(k)$ et un théorème de Wedderburn) Dans cet exercice, on va donner une description des formes[6] de $\mathrm{M}_n(k)$, et montrer que si A est une algèbre à division de dimension finie sur son centre k, alors $\dim_k A$ est un carré.

(a) Vérifier que $\mathrm{M}_n(k)$ est une k-algèbre centrale simple, et que si A est à division, A est simple.

Dans les quatre questions suivantes, $k \subset K$ est une extension de corps fixée.

(b) Soit A une k-algèbre centrale. Montrer que la K-algèbre $A \otimes_k K$ est centrale.

(c*) Soit A une k-algèbre centrale simple. Montrer que la K-algèbre $A \otimes_k K$ est simple.

Indication: On pourra considérer un idéal bilatère I non nul de $A \otimes_k K$ et un tenseur non nul de rang minimal de I.

(d) Soit A une k-algèbre. En déduire que la K-algèbre $A \otimes_k K$ est centrale simple si, et seulement si, la k-algèbre A l'est.

(e) Donner un contre-exemple au (c) si A n'est pas supposée centrale.

(f) Soit A une k-algèbre simple de dimension finie sur k. Soit I un idéal à gauche de A minimal pour l'inclusion (justifier). Montrer que la représentation régulière gauche de A sur I induit un morphisme injectif de k-algèbres $\psi : A \longrightarrow \mathrm{End}_k(I)$, tel que $\psi(A)$ ne stabilise aucun sous-k-espace vectoriel de I différent de $\{0\}$ et I.

(g) Supposons k algébriquement clos. Montrer qu'une k-algèbre centrale simple est k-isomorphe à $\mathrm{M}_n(k)$ pour un certain entier $n \geq 1$.

Indication: On utilisera le théorème de Burnside rappelé dans l'exercice 6. On verra certainement d'autres démonstrations de ces résultats dans la suite du cours.

(h) Soit A une k-algèbre de dimension finie sur k, K une clôture algébrique de k. Montrer l'équivalence : *A est centrale simple si, et seulement si,* $\exists n \geq 1$, $A \otimes_k K \simeq \mathrm{M}_n(K)$.

(i) Soit A un corps gauche de dimension finie sur son centre k, montrer que $\dim_k(A)$ est un carré. Montrer plus généralement ce résultat pour toute k-algèbre centrale simple A de dimension finie sur k.

Exercice 5 (Groupe de Brauer d'un corps) Soit k un corps. On ne considérera dans ce qui suit que des k-algèbres de dimension finie sur k. Cet exercice fait suite au précédent.

(a) Si A et B sont des k-algèbres centrales simples, montrer que la k-algèbre $A \otimes_k B$ est aussi centrale simple.

[6] Si A et B sont deux k-algèbres, on dit que A et B sont des "formes" (ou "formes tordues") l'une de l'autre elles deviennent isomorphes après extension des scalaires à une clôture algébrique de k. Cet exercice peut être vu comme une caractérisation des formes tordues de $\mathrm{M}_n(k)$: ce sont les k-algèbres centrales simples. De même, les k-algèbres diagonalisables sont les k-formes des k^n. On les a caractérisé dans l'exercice 2.(e) si $\mathrm{car}(k)= 0$, et nous verrons le cas général dans le cours de théorie de Galois.

(b) En déduire que si A est centrale simple, alors $A \otimes_k A^{\mathrm{opp}} \simeq \mathrm{M}_n(k)$, $n = \dim_k(A)$. Vérifier aussi que la réciproque est vraie.

Soit $CS(k)$ l'ensemble des classes d'isomorphie[7] de k-algèbres centrales simples de dimension finie sur k. Le (a) montre que $CS(k)$ est muni d'une structure de monoïde à l'aide de $\otimes_k$, de neutre k. Considérons la relation d'équivalence suivante sur $CS(k)$. Si A et A' sont des k-algèbres centrales simples, on dit que $\overline{A} \equiv \overline{A'}$ si, et seulement si, il existe n, $m \geq 1$ tels que $\mathrm{M}_n(A) \simeq \mathrm{M}_m(A')$.

(c) Montrer que $\otimes_k$ induit par passage au quotient une structure de groupe commutatif sur $CS(k)/\equiv$, c'est le *groupe de Brauer de* k, on le note $Br(k)$.

(d) En utilisant l'exercice précédent, montrer que si k est algébriquement clos, $Br(k)$ est le groupe trivial.

Remarques: (i) Il est connu que $Br(k)$ est trivial si k est fini (thm. de Wedderburn), et que $Br(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z} = \langle\overline{\mathbb{H}}\rangle$ (thm. de Frobenius). Un théorème profond de théorie algébrique des nombres dû à Hasse est la détermination de $Br(\mathbb{Q})$.

(ii) On démontrera plus tard dans le cours que si A est une k-algèbre centrale simple, il existe une k-algèbre à division D telle que $A \simeq M_n(D)$. Ainsi, $Br(k)$ est engendré par les classes des algèbres à division. Admettant ceci, la première assertion du (i) ci-dessus est équivalente à un théorème de Wedderburn bien connu, et la seconde assertion est conséquence du dernier exercice du TD1, ainsi que de l'exercice 3.(c) de ce TD. L'exercice 3.(c) est un cas particulier du fait suivant : si A, B, C sont centrales simples et $A \otimes_k B \simeq A \otimes_k C$, alors $B \simeq C$; fait que l'on montrera lorsque l'on disposera d'un peu de techniques de modules semi-simples.

Exercice 6 (Un théorème de Burnside) Soit k un corps algébriquement clos, V un k-espace vectoriel de dimension finie et $A \subset \mathrm{End}_k(V)$ une sous-k-algèbre. On suppose que A agit irréductiblement sur V, i.e. que les seuls sous-espaces vectoriels de V stables par A sont $\{0\}$ et V. On va montrer que $A = \mathrm{End}_k(V)$ (thm. de Burnside).

(a) Montrer que si A contient un endomorphisme de rang 1, alors $A = \mathrm{End}_k(V)$.

(b) Soit r le rang minimal d'un élément non nul de A, disons $r = \mathrm{rg}(a)$. On suppose que $r \geq 2$, et on fixe $x, y \in V$, tels que $\{a(x), a(y)\}$ soit libre. Montrer que l'on peut trouver $b \in A$ tel que $b(y) = x$ (justifier), puis qu'il existe $\lambda \in k$ tel que $ab - \lambda$ induit un endomorphisme non injectif de $\mathrm{Im}(a)$. Conclure.

(c) Trouver un contre-exemple si l'on ne suppose plus k algébriquement clos.

[7] Il est aisé de vérifier que c'est effectivement un ensemble, de même cardinal que $k \times \mathbb{Z}$.

8 Mars 2004

T.D. n^o 3 du cours d'Algèbre II

Exercice 1 Soient k un corps, V un k-espace vectoriel et $n \geq 1$ un entier.

(a) Montrer que l'application canonique $\mathrm{End}_k(V) \to \mathrm{End}_k(\mathrm{Sym}^n(V))$ n'est pas un morphisme de k-algèbres[8] si $n > 1$ et $\dim_k(V) > 1$, mais qu'elle induit toujours un morphisme de groupes $\mathrm{GL}(V) \to \mathrm{GL}(\mathrm{Sym}^n(V))$.

On considère dans ce qui suit les morphismes de groupes $\rho_n : \mathrm{SL}_2(k) \to \mathrm{GL}(\mathrm{Sym}^n(k^2)) \simeq \mathrm{GL}_{n+1}(k)$ donnés par le (a).

(b) Décrire $\mathrm{Ker}(\rho_n)$.

(c) On suppose que k est de caractéristique nulle, montrer que $\rho_n(\mathrm{SL}_2(k))$ ne stabilise aucun sous-espace vectoriel strict de $\mathrm{Sym}^n(k^2)$.

(d) On suppose que k est de caractéristique $p > 0$, vérifier que la question précédente vaut encore si $n < p$ et étudier le cas $n = p$.

Exercice 2 Soient k un corps et V un k-espace vectoriel.

(a) Donner une condition nécessaire et suffisante sur $v_1, \ldots, v_d \in V$ pour que le tenseur pur $v_1 \wedge \cdots \wedge v_d$ soit non nul dans $\Lambda^d(V)$.

(b) Soit $d \in \mathbb{N}$, montrer les équivalences :
i) Le rang de u est $< d$,
ii) Tous les mineurs de taille d de u dans une base fixée quelconque de V sont nuls,
iii) $\Lambda^d(u)$ est l'endomorphisme nul de $\Lambda^d(V)$.

(c) Soit $Gr_d(V) := \{W \subset V, \dim_k(W) = d\}$. Fixons $W \in Gr_d(V)$, montrer que l'image de l'application naturelle $\Lambda^d(W) \to \Lambda^d(V)$ est une k-droite. Montrer que l'application construite $Gr_d(V) \to \mathbb{P}(\Lambda^d(V))$ est une injection d'image les classes d'homothétie de tenseurs purs non nuls de $\Lambda^d(V)$ (*Plongement de Plücker*).

(d) Vérifier que $Gr_d(V) = \mathbb{P}(\Lambda^d(V))$ si $d = 1$ ou $n-1$ ($n = \dim_k(V) < \infty$), puis que $Gr_2(V)$ est une intersection de quadriques projectives[9] si $d = 2$ ou $n-2$ (on utilisera 3.(b)). Montrer que $Gr_2(k^4)$ est une quadrique de $\mathbb{P}^5(k)$ de la forme $xy + zt + uv = 0$.

Indication: Montrer que $f \in \Lambda^2(V)$ est un tenseur pur si, et seulement si, $f \wedge f = 0$ dans $\Lambda^2(V)$.

Exercice 3 Soient k un corps, V un k-espace vectoriel de dimension finie.

(a) Soit $f \in \Lambda^2(V)^*$ une forme bilinéaire alternée sur V. Montrer que $W := \mathrm{Ker}(f)$ est de codimension paire $2r$ et qu'il existe une famille libre $e_1, \ldots, e_{2r}$ de V engendrant un supplémentaire de W telle que si $1 \leq i \leq 2r$ est impair et $1 \leq j \leq 2r$, alors $f(e_i, e_j) = \delta_{j,i+1}$.

(b) En déduire que pour tout $f \in \Lambda^2(V)$, il existe un unique entier $r \leq \dim_k(V)/2$ ainsi qu'une famille libre $f_1, \ldots, f_{2r} \in V$ telle que $f = \sum_{i=1}^{r} f_{2i-1} \wedge f_{2i}$.

[8] Vous pouvez vérifier, comme exercice indépendant, qu'il existe un morphisme de k-algèbres $M_d(k) \to \mathrm{M}_n(k)$ si, et seulement si, $d|n$.

[9] C'est en fait vrai pour tout $d \neq 1, n-1$ (thm. de Plücker).

On considère dans ce qui suit l'action naturelle de $\mathrm{GL}(V)$ sur $\Lambda^2(V)$ (préciser).

(c) Décrire les orbites de $\Lambda^2(V)$ sous cette action.

(d) Fixons une base $(e_i)_{1\leq i\leq n}$ de V. Cela nous permet d'identifier $\Lambda^2(V)^*$ à l'espace $A_n(k)$ des matrices anti-symétriques de $\mathrm{M}_n(k)$ par $f \mapsto (f(e_i, e_j))$, ainsi que $\mathrm{GL}(V)$ à $\mathrm{GL}_n(k)$. Donner une une interprétation de l'entier r du (a) en ces termes.

(e) On suppose[10] $k = \mathbb{R}$ ou $\mathbb{C}$. Montrer qu'il y a une unique orbite ouverte, et décrire l'adhérence de chacune des orbites.

(f*) On suppose que k est fini, calculer le cardinal de ces orbites.

Indication: Si $2r = \dim_k(V)$ et $f \in \Lambda^2(V)^*$ est de rang r, commencer par calculer le nombre de bases $(e_i)_{1\leq i\leq 2r}$ de V telles que si $1 \leq i \leq 2r$ est impair et $1 \leq j \leq n$, alors $f(e_i, e_j) = \delta_{j,i+1}$.

(g) Étudier à la manière de cet exercice l'action de $\mathrm{GL}(V)$ sur $\mathrm{Sym}^2(V)$. On supposera pour cela dans un premier temps que k est un corps algébriquement clos de caractéristique $\neq 2$, puis on pourra aussi traiter le cas $k = \mathbb{R}$, ou k fini de caractéristique impaire.

Exercice 4 Si $\sigma \in \mathfrak{S}_n$, on note $\varepsilon(\sigma)$ sa signature et $|\sigma|$ le nombre de cycles dans sa décomposition canonique. Montrer la relation

$$\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)t^{|\sigma|} = t(t-1)\dots(t-n+1).$$

Indication: Soit $k \geq 1$ un entier, $\mathfrak{S}_n$ agit linéairement sur $(\mathbb{C}^k)^{\otimes n}$ par permutation des coordonnées. On pourra considérer l'élément $p := \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\sigma \in \mathrm{End}_{\mathbb{C}}((\mathbb{C}^k)^{\otimes n})$.

Exercice 5** (Un isomorphisme exceptionnel[11]) Montrer qu'il existe un isomorphisme bicontinu de groupes

$$\mathrm{SL}_4(\mathbb{C})/\{\pm 1\} \xrightarrow{\sim} \mathrm{SO}_6(\mathbb{C}).$$

Indication: Considérer l'application naturelle $\Lambda^2(\mathbb{C}^4) \times \Lambda^2(\mathbb{C}^4) \to \Lambda^4(\mathbb{C}^4)$. On pourra utiliser soit un argument de calcul différentiel, soit le théorème de l'application ouverte : une injection continue $\mathbb{R}^n \to \mathbb{R}^n$ est ouverte (*thm. de Jordan*). Vérifier que $\forall n \geq 1$, $\mathrm{SO}_n(\mathbb{C})$ est connexe.

Les exercices qui suivent sont proches d'être des résultats du cours.

Exercice 6 Soient k un corps, V un k-espace vectoriel de dimension finie et $n \in \mathbb{N}$. Montrer qu'il existe une unique application bilinéaire $f : \Lambda^n(V) \times \Lambda^n(V^*) \to k$ telle que

$$f((v_1 \wedge \dots \wedge v_n, \varphi_1 \wedge \dots \wedge \varphi_n)) = \det((\varphi_i(v_j)).$$

Vérifier qu'elle est non dégénérée, et qu'elle induit un isomorphisme canonique $\Lambda^n(E^*) \to \Lambda^n(E)^*$ que l'on explicitera.

---

[10] On peut aussi supposer k quelconque et considérer la topologie de Zariski sur $\Lambda^2(V)$, comme dans l'exercice 2 du TD1.

[11] De la même manière que dans cet exercice, on pourrait montrer les autres isomorphismes exceptionnels standards : $\mathrm{Sp}_2(\mathbb{C}) \simeq \mathrm{SL}_2(\mathbb{C})$, $\mathrm{SO}_3(\mathbb{C}) \simeq \mathrm{SL}_2(\mathbb{C})/\{\pm 1\}$, $\mathrm{SO}_4(\mathbb{C}) \simeq (\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C}))/\{\pm(1,1)\}$, et $\mathrm{SO}_5(\mathbb{C}) \simeq \mathrm{Sp}_4(\mathbb{C})/\{\pm 1\}$. Vous pouvez aussi donner les versions réelles de ces isomorphismes. On se méfiera par exemple que $\mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$ n'est pas isomorphe à $\mathrm{SO}_3(\mathbb{R})$ mais à $\mathrm{SO}_{(2,1)}(\mathbb{R})$.

Exercice 7 Soient k un anneau commutatif, V un k-module libre.

(a) Fixons $e = (e_i)$ une k-base de V. Montrer qu'il existe un unique morphisme de k-algèbres $\varphi_e : \mathrm{Sym}(V) \to k[T_1, ..., T_n]$ envoyant e_i sur T_i, puis que c'est un isomorphisme d'algèbres graduées.

(b) Soit k^V la k-algèbre des fonctions de V dans k. Montrer que l'injection canonique $V^* \to k^V$ se prolonge en un unique morphisme de k-algèbres $\psi : \mathrm{Sym}(V^*) \to k^V$.

(c) Supposons que k est un corps infini. Montrer que ψ est injective, et non surjective.

Dans ce qui suit on suppose que k est un corps fini.

(d) Montrer que ψ est surjective, et non injective.

(e) Fixons une base $x = (x_i)$ de V^*, ce qui nous permet d'identifier $\mathrm{Sym}(V^*)$ à $k[T_1, ..., T_n]$ via φ_x d'après (a). Déterminer explicitement l'idéal noyau de $\psi.\varphi_x^{-1}$.

(f) Soit $q := |k|$. Montrer que la restriction de ψ à $\mathrm{Sym}^n(V^*)$ est injective si $n < q$.

Remarques: Une fonction k-valuée sur V est dite polynomiale si elle est dans l'image de ψ. Si $x_1, ..., x_n$ est une k-base de V^*, $f \in k^V$ est polynomiale si, et seulement si, c'est un polynôme en les x_i. Cette propriété est en particulier indépendante de la base choisie de V^*.

Exercice 8 Soient k un anneau commutatif, V un k-module libre de rang fini n. En considérant l'application canonique (la préciser)

$$\Lambda^{n-1}(V) \otimes_k V \to \Lambda^n(V),$$

montrer que si $M \in \mathrm{M}_n(k)$, $M\mathrm{co(M)}^{\mathrm{t}} = \det(\mathrm{M}).1$.

Exercice 9 (Principe du prolongement des identités algébriques)

(a) Montrer que $\forall n \in \mathbb{N}$, il existe un morphisme d'anneaux injectif $\mathbb{Z}[X_1, ..., X_n] \to \mathbb{C}$.

(b) Montrer que si k est un anneau commutatif, V un k-module libre de rang n et $u \in \mathrm{End}_k(V)$, alors :

$$\det(u - T.1) = \sum_{i=0}^{n} (-1)^{n-i} \mathrm{tr}(\Lambda^i(u)) T^i.$$

On le montrera d'abord pour $k = \mathbb{C}$ et u diagonalisable, puis on en déduira le cas général par le (a).

(c) Redémontrer le résultat de l'exercice précédent de cette manière.

CHAPITRE 2

Théorie de Galois

15 Mars 2004

T.D. n^o 4 du cours d'Algèbre II

Par défaut, p désignera toujours un nombre premier et q une puissance de p.

Exercice 1

(a) Réaliser $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_9$ et $\mathbb{F}_{25}$ comme corps de rupture de polynômes explicites.

(b) Montrer par réductions modulo p que X^4+X^2+X+1, X^5+3X+1 et X^4+1 sont irréductibles dans $\mathbb{Z}[X]$.

Exercice 2 Donner la structure des groupes additif et multiplicatif de $\mathbb{F}_q$.

Exercice 3 (Symbole quadratique de 2) Soit p premier impair, on va montrer dans ce qui suit que $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

(a) Montrer que $\mathbb{F}_{p^2}$ contient une racine huitième primitive de l'unité, disons ω. Vérifier[1] que $(\omega+\omega^{-1})^2 = 2$.

(b) En déduire 2 est un carré dans $\mathbb{F}_p^*$ si, et seulement si, $p \equiv \pm 1 \bmod 8$.

Exercice 4 Soit G le sous-groupe de $\mathrm{Aut}_{\mathbb{C}-\mathrm{alg}}(\mathbb{C}(T))$ engendré par les deux automorphismes $T \mapsto T^{-1}$ et $T \mapsto jT$, $j := e^{2i\pi/3}$.

(a) Montrer que G est isomorphe à $\mathfrak{S}_3$.

(b) Montrer que $\mathbb{C}(T)^G = \mathbb{C}(T^3+T^{-3})$.

Indication: Calculer tout d'abord le degré de $\mathbb{C}(T)$ sur $\mathbb{C}(T^3+T^{-3})$.

Exercice 5 Soient k un corps, $P \in k[X]$ un polynôme irréductible de degré n et K un corps de décomposition de P sur k.

(a) Montrer que $n \mid [K:k] \mid n!$.

(b) Montrer que $n = [K:k]$ si, et seulement si, K est un corps de rupture de P.

Exercice 6* Soient $p > 2$, et $a, b \in \mathbb{F}_q^*$. Montrer que l'équation $ax^2+by^2 = 1$ a $q - (\frac{-ab}{q})$ solutions dans $(\mathbb{F}_q)^2$.

Indication: On pourra[2] résoudre d'abord l'équation dans $\mathbb{F}_{q^2}$, puis chercher celles qui sont dans $\mathbb{F}_q$.

Exercice 7 (Polynômes sur des corps finis : en vrac)

---

[1] Noter l'analogie avec le cas complexe.

[2] Une autre méthode est de montrer, par dénombrement, qu'il y a au moins une solution, puis d'en déduire par la méthode des cordes qu'il y a $q+1$ solutions dans $\mathbb{P}^2(\mathbb{F}_q)$ à la conique projective $aX^2+bY^2 = Z^2$. Conclure. En fait, toute forme quadratique non dégénérée sur $\mathbb{F}_q^3$ est équivalente à une de la forme précédente, de sorte que toute conique non dégénérée dans $\mathbb{P}^2(\mathbb{F}_q)$ a exactement $q+1$ points. Sous ce point de vue, le terme "correctif" $-1+(\frac{-ab}{q})$ apparaissant dans l'énoncé correspond exactement au nombre de points à l'infini, i.e. aux solutions dans $\mathbb{P}^1(\mathbb{F}_q)$ de $aX^2+bY^2 = 0$.

(a) Soit $P \in \mathbb{F}_q[X]$ de degré d, montrer que P est irréductible si, et seulement si, P n'a pas de racine dans $\mathbb{F}_{q^n}$ si $n \leq d/2$, ou encore si, et seulement si, P est premier à $X^{q^n} - X$ si $n \leq d/2$.

(b) Montrer que $\mathbb{F}_{q^n}$ se plonge comme $\mathbb{F}_q$-algèbre dans $\mathbb{F}_{q^m}$ si, et seulement si, $n|m$.

(c) Montrer que si $P \in \mathbb{F}_q[X]$ est irréductible, de degré d, alors il reste irréductible dans $\mathbb{F}_{q^n}$ pour $(d, n) = 1$.

(d) Montrer que tout polynôme irréductible $P \in \mathbb{F}_q[X]$ de degré n est scindé dans $\mathbb{F}_{q^n}$.

(e) Soient $P \in \mathbb{F}_q[X]$ polynôme irréductible, $n \in \mathbb{N}$. Montrer que P se décompose dans $\mathbb{F}_{q^n}[X]$ comme un produit de polynômes irréductibles, deux à deux distincts, de même degré.

(f) Montrer qu'il existe un isomorphisme de $\mathbb{F}_q$-algèbres :

$$\mathbb{F}_{q^n} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} \simeq \left(\mathbb{F}_{q^{\mathrm{ppcm(n,m)}}}\right)^{\mathrm{pgcd(n,m)}}$$

(g) Montrer que pour tout entier n, il existe un polynôme irréductible de degré n dans $\mathbb{F}_q[X]$.

Exercice 8 (Réduction modulo p des polynômes cyclotomiques) Soient $n \geq 1$ un entier et $\varphi_n \in \mathbb{Z}[X]$ le n^{ieme} polynôme cyclotomique. On fixe k un corps tel que $n.1 \in k$ est non nul.

(a) Montrer que les images de $X^n - 1$ et de $\varphi_n(X)$ dans $k[X]$ sont séparables.

(b) En déduire que l'ensemble des racines de φ_n dans k est exactement l'ensemble des racines primitives n^{iemes} de l'unité dans k, i.e. $\{x \in k^*,\ x^n = 1,\ x^d \neq 1\, \forall\, d|n\}$.

(c*) On suppose $k = \mathbb{F}_q$. Montrer que $\overline{\varphi_n} = P_1 ... P_g \in \mathbb{F}_q[X]$ où les P_i sont des irréductibles de $\mathbb{F}_q[X]$ deux à deux distincts et de même degré d, où d est l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Indication: On regroupera les racines de $\overline{\varphi_n}$ dans $\overline{\mathbb{F}}_q$ par orbites sous l'action du Frobenius $x \mapsto x^q$.

Le (c) a quelques conséquences importantes.

(d) En déduire une CNS pour que $\overline{\varphi_n}$ soit irréductible. Vérifier qu'il faut en particulier que $(\mathbb{Z}/n\mathbb{Z})^*$ soit un groupe cyclique, et que cela implique que n est une puissance d'un nombre premier impair.

(e) En déduire aussi l'existence d'un polynôme irréductible de tout degré sur $\mathbb{F}_q[X]$.

(f) En déduire enfin qu'il existe une infinité de nombres premiers $\equiv 1 \bmod n$.

Exercice 9* (Une construction de $\overline{\mathbb{F}}_p$ par la caractéristique 0) Soit A le sous-anneau de $\mathbb{C}$ engendré par les toutes les racines de l'unité, et p un nombre premier.

(a*) Montrer que pA est un idéal strict de A, puis qu'il existe un idéal maximal P de A contenant p.

Indication: Montrer que si n et m sont des entiers > 1, alors $1/n \notin \mathbb{Z}[e^{2i\pi/m}]$.

(b) Montrer que A/P est une clôture algébrique de $\mathbb{F}_p$.

Exercice 10* Si $n \geq 1$, on pose $u_n = (1+\sqrt{2})^n + (1-\sqrt{2})^n \in \mathbb{Z}$. Soit p premier.

(a) Montrer que si $p \equiv -1, 3 \bmod 8$, alors p divise un des termes de la suite (u_n).

(b) Montrer que si $p \equiv 5 \bmod 8$, p ne divise aucun des termes de la suite (u_n).

Remarques: On pourra raisonner dans $\mathbb{F}_{p^2}$. Les $p \equiv 1 \bmod 8$ ont un comportement plus complexe.

Exercice 11* Soit $P \in \mathbb{Z}[X]$.

(a) Montrer qu'il existe une infinité de nombres premiers p tels que $P \bmod p \in \mathbb{F}_p[X]$ ait une racine dans $\mathbb{F}_p$.

Indication: Traiter d'abord le cas $P(0) = \pm 1$, puis s'y ramener.

(b) Vérifier que $X^4 + 1$ est réductible modulo p pour tout p, bien qu'irréductible dans $\mathbb{Z}[X]$.

Les deux questions suivantes sont plus délicates.

(c) Soit $A \subset \mathbb{C}$ un sous-anneau, de type fini comme groupe abélien. Montrer que tout élément de A est annulé par un polynôme unitaire dans $\mathbb{Z}[X]$, puis que le polynôme minimal unitaire de chaque élément de A est dans $\mathbb{Z}[X]$.

(d*) Montrer qu'il existe une infinité de p tels que $P \bmod p$ est scindé dans $\mathbb{F}_p[X]$.

Indication: On se ramène d'abord au cas P unitaire. Soient $x_1, ..., x_n$ les racines complexes de P, A le sous-anneau $\mathbb{Z}[x_1, ..., x_n]$ de $\mathbb{C}$, il est de type fini comme groupe abélien. Déduire du théorème de l'élément primitif l'existence d'un entier $N \geq 1$ tel que $A[1/N]$ est engendré par un unique élément $x \in A$ comme $\mathbb{Z}[1/N]$-algèbre. Appliquer (a) au polynôme minimal de x, pour en déduire des morphismes d'anneaux $A \to \mathbb{F}_p$ pour une infinité de premiers p. Conclure[3].

On termine par des applications.

(i) (Petit théorème de Dirichlet) Soit $n \geq 1$, montrer qu'il y a une infinité de nombres premiers congrus à 1 modulo n.

(ii) Montrer qu'il y a une infinité de nombres premiers qui sont congrus à 1 mod 19 et tels que 7 est un cube modulo p, et que 13 est un carré modulo p.

Indication: Pour le i), considérer $P = X^n - 1$.

Remarques: Il est connu que si $P \in \mathbb{Z}[X]$ est irréductible de degré > 1, il existe une infinité de premiers p tels que P n'admet pas de racine modulo p (conséquence du thm. de Cebotarev).

Dans les exercices qui suivent, on donne une preuve de la loi de réciprocité quadratique utilisant des corps finis. Soit p un nombre premier impair. On rappelle que si $a \in \mathbb{F}_p^*$, on pose $(\frac{a}{p}) = +1$ si a est un carré modulo p, $(\frac{a}{p}) = -1$ sinon. De plus $(\frac{0}{p}) := 0$. Il est

[3]L'argument montre plus généralement que si $A \subset \mathbb{C}$ est un sous-anneau, de type fini comme groupe abélien, alors il existe un morphisme d'anneaux $A \to \mathbb{F}_p$ pour une infinité de p.

élémentaire [4] de vérifier que $(\frac{a}{p}) = a^{\frac{p-1}{2}}$ et que les carrés forment un sous-groupe d'indice 2 dans $\mathbb{F}_p^*$. En particulier, on a $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$ pour tous a et b dans $\mathbb{F}_p$.

Exercice 12 En imitant la méthode de l'exercice 5, calculer $(\frac{a}{p})$ pour $a = -1$, -3, 5 et -7.

Pour généraliser cette approche à tout nombre premier $q > 2$, il faut réussir à exprimer $\sqrt{q}$ comme combinaison de racines de l'unité. Un ingrédient essentiel pour cela est l'introduction des sommes (quadratiques) de Gauss[5]. On note $\mathbb{F}$ une clôture algébrique de $\mathbb{F}_p$.

Exercice 13 Soit $q > 2$ premier distinct de p, $\omega \neq 1 \in \mathbb{F}$ tel que $\omega^q = 1$. On considère la *somme de Gauss* :

$$g := \sum_{a \in \mathbb{F}_q} (\frac{a}{q})\, \omega^a \in \mathbb{F}$$

(a) Montrer que $g^p = (\frac{p}{q})g$, puis que $g = \sum_{a \in \mathbb{F}_q} \omega^{a^2}$.

(b) Calculer pour tout $a \in \mathbb{F}_q$, le nombre de couples $(x, y) \in (\mathbb{F}_q)^2$ solutions de l'équation $y^2 + x^2 = a$ (cf. ex. 6), en déduire $g^2 = (\frac{-1}{q})q$.

(c) En déduire que $(\frac{-1}{q})q$ est un carré modulo p si, et seulement si, p est un carré modulo q. Autrement dit,

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

(d) S'assurer de l'utilité de cette loi, en calculant par exemple $(\frac{257}{263})$ et $(\frac{23}{1709})$.

[4] Si $x \in \mathbb{F}_p^*$, x est toujours le carré d'un élément de $\mathbb{F}_{p^2}$, i.e. $x = a^2$ avec $a \in \mathbb{F}_{p^2}^*$. Ainsi, si x est un carré dans $\mathbb{F}_p$, on a $a^p = a$, et dans le cas constraire on a nécessairement $a^p = -a$, car $a^2 \in \mathbb{F}_p$. Si $p \neq 2$, on a $X^{p-1} - 1 = \prod_{x \in \mathbb{F}_p^*}(X - x) = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$, et il vient que les carrés de $\mathbb{F}_p^*$ sont exactement les racines de $X^{\frac{p-1}{2}} - 1$, et les non-carrés celles de $X^{\frac{p-1}{2}} + 1$, ce qui conclut.

[5] D'après Weil, elles auraient en fait été introduites par Lagrange.

22 Mars 2004

T.D. n^o 5 du cours d'Algèbre II

Exercice 1 Soit K/k une extension de degré 2, avec $\mathrm{char}(k) \neq 2$.

(a) Montrer qu'il existe $x \in K \backslash k$ tel que $x^2 \in k$, puis que $K = k[x]$. Vérifier que x est uniquement déterminé, à multiplication par un élément de k^* près.

(b) Montrer que K/k est galoisienne, et que si $\mathrm{Gal}(K/k) = \langle \sigma \rangle$, alors $\sigma(a+bx) = a-bx$.

(c) Vérifier que $\mathbb{F}_4/\mathbb{F}_2$ est séparable, mais pas de la forme $\mathbb{F}_2[x]$ avec $x^2 \in \mathbb{F}_2$.

(d) Donner un exemple d'extension $K/\mathbb{Q}$ non normale de degré 3.

Exercice 2 Montrer que les sous-corps de $\mathbb{C}$ suivants sont des extensions galoisiennes de $\mathbb{Q}$ et déterminer leur groupe de Galois :

$$\mathbb{Q}(\sqrt{11}),\ \mathbb{Q}(\sqrt{2},\sqrt{3}),\ \mathbb{Q}(e^{2i\pi/5}),\ \mathbb{Q}(e^{2i\pi/7}),\ \mathbb{Q}(\cos(2\pi/7)),\ \mathbb{Q}(\sqrt[3]{5}, j),\ \mathbb{Q}(\sqrt[4]{2}, i)$$

Lister leurs sous-corps et leurs éléments primitifs.

Exercice 3 (Le théorème de d'Alembert-Gauss) Soit K une extension algébrique de $\mathbb{R}$, on veut montrer que $K = \mathbb{R}$ ou $\mathbb{C}$.

(a) Supposons $K/\mathbb{R}$ galoisienne finie, montrer l'existence d'une tour d'extensions

$$\mathbb{R} \subset K_1 \subset K_2 \subset ... \subset K_n = K$$

telle que $[K_1 : \mathbb{R}]$ est impair, et si $i \in \{1, \ldots, n-1\}$, $[K_{i+1} : K_i] = 2$.

(b) Conclure.

Exercice 4

(a) Soit $K := \mathbb{Q}(\sqrt{1+\sqrt{2}}) \subset \mathbb{C}$. Montrer que $K/\mathbb{Q}$ est de degré 4, puis qu'elle n'est pas normale, bien que $K/\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ le sont.

Indication: Considérer $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ prolongeant l'élément non trivial de $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C})$.

(b) Soient $d \in \mathbb{Z}$, non nul, sans facteur carré, et a, $b \in \mathbb{Z}$. Montrer que $\mathbb{Q}(\sqrt{a+b\sqrt{d}})$ est une extension galoisienne de $\mathbb{Q}$ si, et seulement si, $a^2 - db^2 = c^2$ ou dc^2, avec $c \in \mathbb{Z}$.

(c) Montrer que $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ et $\mathbb{Q}(\sqrt{\frac{9}{7}+\frac{4}{7}\sqrt{2}})$ sont des extensions galoisiennes de $\mathbb{Q}$ de groupes de Galois respectifs $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 5** Trouver une extension galoisienne de $\mathbb{Q}$ de groupe de Galois le groupe d'ordre 8 des quaternions.

Indication: (Dedekind) Essayer $\mathbb{Q}\left(\sqrt{(2+\sqrt{2})(3+\sqrt{6})}\right)$.

Exercice 6 Soient $p_1, \ldots, p_r$ des nombres premiers deux à deux distincts, on pose

$$K_r := \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r}).$$

(a) En raisonnant par récurrence sur r, calculer $\dim_{\mathbb{Q}}(K_r)$ et décrire $\mathrm{Hom}_{\mathbb{Q}}(K_r, \mathbb{C})$.

(b) Montrer que $\sqrt{p_1}+\cdots+\sqrt{p_r}$ n'est pas un entier.

Exercice 7 Soient $\lambda \in \mathbb{C}^*$ et $\mu \in \mathbb{C}\backslash\{0,1\}$.

(a) Montrer que $\mathbb{C}(X)(\sqrt{X(X-\lambda)})$ est isomorphe à $\mathbb{C}(T)$ comme $\mathbb{C}$-algèbre.

(b*) Soient A, $B \in \mathbb{C}[T]$ tels que $(A,B)=1$. On suppose que A, B, $A+B$ et $A+\mu B$ sont des carrés dans $\mathbb{C}[T]$. Montrer que A, $B \in \mathbb{C}$.

(c) En déduire que $y^2 = x(x-1)(x-\mu)$ n'admet de pas de solution (x,y) non constante dans $\mathbb{C}(T)^2$, puis que $\mathbb{C}(X)(\sqrt{X(X-1)(X-\mu)})$ n'est pas isomorphe à $\mathbb{C}(T)$ comme $\mathbb{C}$-algèbre.

Exercice 8 Soit G un sous-groupe de $\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{Aut}_{\mathbb{F}_q-\mathrm{alg}}(\mathbb{F}_q(T))$. Trouver un $f \in \mathbb{F}_q(T)$ tel que $\mathbb{F}_q(T)^G = \mathbb{F}_q(f)$ dans les cas suivants :

(a) G est le sous-groupe des matrices diagonales, puis celui des matrices unipotentes (resp. triangulaires) supérieures.

(b*) $G = \mathrm{PGL}_2(\mathbb{F}_q)$.

Exercice 9 Soient $n \geq 1$, $a_n + b_n\sqrt{2} := (1+\sqrt{2})^n$, a_n, $b_n \in \mathbb{Z}$. Montrer que $(a_n, b_n) = 1$.

Exercice 10 Soient k un corps, $P \in k[X]$ un polynôme séparable de degré n et K un corps de décomposition de P sur k.

(a) Montrer que $[K:k]$ divise $n!$.

(b) Montrer que $[K:k] = n!$ (resp. $\frac{n!}{2}$) si, et seulement si, $\mathrm{Gal}(K/k) \simeq \mathfrak{S}_n$ (resp. $\mathfrak{A}_n$).

Exercice 11 (Équations cubiques) Soient k un corps, $P \in k[X]$ un polynôme irréductible séparable de degré 3, K un corps de décomposition de P, G le groupe de Galois de K/k, x_1, x_2, x_3 les trois racines de P dans K, et $\delta = \prod_{1\leq i<j\leq 3}(x_i - x_j) \in K$.

(a) Montrer que $\delta^2 \in k^*$.

(b) Déterminer G suivant que δ est dans k ou non. Si $P = X^3 + aX + b$, discuter en fonction de $-4a^3 - 27b^2$.

Exercice 12 (Décomposition de Dunford) Soient K un corps parfait et $\overline{K}$ une clôture algébrique de K.

(a) Montrer que toute matrice $M \in \mathrm{M}_n(K)$ s'écrit de manière unique sous la forme $D+N$ où D et $N \in \mathrm{M}_n(K)$ commutent, N est nilpotente, et D est diagonalisable dans $\mathrm{M}_n(\overline{K})$.

(b) Si K n'est pas parfait, montrer que cela vaut encore si, et seulement si, $n < \mathrm{char}K$.

29 Mars 2004

T.D. n^o 6 du cours d'Algèbre II

Exercice 1 Soit $K := \mathbb{Q}(\cos(2\pi/7)) \subset \mathbb{R}$.

(a) Montrer que $K/\mathbb{Q}$ est une extension galoisienne cyclique de degré 3.

(b) Vérifier que K ne contient pas de racine de l'unité différente de ± 1.

(c) Vérifier que $K/\mathbb{Q}$ est résoluble par radicaux, mais que K n'est pas de la forme $\mathbb{Q}(x)$ avec $x^n \in \mathbb{Q}$ et $n \in \mathbb{N}$. Écrire $\cos(2\pi/7)$ comme somme de radicaux de rationnels.

Exercice 2 Soient p, q des indéterminées, $j := e^{2i\pi/3}$, $P := X^3 + pX + q \in \mathbb{Q}(p,q)[X]$ et K un corps de décomposition de P sur $\mathbb{Q}(p,q,j)$.

(a) Montrer que $\mathrm{Gal}(K/\mathbb{Q}(p,q,j)) \simeq \mathfrak{S}_3$, et que P est résoluble par radicaux sur $\mathbb{Q}(p,q)$.
Indication: Soient x_i les 3 racines de P dans K, $\delta := \prod_{i<j}(x_i - x_j) \in K$. On a $\delta^2 = -4p^3 - 27q^2$.

(b) Exprimer explicitement les racines de P comme somme de radicaux emboîtés et retrouver les formules de Cardan.

Exercice 3 Soit $P := X^4 + 4X^3 + 12X^2 + 24X + 24 \in \mathbb{Q}[X]$, on notera $x_1, \ldots, x_4$ ses 4 racines distinctes dans $\mathbb{C}$ (justifier), $K := \mathbb{Q}(x_1, \ldots, x_4)$.

(a) Montrer que P est irréductible dans $\mathbb{Q}[X]$ et que son groupe de Galois est un sous-groupe transitif de $\mathcal{A}_4$.
Données: La réduction modulo 5 de P est $(X^3 + 2X + 1)(X + 4)$. De plus $\prod_{i<j}(x_i - x_j)^2 = 331776 = 2^{12}3^4$.

(b) On pose $Q := (X - y_1)(X - y_2)(X - y_3)$ avec $y_1 = x_1x_2 + x_3x_4$, $y_2 = x_2x_3 + x_1x_4$ et $y_3 = x_3x_1 + x_2x_4 \in K$. Montrer que $Q \in \mathbb{Q}[X]$ et expliquer comment vous feriez pour calculer ses coefficients. Un calcul montrerait en fait que $Q = X^3 - 12X^2 + 192$.

(c) Montrer que Q est irréductible dans $\mathbb{Q}[X]$, puis que $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathcal{A}_4$.

(d) Soit $L := \mathbb{Q}(y_1, y_2, y_3) \subset K$. Montrer que $L/\mathbb{Q}$ est galoisienne cyclique de degré 3, que c'est l'unique sous-corps d'ordre 3 de $\mathbb{Q}(e^{2i\pi/9})$, i.e. $\mathbb{Q}(\cos(2\pi/9))$, et que

$$\{y_1, y_2, y_3\} = \{4 + 2\cos(2\pi/9),\ 4 + 2\cos(8\pi/9),\ 4 + 2\cos(6\pi/9)\}.$$

Données: Si $z := y_1 + jy_2 + j^2y_3 \in L(j)$, alors $z^3 = 1728.j = 12^3.j$, avec $j^3 = 1$.

(e) Donner une écriture de x_i comme somme de radicaux emboîtés de rationnels.

Exercice 4 (Le polygône régulier à 17 côtes)

(a) Montrer que $\cos(2\pi/17)$ est une somme de racines carrées emboitées de nombres rationnels et l'écrire explicitement comme tel.

(b) En déduire que le polygone régulier à 17 côtés est constructible à la règle et au compas (Gauss).

Exercice 5 Soit p un nombre premier.

(a) Montrer qu'un p-cycle et une transposition engendrent $\mathfrak{S}_p$.

(b) En déduire le groupe de Galois sur $\mathbb{Q}$ du polynôme $X^5 - 4X + 2 \in \mathbb{Q}[X]$.

(c) Soit $\mathbb{R}_n[X] \subset \mathbb{R}[X]$ l'espace des polynômes de degré $\leq n$, muni de sa topologie d'espace vectoriel normé. Montrer que l'ensemble des polynômes $P \in \mathbb{Q}[X] \cap \mathbb{R}_n[X]$ qui sont irréductibles dans $\mathbb{Q}[X]$ est dense dans $\mathbb{R}_n[X]$.

Indication: Si $P \in \mathbb{Z}[X]$ et l est un nombre premier assez grand, on pourra par example remarquer $l.P + 1$ est irréductible dans $\mathbb{Z}[X]$ en appliquant convenablement le critère d'Eisenstein[6].

(d) En déduire qu'il existe une extension galoisienne de $\mathbb{Q}$ de groupe de Galois $\mathfrak{S}_p$ (donc non résoluble si $p > 3$).

Exercice 6 Soient p un nombre premier, $a \in \mathbb{Q}^*$ qui n'est pas une puissance p^{ieme} dans $\mathbb{Q}$, $K := \mathbb{Q}(e^{2i\pi/p}, \sqrt[p]{a})$.

(a) Montrer que les extensions $K/\mathbb{Q}$, $K/\mathbb{Q}(\sqrt[p]{a})$, $\mathbb{Q}(e^{2i\pi/p})/\mathbb{Q}$ et $K/\mathbb{Q}(e^{2i\pi/p})$ sont galoisiennes, mais pas $\mathbb{Q}(\sqrt[p]{a})/\mathbb{Q}$ si $p \neq 2$.

(b) Montrer que $X^p - a$ est irréductible dans $\mathbb{Q}[X]$, en déduire $[K : \mathbb{Q}]$.

(c) Déterminer $\mathrm{Gal}(K/\mathbb{Q}(e^{2i\pi/p}))$ et $\mathrm{Gal}(K/\mathbb{Q}(\sqrt[p]{a}))$.

(d) Montrer que $\mathrm{Gal}(K/\mathbb{Q})$ est isomorphe au produit semi-direct de $(\mathbb{Z}/p\mathbb{Z})^*$ par $\mathbb{Z}/p\mathbb{Z}$, pour l'action canonique $(\mathbb{Z}/p\mathbb{Z})^* \xrightarrow{\sim} \mathrm{Aut}_{gr}(\mathbb{Z}/p\mathbb{Z})$.

Exercice 7 Si $n \geq 1$ est un entier, on pose $K_n := \mathbb{Q}(e^{2i\pi/n}) \subset \mathbb{C}$.

(a) Montrer que $K_n/\mathbb{Q}$ est galoisienne de groupe de Galois canoniquement isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.

(b) Déduire du petit théorème de Dirichlet que tout groupe abélien fini est le groupe de Galois d'une extension abélienne de $\mathbb{Q}$.

(c) On suppose $(m, n) = 1$. Montrer que $K_m K_n = K_{mn}$ et $K_m \cap K_n = \mathbb{Q}$.

(d) Soit G un groupe abélien fini. Montrer qu'il existe une infinité d'extensions galoisiennes de $\mathbb{Q}$ de groupe de Galois G deux à deux linéairement disjointes.

(e) En déduire que toute extension finie de $\mathbb{Q}$ admet une extension galoisienne finie de groupe de Galois G.

Exercice 8*

(a) Soient $n \leq m$ des entiers tels que $\mathbb{Q}(\cos(2\pi/n)) = \mathbb{Q}(\cos(2\pi/m))$. Montrer que soit ce corps est $\mathbb{Q}$, i.e. n, m est dans $\pm\{1, 2, 3, 4, 6\}$, soit $m = n$, soit n est impair et $m = 2n$.

(b) Soient r, $r' \in \mathbb{Q}$ tels que $2\cos(2\pi r) = 1 + \cos(2\pi r')$. Montrer que $\cos(2\pi r) \in \{0, 1\}$.

Exercice 9** (Lucy et Lily) Soit $P \subset \mathbb{C}$ un polygône régulier à 5 côtés dont je marque la position initiale sur le plan. Vous fermez les yeux pendant que je fais subir à P une suite

[6]Il y a bien sûr d'autres méthodes pour résoudre cet exercice, par exemple en approchant P par polynôme $Q \in \mathbb{Z}[1/N][X]$ qui est irréductible modulo un nombre premier p ne divisant pas N (pourquoi ?).

finie de reflexions axiales, chacune ayant pour axe un côté de P. Arriverez-vous à ramener P à sa position initiale uniquement par des reflexions axiales comme ci-dessus ?

Exercice 10 Soit $k := \mathbb{C}((T)) := \{\sum_{n\geq n_0} a_n T^n, a_n \in \mathbb{C}, n_0 \in \mathbb{Z}\}$ le corps des séries formelles de Laurent à coefficients complexes.

(a) Montrer que pour tout entier n, k admet une unique extension cyclique k_n/k de degré n, qui est le corps de rupture de $X^n - T$ (i.e. $k_n = \mathbb{C}((T^{1/n}))$).

(b) Montrer que toute extension finie de k résoluble par radicaux est cyclique.

(c) Montrer que l'équation $x^3 - Tx + T = 0$ admet trois solutions dans $\mathbb{C}((T^{1/3}))$.

Remarques: On pourrait démontrer que toute extension finie de k est galoisienne cyclique, puis que pour tout n, k_n/k est l'unique extension de degré n de k (théorème de Puiseux).

Exercice 11* Soient k un corps, p un nombre premier, et $a \in k^*$ un élément qui n'est pas une puissance p^{ieme} dans k. Si $p = 2$, on suppose de plus que a n'est pas de la forme $-4x^4$, $x \in k$. Montrer que pour tout $r \geq 1$, $X^{p^r} - a$ est irréductible dans $k[X]$.

Indication: On pourra commencer raisonner par récurrence sur r et utiliser la norme.

Problème (théorème d'Artin) Soient k un corps[7], K une clôture algébrique de k. On suppose que K/k est finie, on va montrer que $[K : k] \leq 2$.

(a*) On suppose que -1 est un carré dans k, montrer que $K = k$.

Indication: On pourra se ramener au cas K/k de degré premier et utiliser l'exercice précédent.

On suppose dorénavant que -1 n'est pas un carré dans k.

(b) Montrer que $K = k(\sqrt{-1})$, et en particulier que $[K : k] = 2$.

(c) Montrer que la relation binaire sur k définie par

$$x \leq y \Leftrightarrow \exists z \in k,\ y - x = z^2$$

est une relation d'ordre total, telle que $\forall x \in k^*$, $x > 0$ ou $-x > 0$. Vérifier que $\mathrm{char}(k) = 0$ et que l'ordre induit sur $\mathbb{Q}$ est l'ordre usuel.

(d) Soient $a, b \in k$, $P \in k[X]$, montrer que si $P(a) < 0$ et $P(b) > 0$, alors il existe c entre a et b tel que $P(c) = 0$ (cette question ne sera pas utilisée dans la suite).

On termine par une application au groupe de Galois de $\overline{\mathbb{Q}}$ sur $\mathbb{Q}$.

(e) Montrer que si $k/\mathbb{Q}$ est algébrique, alors $(k, \leq)$ est archimédien, *i.e.*

$$\forall x \in k,\ \exists n \in \mathbb{N},\ x < n$$

Indication: On pourra introduire, pour $x \in k$, $|x| := \sup\{x, -x\} \in k$.

(f) En déduire l'existence d'un morphisme de corps croissant $k \to \mathbb{R}$, puis que ce morphisme induit un isomorphisme $k \simeq \mathbb{R} \cap \overline{\mathbb{Q}}$.

(g) Montrer que tout sous-groupe fini non trivial de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est d'ordre 2, et qu'il est engendré par un élément conjugué à la conjugaison complexe (théorème d'Artin).

[7] On pourra supposer que k est de caractéristique nulle en première approche.

5 Avril 2004

T.D. n^o 7 du cours d'Algèbre II

Exercice 1 (Le discriminant) Soient k un corps, $P \in k[X]$, K un corps de décomposition de P sur k, $X := \{x_1, ..., x_n\}$ l'ensemble des racines de P dans K. On pose

$$\delta(P) := \prod_{i<j}(x_i - x_j) \in K, \ \ \mathrm{disc}(P) := \delta(P)^2$$

(a) Montrer que $\mathrm{disc}(P) \in k$, et qu'il est non nul si, et seulement si, P est séparable.

(b) On suppose P séparable. Montrer que l'image du morphisme canonique $\mathrm{Gal}(K/k) \to \mathfrak{S}(X)$ tombe dans le groupe alterné si, et seulement si, $\mathrm{disc}(P)$ est un carré dans k.

(c) On suppose $k = \mathrm{Frac}(A)$, A un anneau intègre, et $P \in A[X]$ unitaire. Montrer que $\mathrm{disc}(P) \in A$, puis que si Q est un idéal premier de A, l'image de $\mathrm{disc}(P)$ dans A/Q est égale à $\mathrm{disc}(\overline{P})$, où $\overline{P} := P \bmod Q \in (A/Q)[X]$.

(d) En conclure que si P est un polynôme unitaire de $\mathbb{Z}[X]$:

i) $\mathrm{disc}(P) \in \mathbb{Z}$,

ii) $\overline{P} \in \mathbb{F}_p[X]$ est séparable si, et seulement si, p se divise pas $\mathrm{disc}(P)$,

iii) si P est séparable dans $\mathbb{Q}[X]$, alors $\overline{P}$ est séparable dans $\mathbb{F}_p[X]$ pour tout p sauf éventuellement un nombre fini.[8]

Exercice 2 Pour chaque polynôme $P \in \mathbb{Q}[X]$ suivant, calculer par réductions modulo p le groupe de Galois d'un corps de décomposition sur $\mathbb{Q}$ de P.

(a) $X^3 - X + 1, \ \ X^3 - 7X + 7$

(b) $X^4 + 25X^3 + 5X^2 + 25X - 19, \ \ X^4 + 4X^3 + 12X^2 + 24X + 24$

(c) $X^5 + X + 3, \ X^5 + X^4 + 5X^3 + 5X^2 + 5X + 4$

Indication: Pour $(b)_1$, vérifier que $1 + X + X^2 + X^3 + X^4$ n'a pas de racine dans $\mathbb{F}_4$, puis qu'il est irréductible dans $\mathbb{F}_2[X]$.

Données: Le discriminant de $(b)_2$ vaut $331776 = 2^{12}3^4$ et sa réduction modulo 5 est $(X^3 + 2X + 1)(X + 4)$. Le polynôme $(c)_1$ est irréductible modulo 7. Le polynôme $(c)_2$ est irréductible modulo 5 et vaut $(X^3 - 2)(X - 1)(X + 2)$ modulo 7.

Exercice 3

(a) Montrer que $\mathfrak{A}_5$ n'a pas de sous-groupe strict d'indice ≤ 4.

Indication: On pourra considérer l'action par translation sur les classes à gauche d'un tel sous-groupe.

(b) Soit G un sous-groupe de $\mathfrak{A}_5$ agissant transitivement sur l'ensemble $\{1, 2, 3, 4, 5\}$. Montrer que G est l'un des sous-groupes suivants :

i) le groupe cyclique engendré par un 5-cycle,

ii) le normalisateur dans $\mathfrak{A}_5$ du sous-groupe engendré par un 5-cycle,

---

[8] Si $P \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Q}[X]$, un théorème de géométrie des nombres dû à Hermite montre que $\mathrm{disc}(P) \neq \pm 1$. Autrement dit, il existe toujours un premier p tel que $P \bmod p$ soit non séparable.

iii) $\mathfrak{A}_5$.

Vérifier que les sous-groupes du type ii) sont isomorphes au groupe dihédral D_5, qui est l'unique produit semi-direct non trivial de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/5\mathbb{Z}$.

Soient $P(X) = X^5 - 5X + 12 \in \mathbb{Z}[X]$, $x_1, x_2, ..., x_5$ ses racines dans $\mathbb{C}$ et $K := \mathbb{Q}(x_1, ..., x_5) \subset \mathbb{C}$. On pourra utiliser les renseignements donnés plus bas pour répondre à la question suivante.

(c) Montrer que P est irréductible dans $\mathbb{Q}[X]$, que $K/\mathbb{Q}$ est une extension galoisienne, et déterminer son groupe de Galois.

(d) Est-ce que $K/\mathbb{Q}$ est résoluble par radicaux ?

(e) Expliquer brièvement comment vous feriez pour vérifier chacune des informations données ci-dessous.

Données :
- $X^5 + 2X + 5$ est irréductible dans $\mathbb{F}_7[X]$,
- le discriminant de P, *i.e.* $\prod_{1\leq i<j\leq 5}(x_i - x_j)^2$, vaut $2^{12}5^6$,
- $Q(X) := \prod_{1\leq i<j\leq 5}(X - (x_i + x_j)) = (X^5 - 5X^3 - 10X^2 + 30X - 36)(X^5 + 5X^3 + 10X^2 + 10X + 4)$.

Exercice 4

(a) Soient $d \geq 1$ un entier, $p_1, ..., p_s$ des entiers premiers entre eux deux à deux et $P_i \in (\mathbb{Z}/n_i\mathbb{Z})[X]$ un polynôme unitaire de degré d, $i = 1, \ldots, s$. Montrer qu'il existe un polynôme $P \in \mathbb{Z}[X]$ irréductible, unitaire de degré d, tel que pour chaque i on ait $P \equiv P_i \bmod p_i$.

(b) Pour tout entier $n \geq 1$, montrer qu'il existe une extension galoisienne finie de $\mathbb{Q}$ de groupe de Galois $\mathfrak{S}_n$.

Indication: Un n-cycle, un $n-1$ cycle et une transposition engendrent toujours $\mathfrak{S}_n$.

Exercice 5* Soient k un corps de caractéristique $\neq 2$, $P := X^4 + aX^2 + b$ un polynôme irréductible de $k[X]$, et K une corps de décomposition de P sur k. Montrer que K/k est galoisienne, et que $\mathrm{Gal}(K/k)$ est isomorphe à :

i) $\mathbb{Z}/4\mathbb{Z}$ si, et seulement si, $\frac{a^2-4b}{b}$ est un carré dans k,
ii) $(\mathbb{Z}/2\mathbb{Z})^2$ si, et seulement si, b est un carré dans k.
iii) D_4, les isométries du carré, sinon.

Indication: On pourra introduire les racines $\pm\alpha, \pm\beta$ de P dans K et considérer $\alpha/\beta - \beta/\alpha$ et $\alpha\beta$.

Exercice 6 (Équations de degré 4)

(a) Montrer que tout sous-groupe transitif strict de $\mathfrak{S}_4$ est l'un des groupes suivants :
i) le sous-groupe alterné $\mathfrak{A}_4$,
ii) le sous-groupe de Klein $V_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2$, engendré par les doubles de transpositions,
iii) un 2-Sylow de $\mathfrak{S}_4$ (qui est isomorphe au groupe D_4 des isométries d'un carré),
iv) le groupe cyclique engendré par un 4-cycle.

On fait agir $\mathfrak{S}_4$ par automorphismes d'anneaux sur $R := \mathbb{Z}[X_1, X_2, X_3, X_4]$ de manière usuelle, i.e. par permutations des X_i. Si $Q \in R$, on note $D(Q)$ le sous-groupe de $\mathfrak{S}_4$ composé des éléments fixant Q.

(b) Soit $P := X_1X_2 + X_3X_4 \in R$, montrer que $D(P)$ est un 2-Sylow de $\mathfrak{S}_4$ et que l'orbite de $P \in R$ sous $\mathfrak{S}_4$ a trois éléments. On pose $P' := (23).P$ et $P'' := (24).P$, vérifier que $D(P')$ et $D(P'')$ sont les stabilisateurs des deux autres 2-Sylow de $\mathfrak{S}_4$.

(c) On considère la résolvante : $Q := (T-P)(T-P')(T-P'') \in R[T]$. Soient Σ_0,...,Σ_3 les polynômes symétriques élémentaires[9] en les X_i, vérifier ou admettre que :

$$Q(T) = T^3 - \Sigma_2 T^2 + (\Sigma_1\Sigma_3 - 4\Sigma_0)T - (\Sigma_0(\Sigma_3^2 - 2\Sigma_2) + \Sigma_1^2 - 2\Sigma_0\Sigma_2)$$

(d) Soit $C = \langle (1234) \rangle \subset D(P')$, montrer que C est exactement le sous-groupe de $D(P')$ fixant le polynôme $X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_1^2$.

Soient k un corps, $P \in k[X]$ un polynôme irréductible, séparable, de degré 4, K le corps de décomposition de P sur k, et $x_1, x_2, x_3, x_4 \in K$ les racines de P dans K.

(d) Montrer que $\mathrm{disc}(P) = \mathrm{disc}(Q)$, puis que $Q(T)(x_1, x_2, x_3, x_4) \in k[T]$ est séparable.

(e) Montrer que $\mathrm{Gal}(K/k)$ est inclus dans un 2-Sylow de $\mathfrak{S}_4$ si, et seulement si, le polynôme $Q(T)(x_1, x_2, x_3, x_4)$ a une racine dans k.

(f) Donner un algorithme pour calculer le groupe de Galois de P.

(g) En déduire le groupe de Galois sur $\mathbb{Q}$ des polynômes suivants :

$$X^4 + 2X^2 + 2, \quad X^4 + 3X^3 + 3X^2 + 3X + 3.$$

Données: Le second vaut $(X+6)(X-1)(X^2+11X+6)$ modulo 13.

Formulaire :

$$\mathrm{disc}(X^2 + aX + b) = a^2 - 4b$$
$$\mathrm{disc}(X^3 + aX + b) = -4a^3 - 27b^2$$
$$\mathrm{disc}(X^n + aX + b) = (n-1)^{n-1}(-1)^{\frac{(n-1)(n-2)}{2}}a^n + n^n(-1)^{\frac{n(n-1)}{2}}b^{n-1}$$
$$\mathrm{disc}(X^n - b) = n^n b^{n-1}(-1)^{\frac{(n-1)(n-2)}{2}}$$
$$\mathrm{disc}(X^3 + aX^2 + bX + c) = -27c^2 + 18abc + a^2b^2 - 4a^3c - 4b^3$$
$$\mathrm{disc}(X^4 + aX^2 + c) = 4^2c(-4c + a^2)^2$$
$$\mathrm{disc}(X^4 + aX^2 + bX + c) = -3^3b^4 + 2^8c^4 - 4a^3b^2 + 2^4a^4c - 2^7a^2c^2 + 3^2 2^4 acb^2$$

Exercice 7 Soient $n \in \mathbb{N}$ et k un corps contenant une racine primitive n^{ieme} de l'unité que l'on note ω. On pose

$$K := k(\{X_i\}_{i \in \mathbb{Z}/n\mathbb{Z}}), \quad Y_j := \sum_{i \in \mathbb{Z}/n\mathbb{Z}} \omega^{ij} X_i \in K,$$

[9] On rappelle que $\prod_{i=1}^4 (T - X_i) = \sum_{i=0}^4 (-1)^{4-i}\Sigma_i T^i$

et on considère l'action de $\mathbb{Z}/n\mathbb{Z}$ sur K définie par $m.X_i = X_{i+m}$.

(a) Montrer que $K = k(\{Y_j\}_{j\in\mathbb{Z}/n\mathbb{Z}})$.

(b) Montrer que $K^{\mathbb{Z}/n\mathbb{Z}} = k(\{\frac{Y_jY_1}{Y_{j+1}}\}_{j\in\mathbb{Z}/n\mathbb{Z}})$.

Exercice 8* (Une preuve par la théorie de Galois du théorème de structure des polynômes symétriques.) Soit $n \geq 1$, pour $0 \leq i \leq n-1$, les $\Sigma_i \in \mathbb{Z}[X_1, \ldots, X_n]$ sont définis par la formule

$$\prod_{i=1}^{n}(X - X_i) = X^n + \sum_{i=0}^{n-1}(-1)^{n-i}\Sigma_i X^i.$$

Si A est un anneau intègre, on considèrera l'action habituelle de $\mathfrak{S}_n$ par permutations des X_i sur l'anneau $A[X_1, \ldots, X_n]$ et sur son corps de fractions $A(X_1, \ldots, X_n)$.

(a) Montrer que $\mathbb{Q}(X_1, \ldots, X_n)^{\mathfrak{S}_n} = \mathbb{Q}(\Sigma_0, \ldots, \Sigma_{n-1})$.

(b) Montrer que les Σ_i sont algébriquement indépendants sur $\mathbb{Q}$.

Indication: Vérifier par exemple que l'application $\mathbb{C}^n \to \mathbb{C}[X]_{\leq n-1}, x \mapsto \prod_{i=1}^{n}(X - x_i) - X^n$ est un difféomorphisme local, donc ouverte, en tout point $x = (x_i)$ tel que $x_i \neq x_j$ si $i \neq j$. Cela pourrait se déduire aussi directement du (a) par un argument de différentielles algébriques : cf. par exemple Lang - Algebra 3ed - VIII.§5.

(c) Montrer que $\mathbb{Q}[X_1, \ldots, X_n]^{\mathfrak{S}_n} = \mathbb{Q}[\Sigma_0, \ldots, \Sigma_{n-1}]$.

Indication: On pourra remarquer qu'un élément de $\mathbb{Q}[X_1, \ldots, X_n]$ est annulé par un polynôme unitaire à coefficients dans l'anneau $\mathbb{Q}[\Sigma_0, \ldots, \Sigma_{n-1}]$, qui est factoriel par (b), et utiliser (a).

(d) En déduire de même que $\mathbb{Z}[X_1, \ldots, X_n]^{\mathfrak{S}_n} = \mathbb{Z}[\Sigma_0, \ldots, \Sigma_{n-1}]$.

Exercice 9* Soit $n \geq 2$ un entier. On considère l'action usuelle de $\mathfrak{S}_n$ sur $A := \mathbb{Z}[X_1, \ldots, X_n]$ et $A_{\mathbb{Q}} := \mathbb{Q}[X_1, \ldots, X_n]$, et on pose $\delta := \prod_{i<j}(X_i - X_j)$. Vérifier que l'on a $\delta^2 \in A^{\mathfrak{S}_n}$, $p := \prod_{i<j}(X_i + X_j) \in A^{\mathfrak{S}_n}$, puis montrer que

$$A_{\mathbb{Q}}^{\mathfrak{A}_n} = A_{\mathbb{Q}}^{\mathfrak{S}_n}[\delta], \quad A^{\mathfrak{A}_n} = A^{\mathfrak{S}_n}[\delta] + A^{\mathfrak{S}_n}\frac{\delta(\delta - p)}{2}.$$

Exercice 10** On considère l'action usuelle de $\mathfrak{S}_4$ sur $A := \mathbb{Q}[X_1, X_2, X_3, X_4]$, et $G \subset \mathfrak{A}_4$ le sous-groupe à 4 éléments engendré par les doubles transpositions. Vérifier que :

$$A^{\mathfrak{A}_4}[\{s(P), s \in \mathfrak{A}_4\}] \subset A^G,$$

où $P := X_1X_2 + X_3X_4$. A-t'on égalité ?

CHAPITRE 3

Algèbre Commutative

26 Avril 2004

T.D. n^o 8 du cours d'Algèbre II

Hormis dans l'exercice 10, tous les anneaux considérés dans ce TD sont supposés commutatifs unitaires.

Exercice 1 Parmi ces nombres algébriques sur $\mathbb{Q}$, lesquels sont entiers sur $\mathbb{Z}$?

$$\frac{1}{5},\ 1+2i,\ \frac{3+4i}{5},\ \frac{1+\sqrt{3}}{2},\ \frac{1+\sqrt{5}}{2},\ e^{2i\pi/n},\ 2\cos(2\pi/n),\ \cos(2\pi/n)$$

Exercice 2 Montrer que $\mathbb{Z}[2i]$ et $\mathbb{C}[T^2, T^3]$ ne sont pas intégralement clos.

Exercice 3 Soient A un anneau intègre, intégralement clos, de corps de fractions K, et L/K une extension finie de K.

(a) Montrer[1] que $x \in L$ est entier sur A si, et seulement si, le polynôme minimal unitaire de x est dans $A[X]$.

Indication: Soient P le polynôme minimal de x sur K et $x_1, \ldots, x_n$ ses racines dans une clôture algébrique de L, montrer que les x_i sont entiers sur A.

Pour $x \in L$, on note $m_x : L \to L$ le K-endomorphisme de multiplication par x, et $\chi_x := \det(T - m_x) \in K[T]$ son polynôme caractéristique[2].

(b) Montrer que χ_x est une puissance du polynôme minimal de x sur K.

(c) En déduire que x est entier sur A si, et seulement si, $\chi_x \in A[X]$.

Exercice 4

(a) Montrer que $\mathbb{Z}[i\sqrt{5}]$ est intégralement clos.

(b) Montrer qu'il n'est pas factoriel.

Exercice 5 Dans les deux cas suivants, en utilisant l'exercice 3 (c), déterminer le sous-anneau formé des éléments de K entiers sur A.

(a) $K = \mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z}$ est sans facteur carré, $A = \mathbb{Z}$.

(b) $K = \mathbb{C}(x, \sqrt{P(x)})$, où $P \in \mathbb{C}[X]$ est sans facteur carré, $A = \mathbb{C}[X]$.

Exercice 6* (L'analogue du théorème de l'élément primitif est faux sur $\mathbb{Z}$) Soient $K_i := \mathbb{Q}(\sqrt{-7})$, $K_2 = \mathbb{Q}(\sqrt{17})$, et $K_3 := K_1K_2$. On note A_i le sous-anneau de K_i composé des éléments entiers sur $\mathbb{Z}$.

(a) Montrer que l'anneau $A_i/2A_i$ est isomorphe à $\mathbb{F}_2 \times \mathbb{F}_2$ si $i = 1, 2$ (utiliser 5 (a)).

[1] En première approche, on pourra supposer que A est factoriel, ce qui est suffisant pour de nombreuses applications.

[2] Si $\chi_x = T^n - a_1T^{n-1} + \ldots + (-1)^n a_n$, alors $a_1 = \mathrm{tr}(m_x) \in K$ (resp. $a_n := \det(m_x) \in K$) est appelée *L/K-trace (resp. L/K norme) de x*, on les note respectivement $\mathrm{tr}_{L/K}(x)$ et $N_{L/K}(x)$. Il est clair que $\mathrm{tr}_{L/K} : L \to K$ est K-linéaire, et que $N_{L/K}$ induit un morphisme de groupes $L^* \to K^*$.

(b) Pour $i = 1, 2$, montrer que le morphisme d'anneaux naturel $\varphi_i : A_i/2A_i \to A_3/2A_3$ est injectif, puis que $\mathrm{Im}(\varphi_1) \cap \mathrm{Im}(\varphi_2) = \mathbb{F}_2.1$.

(c) Soit B une $\mathbb{F}_2$-algèbre de dimension 4 sur $\mathbb{F}_2$ qui contient au moins trois idempotents[3], montrer que B est isomorphe à l'anneau produit $(\mathbb{F}_2)^4$.

(d) En déduire que A_3 n'est pas de la forme $\mathbb{Z}[x]$ avec $x \in K$.

Remarques: On pourrait montrer ici que A_3 est l'anneau engendré par A_1 et A_2. Cependant, si K_1 et K_2 sont des extensions finies de $\mathbb{Q}$, l'inclusion $A_{K_1}.A_{K_2} \subset A_{K_1K_2}$ peut être stricte en général. On peut montrer qu'il y a égalité si les discriminants des formes quadratiques $(\mathrm{tr}_{K_i/\mathbb{Q}})_{|A_{K_i}}$ sont premiers entre eux. C'est en fait ce qui se produit dans cet exercice (ils valent respectivement -7 et 17).

Exercice 7* Montrer que $\mathbb{Z}[\sqrt[3]{2}]$ est intégralement clos.
Indication: Utiliser l'exercice 3.

Exercice 8 Soient $K/\mathbb{Q}$ une extension finie, $\mathcal{O}_K \subset K$ le sous-anneau des éléments entiers sur $\mathbb{Z}$. Nous allons montrer que $\mathcal{O}_K$ est noethérien, de groupe additif libre de rang $[K : \mathbb{Q}]$.

Soit $X := \mathrm{Hom}_{\mathrm{corps}}(K, \mathbb{C})$, $G := \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ agit sur X par $(c, \varphi) \mapsto c \circ \varphi$. On note $\sigma_1, \ldots, \sigma_{r_1+r_2}$ un système de représentants des orbites pour cette action, de sorte que $X^G = \mathrm{Hom}_{\mathrm{corps}}(K, \mathbb{R}) = \{\sigma_1, \ldots, \sigma_{r_1}\}$. On considère le morphisme d'anneaux

$$\varphi : K \to V := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \quad z \mapsto (\sigma_1(z), \ldots, \sigma_{r_1+r_2}(z)).$$

(a) Si $K = \mathbb{Q}(i)$ ou $\mathbb{Q}(\sqrt{2})$, vérifier que $\Gamma := \varphi(\mathcal{O}_K)$ est un sous-groupe discret du $\mathbb{R}$-espace vectoriel V, tel que V/Γ est compact (on dit que Γ est un *réseau* de V).

(b) Montrer que φ est injectif, et que le $\mathbb{R}$-espace vectoriel engendré par $\varphi(K)$ est égal à V.

(c) Montrer que $\varphi(\mathcal{O}_K)$ est un réseau de V.

(d) Conclure.

Remarques: En fait, on pourrait vérifier que la $\mathbb{R}$-algèbre $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ est isomorphe à $K \otimes_{\mathbb{Q}} \mathbb{R}$, de sorte que l'on aurait pu considérer à la place de φ le morphisme canonique $K \to K \otimes_{\mathbb{Q}} \mathbb{R}$.

L'exercice suivant redonne une démonstration du résultat de l'exercice 8 dans un cadre plus général.

Exercice 9 Soient A un anneau intègre, noethérien et intégralement clos, et L une extension finie séparable de K. On note B le sous-anneau de L des éléments entiers sur A. On veut montrer que B est un A-module de type fini, et que c'est un anneau noethérien.

Si $x \in L$, on note m_x l'endomorphisme K-linéaire de L défini par $y \mapsto xy$. On pose $\mathrm{tr}_{L/K}(x) := \mathrm{tr}(m_x)$ et $\chi_{L/K}(x) := \det(T - m_x) \in K[T]$.

(a) Montrer que $\mathrm{tr} : L \times L \longrightarrow K$, $(x, y) \mapsto \mathrm{tr}_{L/K}(xy)$, est une forme bilinéaire symétrique non dégénérée.

[3]Un idempotent d'un anneau est un élément satisfaisant $e^2 = e$.

(b) Montrer que $\mathrm{tr}_{L/K}(B) \subset A$.

(c) Montrer que L possède une K-base constituée d'éléments de B. Soit M le sous A-module de L engendré par une telle base.

(d) Montrer que $M^* := \{x \in L,\ \forall m \in M, \mathrm{tr}(xm) \in A\}$ est un sous A-module de L de type fini sur A, et que $M \subset B \subset M^*$.

(e) Conclure.

Exercice 10 (Exemples de cas "non commutatifs" où les entiers ne forment pas un anneau)

(a) Décrire les éléments de $M_2(\mathbb{Q})$ entiers sur $\mathbb{Z}$. Montrer qu'ils ne forment pas un anneau, pas même un sous-groupe additif.

(b) Montrer que $M_2(\mathbb{Z})$ est un sous-anneau maximal (pour l'inclusion) de $M_2(\mathbb{Q})$ composé d'éléments entiers sur $\mathbb{Z}$. Montrer que tout autre sous-anneau d'entiers maximal de $M_2(\mathbb{Q})$ est de la forme $gM_2(\mathbb{Z})g^{-1}$ pour un $g \in M_2(\mathbb{Q})$.

Soit $\mathbb{H}_\mathbb{Q} := \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ l'algèbre des quaternions usuels sur $\mathbb{Q}$ (*i.e.* satisfaisant $i^2 = -1$, $j^2 = -1$ et $ij = -ji = k$).

(a') Montrer que dans $\mathbb{H}_\mathbb{Q}$, les éléments entiers sur $\mathbb{Z}$ ne forment pas un sous-anneau, pas même un sous-groupe additif.

(b'*) Soit $\mathbb{H}_\mathbb{Z} := \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k + \mathbb{Z}\frac{1+i+j+k}{2} \subset \mathbb{H}_\mathbb{Q}$ ("les quaternions de Hurwitz"), montrer que c'est un sous-anneau d'entiers maximal de $\mathbb{H}_\mathbb{Q}$. Montrer que tout autre sous-anneau d'entiers maximal lui est conjugué (difficile).

La série d'exercice qui suit est un premier pas vers une compréhension de la normalité d'un point de vue géométrique.

Exercice 11 (Localisation de la normalité) Soient A un anneau intègre, K son corps de fractions. Si m est un idéal premier de A, on pose

$$A_m := \{a/b, a \in A, b \in A\backslash m\} \subset K.$$

(a) Montrer que A_m est un sous-anneau de K contenant A, de corps de fractions K.

(b) Montrer que A_m est noethérien (resp. intégralement clos) si A l'est.

Indication: On pourra remarquer que tout idéal I de A_m est engendré par $I \cap A$.

(c) Montrer que A_m est local d'idéal maximal mA_m, et que $mA_m \cap A = m$.

(d) Montrer que $A = \bigcap_{m \in \mathrm{Max}(A)} A_m$, $\mathrm{Max}(A)$ désignant l'ensemble des idéaux maximaux de A.

(e) En déduire que A intégralement clos si, et seulement si, tous les A_m, $m \in \mathrm{Max}(A)$, le sont.

Exercice 12 (normalité des courbes planes aux points lisses) Soient k un corps algébriquement clos, $Q \in k[X,Y]$ un polynôme irréductible, et $C := \{(x,y) \in k^2,\ Q(x,y) = 0\}$. On considère l'anneau $k[C] := k[X,Y]/(Q)$.

(a) Montrer que $k[C]$ est un anneau intègre, noethérien.

(b) Soit $P \in C$, vérifier que l'application $k[C] \to k$, $\overline{f} \mapsto f(P)$ est bien définie, et que c'est un morphisme surjectif d'anneau.

On note m_P l'idéal maximal noyau (justifier), vérifier que m_P est engendré comme $k[C]$-module par $\overline{X}$ et $\overline{Y}$.

(c) Montrer que tout idéal maximal de $k[C]$ est de la forme m_P pour un unique $P \in C$.

Un point $P = (x_0, y_0) \in C$ est dit *lisse*[4] si $(\frac{\partial P}{\partial X}(x_0, y_0), \frac{\partial P}{\partial Y}(x_0, y_0)) \neq (0, 0)$.

(d) Montrer que si P est lisse, $m_P k[C]_{m_P}$ est un idéal principal de $k[C]_{m_P}$ et $k[C]_{m_P}$ est principal. En particulier, $k[C]_{m_P}$ est intégralement clos.

Indication: Utiliser le résultat de l'exercice 14 (b).

(e) Conclure que si C est lisse[5], alors $k[C]$ est un anneau intégralement clos.

(f) (Exemple) Soient $P \in k[X]$ à racines distinctes, $n \geq 1$ un entier inversible dans k, montrer que $k[X, Y]/(Y^n - P(X))$ est un anneau intégralement clos.

Remarques: Il se trouve que les réciproques de (f) et (g) sont aussi vraies, ce qui fournit un critère géométrique de normalité dans le cas des anneaux de courbes planes.

Exercice 13 (Deux exemples) Soit k un corps algébriquement clos de caractéristique $\neq 2, 3$.

(a) Montrer que $A := k[T^2, T^3]$ est isomorphe comme k-algèbre à $k[X, Y]/(X^3 - Y^2)$.

(b) Vérifier que la courbe plane $x^3 = y^2$ est lisse hors du "cusp" $(0, 0)$.

(c) En déduire que tous les A_{m_P} sont intégralement clos, sauf $A_{m_{(0,0)}}$ qui ne l'est pas.

(d) Soit $B := k[X, Y]/(Y^2 - X^3 - X)$. Montrer que B est intégralement clos, et que B_m est principal pour tout idéal maximal m.

(e*) Vérifier cependant que l'idéal maximal $m_{(0,0)}$ de B n'est pas principal[6].

Indication: On pourra remarquer que si $m_{(0,0)} = (\overline{f})$, $f \in k[X, Y]$, alors $f = 0$ ne rencontre la courbe $y^2 = x^3 - x$ qu'en $(0, 0)$.

Exercice 14 (Critères de principalité) Soit A un anneau intègre, noethérien.

(a) Si tout idéal maximal de A est principal, montrer que A est principal.

(b) Supposons A local d'idéal maximal m. Montrer que A est principal si, et seulement si, m/m^2 est de dimension 1 vu comme A/m espace vectoriel.

Indication: Utiliser le lemme de Nakayama.

---

[4]Si $k = \mathbb{C}$ et C est lisse en P, alors le théorème des fonctions implicites appliqué à l'une des coordonnées x ou y montre que C admet une paramétrisation holomorphe au voisinage de P. On pourrait voir que cela permet de définir une structure de variété complexe de dimension 1 sur C^{lisse}. Il n'est pas difficile de montrer qu'il n'y a au plus qu'un nombre fini de points non lisse dans C. Il est par contre relativement difficile de montrer que l'irréductibilité de $Q(X, Y)$ entraîne que C est connexe par arc.

[5]I.e. si tous les points de C sont lisses.

[6]En fait aucun idéal maximal de B n'est principal.

5 et 12 Mai 2004

T.D. n^o 9 du cours d'Algèbre II

Exercice 1 Soient k un corps algébriquement clos, $P \in k[X_1, \ldots, X_n]$ un polynôme irréductible.

(a) Montrer que si $Q \in k[X_1, \ldots, X_n]$ s'annule sur les zéros de P dans k^n, alors[7] P divise Q dans $k[X_1, \ldots, X_n]$.

On fixe maintenant P, $Q \in k[X, Y]$ avec P irréductible et Q non divisible par P.

(b) Montrer qu'il existe A, $B \in k[X, Y]$ et $C \in k[X]\backslash\{0\}$ tels que $AP + BQ = C$.

(c) En déduire que les courbes planes $V(P)$ et $V(Q)$ ne s'intersectent qu'en un nombre fini de points, et retrouver (a) dans le cas $n = 2$ sans utiliser le Nullstellensatz.

(d) Montrer que la topologie de Zariski sur une courbe plane $V(P) \subset k^2$ est l'unique topologie dont les fermés stricts sont les ensembles finis[8].

Exercice 2 Soient k un corps et P un idéal premier non nul de $k[X, Y]$. Montrer que soit P est principal engendré par un polynôme irréductible, soit P est maximal [9].

Indication: Utiliser l'exercice 1 (b).

Exercice 3 Soit k un corps algébriquement clos. Soit a, b, c et d la k-base usuelle de $\mathrm{Hom}_k(\mathrm{M}_2(k), k)$; elle identifie les fonctions polynomiales sur $\mathrm{M}_2(k)$ à $k[a, b, c, d]$. On pose

$$N := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(k[a, b, c, d]),$$

et pour $n \geq 2$ on considère l'idéal I_n de $k[a, b, c, d]$ engendré par les quatre coefficients de la matrice N^n. On pose de plus $I_1 := (a + d, ad - bc) \subset k[a, b, c, d]$.

(a) Montrer que $V(I_n) \subset \mathrm{M}_2(k)$ est indépendant de $n \geq 1$, et le décrire.

(b) Montrer que I_1 est premier, puis que pour tout $n \geq 1$ on a $\sqrt{I_n} = I_1$.

(c) Montrer que si $n \geq 1$, $I_{n+1} \subsetneq I_n$. En particulier, I_n n'est pas radical si $n > 1$.

Indication: Pour montrer que l'inclusion est stricte, on pourra considérer des solutions aux systèmes polynomiaux en question dans des anneaux de la forme $k[t]/(t^r)$.

---

[7] Si k n'est pas algébriquement clos, ce résultat n'est pas toujours vrai, car le lieu des zéros de P peut être vide comme le montre l'exemple de $k = \mathbb{R}$, $P = X^2 + Y^2 + 1$.

[8] En particulier, cette topologie est très faible : deux courbes planes quelconques sont homéomorphes...

[9] La dimension (de Krull) d'un anneau A est le sup. des entiers n tels qu'il existe une chaine d'idéaux *premiers* $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n \subsetneq A$. Cet exercice montre que $k[X, Y]$ est de dimension 2 si k est un corps. On montrerait facilement que les corps sont de dimension nulle, les anneaux principaux de dimension 1, et que $k[X_1, \ldots, X_n]$ de dimension $\geq n$ si k est un corps. Cette dernière inégalité est en fait toujours une égalité, mais ça n'est pas évident.

Exercice 4 (Espaces noethériens) Soit X un espace topologique[10]. On dit que X est *irréductible* s'il n'est pas réunion de deux de ses fermés stricts. On dit qu'il est *noethérien* si toute suite décroissante de fermés de X stationne.

(a) Montrer les équivalences :

i) X est irréductible,

ii) tout ouvert de X est dense.

iii) tout ouvert de X est connexe,

Vérifier de plus qu'un ouvert d'un espace irréductible est encore irréductible, que l'adhérence d'une partie irréductible de X est encore irréductible, et que l'image d'un irréductible par une application continue est aussi irréductible.

(b) Montrer que X est noethérien si, et seulement si, tout ensemble non vide de fermé de X a un élément minimal pour l'inclusion.

Vérifier de plus que si X est noethérien, alors toute partie de X, munie de sa topologie de sous-espace, est noethérienne. Montrer enfin qu'un espace topologique noethérien est quasi-compact, i.e. que de tout recouvrement ouvert de X on peut extraire un sous-recouvrement fini[11].

(c) Si X est un espace noethérien, montrer qu'il existe un nombre fini de fermés irréductibles $F_1, \ldots, F_n \subset X$, tels que

$$X = \bigcup_{i=1}^{n} F_i, \quad \text{et} \quad \mathrm{i} \neq \mathrm{j} \Rightarrow \mathrm{F_i} \not\subseteq \mathrm{F_i}.$$

Vérifier que tout fermé irréductible de X est inclus dans l'un des F_i, qu'aucun des F_i ne peut être omis dans la réunion précédente, puis que les F_i sont exactement les fermés irréductibles maximaux de X : on les appelle les *composantes irréductibles de* X.

Indication: Commencer par montrer tout fermé de X est réunion finie de fermés irréductibles.

(d) Soit k un corps algébriquement clos. Montrer que :

i) k^n est noethérien, irréductible, connexe, ainsi que tous ses ouverts.

ii) un fermé $V(I) \subset k^n$ est irréductible si, et seulement si, $\sqrt{I}$ est un idéal premier,

iii) les points de k^n sont fermés.

(e) Trouver les composantes irréductibles (resp. connexes) de $V(I)$ dans les cas suivants :

i) $I = (P), P \in k[X_1, \ldots, X_n]$,

ii) $I = (Y, Y^2 - XZ) \subset k[X, Y, Z]$,

iii) $I = (X(Y - X^2 + 1), Y(Y - X^2 + 1)) \subset k[X, Y]$.

Exercice 5 Soit k un corps algébriquement clos.

[10]Les notions étudiées dans cet exercice ne sont pas adaptées aux espaces séparés (on vérifie aisément qu'un espace séparé irréductible est réduit à un point, un espace nothérien séparé est fini et discret), ni donc aux espaces métriques.

[11]La différence avec *compact* est que l'on ne suppose pas que X est séparé.

(a) Montrer que $\mathrm{GL}_n(k)$ est un ouvert Zariski, dense dans $\mathrm{M}_n(k)$.

(b) Montrer que le sous-ensemble de $\mathrm{M}_n(k)$ formé des matrices à valeurs propres distinctes est un ouvert Zariski dense.

(c) En déduire par un argument de densité Zariski que si K est un corps :

i) si $M \in \mathrm{M}_n(K)$, P_M le polynôme caractéristique de M, alors $P_M(M) = 0$,

ii) si $A, B \in \mathrm{M}_n(K)$, $P_{AB} = P_{BA}$.

Exercice 6 (Irréductibilité de la stratification par le rang) Soit k un corps algébriquement clos,

(a) Soit $A \in \mathrm{M}_n(k)$, $\varphi_A : \mathrm{M}_n(k) \times \mathrm{M}_n(k) \to \mathrm{M}_n(k)$, $(m_1, m_2) \mapsto m_1 A m_2$, vérifier que φ_A est polynomiale.

(b) Soit $1 \leq i \leq n$, $R_i \subset \mathrm{M}_n(k)$ le sous-ensemble des matrices de rang $\leq i$. Montrer que R_i est un fermé Zariski, et que si $i \leq n-1$, $R_{i+1} \backslash R_i$ est de la forme $\varphi_A(\mathrm{GL}_n(k))$ pour une certaine matrice A.

(c) En déduire que $R_{i+1} \backslash R_i$ est un ouvert Zariski dense, irréductible, de R_{i+1}, puis que les R_i sont irréductibles.

(d) En déduire que $\det(X_{i,j})$ est un polynôme irréductible dans $k[X_{i,j}]$. Montrer ce résultat directement.

(e) (Application) Soit $n = 3$, I l'idéal de $k[X_{i,j}]$ engendré par les 9 mineurs $(2,2)$, montrer que $\sqrt{I}$ est premier. Est-ce que $\sqrt{I} = I$? (difficile)

Exercice 7 (Anneaux de dimension 0 de type fini sur un corps) Soient k un corps, A une k-algèbre de type fini.

(a) Soient $m_1, \ldots, m_n$ des idéaux maximaux 2 à 2 distincts de A, $N \in \mathbb{N}$, montrer que l'application canonique $A/(m_1 \ldots m_n)^N \to \prod_{i=1}^n A/m_i^N$ est un isomorphisme d'anneaux.
Indication: Utiliser l'exercice 8 (c).

(b) Montrer que les conditions suivantes sont équivalentes :

i) A est un anneau artinien, i.e. toute suite décroissante d'idéaux de A stationne,

ii) $\mathrm{Rad}(A)$ est intersection d'un nombre fini d'idéaux maximaux de A,

iii) $\mathrm{Specmax}(A)$ est fini,

iii') $\mathrm{Hom}_{k-alg}(A, \overline{k})$ est fini,

iv) A est isomorphe comme k-algèbre à un produit fini de k-algèbres locales de type fini,

v) A est de dimension finie comme k-espace vectoriel,

v') Tout idéal premier de A est maximal.

Indication: On démontrera circulairement $i) \Leftrightarrow v)$, et à part les équivalences $\star \Leftrightarrow \star'$. On utilisera le lemme de normalisation de Noether pour $\star = v$.

Exercice 8 (Restes chinois) Soient A un anneau commutatif, I et J des idéaux de A premiers entre eux, i.e. tels que $I + J = A$.

(a) Montrer que le morphisme canonique d'anneaux $A \to A/I \times A/J$ est surjectif, de noyau $IJ = I \cap J$.

(b) Montrer que si I est premier avec J_1 et J_2, alors I est premier avec $J_1 J_2$.

(c) En déduire que si I_1, ..., I_n sont des idéaux deux à deux premiers entre eux, et $r_1, \ldots, r_n$ des entiers, alors le morphisme canonique d'anneaux

$$A \longrightarrow \prod_{i=1}^{n} A/I_i^{r_i},$$

est surjectif de noyau $\cap_{i=1}^n I_i^{r_i} = \prod_{i=1}^n I_i^{r_i}$.

Exercice 9 Soit A la $\mathbb{C}$-algèbre des fonctions rationnelles sur la droite qui sont bien définies en l'origine, i.e $\{a/b \in \mathbb{C}(X), a,\, b \in \mathbb{C}[X], b(0) \neq 0\}$.

(a) Montrer que A n'est pas de type fini comme $\mathbb{C}$-algèbre.

(b) Montrer que Specmax(A) est réduit à un élément, et que Rad(A) n'est pas constitué d'éléments nilpotents (comparer à l'exercice 7).

Exercice 10 (Une preuve rapide du Nullstellensatz dans le cas non dénombrable) Soient k un corps non dénombrable, K une k-algèbre de type fini qui est un corps.

(a) Soit $x \in K$ transcendant sur k, montrer que les $(\frac{1}{x-a})_{a \in k}$ forment une famille k-libre dans K.

(b) En déduire que K est une extension finie de k.

Remarques: Cela fournit donc une preuve dans le cas important où $k = \mathbb{C}$, mais ni pour $\overline{\mathbb{Q}}$, ni pour $\overline{\mathbb{F}}_p$.

Exercice 11

(a) Soient $k \subset K$ deux corps algébriquement clos, $P_1, \ldots, P_r$ une famille d'éléments de $k[X_1, \ldots, X_n]$. On suppose que les P_i ont un zéro commun dans K^n, montrer qu'ils en ont un dans k^n.

(b) En déduire que si $P \in k[X_1, \ldots, X_n]$ est irréductible, il l'est aussi dans $K[X_1, \ldots, X_n]$.

(c) Soient $P_1, \ldots, P_r \in \mathbb{Z}[T_1, \ldots, T_n]$, montrer les équivalences :

i) Les P_i ont un zéro commun dans $\mathbb{C}^n$,
ii) Les P_i ont un zéro commun dans $\overline{\mathbb{Q}}^n$,
iii) Pour tout nombre premier p assez grand, les P_i mod p ont un zéro commun dans $\overline{\mathbb{F}}_p^n$.

Indication: Pour ii) implique iii), on pourra montrer que si N est un entier et A est une $\mathbb{Z}[1/N]$-algèbre entière, alors pour tout nombre premier p ne divisant pas N, pA est un idéal strict de A.

Exercice 12 Soient k un corps et A la k-algèbre des suites $(x_n) \in k^{\mathbb{N}}$ qui sont constantes à partir d'un certain rang. Décrire l'espace topologique Specmax(A).

Exercice 13 Soient X un espace topologique compact et $C(X)$ l'anneau des fonctions complexes continues sur X. Pour $x \in X$, on note m_x l'idéal maximal (justifier) $\{f \in C(X), f(x) = 0\}$.

(a) Montrer que tout idéal maximal de $C(X)$ est de la forme m_x pour un unique $x \in X$.

Indication: On pourra d'abord remarquer que tout idéal maximal de $C(X)$ est fermé pour la topologie de la norme sup. sur $C(X)$.

(b) Montrer que l'application $\varphi : X \to \mathrm{Specmax}(C(X))$, $x \mapsto m_x$, est un homéomorphisme.

Les deux exercices qui suivent introduisent la notion de groupe algébrique.

Exercice 14 (groupes algébriques linéaires) Soit k un corps algébriquement clos.

(a) Montrer que $\mathrm{SL}_n(k) \subset \mathrm{M}_n(k)$ est un fermé Zariski, et que la multiplication $\mathrm{SL}_n(k) \times \mathrm{SL}_n(k) \to \mathrm{SL}_n(k)$ (resp. l'inversion $\mathrm{SL}_n(k) \to \mathrm{SL}_n(k)$) provient par restriction d'une application polynomiale $\mathrm{M}_n(k) \times \mathrm{M}_n(k) \to \mathrm{M}_n(k)$ (resp. $\mathrm{M}_n(k) \to \mathrm{M}_n(k)$).

Un sous-groupe de $\mathrm{SL}_n(k)$ qui est un fermé Zariski est dit *algébrique*. Il est clair qu'une intersection de sous-groupes algébriques est encore un sous-groupe algébrique.

(b) Soit f une forme bilinéaire sur k^n, on pose

$$\mathrm{SO}(f) := \{g \in \mathrm{SL}_n(k),\ \forall x,\ y \in k^n, f(gx, gy) = f(x, y)\}.$$

Vérifier que $\mathrm{SO}(f)$ est un sous-groupe algébrique de $\mathrm{SL}_n(k)$.

(c) Soit $G \subset \mathrm{SL}_n(k)$ un sous-groupe, $\overline{G}$ son adhérence pour la topologie de Zariski. Montrer que $\overline{G}$ est un sous-groupe algébrique de $\mathrm{SL}_n(k)$.

(d) Soit $G \subset \mathrm{SL}_n(k)$ un sous-groupe algébrique et H est une partie de $\mathrm{M}_n(k)$. Alors le centralisateur (resp. normalisateur) de H dans G est un sous-groupe algébrique. En particulier, le centre de G est un sous-groupe algébrique.

(e) Soit $G \subset \mathrm{SL}_n(k)$ un sous-groupe algébrique. Montrer que les composantes irréductibles de G sont des composantes connexes, et sont en nombre fini. En particulier, G est connexe si, et seulement si, G est irréductible.

Indication: On montrera d'abord que pour tout fermé algébrique $X \subset k^n$, il existe $x \in X$ qui est dans une seule composante irréductible de X.

(f) Montrer que la composante connexe de 1, noté usuellement G^0, est un sous-groupe distingué d'indice fini de G.

Ainsi, tout groupe algébrique linéaire est extension d'un groupe fini par un groupe algébrique connexe.

Exercice 15 (Application : un théorème de Burnside) Soit k un corps de caractéristique nulle, $G \subset \mathrm{GL}_n(k)$ un sous-groupe. On suppose que G est d'exposant fini, i.e. qu'il existe un entier N tel que pour tout $g \in G$, $g^N = 1$. On va montrer que G est fini.

(a) Montrer que l'on peut supposer que k est algébriquement clos, puis que $G \subset \mathrm{SL}_n(k)$ est un sous-groupe algébrique connexe.

(b) Montrer que l'application polynôme caractéristique $G \to k^n$ est constante.

(c) Conclure.

Exercice 16* (Théorème de comparaison de Riemann) Soit $P \in \mathbb{C}[X,Y]$ un polynôme irréductible, on va montrer que $\{(x,y) \in \mathbb{C}^2,\ P(x,y) = 0\}$ est un connexe de $\mathbb{C}^2$ pour la topologie usuelle.

Soit $S \subset \mathbb{C}$ un ensemble fini de points, H_S l'anneau intègre (justifier) des fonctions méromorphes sur $\mathbb{C}$ sans pôle hors de S.

(a) On note F_S le sous-anneau de H_S constitué de fractions rationnelles. Montrer que F_S est intégralement clos dans H_S, i.e. que si $f \in H_S$ est entier sur F_S, alors $f \in F_S$.
Indication: Si $f^n = \sum_{i=0}^{n-1} a_i f^i$ avec $a_i \in F_S$, $f \in H_S$, alors si $z \notin S$, $|f(z)| \leq (1 + \sum_{i=0}^{n-1} |a_i(z)|)$.

(b) En déduire que si $P \in F_S[T]$ est un polynôme unitaire irréductible, alors il reste irréductible dans $H_S[T]$.

On retourne à la problématique initiale. Quitte à faire un changement de variables linéaire $(x,y) \mapsto (x, \lambda x + y)$, on peut supposer que P est unitaire vu comme élément de $(\mathbb{C}[Y])[X]$ (justifier). On note d son degré et on considère alors la projection

$$p : V(P) \subset \mathbb{C}^2 \longrightarrow \mathbb{C},\ \ (x,y) \mapsto y.$$

(c) Montrer que sur un ouvert Zariski $\mathbb{C} - S := U$ de $\mathbb{C}$, la projection $p : p^{-1}(U) \to U$ est un revêtement à d feuillets.

(d) Soit Z une composante connexe de $p^{-1}(U)$. Considérons la fonction $\psi : \mathbb{C} - S \to \mathbb{C}[T]$ définie par

$$x \mapsto \prod_{z \in Z \cap p^{-1}(x)} (T - z).$$

Montrer que $\psi \in H_S[T]$.

(e) Conclure[12].

On termine par deux exemples.

i) Si $P = X^2 + Y^2 - 1$, montrer que $V(P)$ est homéomorphe[13] à $\mathbb{C}^*$.

ii) De même, si $P = Y^2 - (X^2 - 1)(X^2 - 2)$, montrer que $V(P)$ est homéomorphe à un tore $\mathbb{S}^1 \times \mathbb{S}^1$ privé de deux points.

Dans les deux cas, on pourra reconstituer $V(P)$ à partir de sa projection $V(P) \to \mathbb{C}$, $(x,y) \mapsto x$.

[12] On pourrait généraliser la preuve ci-dessus et montrer qu'en général "un fermé Zariski est connexe pour la topologie de Zariski si, et seulement si, il est connexe pour la topologie usuelle.". Ce résultat est le premier d'une longue série de "théorèmes de comparaison" en géométrie algébrique.

[13] Pour la topologie usuelle !

CHAPITRE 4

Représentations et théorie des invariants

17 Mai 2004

T.D. n^o 10 du cours d'Algèbre II

Exercice 1 (Le groupe symétrique comme groupe de reflexions) Soit $n \geq 2$ un entier. On considère le groupe $W := \mathfrak{S}_n$ agissant linéairement par permutations des coordonnées sur $\mathbb{R}^n$ euclidien, et V l'hyperplan des éléments dont la somme des coordonnées est nulle.

(a) Vérifier que V est stable par W et que $W \subset O(V)$ (justifier l'inclusion) est engendré par des reflexions.

(b) $\mathfrak{A}_n \subset W$ est-il aussi engendré par des reflexions ? par des éléments d'ordre 2 ? Si $1 \leq i \leq n-1$, on note s_i la reflexion orthogonale de V d'axe $e_i - e_{i+1}$. Montrer que les s_i engendrent W, que $s_i s_j = s_j s_i$ si $|i-j| > 1$, et que $s_i s_{i+1}$ est d'ordre 3 si $i < n-1$.

(c) Vérifier qu'aucun sous-espace strict de V n'est stable par W.

(d) On note x_i la restriction à V de la forme linéaire e_i^* sur $\mathbb{R}^n$, V^* est engendré par les x_i avec pour relation $\sum_{i=1}^n x_i = 0$. Montrer en utilisant l'exercice 2 que les $f_j := \sum_{i=1}^n x_i^j,\ j = 2 \ldots n$ engendrent l'algèbre des invariants $\mathrm{Sym}(V^*)^W$.

Remarques: On pourrait démontrer que les générateurs et relations du (b) sont une présentation de W. Le groupe $\mathfrak{S}_n$ vu comme ci-dessus comme sous-groupe de $O_{n-1}(\mathbb{R})$ est appelé "groupe de réflexions de type A_{n-1}".

Exercice 2 Soit k un corps de caractéristique 0 et $W \subset \mathrm{GL}_n(k)$ un groupe fini engendré par des réflexions. Soient $f_1, \ldots, f_n \in k[X_1, \ldots, X_n]^W$ des polynômes homogènes de degrés respectifs e_i.

Montrer que si $\prod_{i=1}^n e_i = |W|$ et si les f_i sont algébriquement indépendants, alors $k[X_1, \ldots, X_n]^W = k[f_1, \ldots, f_n]$ et les e_i sont les degrés de W.

Indication: On pourra montrer tout d'abord que les e_i sont les degrés de W.

Exercice 3 (Théorème de Hilbert-Noether) Soient k un corps, $A = k[x_1, \ldots, x_n]$ une k-algèbre de type fini, et $G \subset \mathrm{Aut}_{k-\mathrm{alg}}(A)$ un groupe fini d'automorphismes. On va montrer que A^G est une algèbre de type fini sur k (noter que l'on ne fait pas d'hypothèse sur la caractéristique du corps k et que A n'est pas nécessairement une algèbre de polynômes.).

(a) Pour $1 \leq i \leq n$, on pose $P_i(T) := \prod_{g \in G}(T - g(x_i)) \in A[T]$ et on note B la sous-k-algèbre de A engendrée par les coefficients des P_i. Montrer que B est de type fini comme k-algèbre et que $B \subset A^G$.

(b) Montrer que A est de type fini comme B-module, puis qu'il en va de même pour A^G.

(c) Conclure.

Exercice 4 (Groupes dihédraux) Soient $n \geq 3$ et $I_2(n) \subset O_2(\mathbb{R})$ le groupe des isométries d'un polygône régulier à n côtes de $\mathbb{R}^2$, centré en 0.

(a) Montrer que $I_2(n)$ est engendré par deux reflexions s et t telles que le produit st est d'ordre n.

(b) Soit $G = \langle s, t\rangle$ un groupe engendré par deux élément s et t d'ordre 2 tels que le produit st est d'ordre fini n. Montrer que $G \simeq I_2(n) \simeq \mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z}$. En particulier, G est fini d'ordre $2n$. Combien $I_2(n)$ contient-il de réflexions ?

(c*) En utilisant l'exercice 2, montrer que $\mathbb{R}[X,Y]^{I_2(n)} = \mathbb{R}[X^2+Y^2, \prod_{i=1}^n L_i]$, où les L_i sont homogènes de degrés 1 bien choisis.

On se propose de redémontrer de manière élémentaire le résultat du (c). Comme $I_2(n) \subset \mathrm{GL}_2(\mathbb{C})$, on peut considérer son action sur $\mathbb{C}[X,Y]$. On note $G_n \subset I_2(n)$ le sous-groupe des rotations.

(d) Déterminer $\mathbb{C}[X,Y]^{G_n}$, puis $\mathbb{C}[X,Y]^{I_2(n)}$.

Indication: On pourra se placer dans une base adéquate de $\mathbb{C}^2$.

(e) Retrouver le résultat du (c), ainsi que $\mathbb{R}[X,Y]^{G_n}$.

Exercice 5 (Cet exercice fait suite à l'exercice 4)

(a) Soient k un corps algébriquement clos, $G \subset \mathrm{GL}_n(k)$ un sous-groupe tel que $G^{ab} := G/D(G)$ est fini. Soient e l'exposant de G^{ab} et $f \in k[X_1, \ldots, X_n]$ un polynôme irréductible. Montrer que G préserve l'hypersurface $f = 0$ de k^n si, et seulement si, $f^e \in k[X_1, \ldots, X_n]^G$.

(b*) On considère l'action de $I_2(3) \subset O_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{C})$ induite sur $\mathbb{C}^2$. Existe-t-il une quartique irréductible de $\mathbb{C}^2$ stable par $I_2(3)$?

Exercice 6 Soient k un corps et $\mathrm{Aff}(k) \subset \mathrm{Aut}_{k-\mathrm{alg}}(k[X])$ le groupe des transformations affines, i.e. de la forme $X \mapsto aX + b$ avec $a \in k^*$ et $b \in k$.

(a) Montrer que $\mathrm{Aff}(k) = \mathrm{Aut}_{k-\mathrm{alg}}(k[X])$.

(b) Déterminer $k[X]^{\mathrm{Aff}(k)}$.

Indication: On commencera par déterminer les invariants par translation.

Exercice 7 (Groupes de type B_n et leurs invariants) Soient $n \geq 2$, e_i la base canonique de $\mathbb{R}^n$, et $W \subset O_n(\mathbb{R})$ le sous-groupe dont les éléments préservent l'ensemble $\{\pm e_i,\ 1 \leq i \leq n\}$.

(a) Montrer que le groupe W est engendré par des reflexions et qu'il ne stabilise aucun sous-espace strict de $\mathbb{R}^n$.

(b) Vérifier que c'est le produit semi-direct de $\mathfrak{S}_n$ par $(\mathbb{Z}/2\mathbb{Z})^n$ pour l'action de permutation $\mathfrak{S}_n \to \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^n)$, et en particulier que $|W| = 2^n n!$.

(c) Décrire $\mathbb{R}[X_1, \ldots, X_n]^W$.

Remarques: On pourrait démontrer que B_3 est le groupe des isométries euclidiennes d'un cube de $\mathbb{R}^3$, de même que $\mathfrak{S}_4 \subset O_3(\mathbb{R})$ (cf. exercice 1) est celui d'un tetraèdre régulier.

Exercice 8** Soit $W \subset O_3(\mathbb{R})$ le groupe des isométries d'un icosaèdre centré en 0.

(a) Montrer que W est un groupe engendré par des réflexions, isomorphe à $(\mathbb{Z}/2\mathbb{Z}) \times \mathfrak{A}_5$.

(b) Quels sont les degrés de W ?

Exercice 9 Faire les exercices 7 à 10 du TD 7.

24 Mai 2004

T.D. n^o 11 du cours d'Algèbre II

Dans ce TD, le terme *représentation* signifiera par défaut "représentation linéaire sur un $\mathbb{C}$-espace vectoriel de dimension finie".

Exercice 1 Montrer que les représentations irréductibles d'un groupe abélien, et plus généralement d'une $\mathbb{C}$-algèbre commutative, sont de dimension 1.

Exercice 2

(a) Trouver une représentation irréductible de dimension 2 de $\mathfrak{S}_3$. Plus généralement, trouver une représentation irréductible de dimension $n-1$ de $\mathfrak{S}_n$, $n \geq 2$.

(b) Trouver une représentation irréductible de dimension 2 du groupe dihédral D_{2n}, $n \geq 3$.

Exercice 3

(a) Trouver une représentation non semi-simple, de dimension 2, du groupe $\mathbb{Z}$.

(b) Soit $r : \mathbb{C}[X] \to \mathrm{M}_n(\mathbb{C})$ une représentation, à quelle condition sur $r(X)$ est-elle semi-simple ?

Exercice 4 Soit G un groupe fini. On regarde l'anneau $\mathbb{C}[G]$ comme un $\mathbb{C}[G]$-module à gauche. On écrit alors $\mathbb{C}[G] \simeq \oplus_{i=1}^r V_i^{m_i}$, où les V_i sont des représentations irréductibles de G qui sont 2 à 2 non isomorphes (justifier).

(a) Montrer que toute représentation irréductible de G est isomorphe à l'une des V_i.

(b) Montrer que $m_i \geq \dim(V_i)$, puis que $\sum_{i=1}^r \dim(V_i)^2 \leq |G|$.

Indication: Considérer le morphisme naturel de $\mathbb{C}$-algèbres $\mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V_i)$.

Remarques: Il n'est pas très difficile de montrer qu'en fait $m_i = \dim_{\mathbb{C}}(V_i)$ (cf. par exemple le problème à la fin de ce TD), et donc que la dernière inégalité est en fait une égalité.

Exercice 5 En utilisant l'exercice 4,

(a) Trouver toutes les représentations irréductibles des groupes $\mathfrak{S}_3$, D_8 et $\mathbb{H}_8$.

(b) Montrer que $\mathfrak{S}_4$ a 5 représentations irréductibles et les réaliser explicitement.

Exercice 6 (Un théoreme de Lie-Kolchin) Soit $\Gamma \subset \mathrm{GL}_n(\mathbb{C})$ un sous-groupe dont tous les éléments sont unipotents, i.e. $(\gamma - 1)^n = 0$, $\forall \gamma \in \Gamma$. On veut montrer que les éléments de Γ sont cotrigonalisables (en particulier, Γ est résoluble).

(a) Montrer qu'il suffit de montrer que si Γ agit de plus irréductiblement sur $\mathbb{C}^n$, alors $n = 1$. On le suppose désormais.

(b) Montrer que la forme bilinéaire sur $\mathrm{M}_n(\mathbb{C})$: $(A, B) \mapsto \mathrm{tr}(AB)$ est non dégénérée.

(c) Montrer que pour tous $\gamma, \gamma' \in \Gamma$, $\mathrm{tr}((\gamma - 1)\gamma') = 0$.

(d) Conclure.

Exercice 7* (Un théorème de Burnside) Soient k un corps de caractéristique 0 et $\Gamma \subset \mathrm{GL}_n(k)$. On suppose qu'il existe $m \geq 1$ tel que $\forall \gamma \in \Gamma,\ \gamma^m = 1$. Montrer que Γ est fini.

Indication: Utiliser une méthode semblable à celle de l'exercice 6.

Exercice 8 (Dual d'un groupe abélien fini) Un morphisme de groupes $G \to \mathbb{C}^*$ est appelé *caractère de dimension* 1 de G. On note $\widehat{G} := \mathrm{Hom}_{\mathrm{gr}}(G, \mathbb{C}^*)$ leur ensemble, la loi de groupe sur $\mathbb{C}^*$ en fait un groupe abélien. On note de plus $A(G)$ la $\mathbb{C}$-algèbre des fonctions sur G à valeurs complexes, que l'on munit du produit hermitien (justifier) :

$$\langle f,\, f' \rangle = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{f'(g)}$$

(a) On note $r : G \to \mathrm{GL}(A(G))$ la représentation par translations à droite définie par $r(g).f = (h \mapsto f(hg))$. Montrer que les $r(g)$, $g \in G$ sont unitaires pour le produit hermitien $\langle , \rangle$.

(b) On suppose désormais que G est un groupe abélien. Montrer que $A(G) = \oplus_{\chi \in \widehat{G}} \mathbb{C}.\chi$ et que la somme est orthogonale.

Indication: On pourra réduire simultanément les $r(g), g \in G$.

(c) En déduire que $|\widehat{G}| = |G|$ et que l'accouplement de dualité naturel

$$(.\,,.) : G \times \widehat{G} \to \mathbb{C}^*,\ (g, \chi) := \chi(g),$$

est non dégénéré à droite et à gauche[1].

(d) Montrer que l'application canonique $\mathbb{C}[G] \to A(\widehat{G})$,

$$\sum_{g \in G} a_g g \mapsto (\chi \mapsto \sum_{g \in G} a_g \chi(g)),$$

est un isomorphisme de $\mathbb{C}$-algèbres.

Exercice 9 (Déterminant[2] d'un groupe abélien) Soit G un groupe abélien fini et $(x_g)_{g \in G}$ des nombres complexes indexés par les éléments de G. Montrer la formule :

$$\det((x_{gh^{-1}})_{g,h \in G}) = \prod_{\chi \in \widehat{G}} (\sum_{g \in G} \chi(g) x_g)$$

[1] Cela signifie que si l'une quelconque des deux variables est fixée, $(.,.)$ est un morphisme de groupes en l'autre variable, puis que les morphismes naturels qu'il induit, $G \to \widehat{\widehat{G}}$ et $\widehat{G} \to \widehat{G}$ sont des isomorphismes. On pourrait en fait déduire (b) du théorème de structure des groupes abéliens fini, en se ramenant au cas G cyclique. Cela montrerait même que G est isomorphe à $\widehat{G}$, bien que non canoniquement. Le (b) montre par contre que l'application naturelle $G \to \widehat{\widehat{G}}$, $g \mapsto (\chi \mapsto \chi(g))$ est un isomorphisme de groupes.

[2] Cette formule généralise par exemple celle pour le déterminant circulant, qui est le cas particulier où $G = \mathbb{Z}/n\mathbb{Z}$. Il en existe une version non abélienne qui se démontre de manière analogue, où les termes du produit de droite sont remplacés par $\prod_{V \in \theta} \det((\sum_{g \in G} x_g g)_{|V})^{\dim(V)}$, θ étant un ensemble de représentants des classes d'isomorphie de représentations irréductibles de G.

Indication: On pourra caluler de deux façons le déterminant de l'endomorphisme $\sum_{g\in G} x_g.r(g)$ de $A(G)$, en utilisant l'exercice 8.

Exercice 10 Soit $A := \mathbb{C}\{X,Y\}/(XY - YX - 1)$, où $\mathbb{C}\{X,Y\}$ désigne la $\mathbb{C}$-algèbre des polynômes non commutatifs en 2 variables à coefficients complexes. Montrer que A n'admet pas de représentation complexe de dimension finie.

Exercice 11 Soit k un corps, montrer que $k[\mathbb{Z}/n\mathbb{Z}] \simeq k[X]/(X^n - 1)$ comme k-algèbre.

Exercice 12 Soit A la sous-$\mathbb{R}$-algèbre de $\mathrm{M}_2(\mathbb{R})$ engendrée par $SO_2(\mathbb{R})$. Montrer que $A \simeq \mathbb{C}$ et en déduire que le théorème de Burnside est faux sur un corps non algébriquement clos.

Exercice 13 Soient p un nombre premier, k un corps de caractéristique p, et P un p-groupe fini.

(a) On suppose que $P \subset \mathrm{GL}_n(k)$ agit irréductiblement sur k^n. Montrer que $n = 1$ et $P = \{1\}$.

(b) En déduire que toute représentation $P \to \mathrm{GL}_n(k)$ est trigonalisable.

(c*) Soient $(a_g)_{g\in P}$ une famille d'entiers indexée par P. Montrer que

$$\det((a_{gh^{-1}})_{g,h\in P}) \equiv \sum_g a_g \bmod p$$

Problème (Modules simples et semi-simples) Soit A un anneau, un A-module M est dit simple si ses seuls sous-modules sont $\{0\}$ et M. Il est dit semi-simple tout sous-A-module N de M admet un A-module supplémentaire, *i.e.* un sous A-module N' de M tel que M soit somme directe de N et N'.

(a) On suppose dans cette question que $A = k$ est un corps gauche [3], montrer que tout k-module est semi-simple, et que les modules simples sont isomorphe au k-module k.

(b*) Montrer que les trois assertions suivantes sont équivalentes :
i) M est somme de sous-modules simples,
ii) M est somme directe de sous-modules simples,
iii) M est semi-simple.

(c) En déduire qu'une somme directe quelconque de modules semi-simples est encore semi-simple, et que tout sous-module et quotient d'un module semi-simple est encore semi-simple.

(d) Un anneau A est dit semi-simple si tous les A-modules sont semi-simples. Montrer que l'anneau A est semi-simple si, et seulement si, il est semi-simple comme A-module. Vérifier que tout A-module simple est isomorphe à un sous-module du A-module A.

[3] C'est un anneau unitaire A associatif tel que tout élément non nul admet un inverse des deux côtés. Un corps gauche commutatif est un corps au sens usuel.

(e) On suppose $A = \mathrm{M}_n(k)$, k un corps gauche, montrer que k^n est l'unique A-module simple, puis que A est semi-simple.

(f) En déduire qu'un produit fini $\prod_{i=1}^r \mathrm{M}_{n_i}(k_i)$, les k_i étant des corps gauches, est un anneau semi-simple.

Dans ce qui suit, on prouve le théorème de Wedderburn classifiant les anneaux semi-simples.

(g) (Lemme de Schur) Soit M un A-module simple. Montrer que l'anneau $\mathrm{End}_A(M)$ est un corps gauche.

(h) Soit M un A-module simple, n un entier, montrer que l'anneau $\mathrm{End}_A(M^n)$ est isomorphe à $\mathrm{M}_n(\mathrm{End}_A(M))$.

(i) Soit M_1, ..., M_r des A-modules simples deux à deux non isomorphes, $n_1, \ldots, n_r$ des entiers, montrer qu'en tant qu'anneaux

$$\mathrm{End}_A(\oplus_{i=1}^r M_r^{n_i}) \simeq \prod_{i=1}^r \mathrm{M}_{n_i}(\mathrm{End}_A(M_i))$$

(j) Si A est un anneau, on note A^{opp} *l'anneau opposé* à A. C'est l'anneau dont le groupe abélien sous-jacent est A, mais dont la multiplication est définie par $x * y := yx$. Vérifier que c'est bien un anneau unitaire si A l'est, et montrer qu'en tant qu'anneaux $\mathrm{M}_n(k)^{\mathrm{opp}} \simeq \mathrm{M}_n(k^{\mathrm{opp}})$.

(k) Montrer que l'application $\mathrm{End}_A(A) \to A^{\mathrm{opp}}$, $f \mapsto f(1)$, est un isomorphisme d'anneaux.

(l) Montrer le théorème de Wedderburn : "Tout anneau semi-simple est isomorphe à un anneau de la forme

$$\prod_{i=1}^r \mathrm{M}_{n_i}(k_i)$$

Un tel anneau a exactement r modules simples non isomorphes deux à deux, M_1,..., M_r et $k_i \simeq \mathrm{End}_A(M_i)^{\mathrm{opp}}$. En particulier, les n_i et les k_i sont uniquement déterminés."

(m) En déduire que si A est un anneau commutatif, A est semi-simple si, et seulement si, A est un produit fini de corps.

Soient G un groupe fini, k un corps dans lequel $|G|$ est inversible, et $\{V_1, \ldots, V_r\}$ l'ensemble des k-représentations irréductibles de G.

(n) Montrer que $k[G] \simeq \prod_{i=1}^r \mathrm{M}_{n_i}(k_i)$, où $k_i^{\mathrm{opp}} = \mathrm{End}_k(V_i)$ est un corps gauche contenant k dans son centre et de dimension finie sur k.

(o) On suppose de plus k algébriquement clos. Montrer que $|G| = \sum_{i=1}^r n_i^2$ et que r est le nombre de classes de conjugaison d'éléments de G.

Indication: Pour la seconde assertion, déterminer de deux façons différentes le centre de $k[G]$.

Remarques: Le théorème de Wedderburn ramène la structure des anneaux semi-simples à celle des corps gauches. Ces derniers sont classifiés par la théorie du groupe de Brauer (voir le TD1 par exemple).

Partiel et examen

Examen partiel du 8 avril 2004

Durée : 2h

Exercice 1.

Les deux questions sont indépendantes.

(a) Soient k un corps, V un k-espace vectoriel et W, W' des sous-espaces vectoriels de V. Montrer que les algèbres tensorielles $T(W)$, $T(W')$, $T(W \cap W')$ s'identifient à des sous-algèbres de $T(V)$ et que : $T(W \cap W') = T(W) \cap T(W')$.

(b) Soient k un corps, V, V', W, W' des k-espaces vectoriels et $f : V \to V'$, $g : W \to W'$ des applications linéaires. Déterminer $Ker(f \otimes g)$ en fonction des noyaux de f et g.

Exercice 2.

Soient $p > 2$ un nombre premier, $\zeta := e^{2i\pi/p}$ et $K := \mathbf{Q}(\zeta) \subset \mathbf{C}$.

(a) Montrer que $K/\mathbf{Q}$ est galoisienne de groupe de Galois $G := (\mathbf{Z}/p\mathbf{Z})^*$.

(b) Montrer que pour chaque entier d divisant $p-1$, K contient un unique sous-corps K_d de degré d sur $\mathbf{Q}$.

Vérifier que $G_d := Gal(K/K_d) = \{g^d, g \in G\}$ et que $K_d/\mathbf{Q}$ est galoisienne cyclique.

(c) Soit $p_d := \frac{d}{p-1} \sum_{g \in G_d} g \in End_{\mathbf{Q}}(K)$. Montrer que p_d est un projecteur d'image K_d tel que $\forall g \in G, gp_d = p_d g$.

(d) En déduire que $K_d = \mathbf{Q}(g_d)$ où $g_d := \sum_{k=0}^{p-1} \zeta^{k^d}$.

(e) Montrer que $K_{(p-1)/2} = \mathbf{Q}(\cos(2\pi/p))$ et (plus difficile) $K_2 = \mathbf{Q}(\sqrt{\varepsilon p})$, avec $\varepsilon = \pm 1$ tel que $p = \varepsilon \bmod 4$. (Indication : on pourra commencer par montrer que $g_2 \bar{g}_2 = p$, où $\bar{z}$ désigne le complexe conjugué de z).

Exercice 3.

1. Soit p un nombre premier. Soient K un corps de caractéristique p et a un élément de K. On suppose que le polynôme $P(X) = X^p - X - a$ n'a pas de racine dans K. Soit $K \subset L$ une extension de décomposition de P.

(a) Si x est une racine de P dans L, montrer que les autres racines sont : $x+1, \cdots, x+p-1$.

(b) Montrer que P est irréductible dans $K[X]$.

(c) Montrer que l'extension $K \in L$ est monogène, galoisienne et déterminer son groupe de Galois.

2. Soit p un nombre premier. Soient K un corps de caractéristique p et $K \subset L$ une extension galoisienne de groupe de Galois $\mathbf{Z}/p\mathbf{Z}$. Soit σ un générateur de $Gal(L/K)$.

(a) Montrer qu'il existe $x \in L$ tel que : $\sum_{i=0}^{p-1} \sigma^i(x) = 1$.

On pose alors : $\alpha = \sum_{i=0}^{p-1} i\sigma^i(x)$.

(b) Montrer que $\alpha \notin K$, mais que $a = \alpha^p - \alpha$ est dans K.

(c) Montrer que $L = K[\alpha]$ et déterminer le polynôme minimal de α sur K.

Exercice 4.

Soient K un corps et $P(X) \in K[X]$ un polynôme séparable. Soient $K \subset L$ une extension de décomposition de P, et $G = Gal(L/K)$ son groupe de Galois.

On considère l'extension des corps de fractions rationnelles :
$K(Y_1, \cdots, Y_n) \subset L(Y_1, \cdots, Y_n)$ déduite de l'extension $K \subset L$. Pour alléger les notations, on pourra écrire $L(Y)$ au lieu de $L(Y_1, \cdots, Y_n)$, etc...

(a) Soit $R \in L(Y)$. Montrer que R peut s'écrire $R = N/D$ avec $N \in L[Y]$ et $D \in K[Y]$. En déduire que l'extension $K(Y) \subset L(Y)$ est finie, de degré inférieur ou égal au degré de L sur K.

(b) On considère l'application naturelle $G \to Aut(L(Y)/K(Y))$ induite par l'action de G sur les coefficients d'une fraction rationnelle de $L(Y)$. Montrer que c'est un morphisme de groupes bijectif. En déduire que l'extension $K(Y) \in L(Y)$ est galoisienne, de groupe de Galois G.

Examen du 8 juin 2004

Durée 3 heures

Exercice 1.

I. Soit $P(X) = \prod_{i=1}^{n}(X - x_i)$ un polynôme, et soient $y_1, \cdots, y_{n-1}$ les racines du polynôme dérivé P'. Montrer que le discriminant de P vaut :

$$(-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(x_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n-1} P(y_k)$$

Soit $P(X) = X^n + aX + b$. Montrer que son discriminant vaut
$(-1)^{\frac{n(n-1)}{2}}((1-n)^{n-1}a^n + n^n b^{n-1})$.

II. On se propose de déterminer le groupe de Galois du polynôme $P = X^5 + 20X - 16$ sur $\mathbf{Q}$.

(a) Vérifier que 2 et 3 sont des racines de sa réduction modulo 7, puis factoriser cette réduction modulo 7.

(b) Montrer que sa réduction modulo 3 est irréductible sur $\mathbf{F}_3$.

On admettra que modulo 23, la réduction de P se factorise en un polynôme de degré 1 et le produit de deux polynômes de degré 2.

(c) Quel est le groupe de galois de P ?

Exercice 2.

I. On fixe dans tout ce qui suit un corps $k \subset \mathbf{R}$. Soient p un nombre premier et $a \in k$ qui n'est pas la puissance p^{ieme} d'un élément de k.

(a) Montrer que $X^p - a$ est irréductible dans $k[X]$ (on pourra considérer le terme constant d'un éventuel facteur).

(b) On suppose $p > 2$. Soit $x \in \mathbf{R}$ tel que $x^p = a$ (justifier), montrer que $k(x)/k$ n'est pas galoisienne.

II. Une extension finie de corps K/k est dite *résoluble par radicaux réels*, ou *r.r.r.* , s'il existe une tour d'extensions

$$k_0 = k \subset k_1 \subset \cdots \subset k_n \subset \mathbf{R},$$

telle que $K \subset k_n$, et pour $0 \leq i < n$, $k_{i+1} = k_i(x_i)$ où $x_i^{m_i} \in k_i$ et $m_i \in \mathbf{N}$.

(c) Supposons que K/k est r.r.r. Montrer que l'on peut trouver une tour comme ci-dessus où les m_i sont des nombres premiers et satisfont $[k_{i+1} : k_i] = m_i$. Vérifier de plus que si $k \subset L \subset K$ est un corps intermédiaire, alors K/L est aussi r.r.r.

Soit K/k une extension galoisienne avec $K \subset \mathbf{R}$. On se propose de démontrer que K/k est résoluble par radicaux réels si, et seulement si, $[K : k]$ est une puissance de 2.

(d) Montrer que si $[K : k]$ est une puissance de 2, alors K/k est r.r.r.

Réciproquement, supposons que K/k est r.r.r. On fixe une tour de résolubilité par radicaux réels comme plus haut, avec des $m_i = [k_{i+1} : k_i]$ premiers.

(e) On suppose de plus que $[K : k]$ est un nombre premier impair, et on note K' le sous-corps de $\mathbf{R}$ engendré par K et k_1. Montrer que $K \not\subset k_1$, puis que K'/k_1 est galoisienne, cyclique de degré $[K : k]$ (on pourra considérer une application naturelle $\mathrm{Gal}(K'/k_1) \to \mathrm{Gal}(K/k)$).

(f) Montrer que si $[K : k]$ est premier impair, alors $[K : k] = 1$.

(g) Conclure.

(h) Montrer que $\mathbf{Q}(\cos(2\pi/7))/\mathbf{Q}$ est résoluble par radicaux, mais pas par radicaux réels ("Casus irreducibilis").

Exercice 3

Les parties II et III sont indépendantes.

I. (Deux résultats généraux, indépendants).

(a) Soient A un anneau commuatif, intègre, unifère et B un sous-anneau de même unité. Soient E et F les corps de fractions respectifs de A et B. On suppose que $E \subset F$ est une extension finie. Montrer que si A est libre de rang r comme B-module, alors $[E : F] = r$.

(b) Soit $S = \mathbf{C}[X_1, \cdots X_n]$ une algèbre de polynômes engendrée par des éléments algébriquement indépendants $X_1, \cdots X_n$ de degré respectifs $p_1, \cdots p_n$. Soit $R \subset S$ une sous-algèbre graduée de polynômes $R = \mathbf{C}[Y_1, \cdots Y_n]$ avec Y_i homogène de degré q_i. On suppose que le R-module S est libre et admet une base finie formée d'éléments homogènes $z_1, \cdots z_N$ de degrés respectifs $f_1, \cdots, f_N$.

Montrer que : $\prod_{i=1}^{n}(1 - t^{q_i}) = (\sum_{j=1}^{N} t^{f_j}) \prod_{i=1}^{n}(1 - t^{p_j})$. Déterminer le rang de S sur R.

II. Soit K un corps et $S = K[X_1, \cdots, X_n]$ une K-algèbre graduée de polynômes, engendrée par des éléments algébriquement indépendants X_i, homogènes de degrés strictement positifs. Soient $Y_1, \cdots, Y_n$ des éléments homogènes de degrés strictement positifs de S et $R = K[Y_1, \cdots, Y_n]$ la sous-algèbre de S engendrée par ces éléments.

(a) Montrer l'équivalence des propriétés suivantes :

(i) S est entier sur R.

(ii) L'idéal de S engendré par $(Y_1, Y_2, \cdots, Y_n)$ est de codimension finie.

(iii) Pour toute extension L de K, le système d'équations $Y_i(x_1, \cdots, x_n) = 0$ $(1 \leq i, \leq n, x_i \in L)$ n'a que la solution triviale $(0, \cdots, 0)$.

On pourra admettre que si ces propriétés sont vérifiées, les Y_i sont algébriquement indépendants sur K, et que S est un R-module libre .

(b) Soit G un groupe fini d'automorphismes de l'algèbre graduée S, soit S^G la sous-algèbre de ses invariants, et soient $Y_1, \cdots, Y_n$ des éléments de S^G vérifiant les conditions (i), (ii), (iii) ci-dessus. Montrer que $S^G = K[Y_1, \cdots, Y_n]$ si et seulement si $\mathrm{Card}(G) = \prod_i deg(Y_i)/\prod_i deg(X_i)$

(c) (Question subsidiaire) Démontrer les assertions admises ci-dessus.

III. Soit V un $\mathbf{C}$-espace vectoriel de dimension finie n et G un sous-groupe fini de $GL(V)$ engendré par des réflexions. Soit S l'algèbre symétrique sur V^* que l'on identifie à une algèbre de polynômes $\mathbf{C}[X_1, \cdots, X_n]$. Soit R la sous-algèbre des invariants de S sous l'action de G. On se propose de montrer que comme R-module, S est un module libre de rang $Card(G)$.

Pour cela, on compare S comme R-module au $\mathbf{C}$ espace vectoriel S/I où I est l'idéal de S engendré par les éléments de R de degré strictement positif :

(a) Si des éléments homogènes g_i de S sont tels que leurs classes modulo I engendrent l'espace vectoriel S/I, montrer qu'ils engendrent S comme R-module.

(b) Si des éléments homogènes $g_1, \cdots g_m$ de S sont tels que leurs classes modulo I sont linéairement indépendantes dans l'espace vectoriel S/I, montrer qu'ils R-libres dans S. On pourra utiliser le lemme technique du cours dont on rappelle l'énoncé :

Si $f_1, \cdots f_r \in R$ sont tels que f_1 n'est pas dans l'idéal de R engendré par $f_2, \cdots f_r$, et si $g_1, \cdots g_r$ sont des éléments homogènes de S tels que $f_1 g_1 + \cdots f_r g_r = 0$ alors $g_1 \in I$.

(c) Conclure.

Exercice 4.

Soit d une dérivation de l'algèbre des matrices $M_n(\mathbf{C})$, i.e. une application linéaire $d : M_n(\mathbf{C}) \to M_n(\mathbf{C})$ telle que : $\forall x, y \in M_n(\mathbf{C}), d(xy) = d(x)y + xd(y)$.

Montrer que d est une dérivation intérieure, i.e. qu'il existe $a \in M_n(\mathbf{C})$ telle que :

$$\forall x \in M_n(\mathbf{C}), \qquad d(x) = ax - xa$$

(On pourra considérer l'application $\phi : M_n(\mathbf{C}) \to M_{2n}(\mathbf{C})$ donnée par

$$\phi(x) = \begin{pmatrix} x & d(x) \\ 0 & x \end{pmatrix},$$

et vérifier que c'est un morphisme d'algèbres).

Quelques corrections

Corrections de quelques exercices des T.D. d'algèbre II

Ci-dessous des corrections pour certains exercices/questions des TD précédents. Veuillez bien me le signalez si vous y trouvez des incorrections/coquilles.

Exercices corrigés : TD11 (ex. 1, 2, 3, 4, 5), TD10 (ex. 1, 2, 3), TD9 (ex. 1, 3), TD8 (ex. 1, 2, 3, 4), TD7 (ex. 2), TD6 (ex. 2, 5, problème), TD5 (ex. 2, 3), TD4 (ex. 3, 9), TD3 (ex.1), TD2 (ex.2).

Exercice 1 du TD 11 Soit A une $\mathbb{C}$-algèbre commutative et $r : A \to M_n(\mathbb{C})$ une représentation. Les matrices $r(a)$, $a \in A$, commutent 2 à 2 et sont donc cotrigonalisables dans $M_n(\mathbb{C})$. En particulier, il existe une droite $D \subset \mathbb{C}^n$ qui est propre pour tous les $r(a)$, $a \in A$. Si r est irréductible, alors $D = \mathbb{C}^n$, et donc $n = 1$.

Noter que si plus généralement r est semi-simple, alors la droite D admet un supplémentaire $H \subset \mathbb{C}^n$ stable par les $r(a)$, $a \in A$, de sorte que par récurrence immédiate, les $r(a)$ sont codiagonalisables.

Exercice 2 du TD 11

(a) Soit $G \subset O_2(\mathbb{R})$ le groupe des isométries euclidiennes d'un triangle équilatéral centré en 0 dans $\mathbb{R}^2$. L'action de G sur les sommets du triangle nous fournit un morphisme $\psi : G \to \mathfrak{S}_3$ qui est clairement un isomorphisme. On considère le morphisme $\rho : \mathfrak{S}_3 \to O_2(\mathbb{R}) \to \mathrm{GL}_2(\mathbb{C})$ qui s'en déduit. Supposons que ρ est réductible, i.e. qu'il existe une droite D de $\mathbb{C}^2$ stable par $\mathfrak{S}_3$. Soit $s \in G$ une réflexion, alors $s_{|D}$ agit par ± 1 de sorte que $D = \mathbb{C}.d$ ou $d \subset \mathbb{R}^2$ est soit l'axe de s soit son orthogonal. Mais un tel d n'est pas stable par les rotations de G, ainsi donc que $\mathbb{C}.d$. Cela montre que ρ est réductible.

Voici un autre argument plus général. Supposons que $H \subset GL_2(\mathbb{C})$ est un groupe fini qui n'agit pas irréductiblement sur $\mathbb{C}^2$, alors H est commutatif. En effet, notons tout d'abord qu'il agit de manière semi-simple par un théorème du cours. Ainsi, s'il admet une droite stable $\mathbb{C}.e_1$, elle admet un supplémentaire $\mathbb{C}.e_2$ stable par H, et H est diagonal (donc commutatif) dans la base (e_1, e_2).

Comme on l'a vu dans l'exercice 1 du TD 10, la représentation naturelle de $\mathfrak{S}_n$ sur $\mathbb{C}^n$ préserve l'hyperplan des vecteurs de somme des coordonnées nulle. On montre comme dans l'exercice loc.cit. (c) que cette représentation est irréductible.

(b) De même que pour $\mathfrak{S}_3$ ci-dessus, D_{2n} s'identifie au sous-groupe de $O_2(\mathbb{R})$ des isométries euclidiennes d'un polygone régulier plan à n côtés centré en 0. La représentation complexe déduite $D_{2n} \to \mathrm{GL}_2(\mathbb{C})$ est irréductible par le même argument que plus haut, car D_{2n} est non commutatif.

Exercice 3 du TD 11

(a) Considérons le morphisme de groupe $\rho : \mathbb{Z} \to \mathrm{GL}_2(\mathbb{C})$ envoyant 1 sur la matrice unipotente supérieure standard

$$u := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

La droite stable $\mathbb{C}.e_1$ n'admet pas de droite supplémentaire stable par u, car u n'est pas diagonalisable.

(b) Comme dans l'exercice 1, on voit que si r est semi-simple, alors r(X)est diagonalisable. Montrons la réciproque. Il suffit de montrer que si k est un corps et u un endomorphisme diagonalisable de k^n, alors tout sous-k-espace stable par u admet un supplémentaire stable par u. Soit V un tel sous-espace, $u_{|V}$ est encore diagonalisable, de sorte que V est somme directe des espaces propres de $u_{|V}$. On se ramène donc au cas où u n'a de plus qu'une seule valeur propre, i.e. u est une homothétie, pour lequel c'est évident.

Exercice 4 du TD 11 On considère la représentation de G par translation à gauche sur $\mathbb{C}[G]$. Comme G est fini, elle est semi-simple par un théorème du cours. Elle se décompose donc comme somme directe de sous-espaces vectoriels stables par G, $\mathbb{C}[G] = W_1 \oplus W_2 \oplus \cdots \oplus W_m$, où les W_j sont stables par G et tels que la représentation induite par restriction $r_j : G \to \mathrm{GL}_{\mathbb{C}}(W_j)$ est irréductible. En regroupant entre eux les (W_j, r_j) qui sont isomorphes, on obtient un ensemble de représentations irréductibles (V_i, ρ_i) de G telles que tout (W_j, r_j) est isomorphe à une et une seule des (V_i, ρ_i). On a donc $\mathbb{C}[G] \simeq \oplus_{i=1}^{r} V_i^{m_i}$, comme dans l'énoncé.

(a) Soit $\rho : G \to \mathrm{GL}_{\mathbb{C}}(V)$ une représentation irréductible de G et $v \neq 0 \in V$. Considérons l'application $\mathbb{C}$-linéaire $L : \mathbb{C}[G] \to V$ définie par $L(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g \rho(g)(v)$. Elle satisfait $L(hx) = \rho(h)L(x)$ pour tout $x \in \mathbb{C}[G]$ et tout $h \in G$. Soit $W_j \subset \mathbb{C}[G]$ comme plus haut. L'application L induit donc un opérateur d'entrelacement

$$L_j := L_{|W_j} : W_j \to V.$$

Comme V et W_j sont irréductibles, le lemme de Schur entraîne que L_j est soit nulle soit un isomorphisme. Si tous les L_j sont nuls, alors L est nul, ce qui est absurde car $v = L(1) \neq 0$. Ainsi, l'un des L_j est un isomorphisme de W_j vers V, ce que l'on cherchait.

(b) On considère $\rho_i : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V_i)$, elle est surjective d'après le théorème de Burnside. Munissons $\mathrm{End}_{\mathbb{C}}(V_i) = \mathrm{Hom}_{\mathbb{C}}(V_i, V_i)$ d'une représentation de G en posant si $u \in \mathrm{End}_{\mathbb{C}}(V_i)$ et $g \in G$, $g(u) := (x \mapsto \rho_i(g(u(x))))$. On vérifie immédiatement que c'est bien une représentation de G, et que ρ_i est un opérateur d'entrelacement entre $\mathbb{C}[G]$ (pour l'action par translation à gauche de G) et $\mathrm{End}_{\mathbb{C}}(V_i)$ (pour l'action ci-dessus).

Notons que si $e_1, \ldots, e_m$ est une $\mathbb{C}$-base de V_i, $m := \dim_{\mathbb{C}}(V_i)$, alors l'application linéaire bijective

$$\psi : \mathrm{End}_{\mathbb{C}}(V_i) \to V_i^m, \;\; u \mapsto (u(e_1), \ldots, u(e_m)),$$

est un opérateur d'entrelacement, où G agit sur V_i^m coordonnée par coordonnée. De plus, notons $p_{i,k} : V_i^m \to V_i$ la projection sur la k-ieme coordonnée, c'est aussi un opérateur d'entrelacement. Considérons finalement l'application linéaire

$$\varphi_{i,k} := p_{i,k} \circ \psi \circ (\rho_i)_{|W_j} : W_j \to V_i,$$

c'est un opérateur d'entrelacement par ce qui précède. Si (W_j, r_j) n'est pas isomorphe à (V_i, ρ_i), le lemme de Schur assure que $\varphi_{i,k} = 0$ pour tout k, et donc que $(\rho_i)_{|W_j} = 0$.

Comme ρ_i est surjective, on en déduit que ρ_i induit une surjection $V_i^{m_i} \to \mathrm{End}_{\mathbb{C}}(V_i)$, puis $n_i \geq \dim_{\mathbb{C}}(V_i)$.

Exercice 1 du TD 10

(a) On note $e_1, \dots, e_n$ la base canonique de $\mathbb{R}^n$. Si $\sigma \in W$, on a $\sigma(e_i) = e_{\sigma(i)}$, autrement dit $\sigma(x_1, \dots, x_n) := (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$. En particulier, x et $\sigma(x)$ ont même somme des coordonnées, et V est préservé. Notons que l'orthogonale de V est la droite $\mathbb{R}(e_1 + \dots + e_n)$, et que W préserve cette droite en agissant par l'identité. En particulier, si $\sigma_{|V}$ est l'identité de V, $\sigma = \mathrm{id}$. Ainsi, la restriction $W \to O(V)$, $\sigma \mapsto \sigma_{|V}$, est injective.

Soit $1 \leq i < j \leq n$, vérifions que la transposition $(i, j) \in W$ est une réflexion de V. Tout d'abord $e_i - e_j \in V$ et $(i, j)(e_i - e_j) = -(e_i - e_j)$. De plus, l'orthogonal dans V de $e_i - e_j$ est l'ensemble des éléments $(x_1, \dots, x_n) \in V$ tels que $x_i = x_j$ et (i, j) agit visiblement par l'identité sur ce sous-espace. On en conclut que W est engendré par des réflexions car il est bien connu que les (i, j) engendrent W.

(b) Comme $\sigma(e_i) = e_{\sigma(i)}$, on voit que $\det(\sigma)$ est la signature de σ. Comme une réflexion de V de la forme σ agit trivialement sur $V^\perp$, elle est de déterminant -1. En particulier, $\mathfrak{A}_n$ ne contient aucune réflexion.

Par contre, si $n \geq 5$, il est engendré par les doubles transpositions, qui sont d'ordre 2. En effet, le sous-groupe engendré par les doubles transpositions est distingué (car le conjugué d'une double transposition en est encore une), c'est donc $\mathfrak{A}_n$ par simplicité ($n \geq 5$). On voit facilement que pour $n \leq 4$, $\mathfrak{A}_n$ n'est pas engendré par des éléments d'ordre 2.

On a déjà vu que $s_i = (i, i+1)$ est la réflexion d'axe $e_i - e_{i+1}$. Si $|i - j| >= 2$, $(i, i+1)$ et $(j, j+1)$ commutent, et $(s_i s_{i+1})^3 = ((i, i+1)(i+1, i+2))^3 = (i, i+1, i+2)^3 = 1$ donc $s_i s_{i+s} s_i = s_{i+1} s_i s_{i+1}$.

(c) Soit $U \subset V$ un sous-$\mathbb{R}$-espace vectoriel non nul stable pour l'action de W. Soit $x = (x_1, \dots, x_n) \neq 0 \in W$. Comme $\sum_i x_i = 0$ et $x \neq 0$, x a au moins deux coordonnées distinctes, disons $x_i \neq x_j$. En particulier, $(x - (i, j).x)/(x_i - x_j) = e_i - e_j$ est dans W. En appliquant les (i, k), il vient que tous les $e_l - e_k$ sont dans W, puis $V = W$, ce que l'on voulait démontrer.

(d) On considère la base $x_1, \dots, x_{n-1}$ du dual de V, $Sym(V^*) = \mathbb{R}[x_1, \dots, x_{n-1}]$, et les $(f_j)_{2 \leq j \leq n}$ comme dans l'énoncé. f_j est un W-invariant homogène de degré j ($x_n = -\sum_{i=1}^{n-1} x_i$). Comme $j! = |W|$ est le produit des degré des f_j, il suffit de montrer que les f_j sont algébriquement indépendants pour conclure. On applique le critère jacobien. Comme $\frac{\partial x_n}{\partial x_i} = -1$ si $i < n$, on a

$$\frac{\partial f_j}{\partial x_i} = j(x_i^{j-1} - x_n^{j-1}).$$

Ainsi, le jacobien J vaut $n!$ fois le déterminant de la matrice carrée $M = (m_{i,j})$ de taille $n - 1$ avec $m_{i,j} = x_i^j - x_n^j$. Rajoutons un 0 au début de chaque ligne de la matrice $(m_{i,j})$ ainsi qu'une n^{ieme} ligne $(1, x_n, x_n^2, \dots, x_n^{n-1})$, le déterminant de la matrice carré de taille n obtenue est exactement celui de M. En ajoutant la dernière ligne aux $n - 1$ premières autres, il vient que $\det(M)$ est le déterminant de Vandermonde de $(x_1, \dots, x_n)$, i.e.

$$J = n! \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Ce déterminant est non nul dans (l'anneau intègre...) $\mathbb{R}[x_1, \ldots, x_{n-1}]$, car aucun de ses termes ne l'est.

Exercice 2 du TD 9 Soient $g_1, \ldots, g_n \in R := k[X_1, \ldots, X_n]^W$ une base de Chevalley de l'algèbre des invariants, de degrés ordonnés $d_1 \leq \cdots \leq d_n$. On suppose de plus que, quitte à renuméroter les f_i, $e_1 \leq e_2 \leq \cdots \leq e_n$.

Montrons que $\forall r \leq n,\ e_r \geq d_r$. Tout d'abord, f_j est un polynôme en les g_i. Comme il est homogène, c'est une somme de monômes de la forme

$$\prod_{i=1}^{n} g_i^{\alpha_{i,j}},\ \text{avec}\ \sum_i \alpha_{i,j} d_i = e_j,\ \text{et}\, alpha_{i,j} \geq 1 \tag{1}$$

Si $e_r < d_r$, alors $e_j < d_i$ pour $j \leq r \leq i$, de sorte que la relation (1) montre que $\alpha_{i,j} = 0$ pour $j \leq r \leq i$. En particulier, cela montre que

$$k[f_1, \ldots, f_r] \subset k[g_1, \ldots, g_{r-1}].$$

Mais cela est impossible pour une raison de degré de transcendance, car $f_1, \ldots, f_r$ sont algébriquement indépendants par hypothèse. Cela conclut $e_r \geq d_r$. Comme $\prod_r e_r = |W| = \prod_r g_r$, il vient en fait que $e_r = g_r$ pour tout r.

Soient $S := k[f_1, \ldots, f_r] \subset R$ et $d \geq 1$ un entier. On notera S_d (resp. R_d) le sous-espace des éléments homogènes de degré d. Les f_i et g_j étant homogènes, $S = \sum_{d \geq 1} S_d$ et $R = \sum_{d \geq 1} R_d$. Comme les f_i (resp. les g_i) sont homogènes de degré e_i (resp. d_i) et algébriquement indépendants :

$$\dim_k S_d = |\{(k_1, \ldots, k_n) \in \mathbb{N}^n, \sum_{i=1}^{n} k_i e_i = d\}|,\ \dim_k R_d = |\{(k_1, \ldots, k_n) \in \mathbb{N}^n, \sum_{i=1}^{n} k_i d_i = d\}|$$

La relation $\forall i,\ e_i = d_i$ entraîne que $\dim_k S_d = \dim_k R_d$. L'inclusion $S_d \subset R_d$ est donc une égalité, et $S = R$. □

Exercice 3 du TD 9

(a) L'anneau B est engendré comme k-algèbre par les coefficients des polynômes P_i, qui sont en nombre fini, donc B est une k-algèbre de type fini.

Faisons agir G sur $A[T]$ par $g(a_0 + a_1 T + \cdots + a_n T^n) := g(a_0) + g(a_1)T + \cdots + g(a_n)T^n$, il est clair que c'est une action par automorphismes de k-algèbres qui induit l'action donnée sur A, et que $(A[T])^G = A^G[T]$. On veut donc montrer que si $h \in H$, $h(P_i(T)) = P_i(T)$. Mais $h(\prod_{g \in G}(T - g(x_i))) = \prod_{g \in G}(T - hg(x_i)) = \prod_{g \in G}(T - g(x_i)) = P_i(T)$. Ainsi $B \subset A^G$.

(b) On vient de voir que $P_i \in B[T]$. C'est de plus un polynôme unitaire tel que $P_i(x_i) = 0$, on en déduit que chaque x_i est entier sur B. Comme $k \subset B$ et que A est engendré comme k-algèbre par l'ensemble fini des x_i, il vient non seulement que A est entier sur B, mais aussi que A est fini sur B. Ainsi, A est un B-module de type fini. Comme B est une k-algèbre de type fini, le théorème de la base de Hilbert assure qu'il est noethérien. Ainsi, tous les sous-B-modules de A sont de type fini, ainsi donc que A^G (qui contient B par (a)).

(c) Soient $f_1, \ldots, f_r \in A^G$ tels que $A^G = \sum_i Bf_i$, cela existe par (b). Si B est engendré comme k-algèbre par $g_1,\ldots,g_s$, alors il est immédiat que A^G est engendré comme k-algèbre par $f_1, \ldots, f_r, g_1, \ldots, g_s$.

Exercice 1 du TD 9

(a) D'après le Nullstellensatz, $I(V((P)))$ est le radical de (P). Comme $k[X_1, \ldots, X_n]$ est factoriel, l'idéal engendré par le polynôme irréductible P est premier, et en particulier égal à son radical : $I(V((P)) = (P)$. Si Q s'annule sur $V((P))$, par définition $Q \in I(V(P))$, ce qui conclut.

(b) Si $P \in k[X,Y]$ est irréductible, il reste irréductible dans $(k(X))[Y]$ car $k[X]$ est factoriel et par le théorème du contenu de Gauss. De plus, si $Q \in k[X,Y]$ est divisible P dans $(k(X))[Y]$, le lemme du contenu montre aussi que Q est divisible P par $k[X,Y]$. En effet, $Q = PR \Rightarrow c(Q) = c(P)c(R)$, mais $c(P) = 1$ par irréductibilité de P dans $k[X,Y]$, puis $c(R) = c(Q) \in k[X]$ par l'hypothèse $Q \in k[X,Y]$. Ainsi, sous les hypothèses du (b), P et Q sont premiers entre eux dans $(k(X))[Y]$. Cet anneau étant principal, il existe une relation de Bezout entre P et Q, i.e. $A'P + B'Q = 1$, avec A', $B' \in (k(X))[Y]$. Mais si C est un dénominateur commun des coefficients de A' et B', et $A := CA'$ et $B := CB'$, alors A, $B \in k[X,Y]$, $C \neq 0 \in k[X]$, et $AP + BQ = C$.

(c) Soit $M = (x,y) \in V(P) \cap V(Q)$. Par hypothèse, $P(x,y) = Q(x,y) = 0$ et donc $C(x) = 0$, C étant le polynôme non nul défini en (b). Cela ne laisse qu'un nombre fini d'abscisses x possibles pour M. Mais il est clair que ce qui a été fait au (b) pour le couple de variables (X,Y) peut aussi être fait pour (Y,X), de sorte que le même argument montre qu'il n'y a qu'un nombre fini d'ordonnées possibles pour M. Ainsi, $V(P) \cap V(Q)$ est fini.

Pour retrouver le (a) il suffit de montrer que si $P \in k[X,Y]$ est irréductible, $V(P)$ est infini. Écrivons

$$P(X,Y) = a_0(X) + a_1(X)Y + \cdots + a_n(X)Y^n, a_i \in k[X].$$

Comme P est irréductible, soit l'un des a_i avec $i > 0$ est non nul, soit $P(X,Y) = (X - x)$, avec $x \in \mathbb{C}$. Le résultat est trivial dans le second cas car $V(P) = \{x\} \times k$ et k est infini[4]. Dans le premier cas, si $a_j \neq 0$, il existe une infinité de $x \in k$ tels que $a_j(x) \neq 0$, et donc tels que $P(x,Y) \in k[Y]$ est un polynôme non constant car $j > 0$. Un tel polynôme a donc toujours une racine $y \in k$ car k est algébriquement clos. Cela conclut.

(d) Par définition, la topologie sur $V(P)$ admet pour base de fermés les $V(f) \cap V(P)$ où $f \in k[X,Y]$. Si $f = gh$, $V(f) = V(g) \cup V(h)$ de sorte que l'on peut supposer que f irréductible et que $f \neq \lambda.P$ pour $\lambda \in k^*$. Dans ce cas, P ne divise pas f le (b) montre que $V(f) \cap V(P)$ est fini. Les fermés de $V(P)$ sont donc tous finis. Réciproquement, il suffit de voir que les points sont fermés. Mais cela vient de ce que $\{(x,y)\} = V(P) \cap V((X-x, Y-y))$.

Exercice 3 du TD 9

[4]Un corps algébriquement clos est infini. En effet, si K est fini, $1 + \prod_{x \in K}(X - x) \in K[X]$ n'a pas de racine dans K.

(a) Soit $n \geq 2$. Par définition, $M \in M_2(k)$ est dans $V(I_n)$ si, et seulement si, $M^n = 0$. De plus, $M \in V(I_1)$ si, et seulement si, $\mathrm{tr}(M) = \det(M) = 0$. Le lemme classique suivant montre alors que $V(I_n)$ est toujours égal à l'ensemble des matrices nilpotentes de $M_2(k)$, et donc à fortiori qu'il est indépendant de n.

Lemme Si k est un corps et $M \in M_2(k)$, les conditions suivantes sont équivalentes :

i) $\exists n \geq 1$, $M^n = 0$ ("M est nilpotente"),

ii) $\forall n \geq 2$, $M^n = 0$,

iii) $\mathrm{tr}(M) = \det(M) = 0$.

Il est en effet clair que ii) $\Rightarrow$ i). Puis i) implique que M est trigonalisable avec des 0 sur la diagonale, donc iii). Enfin, par Cayley-Hamilton, iii) $\Rightarrow M^2 = 0 \Rightarrow$ ii).

(b) Moralement, on a envie de considérer la k-algèbre quotient $k[a,b,c,d]/(a+d, ad-bc)$, et de dire que $a \equiv -d$, de sorte qu'elle s'identifie à $k[a,b,c]/(a^2+bc)$. Admettons ceci. Cette dernière k-algèbre est intègre car a^2+bc est un irréductible de l'anneau factoriel $k[a,b,c]$. Ainsi, la première l'est aussi, i.e. I_1 est premier. Nous allons justifier proprement la première identification plus haut.

On pose $u := a + d$. Il est clair que $k[a,b,c,d] = k[a,b,c,u]$ et que $I_1 = (u, ad - bc) = (u, a^2 + bc)$. Considérons le morphisme de k-algèbres

$$\varphi : k[a,b,c,u] \to k[a,b,c]/(a^2+bc),$$

envoyant $P(a,b,c,u)$ sur $P(a,b,c,0)$. Il est surjectif et contient (u, a^2+bc) dans son noyau. Soit $P \in \mathrm{Ker}(\varphi)$, il vient que $P(a,b,c,0) = A(a,b,c)(a^2+bc)$ où $A \in k[a,b,c]$, puis $P(a,b,c,u) = A(a,b,c)(a^2+bc)+uB(a,b,c,d)$, $B \in k[a,b,c,u]$. Ainsi, $\mathrm{Ker}(\varphi) = (u, a^2+bc)$. Cela justifie l'affirmation plus haut, et conclut que I_1 est premier.

D'après le (a), $V(I_n) = V(I_1)$. Le Nullstellensatz assure donc que $\sqrt{I_n} = I(V(I_n)) = \sqrt{I_1}$. Mais $\sqrt{I_1} = I_1$ car I_1 est premier par le paragraphe précédent.

(c) En écrivant $N^{n+1} = N.N^n$, on voit que $I_{n+1} \subset I_n$. Nous allons expliquer de deux façons que l'inclusion est stricte. La première méthode repose sur l'étude des solutions infinitésimales des systèmes d'équations polynomiales définis par les I_n, et la seconde sur un argument d'homogénéité.

– L'idée est la suivante. Le lemme plus haut caractérisant les matrices nilpotentes n'est plus vrai en général si k est remplacé par un anneau qui n'est intègre, par exemple par $k_n := k[\varepsilon]/(\varepsilon^{n+1})$, $n \geq 1$. En effet, sur cet anneau, la matrice diagonale $M := \mathrm{diag}(\varepsilon, 0)$ satisfait $M^{n+1} = 0$ mais $M^n \neq 0$. Les systèmes d'équations polynomiales définis par les idéaux I_n et I_{n+1} n'ont donc pas les mêmes solutions dans $M_2(k_n)$ et ne peuvent donc pas être égaux. Justifions ce dernier point.

  Soit I un idéal de $k[X_1, \ldots, X_n]$ et B une k-algèbre commutative quelconque. On pose

$$V(I,B) := \{(b_1, \ldots, b_n) \in B^n,\ \forall f \in I, f(b_1, \ldots, b_n) = 0\} \subset B^n.$$

Il est clair que $V(I) = V(I,k)$, et que si $I \subset J$, $V(J,B) \supset V(I,B)$. Le Nullstellensatz assure que la connaissance de $V(I,k)$ permet de retrouver $\sqrt{I}$, mais pas I. En général, on a besoin des $V(I,B)$ avec B contenant des éléments nilpotents pour distinguer deux idéaux ayant même radical.

Appliquons ceci à nos idéaux I_n et I_{n+1}, et $B = k_n$. L'exemple plus haut montre que $V(I_n, k_n) \subsetneq V(I_{n+1}, k_n)$, et donc $I_n \neq I_{n+1}$. Ce que l'on voulait.

– (solution de Bruno J. et Sylvain R.) Soient a_n, b_n, c_n et $d_n \in k[a,b,c,d]$ les coefficients de N^n. Il est clair qu'ils sont homogènes de degré n, i.e. satisfont $f(ta, tb, tc, td) = t^n f(a,b,c,d)$, de sorte que I_n est engendré par des éléments homogènes de degré n. En particulier, tout polynôme homogène de I_n est de degré $\geq n$. Ainsi $I_{n+1} \subsetneq I_n$ car le second contient un élément homogène de degré n et pas le premier.

Exercice 1 du TD 8

D'après un résultat du cours, l'ensemble $\overline{\mathbb{Z}}$ des nombres complexes qui sont entiers algébriques sur $\mathbb{Z}$ est un sous-anneau de $\mathbb{C}$. Il contient toutes les racines de l'unité (annulées par un $X^n - 1$), ainsi donc que $1 + 2i$, $\zeta := e^{2i\pi/n}$ et $\zeta + \zeta^{n-1} = 2\cos(2\pi/n)$.

Si $n \in \mathbb{Z}$ est $\equiv 1 \bmod 4$, alors $\frac{1+\sqrt{n}}{2}$ est annulé par $X^2 + X + \frac{1-n}{4} \in \mathbb{Z}[X]$, ce qui montre que $\frac{1+\sqrt{5}}{2} \in \overline{\mathbb{Z}}$.

D'après un résultat du cours, $\mathbb{Q}$ est intégralement clos, et donc $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z} : 1/5 \notin \overline{\mathbb{Z}}$.

Si $K \subset \mathbb{C}$ est un sous-corps galoisien fini sur $\mathbb{Q}$ et $x \in \overline{\mathbb{Z}} \cap K$, alors pour tout $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(x) \in K \cap \overline{\mathbb{Z}}$ (appliquer σ à une équation polynomiale unitaire à coefficients entiers satisfaite par x). En particulier, $\frac{3+4i}{5} \in \overline{\mathbb{Z}} \Rightarrow \frac{3+4i}{5} + \frac{3-4i}{5} = 6/5 \in \overline{\mathbb{Z}}$, ce qui est absurde par le paragraphe précédent. De même, $\frac{1+\sqrt{3}}{2}\frac{1-\sqrt{3}}{2} = -1/2$ montre que[5] $\frac{1+\sqrt{3}}{2} \notin \overline{\mathbb{Z}}$.

Soient $n \geq 1$, $\zeta := e^{2i\pi/n}$ et $x := \cos(2\pi/n) = \frac{\zeta+\zeta^{-1}}{2}$, tous ces nombres sont dans l'extension galoisienne $\mathbb{Q}(\zeta)$. Soient $x_1, \ldots, x_k$ les conjugués de x sur $\mathbb{Q}$, i.e. les autres racines du polynôme minimal de x sur $\mathbb{Q}$. Il sont tous de la forme

$$\sigma(x) = \frac{\sigma(\zeta) + \sigma(\zeta)^{-1}}{2}, \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}),$$

donc de la forme $\cos(2k\pi/n)$ pour avec $(k,n) = 1$. Supposons que x, et donc tous les x_i, sont dans $\overline{\mathbb{Z}}$. Il en va de même pour leur produit $p := \prod_{i=1}^n x_i \in \mathbb{Z}$. Mais pour tout i, x_i est un nombre réel dans $[-1,1]$, ainsi donc que p, d'où $p = 0$, -1 ou 1. Si $p = 0$, c'est que l'un des x_i est nul, mais alors $x_i = x = 0$ est de degré 1 sur $\mathbb{Q}$ et $n = 4$. Si $p = \pm 1$, il en va de même pour tous les x_i, et donc encore $x = x_i = p = \pm 1$. Ainsi, $x \in \overline{\mathbb{Z}}$ si, et seulement si, $n = 1, 2, 4$, auquel cas $x = 1, -1, 0$ respectivement.

Remarques: La preuve ci-dessus est une variante de celle que nous avions donnée en TD qui n'utilise pas le fait que $[\mathbb{Q}(x) : \mathbb{Q}] = \varphi(n)/2$. Rappelons que cette dernière égalité vient de ce que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ par irréductibilité du n^{ieme} polynôme cyclotomique, et de ce que $[\mathbb{Q}(\zeta) : \mathbb{Q}(x)] = 2$ car $\zeta^2 - 2\zeta x + 1 = 0$.

[5] Par contre, vous pouvez vérifier que $\frac{1+\sqrt{3}}{\sqrt{2}} \in \overline{\mathbb{Z}}$!

L'exercice 3 donne en fait une condition nécessaire et suffisante sur le polynôme minimal unitaire P_x d'un nombre algébrique $x \in \mathbb{C}$ pour qu'il soit entier sur $\mathbb{Z}$: il faut et suffit que $P_x \in \mathbb{Z}[X]$. Ce critère aurait cependant été assez peu pratique pour vérifier que $\cos(2\pi/n) \notin \overline{\mathbb{Z}}$.

Exercice 2 du TD 8 Le corps de fraction de l'anneau $A = \mathbb{Z}[i]$ (resp. $A = \mathbb{C}[T^2, T^3]$) est $\mathbb{Q}(i)$ (resp. $\mathbb{C}(T)$). Il contient l'élément i (resp. T), qui n'est pas dans A, mais qui est entier sur A car $i^2 \in \mathbb{Z} \subset \mathbb{Z}[i]$ (resp. $T^2 \in A$).

Exercice 3 du TD 8

(a) Soit $x \in L$ et P son polynôme minimal unitaire sur K, $P(x) = 0$. Si P est dans $A[X]$, x est entier sur A. Réciproquement, supposons x entier sur A, et considérons $x_1, \ldots, x_n$ les racines de P dans une clôture algébrique de L. Soit $Q \in A[X]$ unitaire tel que $Q(x) = 0$. Alors P divise Q dans $K[X]$ et donc $Q(x_i) = 0$ pour chaque i. Ainsi, x_i est entier sur A, ce qui montre l'indication. Mais chaque coefficient de P est dans $\mathbb{Z}[x_1, \ldots, x_n]$, donc entier sur A par un résultat du cours ("les entiers sur A de $\overline{L}$ forment un sous-anneau"), mais aussi dans K. L'anneau A étant intégralement clos, il vient que $P \in A[X]$, ce que l'on voulait.

(b) Notons que si $P \in K[X]$, $P(m_x) = m_{P(x)}$, et que $m_x = 0$ si, et seulement si, $x = 0$, de sorte que le polynôme minimal de m_x vu comme K-endomorphisme de L est aussi celui de x. On conclut par le lemme général standard d'algèbre linéaire : "Soit K un corps et $M \in M_n(K)$, le polynôme minimal de M et son polynôme caractéristique ont les mêmes facteurs irréductibles".

Dans le cas qui nous intéresse plus particulièrement où le polynôme minimal de M est irréductible, i.e. $K[M]$ est un corps, il suffit de considérer une base (e_i) de K^n comme $K[M]$-espace vectoriel, puis de calculer le déterminant de $X.1 - M$ dans la base télescopique des $M^j e_i$, $j \leq \deg(P) - 1$.

(c) On a vu au (b) que $\chi_x = P^m$. Par le (a), si x est entier sur A, $P \in A[X]$ et donc $\chi_x = P^m \in A[X]$. La réciproque est évidente car χ_x est unitaire.

Exercice 4 du TD 8

(a) Le corps de fractions de $\mathbb{Z}[i\sqrt{5}]$ est $K := \mathbb{Q}(i\sqrt{5})$. Comme $\mathbb{Z}[i\sqrt{5}]$ est entier sur $\mathbb{Z}$, $x \in K$ est entier sur $\mathbb{Z}[i\sqrt{5}]$ si, et seulement si, il est entier sur $\mathbb{Z}$. Soit $z := a + bi\sqrt{5}$ entier sur $\mathbb{Z}$ avec a, $b \in \mathbb{Q}$. Par un argument déjà donné dans la correction de l'exercice 1, $z' := a - bi\sqrt{5}$ est aussi entier sur $\mathbb{Z}$, ainsi que $z + z' = 2a$ et $zz' = a^2 + 5b^2$. Comme ils sont dans $\mathbb{Q}$, ils sont donc dans $\mathbb{Z}$ ("$\mathbb{Q}$ est intégralement clos"). Si $2a$ est un entier impair, il vient que $5(2b)^2 \in -1 + 4\mathbb{Z}$. En particulier, $2b$ aussi est un entier impair, et on obtient une contradiction modulo 4. Ainsi, $2a$ est un entier pair, puis $a \in \mathbb{Z}$, et $5b^2 \in \mathbb{Z} \Rightarrow b \in \mathbb{Z}$.

(b) Considérons la relation $6 = 2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5}) \in \mathbb{Z}[i\sqrt{5}]$. S'il on montre que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont des irréductibles, et que ni 2 ni 3 n'est associé à $1 + i\sqrt{5}$, alors $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel. Soit z l'un de ces nombres, s'il est réductible il s'écrit $z = ab$ avec a, $b \in \mathbb{Z}[i\sqrt{5}]$ non unités. Nous allons chercher une contradiction.

Il importe en premier lieu de trouver les unités de l'anneau $A := \mathbb{Z}[i\sqrt{5}]$. Si u, $u' \in A$ satisfont $uu' = 1$, alors en notant N la norme complexe au carré il vient que $N(u)N(u') = 1$, donc $N(u) = 1 = c^2 + 5d^2$ si $u = c + id\sqrt{5}$. Ainsi, $d = 0$ et $u = u' = \pm 1$. On a montré que $A^* = \{\pm 1\}$ et que $u \in A^*$ si, et seulement si, $N(u) = 1$.

Revenons à $z = ab$ et prenons encore le carré de la norme. On a $N(z) = N(a)N(b)$ avec $N(a)$, $N(b) > 1$. Les $N(z)$ possibles pour les différents z sont 4, 9 et 6. On conclut car il n'existe aucun élément $x \in A$ tel que $N(x) = 2$ ou 3, car $c^2 + 5d^2$ ne prend jamais ces valeurs sur $\mathbb{Z}^2$.

Il ne reste qu'à voir que $z = 1 + i\sqrt{5}$ n'est associé ni à 2 ni à 3. Mais il est évident que z n'est pas de la forme $z = 2u$ ou $3u$ pour $u \in A$ (soit en prenant N, soit car l'écriture sous la forme $c + id\sqrt{5}$ avec $c, d \in \mathbb{Z}$ est unique et ni 2 ni 3 ne divise 1...).

Exercice 1 du TD 7

(a) Considérons $\Delta := \prod_{i<j}(X_i - X_j)^2 \in R := \mathbb{Z}[X_1, \ldots, X_n]$. Alors Δ est invariant par $\mathfrak{S}_n$, il est donc dans $\mathbb{Z}[\Sigma_0, \ldots, \Sigma_{n-1}]$, Σ_i étant le i^{eme} polynôme symétrique élémentaire.

Considérons le morphisme d'anneaux $f : R[X] \to K[X]$ défini par $X_i \mapsto x_i$, $X \mapsto X$. Alors $f(\Delta) = \mathrm{disc}(P)$ et appliquant f à $\prod_{i=1}^n (X - X_i) = \sum_{i=0}^n \Sigma_i (-1)^{n-i} X^i$, on trouve que

$$P(X) = \sum_{i=0}^{n} f(\Sigma_i)(-1)^{n-i} X^i. \tag{2}$$

Mais $f(X) \in k[X]$ et donc les $f(\Sigma_i)$, puis $\mathrm{disc}(P)$, sont dans k. Par définition, $\mathrm{disc}(P) = 0$ si, et seulement si, P a une racine multiple dans $\overline{k}$, si, et seulement si, P n'est pas séparable.

(b) Soit $\sigma \in \mathrm{Gal}(K/k) \subset \mathfrak{S}(\{x_1, \ldots, x_n\}) \simeq \mathfrak{S}_n$ (noter que P est séparable par hypothèse). On remarque que σ permute les couples (i, j) avec $i \neq j$, et que si $n(\sigma)$ désigne le nombre de couples $i < j$ tels que $\sigma(i) < \sigma(j)$ alors on sait que $(-1)^{n(\sigma)}$ est la signature $\varepsilon(\sigma)$ de σ. Ainsi, $\sigma(\delta) = \varepsilon(\sigma).\delta$. En particulier, K/k étant galoisienne, $\mathrm{Gal}(K/k) \subset \mathfrak{A}_n$ si, et seulement si, $\delta \in K^{\mathrm{Gal}(K/k)} = k$, si, et seulement si, $\mathrm{disc}(P) = \delta(P)^2$ est le carré d'un élément de k.

(c) On considère le même morphisme $f : R[X] \to K[X]$ qu'en (a). Notons que par hypothèse, $P(X) \in A[X]$, de sorte que par la formule (2), les $f(\Sigma_i)$ et $\mathrm{disc}(P)$ sont dans A.

D'après le (a), il suffit de voir que l'image de $\mathrm{disc}(P)$ dans A/Q est égale à $\mathrm{disc}(\overline{P})$. Soit $L \supset A/Q$ un corps de décomposition de $\overline{P} \in (A/Q)[X]$, $\{y_i\}$ les n racines de $\overline{P}$ dans L (éventuellement avec multiplicité) $f' : R[X] \to L[X]$ le morphisme d'anneaux naturel défini par $X_i \mapsto y_i$. On a vu au (a), on a que $\mathrm{disc}(P) = f(\Delta)$ et $\mathrm{disc}(\overline{P}) = f'(\Delta)$ où Δ est dans le sous-anneau $R' := \mathbb{Z}[\Sigma_0, \ldots, \Sigma_{n-1}]$. Mais on a vu ci-dessus que $f(R') \subset A[X]$, de sorte que l'on peut considérer $\overline{f} : R'[X] \to (A/Q)[X] \subset L[X]$ par projection $A \to A/Q$. Il suffit donc de voir que $\overline{f} = f'_{|R'[X]}$. Mais comme ces deux morphismes coïncident sur X, il suffit de voir qu'ils coïncident sur les Σ_i, mais cela est une conséquence directe de la formule (2).

(d) Le (i) est un cas particulier de la première assertion de (c), le (ii) de la seconde. Le (iii) est conséquence du (ii) et du second point du (a), car un entier non nul n'a qu'un nombre fini de diviseurs premiers.

Exercice 2 du TD 7 (Avec exemple d'utilisation de Maple)

maple Maple Output 2D Math 2D Output active1da :=$X^3 - X + 1$;
inert2da := $X^3 - X + 1$; $a := X^3 - X + 1$
active1dBerlekamp(a,X) mod 2 ;
inert2d{$X^3 + X + 1$}; $\{X^3 + X + 1\}$
active1dBerlekamp(a,X) mod 5 ;
inert2d{$X^2 + 3 * X + 3, X + 2$}; $\{X^2 + 3\,X + 3,\ X + 2\}$
active1dgalois(a,X) ;
inert2d"3T2", {"S(3)"}, "-", 6, {"(1 2)", "(1 2 3)"} ;

"3T2", {"S(3)"}, "-", 6, {"(1 2)", "(1 2 3)"}

a est irréductible modulo 2 car n'a pas de racines dans $\mathbb{F}_3$. Le théorème de Gauss implique qu'il est irréductible dans $\mathbb{Q}[X]$. Son groupe de Galois sur $\mathbb{Q}$ est alors un sous-groupe transitif G de $\mathfrak{S}_3$. Il contient donc un 3-cycle (cela se déduirait aussi de ce que a est irréductible mod. 2). Comme a mod 5 est séparable de type $(2, 1)$, il vient que G contient une transposition, donc $G = \mathfrak{S}_3$.

---

active1db :=$X^3 - 7 * X + 7$;
inert2db := $X^3 - 7 * X + 7$; $b := X^3 - 7\,X + 7$
active1difactor(discrim(b,X)) ;
inert2d"$(7)^2$; $(7)^2$
active1dBerlekamp(b,X) mod 2 ;
inert2d{$X^3 + X + 1$}; $\{X^3 + X + 1\}$
active1dgalois(b,X) ;
inert2d"3T1", {"A(3)"}, "+", 3, {"(1 2 3)"} ;

"3T1", {"A(3)"}, "+", 3, {"(1 2 3)"}

Comme précédemment, G est un sous-groupe transitif de $\mathfrak{S}_3$. Comme son discriminant est un carré dans $\mathbb{Q}$, il tombe dans $\mathfrak{A}_3$. C'est donc $\mathfrak{A}_3$.

En fait, voici comment on peut construire plein d'exemples de polynômes de groupes de Galois $\mathfrak{A}_3$. Soit p un nombre premier congru à 1 mod 3. C'est un théorème de Gauss que $4p = A^2 + 27B^2$ pour des entiers A et B, et aisé à vérifier en pratique. Ici $4.7 = 1 + 27$. Notons que l'on a $4p^3 - 27(pB)^2 = (pA)^2$, de sorte que le discriminant du polynôme

$$X^3 - pX + pB,$$

est un carré. Noter de plus que ce polynôme est toujours irréductible par Eisenstein en p, de sorte que son groupe de Galois est $\mathfrak{A}_3$.

---

active1dc :=X^4 + 25 * X^3 + 5 * X^2 + 25 * X − 19;
inert2dc := X^4 + 25 * X^3 + 5 * X^2 + 25 * X − 19; $c := X^4 + 25\,X^3 + 5\,X^2 + 25\,X - 19$
active1dBerlekamp(c,X) mod 2 ;
inert2d{X^4 + X^3 + X^2 + X + 1}; $\{X^4 + X^3 + X^2 + X + 1\}$
active1dBerlekamp(c,X) mod 3 ;
inert2d{X^3 + 2 * X + 2, X + 1}; $\{X^3 + 2\,X + 2,\ X + 1\}$
active1dgalois(c,X) ;
inert2d"4T5", {"S(4)"}, "-", 24, {"(1 3 2 4)", "(1 3 4 2)"} ;
“4T5”, {“S(4)”}, “-”, 24, {“(1 3 2 4)”, “(1 3 4 2)”}

Comme précédemment, l'irréductibilité de la réduction mod 2 de c montre que c est irréductible dans $\mathbb{Q}[X]$ et que son groupe de Galois G est un sous-groupe transitif de $\mathfrak{S}_4$ par l'action naturelle sur les 4 racines de c. Pour vérifier l'irréductibilité de c mod 2. On peut remarquer que c'est un polynome cyclotomique : précisément c'est φ_5 mod 2, qui est donc irréductible car 2 engendre $(\mathbb{Z}/5\mathbb{Z})^*$ (cf. ex. 8 TD4). Sinon, il suffit de vérifier qu'il n'a pas de racines dans $\mathbb{F}_4 = \{0, 1, j, j^2\}$ ($j^3 = 1$), ce qui est tres facile : c'est clair pour 0 et 1, et pour $x = j$, j^2 on a $c(x) = x + 1$. De plus, le polynôme $X^3 - X - 1$ induit la fonction polynomiale 1 sur $\mathbb{F}_3$, il n'y a donc pas de racines : il est irréductible[6]. c mod 3 est donc séparable de type $(3, 1)$.

Ainsi, G contient un 3-cycle et un 4-cycle. Cela suffit pour engendrer $\mathfrak{S}_4$ car un tel sous-groupe a au moins 12 éléments et n'est pas $\mathfrak{A}_4$ (noter que $\mathfrak{A}_n$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$). Donc $G = \mathfrak{S}_4$.

---

active1dd :=X^4 + 4 * X^3 + 12 * X^2 + 24 * X + 24;

inert2dd := X^4 + 4 * X^3 + 12 * X^2 + 24 * X + 24; $d := X^4 + 4\,X^3 + 12\,X^2 + 24\,X + 24$
active1difactor(discrim(d,X)) ;
inert2d“(2)^12 * “(3)^4; (2)^12 (3)^4
active1dBerlekamp(d,X) mod 5 ;
inert2d{X^3 + 2 * X + 1, X + 4}; $\{X^3 + 2\,X + 1,\ X + 4\}$
active1dgalois(d,X) ;
inert2d"4T4", {"A(4)"}, "+", 12, {"(1 3 2)", "(1 4 2)"} ;
“4T4”, {“A(4)”}, “+”, 12, {“(1 3 2)”, “(1 4 2)”}

Même raisonnement que précédemment. La donnée de d mod 5 (et le thm de Gauss) montre que d est irréductible car il n'a pas de racine. La donnée du discriminant montre

[6]En fait c'est même un polynôme d'Artin-Schreier : $X^q - X + a$, toujours irréductible sur $\mathbb{F}_q$

que $G \subset \mathfrak{A}_4$. On conclut que $G = \mathfrak{A}_4$ car $4||G|$ par transitivité sur $\{1, ..., 4\}$ et $3||G|$ à cause du 3-cycle donné par d mod 5.

---

active1de :=$X^5 + X + 3$;
inert2de := $X^5 + X + 3$; $e := X^5 + X + 3$
active1dBerlekamp(e,X) mod 2 ;
inert2d{$X^2 + X + 1, X^3 + X^2 + 1$}; {$X^2 + X + 1$, $X^3 + X^2 + 1$}
active1dBerlekamp(e,X) mod 7 ;
inert2d{$X^5 + X + 3$}; {$X^5 + X + 3$}
active1dgalois(e,X) ;
inert2d"5T5", {"S(5)"}, "-", 120, {"(1 2 3 4 5)", "(1 2)"} ;
"5T5", {"S(5)"}, "-", 120, {"(1 2 3 4 5)", "(1 2)"}

---

active1df :=$X^5 + X^4 + 5 * X^3 + 5 * X^2 + 5 * X + 4$;
inert2df := $X^5+X^4+5*X^3+5*X^2+5*X+4$; $f := X^5 + X^4 + 5\,X^3 + 5\,X^2 + 5\,X + 4$
active1dBerlekamp(f,X) mod 2 ;
inert2d{X, $X^4 + X^3 + X^2 + X + 1$}; {X, $X^4 + X^3 + X^2 + X + 1$}
active1dBerlekamp(f,X) mod 5 ;
inert2d{$X^5 + X^4 + 4$}; {$X^5 + X^4 + 4$}
active1dBerlekamp(f,X) mod 7 ;
inert2d{$X^3 + 5, X + 6, X + 2$}; {$X^3 + 5$, $X + 6$, $X + 2$}
active1dgalois(f,X) ;
inert2d"5T5", {"S(5)"}, "-", 120, {"(1 2 3 4 5)", "(1 2)"} ;
"5T5", {"S(5)"}, "-", 120, {"(1 2 3 4 5)", "(1 2)"}

Exercice 2 du TD 6 P est irréductible dans $\mathbb{Q}(j)[p, q][X]$ car il est unitaire de degré 1 en q. L'anneau $\mathbb{Q}(j)[p, q]$ étant factoriel, il l'est encore dans $\mathbb{Q}(j, p, q)[X]$.

Enfin, P est séparable car on est en caractéristique 0. Son groupe de Galois est un sous-groupe transitif de $\mathfrak{S}_3$, qui est $\mathcal{A}_3$ si, et seulement si, le discriminant de P est un carré dans $\mathbb{Q}(p, q, j)$. Mais ce discriminant est $d := -4p^3 - 27q^2$. Par factorialité de $\mathbb{Q}(j)[p, q]$, il suffit de voir que d n'est pas un carré dans $\mathbb{Q}(j)[p, q]$. Mais ceci est clair car modulo q, *i.e.* dans $\mathbb{Q}(j)[p]$, c'est $-4p^3$ qui pas un carré car de degré impair en p.

(b) Soient X_1, X_2 et X_3 les trois racines de P dans K, $\delta := (X_1-X_2)(X_1-X_3)(X_2-X_3)$, on sait que $\delta^2 = d = -4p^3 - 27q^2$. On pose $k := \mathbb{Q}(j, p, q)$. $K/k(\delta)$ est une extension de Kummer (de degré 3) car $j \in k(\delta)$, elle est donc obtenue par extraction d'une racine cubique. D'après le (a), il existe $\sigma \in \mathrm{Gal}(K/k(\delta))$ un automorphisme correspondant au 3-cycle $(1, 2, 3)$, $\langle\sigma\rangle = \mathrm{Gal}(K/k(\delta))$. Explicitement, si $A := X_1 + j^2X_2 + jX_3$, $\sigma(A) = jA$

et donc $A^3 \in k(\delta)$. On sait donc que l'on peut exprimer explicitement A^3 en fonction de p, q, j et δ, de même pour le cube de $B = X_1 + jX_2 + j^2X_3$. On trouve :

$$A^3 = \frac{-3\sqrt{-3}\delta - 27q}{2},\ B^3 = \frac{3\sqrt{-3}\delta - 27q}{2}$$

En maple, il suffirait d'écrire :
⟩ simplify$((X+u*Y+u^2*Z)^3, \{u^2+u+1, X+Y+Z, X*Y*Z = -q, X*Y+X*Z+Y*Z = p, (X-Y)*(X-Z)*(Y-Z) = d\})$;

Cela renvoie

$$3*u*d - 27/2*q + 3/2*d$$

Enfin, par hypothèse, on a $X_1 + X_2 + X_3 = 0$. On dispose ainsi d'un système linéaire 3,3 sur les X_i dont la matrice est celle de Vandermonde pour $(1, j^2, j)$, donc inversible. L'inversion de cette matrice est facilité par le fait que c'est une similitude unitaire de rapport 3, son inverse est donc le tiers de son adjoint. On trouve que :

$$X_1 = \frac{A+B}{3},\ X_2 = \frac{jA+j^2B}{3},\ X_3 = \frac{j^2A+jB}{3},$$

A et B étant des racines cubiques d'éléments explicites de $\mathbb{Q}(j, p, q, \delta)$ donnés plus haut. Ce sont les formules de Cardan-Tartaglia.

Exercice 5 du TD 6

(a) Le sous-groupe de $\mathfrak{S}_n$ engendré par $\tau := (1, 2)$ et $c := (1, 2, .., n)$ contient les $c^{i-1}\tau c^{1-i} = (i, i+1)$, puis les $(1, i) = (i-1, i)(1, i-1)(i, i-1)$, puis $(i, j) = (1, j)(1, i)(1, j)$, c'est donc tout $\mathfrak{S}_n$.

Un élément d'ordre p de $\mathfrak{S}_p$ est un p-cycle, et on peut toujours supposer, quitte à renuméroter, que la transposition de l'énoncé est $(1, 2)$. Mais p étant premier, une puissance $< p$ du p-cycle envoie 1 sur 2, et c'est encore un p-cycle car p est premier, ce qui nous ramène au cas du paragraphe précédent.

Vérifier que dans $\mathfrak{S}_4$, $(1, 3)$ et $(1, 2, 3, 4)$ satisfont $\tau c = c^{-1}\tau$. Ils engendrent donc un groupe de cardinal 8, strictement inclus dans $\mathfrak{S}_4$. Ainsi, l'hypothèse p premier est bien nécessaire.

(b) $P = X^5 - 4X + 2$ est irréductible dans $\mathbb{Q}[X]$ par le critère d'Eisenstein, on note $S := \{x_1, \ldots, x_5\}$ l'ensemble de ses 5 racines, $K := \mathbb{Q}(x_1, \ldots, x_5)$, $G := \mathrm{Gal}(K/\mathbb{Q})$. G agit par permutation sur les éléments de S, d'où un morphisme $\varphi : G \to \mathfrak{S}(S) \simeq \mathfrak{S}_5$, ce morphisme est injectif car S engendre K comme $\mathbb{Q}$-algèbre. On sait que l'action de G sur S est transitive car P est irréductible. Écrivons S comme l'orbite de x_1 sous G disons, le cardinal de l'orbite divisant celui de G, on a que 5 divise $|G| = |\varphi(G)|$. 5 étant premier, G a donc un élément d'ordre 5. Les seuls éléments d'ordre 5 dans $\mathfrak{S}_5$ étant les 5-cycles, $\varphi(G)$ contient un 5-cycle. De plus, une étude rapide de la fonction d'une variable réelle $x \mapsto P(x)$ montre que P a exactement 3 racines réelles. Ainsi, la conjugaison complexe agit sur S par un élément qui est une transposition dans $\varphi(G)$. Le (a) conclut que $\varphi(G) \simeq G \simeq \mathfrak{S}_5$.

(c,d) Le raisonnement précédent montre qu'il suffit de trouver un polynôme irréductible de degré premier p ayant exactement 2 racines complexes. Le problème étant trivial pour $p = 2$, on peut supposer $p > 2$. Soit $P_n := (X^2+1)X(X-1)(X-2)(X-(p-3))+1/n$. Par continuité des racines d'un polynôme en fonction de ses coefficients, P_n a exactement deux racines complexes non réelles quand n est assez grand. Montrons que l'on peut le choisir irréductible dans $\mathbb{Q}[X]$. Notons que $P_n(X)$ est irréductible dans $\mathbb{Q}[X]$ si, et seulement si, $X^p P_n(1/X)$ l'est. Mais si n est premier, on voit que $nX^p P_n(1/X)$ est un polynôme d'Eisenstein, donc irréductible. On conclut donc en prenant n premier assez grand.

Exercice 9 du TD 6 (Lucy et Lily) Voir l'adresse web :

http ://www.math.umd.edu/˜res/Java/App13/test1.html

Exercice 12 du TD 6 (Problème) On supposera k de caractéristique nulle pour simplifier.

(a) k étant parfait, K/k est galoisienne finie, soit G son groupe de Galois. On suppose par l'absurde que $G \neq \{1\}$, on peut donc trouver $H \subset G$ un sous-groupe cyclique d'ordre premier, disons p. On pose $L := K^H$. L'extension K/L est galoisienne cyclique d'ordre p. Si p est impair, montrons que L contient les racines p^{iemes} de l'unité : une telle racine est de degré $\leq p-1$ sur L, et divisant $p = [K : L]$, donc de degré 1. Par le théorème de structure des extensions cycliques d'ordre n quand le corps de base contient toutes les n racines n^{ieme} de l'unité, on peut donc écrire $K = L(\sqrt[p]{a})$, a non une puissance p^{ieme} dans L. Mais alors $X^{p^2} - a$ est irréductible dans $L[X]$ par l'exercice précédent du TD, et donc $[K : L] \geq p^2$: c'est absurde. On a donc $p = 2$, et $K = L(\sqrt{a})$, $a \in L$ qui n'est pas un carré.

Encore par l'exercice précédent du TD, $a = -4b^4$ pour un $b \in L$ (sinon $X^4 - a$ est irréductible dans $L[X]$ et $[K : L] \geq 4$). On en déduit que $L(\sqrt{a}) = L(\sqrt{-1})$, ce qui est absurde car -1 est un carré dans L par hypothèse. Ainsi, $K = k$.

(b) On applique la question précédente à $k(\sqrt{-1})$.

(c) Montrons qu'une somme de deux carrés est un carré, on pose $i = \sqrt{-1} \in K$. Si $x, y \in k$, $x^2 + y^2 = (x + iy)(x - iy)$, et on peut trouver $u \in K$ tel que $x + iy = u^2$ (K est algébriquement clos). Si σ désigne l'unique automorphisme non trivial de l'extension galoisienne K/k (de degré 2), $\sigma(i) = -i$, et on a $x^2+y^2 = u^2\sigma(u^2) = (u\sigma(u))^2$ et $u\sigma(u) \in k$.

$x \leq x$ est évident pour tout $x \in k$. Une somme de deux carré étant un carré, $x \leq y$ et $y \leq z$ impliquent que $x \leq z$. Notons que pour x, y et z dans k, $x \leq y$ si, et seulement si, $x + z \leq y + z$. Ainsi, si $x \leq y$ et $y \leq x$, $y - x$ est un carré dans k ainsi que son opposé. Si $y - x \neq 0$, cela implique que -1 est un carré, ce qui n'est pas, donc $y = x$. De même, pour voir que l'ordre est total, il suffit de voir que tout élément de k, ou son opposé, est un carré dans k. Mais si $x \in k$, $x = u^2$ dans K, et $\sigma(u)^2 = x = u^2$ implique que $\sigma(u) = u$ ou $-u$, puis respectivement que x ou $-x$ est un carré dans k.

L'ordre induit sur $\mathbb{Q}$ satisfait $1 > 0$ donc $p/q > 0$ si, et seulement si, p/q est positif au sens usuel, ce qui conclut immédiatement.

(d) Il suffit de remarquer qu'un polynôme irréductible unitaire $P \in k[X]$ est de degré 1 ou 2, et que s'il est de degré 2, il est de la forme $x^2 + ax + b = (x + a/2)^2 + \Delta^2$ avec $\Delta \in k$, donc strictement positif. On conclut en regardant les changements de signe.

(e) Pour voir que k est archimédien, il suffit de voir que si $1 < x \in k$, il existe $n \in \mathbb{N}$ tel que $x < n$. x étant algébrique sur $\mathbb{Q}$, on a $x^n = a_{n=1}X^{n-1} + \cdots + a_0$, les a_i étant dans $\mathbb{Q}$. Il est facile de voir que $|.|$ satisfait l'inégalité triangulaire, et $|xy| = |x||y|$. Il vient que

$$|x|^n = |x^n| \leq n(\sup_i |a_i|)|x|^{n-1},$$

puis $|x| \leq n \sup_i\{|a_i|\} \in \mathbb{Q}^{>0}$, puis ce qu'on voulait.

(f) On déduit de la propriété d'être archimédien que les nombres rationnels sont denses dans k pour la topologie engendrée par les intervalles ouverts. En effet, si $0 < x < y \in k$, soit $n \in \mathbb{N}$ tel que $n(y-x) > 2$, alors l'intervalle $]nx, ny[$ contient un entier m : le successeur du plus grand élément de l'ensemble fini (car k archimédien) des entiers inférieur à nx.

On considère l'application $\iota : k \to \mathbb{R}$, $x \mapsto \sup_{z\in\mathbb{Q}, z<x\in k} z$. Il est aisé de vérifier que ι est $\mathbb{Q}$-linéaire, strictement croissante (par densité de $\mathbb{Q}$ dans k), puis continue. Sa restriction à $\mathbb{Q}$ est un morphisme de corps (l'identité !), ainsi donc que sur k par densité.

L'image de ι tombe dans $\overline{\mathbb{Q}} \cap \mathbb{R}$, qui est d'indice 2 dans $\overline{\mathbb{Q}}$ par le théorème d'Artin (ce sont les invariants de la conjugaison complexe). ι s'étend un morphisme $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$, qui est un isomorphisme comme tout tel morphisme, en particulier $2 = [\overline{\mathbb{Q}} : K] = [\overline{\mathbb{Q}} : \iota(K)] = [\overline{\mathbb{Q}} : \mathbb{R} \cap \overline{\mathbb{Q}}][\mathbb{R} \cap \overline{\mathbb{Q}} : \iota(K)]$ montre que ι est un isomorphisme de K sur $\overline{\mathbb{Q}} \cap \mathbb{R}$.

(g) Si $H \subset G := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ est d'ordre fini, le théorème d'Artin nous dit que $\overline{\mathbb{Q}}/\overline{\mathbb{Q}}^H$ est finie de degré $|H|$. Le (b) assure que cet ordre est donc 2. On note τ l'élément non trivial de H.

Soit $K := \overline{\mathbb{Q}}^{\langle\tau\rangle}$, d'après (f) il existe un isomorphisme de corps $\sigma : K \to \mathbb{R} \cap \overline{\mathbb{Q}}$. On en déduit que $\tau = \sigma^{-1}c\sigma$, $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ désignant la conjugaison complexe.

Exercice 2 du TD 5 Toute extension finie de $\mathbb{Q}$ est séparable car $\mathbb{Q}$ est de caractéristique 0. Une extension finie du type $\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}$ est donc galoisienne si, et seulement si, elle est normale, ce qui est équivalent à demander que les polynômes minimaux des x_i sur $\mathbb{Q}$ soient scindés dans $\mathbb{Q}(x_1, \ldots, x_n)$. En particulier, si les x_i sont les racines d'un polynôme dans $\mathbb{Q}[X]$, $\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}$ est galoisienne. Si $K/\mathbb{Q}$ est le corps de décomposition sur $\mathbb{Q}$ d'un polynôme dans $\mathbb{Q}[X]$, $K/\mathbb{Q}$ est donc galoisienne. On verra toutes les extensions finies qui suivent comme des sous-corps de $\mathbb{C}$.

(a) 11 n'est pas un carré dans $\mathbb{Q}$, $X^2 - 11$ est donc irréductible dans $\mathbb{Q}[X]$ et $[\mathbb{Q}(\sqrt{11}) : \mathbb{Q}] = 2$. $\mathbb{Q}(\sqrt{11})/\mathbb{Q}$ galoisienne car c'est le corps de décomposition sur $\mathbb{Q}$ de $X^2-11 \in \mathbb{Q}[X]$. On en déduit que $\mathrm{Gal}(\mathbb{Q}(\sqrt{11})/\mathbb{Q})$ a deux éléments, c'est donc $\mathbb{Z}/2\mathbb{Z}$. L'élément non trivial est uniquement déterminé sur $\sqrt{11}$ et ne le fixe pas (sinon il fixerait tout $\mathbb{Q}(\sqrt{11})$), il l'envoie donc sur $-\sqrt{11}$ [7].

[7] Noter que l'on a montré ainsi qu'il existe un automorphisme de $\mathbb{Q}(\sqrt{11})$ envoyant $a + b\sqrt{11}$ sur $a - b\sqrt{11}$ $(a, b \in \mathbb{Q})$. En particulier, cela prouve que $a + b\sqrt{11} \mapsto a - b\sqrt{11}$ est un morphisme de corps.

Un sous-corps de $\mathbb{Q}(\sqrt{11})$ est de degré 1 ou 2 sur $\mathbb{Q}$, c'est donc $\mathbb{Q}$ ou $\mathbb{Q}(\sqrt{11})$, et tout élément non dans $\mathbb{Q}$ est primitif. Il est clair que l'on peut remplacer 11 par tout entier n qui n'est pas un carré dans $\mathbb{Z}$, et que tout ce que l'on a dit ci-dessus pour $\mathbb{Q}(\sqrt{11})$ vaut pour $\mathbb{Q}(\sqrt{n})$.

(b) Soit $K := \mathbb{Q}(\sqrt{2}, \sqrt{3})$. K contient $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ qui sont de degré 2 sur $\mathbb{Q}$ par la remarque terminant le (a). Montrons que $X^2 - 2$ est irréductible dans $\mathbb{Q}(\sqrt{3})[X]$. En effet, s'il ne l'est pas, il a une racine dans $\mathbb{Q}(\sqrt{3})$. Supposons donc que $\sqrt{2} = a + b\sqrt{3}$ $(a, b \in \mathbb{Q})$, en appliquant l'automorphisme non trivial de $\mathbb{Q}(\sqrt{3})$ on trouve $\pm\sqrt{2} = a - b\sqrt{3}$. On en déduit $\sqrt{2} = a$ ou $\sqrt{2} = b\sqrt{3}$, les deux sont absurdes en élevant au carré. Ainsi, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$.

$K/\mathbb{Q}$ est galoisienne car c'est le corps de décomposition de $(X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$. Soit $G := \mathrm{Gal}(K/\mathbb{Q})$, on sait donc que $|G| = 4$. Soit $\sigma \in G$, comme $\sqrt{2}$ et $\sqrt{3}$ engendrent K comme $\mathbb{Q}$-algèbre, σ est entièrement déterminé par ses valeurs sur $\sqrt{3}$ et $\sqrt{2}$, qui valent respectivement $\pm\sqrt{3}$ et $\pm\sqrt{2}$. Comme $|G| = 4$ (et pas moins), tous les cas sont effectivement possibles. On voit de plus que G est alors commutatif et que $\sigma^2 = 1$ pour tout $\sigma \in G$, donc $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Une autre façon de le dire est de remarquer que l'application

$$\sigma \in G \mapsto (\sigma(\sqrt{2})/\sqrt{2}, \sigma(\sqrt{3})/\sqrt{3}) \in \{\pm 1\}^2$$

est un isomorphisme de groupes.

K a trois sous-corps de degré 2 sur $\mathbb{Q}$ évidents qui sont $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\sqrt{6})$. Il est immédiat de constater que ce sont respectivement les corps fixés par les éléments $(1, -1)$, $(-1, 1)$ et $(-1, -1)$ du groupe de Galois via l'isomorphisme ci-dessus. Comme les sous-groupes d'ordre 2 qu'ils engendrent sont les seuls sous-groupes stricts de $\{\pm 1\}^2$, la correspondance de Galois nous assure que les 3 corps donnés plus haut sont les seuls sous-corps stricts de K.

Un élément primitif est un élément qui n'engendre pas un sous-corps strict, c'est donc un élément qui n'est pas dans $\mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3}) \cup \mathbb{Q}(\sqrt{6})$.

(c) Soit $K := \mathbb{Q}(\alpha)$, $\alpha := e^{2i\pi/5}$. $P := 1 + X + X^2 + X^3 + X^4 \in \mathbb{Q}[X]$ annule α, montrons qu'il est irréductible dans $\mathbb{Q}[X]$. Notons que P est irréductible si, et seulement si, $P(X + 1)$ l'est, De plus, $P(X + 1) = ((X + 1)^5 - 1)/X = X^4 + 5X^3 + 10X^2 + 10X + 5$ est un polynôme d'Eisenstein pour $p = 5$, il est donc irréductible dans $\mathbb{Q}[X]$ ("critère d'Eisenstein", cf. rappels du TD 1). Notons que l'argument montre plus généralement que si p est premier, $1 + X + \cdots + X^{p-1}$ est irréductible dans $\mathbb{Q}[X]$.

Ainsi, $[K : \mathbb{Q}] = 4$. $K/\mathbb{Q}$ est galoisienne car c'est le corps de décomposition du polynôme $P \in \mathbb{Q}[X]$ (ses racines sont toutes des puissances de α, donc dans K). On sait donc que si $G := \mathrm{Gal}(K/\mathbb{Q})$, $|G| = 4$. Comme α engendre K comme $\mathbb{Q}$-algèbre, un automorphisme de K est uniquement déterminé par sa valeur sur α, qui est une racine de P donc de la forme α^k, $k \in (\mathbb{Z}/5\mathbb{Z})^*$. Un vérification facile montre que l'application ainsi construite :

$$\psi : G \to (\mathbb{Z}/5\mathbb{Z})^*, \quad \text{définie par } \sigma(\alpha) := \alpha^{\psi(\sigma)}$$

est un isomorphisme de groupes. G est donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

G a un unique sous-groupe strict, d'ordre 2 engendré par l'élément $\psi^{-1}(-1)$, envoyant α sur α^{-1} (cet automorphisme coïncide en fait avec la conjugaison complexe). Par la correspondance de Galois, K a donc un unique sous-corps, qui est le corps fixé par $\psi^{-1}(-1)$. Remarquons que $\alpha+\alpha^{-1}$ est dans ce sous-corps, et il n'est pas dans $\mathbb{Q}$ car sinon α serait de degré ≤ 2 sur $\mathbb{Q}$, ce qui n'est pas. L'unique sous-corps strict cherché est donc $\mathbb{Q}(\alpha+\alpha^{-1})$. Notons que $\alpha+\alpha^{-1} = 2\cos(2\pi/5)$, ainsi l'unique sous-corps de K est $\mathbb{Q}(\cos(2\pi/5))$. On vérifie en fait facilement que $\alpha+\alpha^{-1}$ a pour polynôme minimal X^2+X-1, ce qui montre que $\mathbb{Q}(\cos(2\pi/5)) = \mathbb{Q}(\sqrt{5})$. Les éléments primitifs sont les éléments qui ne sont pas dans ce dernier sous-corps (c'est aussi l'ensemble des éléments non réels dans K).

(d) Posons $\alpha := e^{2i\pi/7}$, $K := \mathbb{Q}(\alpha+\alpha^{-1})$, $L := \mathbb{Q}(\alpha)$. On procédant comme dans le cas (c), on trouve que $L/\mathbb{Q}$ est une extension galoisienne de degré 6, de groupe de Galois isomorphe à $(\mathbb{Z}/7\mathbb{Z})^* \simeq \mathbb{Z}/6\mathbb{Z}$. K est le sous-corps de L fixé par la conjugaison complexe, qui correspond au sous-groupe d'ordre 2 engendré par l'élément $-1 \in (\mathbb{Z}/7\mathbb{Z})^*$. On en déduit que $[K:\mathbb{Q}] = 3$, puis que $K/\mathbb{Q}$ est galoisienne car ce sous-groupe est distingué [8]. Le groupe de Galois de $K/\mathbb{Q}$ est donc $(\mathbb{Z}/7\mathbb{Z})^*/\{\pm 1\} \simeq (\mathbb{Z}/3\mathbb{Z})$. La classe de 2 dans $\mathbb{Z}/7\mathbb{Z}$ engendre $(\mathbb{Z}/7\mathbb{Z})^*$, ainsi donc que son quotient par $\{\pm 1\}$. $\mathrm{Gal}(K/\mathbb{Q})$ est donc engendré par l'unique automorphisme envoyant $\alpha+\alpha^{-1}$ sur $\alpha^2+\alpha^{-2}$, *i.e.* $\cos(2\pi/7)$ sur $\cos(4\pi/7)$.

On aurait aussi pu montrer que $K/\mathbb{Q}$ est normale en remarquant par calcul explicite que les conjugués de $\cos(2\pi/7)$ sur $\mathbb{Q}$ sont $\cos(4\pi/7)$ et $\cos(8\pi/7)$, et en notant que ces derniers s'obtiennent comme des polynômes en $\cos(2\pi/7)$ par les formules de duplication des cosinus.

$K/\mathbb{Q}$ étant de degré 3 n'a pas de sous-corps stricts, tous les éléments non dans $\mathbb{Q}$ sont donc primitifs.

(e) Posons $K := \mathbb{Q}(\alpha, j)$, $\alpha := \sqrt[3]{5}$ et $j := e^{2i\pi/3}$. Le polynôme X^3-5 est irréductible dans $\mathbb{Q}[X]$ car il est de degré 3 sans racines dans $\mathbb{Q}$. $1+X+X^2$ est irréductible dans $\mathbb{Q}(\alpha)$ car j n'est pas dans $\mathbb{Q}(\alpha) \subset \mathbb{R}$. Ainsi, $[K:\mathbb{Q}] = 6$.

$K/\mathbb{Q}$ est galoisienne car c'est le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^3-5 \in \mathbb{Q}[X]$. Posons $G := \mathrm{Gal}(K/\mathbb{Q})$, on sait donc que $|G| = 6$. Notons que le sous-ensemble $\{\alpha, j\alpha, j^2\alpha\}$ de K est stabilisé par G, ce qui nous fournit un morphisme de groupes :

$$G \longrightarrow \mathfrak{S}_3$$

Ce morphisme est injectif car α et $j\alpha$ engendrant K comme $\mathbb{Q}$-algèbre, un automorphisme qui les fixe est donc trivial. Le morphisme ci-dessus est alors surjectif car $|G| = 6$. Ainsi, $G \simeq \mathfrak{S}_3$.

G a 4 sous-groupes stricts, qui sont ceux engendrés (via l'isomorphisme ci-dessus) respectivement par les transpositions $(\alpha, j\alpha)$, $(\alpha, j^2\alpha)$, $(j\alpha, j^2\alpha)$, et par le 3-cycle $(\alpha, j\alpha, j^2\alpha)$. On les note H_1, H_2, H_3 et H. Notons que les éléments de H_1 fixent $j^2\alpha$, et donc $K^{H_1} \supset$

[8] Noter en fait que si K/k est une extension galoisienne finie de groupe de Galois abélien, alors tous les sous-groupes de $\mathrm{Gal}(K/k)$ étant distingués, toutes les sous-k-extensions $L \subset K$ sont galoisiennes sur k.

$\mathbb{Q}(j^2\alpha)$. Mais par la théorie de Galois, $[K^{H_1} : \mathbb{Q}] = |G/H_1| = 3$. De plus $[\mathbb{Q}(j^2\alpha) : \mathbb{Q}] = 3$ car $X^3 - 5$ est irréductible sur $\mathbb{Q}$, on a donc $K^{H_1} = \mathbb{Q}(j^2\alpha)$. On démontre de même que $K^{H_2} = \mathbb{Q}(j\alpha)$ et $K^{H_3} = \mathbb{Q}(\alpha)$. Enfin, on voit de même que $\mathbb{Q}(j) \subset K^H$, puis l'égalité.

Par la correspondance de Galois, on a exhibé tous les sous-corps de K, puis tous les éléments primitifs.

(f) Posons $K := \mathbb{Q}(\alpha, i)$, $\alpha^4 = -2$, $i^2 = -1$. Le polynôme $X^2 + 1$ est irréductible dans $\mathbb{Q}[X]$. Montrons que $Q := X^4 + 2$ est irréductible dans $\mathbb{Q}(i)[X]$. Supposons par l'absurde que Q est réductible dans $\mathbb{Q}(i)[X]$. Notons tout d'abord que $X^4+2 = (X-\alpha)(X-i\alpha)(X+i\alpha)(X+\alpha) \in K[X]$. Si Q a une racine dans $\mathbb{Q}(i)$, $\alpha \in \mathbb{Q}(i)$, puis en posant $z := (\alpha\bar{\alpha})^2$ et prenant le module au carré de l'équation $\alpha^4 = 2$, on trouve $4 = z^4$, $z \in \mathbb{Q}^*$, ce qui est absurde. Si Q a un facteur de degré 2 dans $\mathbb{Q}(i)$, on voit que si son terme en X est non nul, $\alpha \in \mathbb{Q}(i)$ et on conclut comme précédemment. Une factorisation de Q dans $\mathbb{Q}(i)[X]$ donc nécessairement (par factorisation unique dans $\mathbb{Q}(i)[X]$) $(X^2 - \alpha^2)(X^2 + \alpha^2)$. Mais $\alpha^2 = \pm\sqrt{-2}$ n'est pas dans $\mathbb{Q}(i)$ comme on le vérifie facilement : on a l'absurdité. Ainsi, $[K : \mathbb{Q}] = 8$.

$K/\mathbb{Q}$ est galoisienne car c'est le corps de décomposition sur $\mathbb{Q}$ de $Q \in \mathbb{Q}[X]$. Si $G := \mathrm{Gal}(K/\mathbb{Q})$, on sait donc que $|G| = 8$. Soit $C := \{\pm\alpha, \pm i\alpha\} \subset K$, l'action de G sur G permute les éléments de C. Comme C engendre K comme $\mathbb{Q}$-algèbre, on dispose donc d'un morphisme injectif :

$$G \to \mathfrak{S}_4$$

G est donc un 2-Sylow de $\mathfrak{S}_4$, il est donc isomorphe au groupe D_4 des isométries du carré. On peut retrouver ceci plus simplement en remarquant que $C \subset \mathbb{C}$ est l'ensemble des sommets d'un carré centré en 0 stable par la conjugaison complexe, et que G y agit par isométries (voyant C munit de la distance induite par $\mathbb{C}$) car il préserve les milieux des sommets opposés (si dans C on a $x + y = 0$, $\sigma \in G$, alors $\sigma(x) + \sigma(y) = 0$).

En particulier, il existe un élément $r \in G$ d'ordre 4 agissant par multiplication par i sur les éléments de C, et un autre τ d'ordre 2 y agissant par la conjugaison complexe, on a $\tau r \tau = r^{-1}$. Il est aisé de vérifier que G a exactement 8 sous-groupes stricts, dont 4 distingués :

$$H := \langle r^2 \rangle = Z(G),\ H_1 := \langle r \rangle,\ H_2 := \langle r^2, \tau \rangle,\ H_3 := \langle r^2, r\tau \rangle$$

et deux classes de conjugaison de sous-groupes d'ordre 2 (symétries du carré selon une diagonale ou un axe perpendiculaire à un côté) :

$$Q_1 := \langle r\tau \rangle,\ rQ_1r^{-1} = \langle r^{-1}\tau \rangle, \quad \text{et } Q_2 := \langle \tau \rangle,\ rQ_2r^{-1} = \langle r^2\tau \rangle$$

En procédant comme en (e), on montre que

$$K^H = \mathbb{Q}(\alpha^2, i) = \mathbb{Q}(e^{2i\pi/8}),\ K^{H_1} = \mathbb{Q}(i),\ K^{H_2} = \mathbb{Q}(\sqrt{2}),\ K^{H_3} = \mathbb{Q}(i\sqrt{2}),$$

ces extensions étant toutes galoisiennes sur $\mathbb{Q}$ de groupes de Galois $(\mathbb{Z}/2\mathbb{Z})^2$ pour la première, $(\mathbb{Z}/2\mathbb{Z})$ pour les trois autres. De même,

$$K^{Q_1} = \mathbb{Q}(\alpha),\ K^{rQ_1r^{-1}} = r(K^{Q_1}) = \mathbb{Q}(i\alpha)$$
$$K^{Q_2} = \mathbb{Q}(\alpha + \bar{\alpha}) = \mathbb{Q}(\sqrt[4]{2}),\ K^{rQ_2r^{-1}} = r(K^{Q_2}) = \mathbb{Q}(i\sqrt[4]{2})$$

Par la correspondance de Galois, on a donc trouvé tous les sous-corps de $K/\mathbb{Q}$.

Exercice 3 du TD 5 On démontre dans cet exercice que $\mathbb{C}$ est algébriquement clos, on prendra donc garde à ne pas l'utiliser...

(a) Soit $G := \mathrm{Gal}(K/\mathbb{R})$. Par la correspondance de Galois, la question posée est équivalente à montrer qu'il existe une tour de sous-groupes

$$G_n = \{1\} \subsetneq G_{n-1} \subsetneq G_{n-2} \subsetneq \cdots \subsetneq G_1 \subsetneq G$$

tels que G_1 soit d'indice impair et G_{i+1} soit un sous-groupe d'indice 2 de G_i si $i \geq 1$. En effet, on conclura alors en posant $K_i := K^{G_i}$, et en se rappelant que par le lemme d'Artin $[K : K^{G_i}] = |G_i|$, et donc que $[K^{G_i} : \mathbb{R}] = |G|/|G_i|$.

On choisit pour G_1 un 2-Sylow de G. On conclut le dévissant de G_1 en utilisant de manière répétée le lemme suivant :

Lemme Soit P un p-groupe fini, alors il admet un sous-groupe d'indice p.

Preuve: On raisonne par récurrence sur $|P|$. On sait que le centre de P est non trivial, on peut donc y choisir un sous-groupe Z d'ordre p. Z est distingué dans P et $|P/Z| = |P|/p$. Par récurrence on choisit S un sous-groupe d'indice p dans le p-groupe P/Z, et on note S' son image réciproque par la surjection canonique $P \to P/Z$. S' est d'indice p par construction. □

(b) Supposons encore $K/\mathbb{R}$ est galoisienne finie, on considère le dévissage du (a). Si $x \in K_1$, $[\mathbb{R}(x) : \mathbb{R}]$ est impair car il divise $[K_1 : \mathbb{R}]$. Le polynôme minimal de x est donc irréductible de degré impair. Le théorème des valeurs intermédiaires assure qu'il admet une racine dans $\mathbb{R}$, il est donc de degré 1. Ainsi, $K_1 = \mathbb{R}$. Si $n \geq 2$, $[K_2 : \mathbb{R}] = 2$. Mais il est immédiat que $\mathbb{C}$ est la seule extension quadratique de degré 2 (cf. TD1.ex.1), donc $K_2 \simeq C$. Si $n \geq 3$, K_3 est une extension quadratique de $\mathbb{C}$. La formule pour les racines d'un trinôme, ainsi que le fait que tout nombre complexe non nul est un carré dans $\mathbb{C}$, montre qu'il n'y a pas de polynôme irréductible de degré 2 dans $\mathbb{C}[X]$. Il est donc absurde que $n \geq 3$. On a donc montré que les seules extensions finies galoisiennes de $\mathbb{R}$ sont $\mathbb{R}$ et $\mathbb{C}$.

Soit $K/\mathbb{R}$ une extension finie de $\mathbb{R}$, sa clôture normale K^n est encore finie sur $\mathbb{R}$, et galoisienne car $\mathbb{R}$ est de caractéristique 0. Il vient que $K \subset K^n = \mathbb{R}$ ou $\mathbb{C}$, puis $K = \mathbb{R}$ ou $\mathbb{C}$, on a donc montré que la seule extension finie non triviale de $\mathbb{R}$ est $\mathbb{C}$. Enfin, soit $K/\mathbb{R}$ algébrique, $x \in K\backslash\mathbb{R}$. Par ce que l'on vient de montrer, $\mathbb{R}[x] \simeq \mathbb{C}$. Enfin, si $y \in K\backslash\mathbb{R}[x]$, on aboutit a une contradiction en considérant $\mathbb{R}[x][y]/\mathbb{R}$.

Exercice 3 du TD 4 (a) i) Une racine primitive huitième de l'unité est un élément $w \in \mathbb{F}_{p^2}^*$ tel que $w^8 = 1$ et $w^4 \neq 1$ (ce qui est équivalent à $w^4 = -1$ finalement), i.e. un élément d'ordre 8 du groupe multiplicatif $\mathbb{F}_{p^2}^*$. Comme on sait que ce groupe est cyclique, un tel élément existe si, et seulement si, 8 divise son cardinal, i.e. $8|p^2 - 1$. Mais si n est un entier impair, $n^2 - 1 = (n-1)(n+1)$ est toujours divisible par 8.

ii) Enfin, on a $w^4 = -1$, donc $w^2 = -w^{-2}$, puis $(w + w^{-1})^2 = 2 + w^2 + w^{-2} = 2$.

Remarques :

- Un autre argument pour le (i) est de dire que certainement une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$ (ou même $\mathbb{F}_{p^{4!}} = \mathbb{F}_{p^{24}}$) contient un tel élément w. Comme $w^8 = 1$, et $8|p^2 - 1$, il vient que w est fixé par $x \mapsto x^{p^2}$, il est donc dans $\mathbb{F}_{p^2}$.
- Encore autre méthode est de dire que $\mathbb{F}_{p^2}$ contient toutes les racines carrés des éléments de $\mathbb{F}_p$, et en particulier un élément i tel que $i^2 = -1$, et un autre x tel que $x^2 = 2$. Un calcul immédiat montre alors que $w := (i+1)/x$ satisfait $w^4 = -1$, et donc qu'il est d'ordre 8. L'idée ici est l'analogie avec la formule sur $\mathbb{C}$: $e^{2i\pi/8} = (1+i)/\sqrt{2}$. Cet argument de réduction modulo p d'une identité sur $\mathbb{C}$ peut être rendu parfaitement rigoureux (cf. la correction de l'exercice 9).
- Une dernière façon de voir tout cela, très semblable à la dernière, est de remarquer que $X^4 + 1$ est toujours réductible dans $\mathbb{F}_p[X]$ car l'un au moins des nombres -1, -2 ou 2 est toujours un carré dans $\mathbb{F}_p$ (pourquoi ?), et que

$$X^4 + 1 = (X - w)(X - w^{-1})(X - w^3)(X - w^{-3}) =$$

$$= (X^2 + i)(X^2 - i) = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1) = (X^2 - i\sqrt{2}X + 1).$$

(b) D'après le (a), 2 est le carré de $w + w^{-1}$ dans $\mathbb{F}_{p^2}$. Comme 2 n'a que deux racines carrées dans $\overline{\mathbb{F}}_p$, 2 est un carré dans $\mathbb{F}_p$ si, et seulement si, $(w + w^{-1})$ est dans $\mathbb{F}_p$. Mais ceci est équivalent à demander que $w + w^{-1}$ soit fixé par le Frobenius $x \mapsto x^p$ de $\mathbb{F}_{p^2}/\mathbb{F}_p$. Comme $w^8 = 1$, si $p \equiv \pm 1 \bmod 8$, $w^p + w^{-p} = w + w^{-1}$ et donc 2 est un carré dans $\mathbb{F}_p$. Si $p \equiv \pm 3 \bmod 8$, $w^p + w^{-p} = w^3 + w^{-3} = -(w + w^{-1}) \neq w + w^{-1}$ car $2 \neq 0$. Cela conclut que 2 est un carré si, et seulement si, $p \equiv \pm 1 \bmod 8$.

Exercice 9 du TD 4 Dans ce qui suit, je justifie la seconde remarque faite dans la correction de l'exercice 3 TD 4. Il est facile d'extraire de ce qui suit une correction de l'exercice 9 du TD 4.

Un nombre algébrique $x \in \mathbb{C}$ est dit "entier algébrique" s'il est annulé par un polynôme unitaire à coefficients entiers. Cela implique que $\mathbb{Z}[x] := \{P(x), P \in \mathbb{Z}[X]\} \subset \mathbb{C}$ est de type fini comme groupe abélien, même engendré par 1, $x\, x^2$, ..., x^{d-1} si d est le degré d'un polynôme annulateur Π de x unitaire à coefficients entiers. Par exemple, si $n > 1 \in \mathbb{N}$, $\sqrt{n}$, $e^{2i\pi/n}$, sont des entiers algébriques, mais pas $1/n$ (pourquoi ?). Leur forme est parfois trompeuse : $(1 + \sqrt{5})/2$ est dans $\overline{\mathbb{Z}}$, mais pas $(1 + \sqrt{3})/2$. C'est un fait que la somme et le produit de deux entiers algébriques est encore un entier algébrique, de sorte qu'ils forment un sous-anneau de $\mathbb{C}$. Reportons la preuve de ceci à la fin de ce corrigé.

On peut parler de congruences modulo un idéal dans $\overline{\mathbb{Z}}$, comme dans tout anneau commutatif[9]. Soit $n > 1$ un entier naturel, j'affirme que l'idéal $n\overline{\mathbb{Z}} \subset \overline{\mathbb{Z}}$ est strict. En effet, dans le cas contraire, $1 \in n\overline{\mathbb{Z}}$ et donc $1/n \in \overline{\mathbb{Z}}$, ce qui est faux. Ainsi, l'anneau $\overline{\mathbb{Z}}/n\overline{\mathbb{Z}}$ est

[9]Bien sûr, cela serait aussi possible dans $\overline{\mathbb{Q}}$, mais comme ce dernier est un corps, et il n'a donc pas d'idéal non trivial.

non trivial, et on peut donc s'en servir pour y étudier des congruences. Cependant, même quand n est premier, ce quotient est très loin d'être intègre et sa structure d'anneau est plutôt complexe. Par exemple on a toujours $n = \sqrt{n}^2$, mais $\sqrt{n} \notin n\overline{\mathbb{Z}}$ car sinon $1/\sqrt{n} \in \overline{\mathbb{Z}}$, puis $1/n \in \overline{\mathbb{Z}}$: absurde. On raffine donc un peu le procédé comme suit.

On fixe désormais $n = p$ un nombre premier. Comme $p\overline{\mathbb{Z}}$ est strict, on peut l'inclure dans un idéal maximal $P \subset \overline{\mathbb{Z}}$. En particulier, $\mathbb{F} := \overline{\mathbb{Z}}/P$ est un corps de caractéristique p (car $p \in P$), algébrique sur $\mathbb{F}_p$: tout $x \in \overline{\mathbb{Z}}$ satisfait une équation algébrique sur $\mathbb{Z}$, ainsi donc que son image dans $\mathbb{F}$ sur $\mathbb{F}_p = \mathbb{Z}.\overline{1} \in \mathbb{F}$. Enfin, $\mathbb{F}$ contient tous les corps finis (et en est donc la réunion) car $X^{p^n} - X$ est scindé dans $\overline{\mathbb{Z}}[X]$, ainsi donc que son image dans $\mathbb{F}[X]$.

Ce qui a été fait ici avec $\overline{\mathbb{Z}}$ peut être fait avec tout sous-anneau $A \subset \overline{\mathbb{Z}}$, donc par exemple $\mathbb{Z}[i]$, $\mathbb{Z}[e^{2i\pi/n}, \sqrt{2}]$... mais aussi $\mathbb{Z}[\{e^{2i\pi/n}, n > 1\}]$ (cas de l'exercice 9), $\mathbb{Z}[\{e^{2i\pi/p^n}, n \geq 1\}]$ ou $\mathbb{Z}[\{\sqrt{n}, n \in \mathbb{Z}\}]$. Dans cette généralité, A/P n'est pas toujours une clôture algébrique de $\mathbb{F}_p$. Vous pouvez vérifier que dans les trois derniers cas ci-dessus on obtient pour A/P respectivement : $\overline{\mathbb{F}}_p$, $\mathbb{F}_p$, $\mathbb{F}_{p^2}$ (sauf si $p = 2$ auquel cas on a $\mathbb{F}_2$). En exercice, vous pouvez aussi regarder ce qui se passe pour $A = \mathbb{Z}[i]$.

Pour en revenir à la question initiale soulevée dans l'exercice 3. Notons que $w := e^{2i\pi/8}$, i et $\sqrt{2}$ sont des entiers algébriques, et considérons les relations $\sqrt{2} = (w+w^{-1})^2$, ou encore $\sqrt{2}w = (1+i)$, qui sont dans $\overline{\mathbb{Z}}$. On peut donc les réduire modulo P. Évidemment, les images respectives $\overline{w}$, $\overline{i}$ et $\overline{\sqrt{2}}$ de w, i et $\sqrt{2}$ satisfont encore $\overline{w}^4 = -1$, $\overline{i}^2 = -1$ et $\overline{\sqrt{2}}^2 = 2$. Par des arguments que l'on a déjà donnés en (a), ces images sont toutes fixées par $x \mapsto x^{p^2}$, elles sont donc toutes dans $\mathbb{F}_{p^2} \subset \mathbb{F}$. Cela montre que la première relation est valable dans $\mathbb{F}_{p^2}$. Si $p \neq 2$, $\overline{\sqrt{2}}$ est inversible car son carré l'est, et on a donc aussi $\overline{w} = (1+\overline{i})/\overline{\sqrt{2}}$.

Il ne reste qu'à montrer que $\overline{\mathbb{Z}}$ est un anneau. Soit $M \subset \mathbb{C}$ un sous-groupe abélien non nul de type fini, et $x \in \mathbb{C}$ tel que $xM \subset M$. Montrons que x est dans $\overline{\mathbb{Z}}$. Comme M est sans torsion et de type fini, il est libre de rang fini $\simeq \mathbb{Z}^n$, et la multiplication par x, peut être vue comme un endomorphisme de $\mathbb{Z}^n$. Le théorème de Cayley-Hamilton nous fournit alors un polynôme annulateur unitaire P à coefficients entiers tel que $P(x)M = 0$. Comme M est non nul et $\mathbb{C}$ intègre, cela implique que $P(x) = 0$ ce qui conclut. Si x et y sont dans $\overline{\mathbb{Z}}$, alors on voit de suite que $M = \mathbb{Z}[x,y] := \{P(x,y), P \in \mathbb{Z}[X,Y]\} \subset \mathbb{C}$ est de type fini, préservé par multiplication par $x+y$ et xy. Ainsi, xy et $x+y$ sont dans $\overline{\mathbb{Z}}$.

Exercice 1 du TD 3 (a) L'application $\mathrm{End}_k(V) \to \mathrm{End}_k(\mathrm{Sym}^n(V))$ est celle notée $u \mapsto S(u)$ dans le cours. Elle satisfait $S(u \cdot v) = S(u) \cdot S(v)$, car c'est vrai sur le sous-espace (générateur) des tenseurs purs. Ainsi, elle induit un morphisme de groupes $GL(V) \to GL(Sym^n(V))$.

Supposons $n > 1$ et $\dim_k(V) > 1$, vérifions que l'on peut trouver u et v tels que $S(u+v) \neq S(u) + S(v)$. Soient e et f dans V et k-libres, et u et $v \in \mathrm{End}_k(V)$ tels que $u(e) = 0$ et $u(f) = f$ (resp. $v(e) = e$ et $v(f) = 0$). Alors $S(u+v)(e^{n-1}f) = ((u+v)(e))^{n-1}((u+v))(f) = e^{n-1}f$, alors que $S(u)(e^{n-1}f) = S(v)(e^{n-1}f) = 0$. Cela conclut.

Si $\dim_k(V) = 1$, on vérifie aisément que S est k-linéaire si, et seulement si, n est de la forme p^r avec p premier[10] et $k \subset \mathbb{F}_{p^r}$.

(b) On note e_1, e_2 la base canonique de k^2. Si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Ker}(\rho_n)$, alors $\rho_n(g).e_1^n = (ae_1 + be_2)^n = \sum_{i=0}^n \binom{n}{i} a^i e_1^i b^{n-i} e_2^{n-i} = e_1^n$. Comme les monômes en e_1 et e_2 sont k-libres dans $\mathrm{Sym}^n(ke_1 \oplus ke_2)$ d'après un résultat du cours, il vient que $a^n = 1$ et $b = 0$. De même $c = 0$ et $d^n = 1$, on a alors $d = a^{-1}$. Mais comme $\rho_n(g)(e_1^{n-1}e_2) = a^{n-2}e_1^{n-1}e_2$, il vient $a^2 = 1$, puis $g = \pm 1 \in SL_2(k)$. On voit alors de suite que $\mathrm{Ker}(\rho_n) = \{\pm 1\}$ si n est pair, $\{1\}$ si n est impair.

(c) Dans le TD nous avons corrigé cet exercice en considérant l'action des matrices diagonales, mais on avait vu que la preuve se généralisait mal pour le (d). On raisonne un peu différemment ci-dessous en utilisant l'action de $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, on pose $u = \rho_n(g)$. On a $u(e_1) = e_1$ et $u(e_2) = e_1 + e_2$. Dans la base $e_1^n, e_1^{n-1}e_2, \ldots, e_2^n$, la matrice de u est donc une troncature du triangle de Pascal :

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \ldots \\ 0 & 1 & 2 & 3 & \ldots \\ 0 & 0 & 1 & 3 & \ldots \\ 0 & 0 & 0 & 1 & \ldots \\ 0 & 0 & 0 & 0 & \ldots \end{pmatrix}$$

Notons que $u-1$ est nilpotente d'indice $n+1$. En effet, on voit que $(u-1)^n(e_2^n) = n!e_1^n$, qui est non nul car $n!$ est non nul dans k (de caractéristique nulle ici.). En particulier, $\mathrm{Ker}(u-1) = k.e_1^n$.

Soit W un sous-espace vectoriel de $Sym^n(k^2)$ stable par $\rho_n(G)$, non nul. Il est donc stable par $u-1$. Si $w \neq 0 \in W$, alors pour tout m, $(u-1)^m(w) \in W$, et si m est le plus grand entier pour lequel $(u-1)^m(w)$ est non nul, alors $(u-1)^m(w)$ est dans $\mathrm{Ker}(u-1) = k.e_1^n$. Ainsi, $e_1^n \in W$. Mais alors $e_2^n \in W$ en considérant un élément de $SL_2(k)$ échangeant ke_1 et ke_2 (cela existe). En écrivant successivement que $(u-1)^m(e_2) \in W$ pour $m = n, n-1, \ldots, 1$, on voit que tous les monômes sont dans W (cela utilise le fait e_2^n est un vecteur cyclique pour $(u-1)$, ce qui découle de ce que l'indice de nilpotence de $u-1$ est $n+1 = \dim_k(Sym^n(k^2))$).

(d) Le même argument que précédemment vaut pour $n < p$ car $n!$ est non nul dans k. Pour $n = p$, on remarque $ke_1^p \oplus ke_2^p$ est un sous-espace stable non trivial : $(ae_1 + be_2)^p = a^p e_1^p + b^p e_2^p$ car on est en caractéristique p. Le raisonnement du (c) dans ce cas nous montrerait même que $Sym^p(k^2)$ n'admet pas d'autre sous-espace stable strict que l'espace exhibé ci-dessus[11].

---

[10](Remarque indépendante) Vous pouvez vérifier aussi que si V est un $\mathbb{F}_q$-espace vectoriel de dimension 1, alors $\mathrm{Sym}^{q-1}(V)$ est *canoniquement* isomorphe à $\mathbb{F}_q$.

[11]Il est connu que si $\rho : SL_2(\mathbb{R}) \to \mathrm{GL}_{n+1}(\mathbb{R})$ est un morphisme continu tel que $\rho(G)$ n'admet pas de sous-espace stable strict, alors ρ est conjugué à la représentation ρ_n étudié dans cet exercice. De plus, il

Exercice 2 du TD 2 Les questions un peu formelles sont volontairement très détaillées. Les questions (d) et (e) étaient plus difficiles.

(a)[12] L'application de l'énoncé $\psi : A \to \mathrm{End}_k(A)$, $a \mapsto (x \mapsto ax)$, est clairement un morphisme de k-algèbres, injectif car A est unitaire de sorte que $\psi(a) : 1 \mapsto a$. On conclut car le choix d'une k-base de A identifie $\mathrm{End}_k(A)$ à $M_n(k)$ comme k-algèbre, $n := \dim_k(A)$.

(a') On explicite l'application précédente. Si $k = \mathbb{Q}$, $A = \mathbb{Q}(\sqrt{2})$, on fixe par exemple la $\mathbb{Q}$-base $1, \sqrt{2}$ de A. On voit alors que ψ est l'application :

$$a + b\sqrt{2} \mapsto \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}.$$

De même, si $A = \mathbb{Q}[X]/(X^n)$, le choix de la $\mathbb{Q}$-base $1, X, \ldots, X^{n-1}$ de A donne[13] :

$$a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} \mapsto \begin{pmatrix} a_0 & 0 & \ldots & 0 \\ a_1 & a_0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ a_{n-1} & a_{n-2} & \ldots & a_0 \end{pmatrix}.$$

(b) On commence par rappeler la conséquence suivante d'un résultat du cours :

Lemme : Soit V un k-espace vectoriel, K/k une extension de corps, alors si (e_i) est une k-base de V, $(e_i \otimes 1)$ est une K-base de $V \otimes_k K$.

Preuve : On sait du cours que si N et $(M_i)_{i\in I}$ sont des A-modules, l'application canonique $\bigoplus_{i\in I}(M_i \otimes_A N) \to (\bigoplus_{i\in I} M_i) \otimes_A N$ est un isomorphisme. On l'applique à $M_i := k.e_i$, $N = K$, $A = k$. Ainsi, tout élément de $V \otimes_k K$ s'écrit de manière unique comme somme finie $\sum_i v_i \otimes k_i$, le "unique" désigne ici que l'élément $v_i \otimes k_i$ de $(ke_i) \otimes_k K$ est uniquement déterminé. On conclut car ce dernier s'écrit de manière unique sous la forme $e_i \otimes \lambda_i = \lambda_i.(e_i \otimes 1)$ avec $\lambda_i \in K$ (l'égalité provenant par définition de la structure de K-espace vectoriel sur $V \otimes_k K$).

Pour les plus sceptiques, on peut aussi donner la preuve ad hoc suivante. Les tenseurs purs engendrent $V \otimes_k K$ comme k-espace vectoriel, donc à fortiori comme K-espace vectoriel aussi. Par définition de la structure de K-espace vectoriel sur $V \otimes_k K$, $e_i \otimes \lambda = \lambda.(e_i \otimes 1)$ si $\lambda \in K$, donc la famille de l'énoncé est génératrice, montrons qu'elle est libre. Supposons que l'on ait une relation $\sum_i \lambda_i.(e_i \otimes 1) = 0 = \sum_i e_i \otimes \lambda_i$. Considérons la forme k-linéaire $p_i : V \to k$ projection sur ke_i parallèlement aux e_j, $j \neq i$, $p_i(\sum_k a_k e_k) := a_i$. L'application

est aussi connu que si $\rho : SL_2(\mathbb{F}_q) \to \mathrm{GL}_{n+1}(\mathbb{F}_q)$ est un morphisme de groupe tel que ρ n'admet pas de sous-espaces stable strict, alors $n < q$ et ρ est conjugué à ρ_n ci-dessous.

[12]Cette question est l'analogue pour les k-algèbres de dimension finie sur k du fait que tout groupe fini G est isomorphe à un sous-groupe de $\mathfrak{S}_n$ avec $n = |G|$.

[13]De manière générale, si $P \in k[X]$ et $A = k[X]/(P)$ on retrouve la matrice compagnon de P dans la base $X^{deg(P)-1}, \ldots, X, 1$, et cela montre immédiatement le fait bien connu (et élémentaire) que le polynôme minimal de cette dernière est P, car P est le polynôme minimal de l'image de X dans A. On peut remarquer aussi que $M_n(k)$ contient donc comme sous-k-algèbre toute extension K/k de corps de degré divisant n (cette condition sur le degré est nécessaire : pourquoi ?). Noter qu'il peut y en avoir une infinité deux à deux non isomorphes, comme le montre le cas des $K/\mathbb{Q}$ de degré 2 dans $M_2(\mathbb{Q})$.

$V \times K \to K$, $(v, \lambda) \mapsto \lambda p_i(v)$ est k-bilinéaire, et se factorise donc en une application k-linéaire envoyant $e_j \otimes \lambda$ sur λ si $j = i$, sur 0 sinon. En l'appliquant à la relation plus haut il vient $\lambda_i = 0$, et ce donc pour tout i, ce que l'on voulait. □

Revenons-en à la question de l'exercice. L'application $A \times K \to M_n(K)$, $(a, \lambda) \mapsto \lambda a$, est clairement k-bilinéaire. Elle se factorise donc en une application k-linéaire $\psi : A \otimes_k K \to M_n(K)$. Il est immédiat que ψ ainsi définie est un morphisme de K-algèbres, d'image la K-algèbre engendrée par A. Il faut voir que ψ est injective. Soit (e_i) une k-base de A. Par le lemme, $(e_i) \otimes 1$ est une K-base de $A \otimes_k K$, de sorte qu'il suffit de montrer que la famille des $\psi(e_i \otimes 1) = e_i$ est K-libre dans $M_n(K)$, soit le[14] :

Lemme : Soit K/k une extension de corps, I un ensemble, alors une famille k-libre de $k^{(I)}$ est K-libre vue dans $K^{(I)} \supset k^{(I)}$.

Preuve : C'est une conséquence directe de ce que l'application canonique $k^{(I)} \otimes_k K \to K^{(I)}$ est un isomorphisme, qui est un cas particulier du résultat du cours énoncé plus haut.

Donnons tout de même une preuve ad hoc. Soit (f_j) une telle famille, et $\sum_j \lambda_j f_j = 0$ une relation de dépendance linéaire avec les λ_j dans K presque tous nuls. Soit $p : K \to k$ une forme k-linéaire, $p' : K^{(I)} \to k^{(I)}$ l'application définie par $p'((x_i)) := (p(x_i))$. Alors p' est k-linéaire, et satisfait $p'(\lambda.x) = p(\lambda)x$ si $x \in k^{(I)}$ et $\lambda \in K$. En appliquant p' a la relation plus haut, il vient donc $\sum_i p(\lambda_i) f_j = 0 \in k^{(I)}$. Ainsi, $p(\lambda_i) = 0$ pour tout i et $p \in \mathrm{Hom}_k(K, k)$, puis $\lambda_i = 0$ pour tout i. □

(c) On vérifie immédiatement que l'application $\mathrm{diag}(x_1, \ldots, x_n) \in D_n(k) \mapsto (x_1, \ldots, x_n) \in k^n$ est un isomorphisme de k-algèbres.

(d) On peut supposer que $A \subset M_n(k)$, $n = dim_k(A)$ par la question (a). D'après la question (c), il faut montrer que la K-algèbre engendrée par A est K-isomorphe à K^n. Vérifions qu'il suffit de montrer que tous les éléments de A sont diagonalisables dans $M_n(K)$. En effet, comme ils commutent, tous les éléments de $K.A$ seront codiagonalisables. Ainsi quitte à conjuguer $M_n(K)$ par un $P \in GL_n(K)$, ce qui est un automorphisme de K-algèbre, on aura donc $K.A \subset D_n(K)$, puis $K.A = D_n(K)$ car $\dim_K(K.A) = \dim_k(A) = n$ d'après le (b). Ce que l'on voulait. Il faut donc montrer que tout élément $a \in A$ est annulé par un polynôme scindé à racines simples dans $K[X]$, fixons un tel a. Soit $P \in k[X]$ le polynôme minimal de $a \in A$. Comme A est un corps, P est irréductible. L'indication assure alors que P est à racines distinctes dans $K[X]$, cela conclut.

Preuve de l'indication : Si k est de caractéristique nulle, $P \in k[X]$ non constant, alors P' est un polynôme non nul. En particulier, si P est irréductible, P' est premier avec P, de sorte que l'on peut écrire une relation de Bezout dans $k[X]$, $AP + BP' = 1$. Cette relation vaut dans $K[X]$, de sorte que P et P' n'ont pas de racines en commun, i.e. P n'a pas de racine multiple [15].

---

[14] Ce lemme peut aussi se déduire du lemme précédent combiné au résultat du cours : si V et W sont des k-espaces vectoriels, l'application canonique $V^{(I)} \otimes_k W \to (V \otimes_k W)^{(I)}$ est un isomorphisme , appliqué à $V = k^{(I)}$ et $W = K$.

[15] Si k est de caractéristique p et $a \in k^*$ n'est pas une puissance p^{ieme} dans k, alors $X^p - a$ est irréductible dans $k[X]$ mais n'a qu'une racine de multiplicité p dans $K[X]$. Par contre, si $x \mapsto x^p, k \to k$,

(e) Le premier lemme de la question (b) assure que l'application canonique $A \to A \otimes_k K$, $a \mapsto a \otimes 1$ est injective. C'est de plus un morphisme de k-algèbres. Ainsi, si $A \otimes_k K$ n'a pas d'élément nilpotent non nul (resp. est commutative), alors A a la même propriété. Cela montre la nécessité.
En raisonnant, comme en (d), il suffit de montrer que tout élément de a est annulé par un polynôme $P \in k[X]$ qui est sans facteur carré. En effet, on aura alors que $(P, P') = 1$ (car la caractéristique de k est nulle), puis par Bezout que P n'a que des racines simples dans K. Soit $a \in A$, P son polynôme minimal unitaire. On écrit $P = \pi^n Q$ où Π est irréductible premier à Q. Si S est un polynôme valant $X \bmod \Pi^n$ et $0 \bmod Q$, $b := S(a)$ est donc un élément de A de polynôme minimal Π^n. En particulier, $\Pi(b)$ est nilpotent, donc nul, de sorte que $n = 1$, ce que l'on voulait.

(f) Le polynôme $X^p - T$ est irréductible dans $(\mathbb{F}_p[T])[X]$ par exemple d'après le critère d'Eisenstein, il l'est donc dans $k[X]$ par le lemme du contenu de Gauss. Par l'exercice 1.(a), $(k[X]/(X^p - T)) \otimes_k K$ est isomorphe comme K-algèbre à $K[X]/(X^p - T)$. Soit $x \in K$ tel que $x^p = T$, on remarque que $X^p - T = (X - x)^p$, de sorte que le changement de variable $u := X - x$ répond à la première question. Comme $p > 1$, l'algèbre obtenue a des éléments nilpotents non nuls, elle n'est donc pas K-isomorphe à K^p.

(g) Si $x = (x_1, \ldots, x_n) \in k^n$ engendre k^n comme k-algèbre, alors il est évident que tous les x_i sont distincts. Réciproquement, supposons que tous les x_i sont distincts et fixons $y = (y_1, \ldots, y_n)) \in k^n$ quelconque. Les x_i étant distincts on peut trouver un polynôme interpolateur de Lagrange $P \in k[X]$ tel que $P(x_i) = y_i$, de sorte que $P(x) = y$ dans k^n, c'est la réciproque attendue.
Enfin, soit L/k une extension finie comme dans l'énoncé. Par le d, il existe un K-isomorphisme $L \otimes_k K \to K^n$. On rappelle que le morphisme naturel de k-algèbres $L \to L \otimes_k K$, $x \mapsto x \otimes 1$, est injectif (par exemple par le premier lemme du (b), ou par l'exercice 1.(b) du TD1, car le produit tensoriel est pris sur un corps), et que son image engendre tout $L \otimes_k K \simeq K^n$ comme K-espace vectoriel. Pour tout $1 \leq i \neq j \leq n$, notons $H_{i,j}$ le sous-k-espace vectoriel de L formé des éléments dont l'image dans K^n a ses i^{ieme} et j^{ieme} coordonnée qui coïncident. C'est un sous-espace strict car $K.L = K^n$. Comme k est de caractéristique nulle donc infini, la réunion (finie) des $H_{i,j}$ est un sous-espace vectoriel strict de L, de sorte qu'il existe $x \in L$ dans aucun des $H_{i,j}$, il engendre donc K^n comme K-algèbre d'après le premier point. À fortiori, x engendre L comme k-espace vectoriel car $K^n = L \otimes_k K$.

(h) Par un résultat du cours, l'application naturelle

$$\mathrm{Hom}_{k-alg}(L, K) \to \mathrm{Hom}_{K-alg}(L \otimes_k K, K)$$

est bijective, de sorte qu'il suffit de montrer, grâce au (d), que $|\mathrm{Hom}_{K-alg}(K^n, K)| = n$. Soit e_i l'élément de K^n partout nul sauf à la i^{ieme} coordonnée où il vaut 1. On a $e_i^2 = e_i$, $1 = e_1 + \cdots + e_n$, et $e_i e_j = 0$ si $i \neq j$. Si $\psi : K^n \to K$ est un morphisme de K-algèbre, chaque $\psi(e_i)$ est égal à son carré, et vaut donc 0 ou 1. Les relations $\psi(e_j)\psi(e_i) = 0$ si $i \neq j$

est bijective (on dit que k est parfait), alors vous pouvez vérifier que si P est irréductible, P' n'est pas nul, et donc à racines simples dans $K[X]$. C'est en particulier vrai si k est fini. Ces notions seront reprises dans le cours de théorie de Galois.

et $1 = \psi(e_1) + \cdots + \psi(e_n)$ montrent qu'un, et un seul, des $\psi(e_i)$ est non nul. On en déduit que ψ est la projection sur l'une des coordonnées de K^n, puis le résultat.