Exercices de théorie de Galois

Le niveau des exercices est indiqué comme suit :

- V piste verte : fait manipuler les définitions, présente un fait classique élémentaire
- B piste bleue : mobilise les concepts et résultats du cours pour établir un fait intéressant
- R piste rouge : nécessite un enchaînement d'arguments, un calcul long, une bonne idée
- N piste noire : nécessite les résultats importants du cours et de la créativité !

1 Anneaux et corps

Rappels sur les anneaux et les corps

V **Exercice 1**. (Sous-corps premier)
Montrer qu'il n'existe pas de morphisme entre deux corps de caractéristiques différentes.

V **Exercice 2**. (Sous-corps des puissances p-ièmes)
Soit K un corps de caractéristique $p > 0$. Montrer que $K_0 = \{x^p \in K \,|\, x \in K\}$ est un sous-corps de K.

B **Exercice 3**. (Un idéal premier non maximal)
Soit $\mathbb{Z}[X]$ l'anneau des polynômes à coefficients entiers. Montrer que 2 est premier dans $\mathbb{Z}[X]$. Montrer que l'idéal (2) n'est pas maximal.

B **Exercice 4**. (Points fixes d'un endomorphisme)
Soit A un anneau et $f : A \to A$ un endomorphisme de A.

1. Montrer que l'ensemble $A^f = \{x \in A \,|\, f(x) = x\}$ des points fixes de f est un sous-anneau de A. Si A est un corps, montrer que A^f est un corps.
2. On pose $A := \{a + b\sqrt{2} \in \mathbb{R} \,|\, a, b \in \mathbb{Z}\}$. Montrez que A est un sous-anneau de $\mathbb{R}$. Montrez que $f : A \to A$ défini par $f(a + b\sqrt{2}) = a - b\sqrt{2}$ est un automorphisme de A et calculez A^f.

R **Exercice 5**. (Groupe additif vs groupe multiplicatif d'un corps)
Soit K un corps. Montrer que $(K, +)$ et $(K^\times, \times)$ ne sont pas isomorphes. Montrer qu'en revanche, il peut arriver que $(K, +)$ soit isomorphe à un sous-groupe de $(K^\times, \times)$.

R **Exercice 6**. (Entiers quadratiques)
Posons $A := \{a + b\sqrt{2} \in \mathbb{R} \,|\, a, b \in \mathbb{Z}\}$.

1. Montrez que A est un sous-anneau de $\mathbb{R}$.
2. Montrez que A n'est pas isomorphe à $\mathbb{Z} \times \mathbb{Z}$
3. Montrez que l'idéal I de A engendré par $\sqrt{2}$ est maximal. Montrez que A/I est isomorphe à $\mathbb{F}_2$.
4. Montrez que, si $a, b \in \mathbb{Z}$ sont tels que $3|a^2 - 2b^2$, alors $3|a$ et $3|b$. En déduire que l'idéal J engendré par 3 est premier puis que le quotient A/J est un corps. Quelle est sa caractéristique ? Quel est son cardinal ?

Ⓡ **Exercice 7**. (Entiers de Gauss)
Dans l'anneau $\mathbb{Z}[i]$, est-ce que i est un élément premier ? Et 2 ? Et 3 ?

Rappels sur l'algèbre des polynômes

Ⓑ **Exercice 8**. (Idéaux maximaux de $K[X]$)
Soient K un corps et $P \in K[X]$ un polynôme irréductible. On souhaite montrer, par deux démonstrations différents, que l'idéal (P) est maximal.

1. Démontrez directement que si I est un idéal qui contient strictement (P), alors $I = K[X]$. (Indication : par exemple, pensez au théorème de Bézout.)
2. Démontrez que l'algèbre $K[X]/(P)$ est un corps. (Indication : montrez qu'une K-algèbre intègre de dimension finie est un corps.)

Ⓡ **Exercice 9**. (Groupe multiplicatif d'un corps)

1. Soit $A = \mathbb{Z}$ et $K = \mathbb{Q}$ son corps de fractions. Démontrez les assertions suivantes :
   (a) on a un isomorphisme de groupes $A^\times \simeq \mathbb{Z}/2\mathbb{Z}$.
   (b) l'anneau A possède un ensemble $\mathcal{P}$ de représentants des éléments irréductibles à association près qui est dénombrable.
   (c) tout élément $x \in K^\times$ possède une écriture $x = up_1^{a_1} \cdots p_n^{a_n}$ avec $u \in A^\times$, $n \geqslant 0$, $p_i \in \mathcal{P}$ et $\alpha_i \in \mathbb{Z} \setminus \{0\}$, unique à l'ordre près des facteurs.
   (d) on a un isomorphisme de groupes $K^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}^{(\mathbb{N})}$.
2. Montrez que pour $A = \mathbb{F}_3[X]$ et $K = \mathbb{F}_3(X)$, les quatre assertions de la question précédente sont encore vraies. Donnez deux corps non isomorphes K_1 et K_2 tels que $K_1^\times \simeq K_2^\times$.

Corrigé. Pour 1. (c) *Existence*. Soit $x \in K^\times$. Choisissons une écriture sous forme de fraction $x = ua/b$ avec $u \in \{\pm 1\}$ et a, b entiers naturels non nuls et premiers entre eux. Notons P_+ l'ensemble des nombres premiers qui divisent a et P_- l'ensemble des nombres premiers qui divisent b. Posons $P(x) = P_+ \cup P_-$. Ces ensembles sont finis (peut-être vides) et disjoints puisque a et b sont premiers entre eux. Les décompositions en facteurs premiers de a et b ont la forme $a = \prod_{p \in P_+} p^{r_p}$ et $b = \prod_{p \in P_-} p^{s_p}$ avec $r_p, s_p > 0$. On a obtenu une écriture :

$$x = u \prod_{p \in P_+} p^{r_p} \prod_{p \in P_-} p^{-s_p}.$$

Si l'on énumère $P(x) = \{p_1, \ldots, p_n\}$, ceci est bien une écriture de la forme $x = up_1^{a_1} \cdots p_n^{a_n}$ où les entiers r_p sont les exposants $a_i > 0$ et les entiers $-s_p$ sont les exposants $a_i < 0$.

Unicité. Considérons deux écritures $x = up_1^{a_1} \cdots p_n^{a_n} = vq_1^{b_1} \cdots q_m^{b_m}$ dans lesquelles les p_i sont tous distincts, et les q_j sont tous distincts. Alors $u = v = \operatorname{sgn}(x)$. Notons :

$$I_+ = \{i \in \{1, \ldots, n\} \mid a_i > 0\} \qquad I_- = \{i \in \{1, \ldots, n\} \mid a_i < 0\}$$
$$J_+ = \{j \in \{1, \ldots, m\} \mid b_j > 0\} \qquad J_+ = \{j \in \{1, \ldots, m\} \mid b_j < 0\}.$$

De l'égalité $p_1^{a_1} \cdots p_n^{a_n} = q_1^{b_1} \cdots q_m^{b_m}$ on tire une égalité où tous les exposants sont > 0 :

$$\prod_{i \in I_+} p_i^{a_i} \prod_{i \in J_-} q_j^{-b_j} = \prod_{i \in I_-} p_i^{-a_i} \prod_{j \in J_+} q_j^{b_j}.$$

Comme les p_i sont tous distincts, le lemme d'Euclide montre que chaque p_i avec $i \in I_+$ apparaissant dans le membre de gauche est égal à un q_j avec $j \in J_+$ du membre de droite, et que les exposants (multiplicités) de p_i et q_j sont égales. La même chose vaut avec les p_i avec $i \in I_-$, qui sont associés à un unique q_j avec $j \in J_-$. On construit ainsi deux bijections $\sigma_+ : I_+ \to J_+$ et $\sigma_- : I_- \to J_-$ d'où une bijection unique

$$\sigma : I_+ \amalg I_- = \{1, \dots, n\} \to J_+ \amalg J_- = \{1, \dots, m\},$$

telle que $p_i = q_{\sigma(j)}$ et $a_i = b_{\sigma(j)}$ pour tout i. Ceci est exactement dire que l'écriture est « unique à l'ordre près des facteurs ».

B **Exercice 10**. (Une divisibilité et une application)
Soient K un corps, A une K-algèbre et $a, b \in A$.

1. Démontrez que pour tout polynôme $P \in K[X]$ il existe $Q \in K[X, Y]$ tel que
$$P(a) - P(b) = (a - b)\, Q(a, b).$$
(Indication : commencez par le cas $P = X^n$.)
2. Application : soit E un K-espace vectoriel et $f : E \to E$ un endomorphisme linéaire. On note $\chi \in K[X]$ le polynôme caractéristique de f et $\mu \in K[X]$ son polynôme minimal.
   (a) Rappelez la définition de μ.
   (b) Démontrez qu'il existe $Q \in K[X, Y]$ tel que $\mu(X) \cdot \mathrm{id}_E = (X\mathrm{id}_E - f)\, Q(X\mathrm{id}_E, f)$.
   (Indication : notez que $\mu(X) \cdot \mathrm{id}_E = \mu(X\mathrm{id}_E)$ et appliquez la question 1.)
   (c) Démontrez les divisibilités $\mu \mid \chi \mid \mu^n$.
   (Indication : prenez le déterminant.)
   (d) Déduisez-en que μ et χ ont les mêmes facteurs irréductibles.

Irréductiblité

B **Exercice 11**. (Irréductibilité de $P \circ Q$)
Soient K un corps et $P \in K[X]$ un polynôme. Soient $a, b \in K$, $a \neq 0$.

1. Montrer que $Q = P(aX + b)$ est irréductible si et seulement si P est irréductible.
2. Donnez un exemple avec P irréductible mais $P(X^2)$ réductible.
3. Montrer que si $P(X^2)$ est irréductible alors P est irréductible.

Pour l'exercice suivant, on rappelle quelques notions sur les anneaux factoriels. Soit A un anneau factoriel de corps de fractions K.

- Deux éléments $x, y \in K$ sont *associés* s'il existe $u \in A^\times$ tel que $x = uy$.
- Pour $P \in A[X] \setminus \{0\}$, le *contenu* $\mathrm{c}(P)$ est le pgcd des coefficients, bien défini à association près.
- Le contenu est multiplicatif : $\mathrm{c}(P_1 P_2) = \mathrm{c}(P_1)\, \mathrm{c}(P_2)$.
- Le contenu s'étend au corps de fractions $\mathrm{Frac}(A[X]) \setminus \{0\}$ par $\mathrm{c}(P/Q) := \mathrm{c}(P)/\mathrm{c}(Q)$.
- On dit que P est *primitif* si $\mathrm{c}(P) = 1$.

R **Exercice 12**. (Critère d'Eisenstein)
Soit A un anneau factoriel de corps de fractions K.

1. Soit $P \in K[X]$ non nul. Montrez qu'il existe une écriture $P = aP'$ avec $a \in K \setminus \{0\}$ et $P' \in A[X]$ primitif, et que cette écriture est unique à association près.

2. Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire de degré $n \geqslant 1$ avec $a_i \in A$. On suppose qu'il existe un élément premier $p \in A$ tel que $p \mid a_i$ pour $i = 0, \ldots, n-1$ et $p^2 \nmid a_0$. Montrez qu'alors P est irréductible dans $K[X]$.

B **Exercice 13**. (Polynôme cyclotomique Φ_p)
Soit p un nombre premier. Démontrez que le polynôme $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$ est irréductible dans $\mathbb{Q}[X]$. (Indication : on pourra s'intéresser à $\Phi_p(X+1)$.)

2 Extensions de corps

Éléments algébriques, extensions algébriques

V **Exercice 14**. (Un classique)
Montrez que $[\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q}] = 6$, avec $j := e^{2i\pi/3}$.

B **Exercice 15**. (Degrés premiers entre eux)
Soit E/K une extension de corps. Soient $\alpha, \beta \in E$ des éléments algébriques sur K, de degrés m et n.

1. On suppose m et n premiers entre eux. Montrez que $[K(\alpha, \beta) : K] = mn$.
2. Le résultat subsiste-t-il sans l'hypothèse de primalité ?

B **Exercice 16**. (Extensions quadratiques de $\mathbb{Q}$)
Soit $K/\mathbb{Q}$ une extension de degré 2, avec $K \subset \mathbb{C}$. Montrez qu'il existe $n \in \mathbb{N}^*$ tel que $K = \mathbb{Q}(\sqrt{n})$ ou $K = \mathbb{Q}(i\sqrt{n})$. (Indication : commencer par fixer un $x \in K \setminus \mathbb{Q}$. Montrer que son polynôme minimal est de degré 2 puis que la racine carrée de son discriminant se trouve dans $K \setminus \mathbb{Q}$, et conclure.)

B **Exercice 17**. (Extension biquadratique)
Montrez que $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ est une extension monogène de $\mathbb{Q}$, c'est-à-dire de la forme $\mathbb{Q}(x)$.

R **Exercice 18**. (Degré de sommes de nombres algébriques)
Dans chaque cas, trouver le degré sur $\mathbb{Q}$ de α, de β et de $\alpha + \beta$.

1. $\alpha = \sqrt{2}$ et $\beta = \sqrt[3]{5}$.
2. $\alpha = \sqrt[3]{2 + \sqrt{3}}$ et $\beta = \sqrt[3]{2 - \sqrt{3}}$. (Indication : on pourra calculer $(\alpha + \beta)^3$.)

Corrigé. 1. Nous nous limitons à calculer le degré de $\alpha + \beta$. Posons $\gamma := \alpha + \beta$. On peut commencer en essayant de trouver un polynôme annulateur pour γ, en espérant qu'on saura montrer qu'il est irréductible. En tenant compte du fait que $\alpha^2 = 2$, on calcule :

$$5 = \beta^3 = (\gamma - \alpha)^3 = \gamma^3 - 3\alpha\gamma^2 + 6\gamma - 2\alpha.$$

On en déduit que $(\star)$ $\gamma^3 + 6\gamma - 5 = 3\alpha\gamma^2 + 2\alpha = (3\gamma^2 + 2)\alpha$ puis

$$(\gamma^3 + 6\gamma - 5)^2 = 2(3\gamma^2 + 2)^2.$$

Ceci fournit un polynôme de degré 6 annulateur de γ. Mais montrer qu'il est irréductible sur $\mathbb{Q}$ semble une tâche effrayante... Procédons différemment : si on démontre que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$, en utilisant le résultat de l'exercice 15, comme $\deg(\alpha) = 2$ et $\deg(\beta) = 3$ sont premiers entre eux, on obtiendra $\deg(\gamma) = 6$. Et en effet cette stratégie fonctionne, car l'égalité $(\star)$ ci-dessus donne :

$$\alpha = \frac{\gamma^3 + 6\gamma - 5}{3\gamma^2 + 2} \in \mathbb{Q}(\gamma)$$

donc aussi $\beta = \gamma - \alpha \in \mathbb{Q}(\gamma)$. Ainsi l'inclusion $\mathbb{Q}(\gamma) \subset \mathbb{Q}(\alpha, \beta)$ est une égalité. Ouf !

2. Nous nous limitons à calculer le degré de α et le degré de β. Comme $\alpha^3 = 2 + \sqrt{3}$ et $\beta^3 = 2 - \sqrt{3}$, on a $(\alpha^3 - 2)^2 = (\beta^3 - 2)^2 = 3$. Ceci signifie que α et β sont tous deux racines du polynôme

$$P(X) = (X^3 - 2)^2 - 3 = (X^3 - 2 - \sqrt{3})(X^3 - 2 + \sqrt{3}) = X^6 - 4X^3 + 1.$$

Nous allons montrer que ce polynôme est irréductible sur $\mathbb{Q}$, et ce sera donc le polynôme minimal de α et β qui seront alors de degré 6. Pour cela on peut s'aider de la factorisation de P dans $\mathbb{R}[X]$, qui est facile à obtenir :

$$P(X) = (X^3 - 2 - \sqrt{3})(X^3 - 2 + \sqrt{3}) = (X - \alpha)(X^2 + \alpha X + \alpha^2)(X - \beta)(X^2 + \beta X + \beta^2).$$

Les facteurs de degré 2 sont bien irréductibles sur $\mathbb{R}$ car leur discriminant est < 0. Considérons une factorisation $P = QR$ dans $\mathbb{Q}[X]$. Comme $\deg(P) = 6$, l'un des deux facteurs est de degré $\leqslant 3$, disons par exemple que $\deg(Q) \leqslant 3$.

1. L'éventualité $\deg(Q) = 1$ est impossible car ni $(X - \alpha)$ ni $(X - \beta)$ n'est à coefficients dans $\mathbb{Q}$.
2. L'éventualité $\deg(Q) = 2$ est impossible car :
   (a) $(X^2 + \alpha X + \alpha^2) \notin \mathbb{Q}[X]$,
   (b) $(X^2 + \beta X + \beta^2) \notin \mathbb{Q}[X]$,
   (c) $(X - \alpha)(X - \beta) \notin \mathbb{Q}[X]$. Démontrer ceci est plus difficile. On note que le coefficient constant est $\alpha\beta = 1$. Il faut donc montrer que $\gamma := \alpha + \beta \notin \mathbb{Q}$. Or on peut facilement trouver un polynôme annulateur pour γ, car $\alpha^3 + \beta^3 = 4$ (par définition de α et β) donc

   $$\gamma^3 = \alpha^3 + 3\alpha^2\beta + 3\alpha\beta^2 + \beta^3 = 4 + 3\alpha\beta(\alpha + \beta) = 4 + 3\gamma.$$

   Ainsi γ est racine de $P(X) = X^3 - 3X - 4$. Le critère d'existence d'une racine rationnelle $x = p/q$ fournit $p \mid 4$ et $q \mid 1$, donc $q = 1$ et $p \in \{\pm 1, \pm 2, \pm 4\}$. Aucun des nombres $\pm 1, \pm 2, \pm 4$ n'est racine, ce qui montre bien que $\alpha + \beta =\notin \mathbb{Q}$.
3. L'éventualité $\deg(Q) = 3$ est impossible car :
   (a) $(X - \alpha)(X^2 + \alpha X + \alpha^2) \notin \mathbb{Q}[X]$ puisque son coefficient constant est $-2 - \sqrt{3}$,
   (b) $(X - \alpha)(X^2 + \beta X + \beta^2) \notin \mathbb{Q}[X]$ puisque son coefficient constant est $-\beta$,

   et de même les symétriques en échangeant α et β ne sont pas à coefficients dans $\mathbb{Q}$.

La seule possibilité restante est $\deg(Q) = 0$, donc P est irréductible dans $\mathbb{Q}[X]$.

Clôture algébrique

V **Exercice 19**. (Algébriquement clos implique infini)
Montrer qu'un corps algébriquement clos n'est jamais fini.

V **Exercice 20**. (Extension contenant une clôture algébrique)
Soit E/K une extension telle que E contient une clôture algébrique $\bar{K}$ de K. Monter que, si H est une extension algébrique de K dans E, alors $H \subset \bar{K}$.

B **Exercice 21**. (Racines n-ièmes de l'unité dans $\bar{K}$)
Soit K un corps de caractéristique $p \geqslant 0$ et $\bar{K}$ une clôture algébrique. Pour tout entier $n \geqslant 1$ on note $\mu_n(\bar{K})$ l'ensemble des racines n-ièmes de l'unité dans $\bar{K}$.

1. On suppose que $p = 0$ ou $p > 0$, $p \nmid n$. Montrez que card $\mu_n(\bar{K}) = n$.
2. On suppose que $p > 0$ et on note $n = p^s m$ avec $s \geqslant 0$ et $p \nmid m$. Montrez que card $\mu_n(\bar{K}) = m$.

Corps de rupture, corps de décomposition

B **Exercice 22**. (Un cas de permanence d'irréductibilité)
Soit E/K une extension finie de degré m et $P \in K[X]$ un polynôme de degré n irréductible sur K.

1. On suppose m et n premiers entre eux. Montrez que P reste irréductible sur E. (Indication : considérez un facteur irréductible Q de P, et son corps de rupture E'.)
2. Le résultat subsiste-t-il sans l'hypothèse de primalité ?

B **Exercice 23**. (Extensions finies de $\mathbb{R}$)
Montrer qu'il n'existe pas d'extension de $\mathbb{R}$ de degré 4.

N **Exercice 24**. (Irréductibilité de $X^p - t$)
Soit K un corps. On considère le polynôme $P = X^p - t$ où p est un nombre premier et $t \in K$ n'est pas une puissance p-ième dans K. On souhaite montrer que le polynôme $P = X^p - t$ est irréductible.

1. Montrez qu'un corps de décomposition de P est de la forme $K' = K(\zeta, a)$ où $a^p = t$ et $\zeta^p = 1$.

Supposons que $P = QR$ avec $Q, R \in K[X]$ unitaires de degrés $i, j \in \{1, \ldots, p-1\}$.

2. Montrez que i et j sont premiers entre eux.
3. On suppose que la caractéristique de K est différente de p. Écrivez la factorisation de P dans K' et déduisez-en la forme des coefficients constants $q = Q(0)$ et $r = R(0)$. En utilisant une relation de Bézout $ui + vj = 1$, montrez que $\pm q^u r^v$ est une racine de P dans K. Concluez.
4. On suppose que la caractéristique de K est p. En regardant le coefficient de X^{i-1} dans Q, montrez que $a \in K$. Concluez.
5. Calculez le degré $[K' : K]$ (on distinguera selon que $\mu_p(\bar{K}) \subset K$ ou non).

R **Exercice 25**. (Irréductibilité de $X^{p^k} - t$)
Soient K un corps de caractéristique $p > 0$ et le polynôme $P = X^p - t$ où $t \in K$ n'est pas une puissance p-ième dans K. Montrez que pour tout entier $k \geqslant 1$, le polynôme $P = X^{p^k} - t$ est irréductible.

B **Exercice 26**. (L'habit ne fait pas le moine)

1. Montrer que $[\mathbb{Q}(\sqrt{1+\sqrt{5}}) : \mathbb{Q}] = 4$.
2. Donner un exemple d'un nombre rationnel r tel qu'on ait $[\mathbb{Q}(\sqrt{r+\sqrt{5}}) : \mathbb{Q}] = 2$.

R **Exercice 27**. (Polynômes réductibles modulo p pour tout p)
Le but de cet exercice est de démontrer qu'un polynôme de la forme $P(x) = x^4 + ax^2 + b^2$ avec $a, b \in \mathbb{Z}$ est réductible modulo p, pour tout p premier (c'est un cas particulier de *polynôme bicarré*).

1. Donnez un exemple de polynôme bicarré $P \in \mathbb{Z}[x]$ qui est irréductible.
2. Démontrez que P est réductible modulo 2.

Dans la suite, on réduit modulo un nombre premier p impair. On note $a = 2s \in \mathbb{F}_p$.

3. Démontrez que le groupe multiplicatif des carrés $(\mathbb{F}_p^\times)^2$ est d'indice deux dans $\mathbb{F}_p^\times$. Déduisez-en que si deux éléments $u, v \in \mathbb{F}_p^\times$ ne sont pas des carrés, alors leur produit uv est un carré.
4. Démontrez que modulo p, on a :

$$P(x) = (x^2+b)^2 - (2b-2s)x^2 = (x^2-b)^2 - (-2b-2s)x^2 = (x^2+s)^2 - (s^2-b^2).$$

5. En utilisant la question 3, déduisez-en que P est réductible modulo p.

B **Exercice 28**. (Un multiple irréductible défini sur le corps de base)
Démontrer que si E/K est une extension finie et $P \in E[X]$ est irréductible sur E, il existe $Q \in K[X]$ irréductible sur K tel que P divise Q dans $E[X]$.
(Indication : on pourra introduire le corps de rupture de P.)

3 Corps finis

V **Exercice 29**. (Corps à 4 éléments)
Soit K un corps à 4 éléments. Dressez la table d'addition et la table de multiplication de K. Pour fixer les notations, on pourra noter $a \in K$ un élément distinct de 0 et 1.

B **Exercice 30**. (Polynômes irréductibles de petit degré)

1. Dressez la liste des polynômes irréductibles unitaires sur $\mathbb{F}_2$ de degré $n \leqslant 3$.
2. Dressez la liste des polynômes irréductibles unitaires sur $\mathbb{F}_3$ de degré $n \leqslant 2$.

V **Exercice 31**. (Exponentielles et logarithmes sur un corps fini)

1. Soit K un corps fini. Décrivez tous les morphismes de groupes $e : K \to K^\times$ et $\ell : K^\times \to K$.
2. Application : démontrez que le corps des réels $\mathbb{R}$ n'est pas un corps fini.

V **Exercice 32**. (Clôture algébrique)
Soit $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$ et, pour tout entier $d \geqslant 1$, soit $\mathbb{F}_{p^d}$ son unique sous-corps à p^d éléments. Démontrez que $\overline{\mathbb{F}}_p$ est une réunion *croissante* :

$$\overline{\mathbb{F}}_p = \bigcup_{n \geqslant 0} \mathbb{F}_{p^{n!}}.$$

B **Exercice 33**. (Corps de rupture égale corps de décomposition)
Soient K un corps fini de cardinal q et $P \in K[X]$ un polynôme irréductible de degré n. On note (K_P, α) le corps de rupture de P, où $\alpha \in K_P$ est une racine de P.

1. Démontrez que pour tout $i \geqslant 1$, l'élément α^{q^i} est une racine de P.
2. Démontrez que $\alpha^{q^i} = \alpha \Rightarrow n \mid i$.
3. Déduisez-en que K_P est un corps de décomposition de P.

B **Exercice 34**. (Polynômes irréductibles sur un corps parfait)
Soit K un corps parfait, c'est-à-dire que $\mathrm{car}(K) = 0$ ou $\mathrm{car}(K) = p > 0$ avec un Frobenius bijectif.

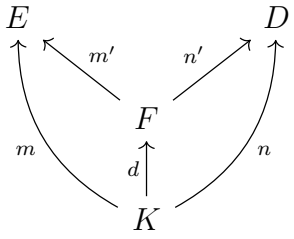
1. Soit $P \in K[X]$. On suppose que $\mathrm{car}(K) = p > 0$. Montrez que si $P' = 0$, alors il existe $Q \in K[X]$ tel que $P = Q^p$.
2. Soit $P \in K[X]$ irréductible. Montrez que ses racines dans un corps de décomposition (ou dans une clôture algébrique) sont toutes simples.

Ⓝ Exercice 35. (Décomposition d'un polynôme irréductible dans une extension)
Soient K un corps fini et $P \in K[X]$ un polynôme irréductible. Dans cet exercice, on explique comment décrire la factorisation de P en produit d'irréductibles dans une extension E/K.

Précisément, on note $q = \mathrm{card}(K)$, $n = \deg(P)$, $m = [E : K]$, $d = \mathrm{pgcd}(n, m)$ et on pose $n = dn'$, $m = dm'$. Nous allons démontrer que la décomposition de P dans $E[X]$ est de la forme $P = P_1 \cdots P_d$ avec $\deg(P_i) = n'$ pour tout i. D'après l'exercice 33, tout corps de rupture de P est également un corps de décomposition. On notera D un tel corps ; l'extension D/K est de degré n.

Dans la résolution de l'exercice, on pourra fixer une clôture algébrique $\overline{K}$ de K et noter $\mathbb{F}_{q^i}$ l'unique sous-corps à q^i éléments de $\overline{K}$ (par exemple $K = \mathbb{F}_q$). On prendra donc $E = \mathbb{F}_{q^m}$ et $D = \mathbb{F}_{q^n}$.

1. On note F un corps à q^d éléments. Démontrez qu'il existe des extensions :



On note $G = \mathrm{Gal}(D/K)$ le groupe de Galois de l'extension D/K, qui est un groupe cyclique de cardinal n engendré par l'automorphisme $\Phi : D \to D$, $\Phi(x) = x^q$. On note $H = \mathrm{Gal}(D/F)$ le groupe de Galois de D/F, qui est le sous-groupe de G engendré par Φ^d.

2. Démontrez que l'action naturelle de G sur l'ensemble R des racines de P dans D est libre et transitive.
3. Soient $\alpha_1, \ldots, \alpha_d$ des représentants des H-orbites dans R. Pour chaque i, on pose
$$P_i = \prod_{h \in H} (X - h(\alpha_i)).$$
Démontrez que $P_i \in F[X]$ et que P_i est irréductible dans $F[X]$.
(On pourra démontrer que P_i est le polynôme minimal de α_i sur F.)
4. Démontrez que $P = P_1 \cdots P_d$ est la décomposition de P en facteurs irréductibles dans E.

Corrigé. 1. Comme $d \mid m$ et $d \mid n$, il existe des morphismes $\mathbb{F}_{q^d} \to \mathbb{F}_{q^m} = E$ et $\mathbb{F}_{q^d} \to \mathbb{F}_{q^n} = D$. Puisque $F \simeq \mathbb{F}_{q^d}$, on obtient les extensions demandées. Le théorème de la base téléscopique fournit les degrés $[E : F]$ et $[D : F]$ qui sont indiqués sur la figure.

2. Un élément de G est de la forme $g = \Phi^i$ pour un certain entier i modulo n. Soit $\alpha \in R$ une racine de P. Supposons que $g(\alpha) = \alpha$, c'est-à-dire $\alpha^{q^i} = \alpha$. Alors $\alpha \in \mathbb{F}_{q^i}$, donc $K(\alpha) \subset \mathbb{F}_{q^i}$. Or $K(\alpha)$ est le corps de rupture D de P sur K, donc $n \mid i$. Alors i est nul modulo n et $g = \mathrm{id}$. L'action est donc libre. Il en découle que l'application d'orbite $G \to R$, $g \mapsto g(\alpha)$ est injective. Comme la source et le but sont de cardinal n, cette application est bijective, et en particulier l'action est transitive.

3. On prend $F = \mathbb{F}_{q^d}$. Par définition de $\mathbb{F}_{q^d}$ ou par théorème de correspondance de Galois des corps finis, le corps F est l'ensemble des points fixes de Φ^d ou, c'est la même chose, du groupe qu'il engendre et qui n'est autre que H. L'action de H sur D s'étend d'ailleurs en une action sur $D[X]$ en agissant sur les coefficients, c'est-à-dire que si $P = \sum a_i X^i$ et $h \in H$ on pose $h \cdot P := \sum h(a_i) X^i$.

Le polynôme P_i est scindé à racines dans D, en particulier c'est un élément de $D[X]$. Pour tout $h_0 \in H$, en faisant le changement de variable $h \to h_0 h$ on calcule :
$$h_0 \cdot P = h_0 \cdot \prod_{h \in H} (X - h(\alpha_i)) = \prod_{h \in H} (X - h_0 h(\alpha_i)) = \prod_{h \in H} (X - h(\alpha_i)) = P.$$

Ceci démontre que P est à coefficients dans F. Démontrons que P_i est le polynôme minimal de α_i sur F. Soit $Q \in F[X]$ un polynôme annulateur de α_i, i.e. $Q(\alpha_i) = 0$. Comme tout élément $h \in H$ fixe les éléments de F, en appliquant h à cette dernière égalité, les coefficients de Q sont inchangés et on obtient $Q(h(\alpha_i)) = 0$. On déduit que Q s'annule en tout les $h(\alpha_i)$, qui sont distincts, donc P divise Q. Ceci démontre que $P = P_{\alpha_i,F}$ et en particulier P est irréductible.

4. D'après la question 2 l'application d'orbite $G \to R$, $g \mapsto g(\alpha)$ est bijective. Il s'ensuit qu'elle transporte la partition de G en classes à droite modulo H sur la partition de R en H-orbites, qui (par définition des α_i) sont les ensembles $H\alpha_1, \dots, H\alpha_d$. Comme P est scindé dans D, on a :

$$P = \prod_{r \in R}(X - r) = \prod_{i=1}^{d}\prod_{h \in H}(X - h(\alpha_i)) = \prod_{i=1}^{d} P_i.$$

Puisque les P_i sont irréductibles dans F, c'est la décomposition de P en facteurs irréductibles dans F. Pour conclure, on note que le degré $\deg(P_i) = |H| = n/d = n'$ est premier avec $[E : F] = m'$. D'après le résultat de l'exercice 22, chaque P_i reste irréductible dans E, donc l'écriture précédente est aussi la décomposition de P en facteurs irréductibles dans E.

B **Exercice 36**. (Générateurs de $\mathbb{F}_{64}$)
On considère l'extension $\mathbb{F}_2 \subset \mathbb{F}_{64}$.

1. Déterminer les corps k vérifiant $\mathbb{F}_2 \subset k \subset \mathbb{F}_{64}$.
2. En déduire qu'il existe 54 éléments $\xi \in \mathbb{F}_{64}$ tels que $\mathbb{F}_{64} = \mathbb{F}_2(\xi)$. Pourquoi ce nombre est-il a priori divisible par 6 ?

Corrigé. 1. On a $64 = 2^6$ et les corps intermédiaires sont les corps $\mathbb{F}_{2^d}$ avec $d \mid 6$, donc ce sont $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{64}$.

2. Les éléments $\xi \in \mathbb{F}_{64}$ qui n'engendrent pas $\mathbb{F}_{64}$ sont ceux qui appartiennent à un sous-corps strict. Ce sont les éléments de $\mathbb{F}_8$ (qui inclut $\mathbb{F}_2$) et les deux éléments supplémentaires de $\mathbb{F}_4 \setminus \mathbb{F}_8$ (notez que $\mathbb{F}_4 \cap \mathbb{F}_8 = \mathbb{F}_2$). Au total cela en fait 10, il reste donc 54 éléments ξ tels que $\mathbb{F}_{64} = \mathbb{F}_2(\xi)$. On pouvait anticiper que ce nombre serait divisible par 6 car le groupe de Galois $G = \mathrm{Gal}(\mathbb{F}_{64}/\mathbb{F}_2)$ est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ et agit librement sur l'ensemble des générateurs ξ. L'orbite de ξ s'identifie à son polynôme minimal $P := P_{\xi,\mathbb{F}_2}$ puisque ses racines sont les ξ^{2^i}, voir les exercices 33 et 35.

N **Exercice 37**. (Polynômes irréductibles sur $\mathbb{F}_q$)
Soient $\mathbb{F}_q$ un corps fini de cardinal q et $P \in \mathbb{F}_q[X]$ un polynôme irréductible de degré d.

1. Démontrez que $P \mid X^{q^n} - X$ dans $\mathbb{F}_q[X]$ si et seulement si $d \mid n$.
   (On pourra introduire le corps de rupture de P et le corps de décomposition de $X^{q^n} - X$.)
2. Pour tout entier $m \geqslant 1$, on note $\mathscr{I}_m(\mathbb{F}_q)$ l'ensemble des polynômes irréductibles unitaires de degré m dans $\mathbb{F}_q[X]$, et $I(d, q)$ son cardinal. Démontrez que l'on a, pour tout $n \geqslant 1$:

$$X^{q^n} - X = \prod_{d \mid n}\prod_{P \in \mathscr{I}_d(\mathbb{F}_q)} P \qquad \text{et} \qquad q^n = \sum_{d \mid n} d\, I(d, q).$$

3. On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \mathbb{N}$ par $\mu(n) = 0$ si n possède un facteur carré et $\mu(n) = (-1)^r$ si n est produit de r nombres premiers distincts (en particulier $\mu(1) = 1$).
   (a) Démontrez que $\sum_{d \mid n} \mu(d)$ est égal à 0 si $n \neq 1$, et à 1 si $n = 1$.
   (b) Démontrez que si (a_n) et (b_n) sont deux suites complexes telles que $a_n = \sum_{d \mid n} b_d$ pour tout n, alors $b_n = \sum_{d \mid n} \mu(n/d) a_d$ pour tout n.

(c) En déduire une expression pour $I(n,q)$.

Corrigé. Notons $K_P = K[X]/(P)$ le corps de rupture de P avec la racine $x \in K_P$ égale à la classe résiduelle de X, et $E = \mathrm{Dec}_K(X^{q^n} - X) = \mathrm{Rac}_E(X^{q^n} - X)$, un corps à q éléments.

1. Supposons que $P \mid X^{q^n} - X$. Comme le polynôme $X^{q^n} - X$ est scindé dans E (par définition de E), alors P est scindé dans E lui aussi. En particulier P a une racine $\alpha \in E$. Elle fournit un morphisme $K_P \to E$ qui envoie x sur α. Ceci fait de E une extension de K_P, d'où $n = [E : K] = [E : K_P]\,[K_P : K] = d\,[E : K_P]$ par le théorème de la base télescopique.

Réciproquement supposons que $d \mid n$. Comme $K_P \simeq \mathbb{F}_{q^d}$ et $E \simeq \mathbb{F}_{q^n}$, l'hypothèse entraine l'existence d'un morphisme $K_P \to E$. En particulier, le polynôme $X^{q^n} - X$ s'annule en x. Comme P est irréductible, c'est le polynôme minimal de x sur K, donc il divise $X^{q^n} - X$.

2. Le polynôme $Q = X^{q^n} - X$ est séparable (i.e. sans racine double dans une clôture algébrique) car il est premier avec son dérivé $Q' = 1$. En particulier, ses facteurs irréductibles dans $K[X]$ sont de multiplicité 1. Or d'après la question 1, les facteurs irréductibles unitaires de Q sont exactement les polynômes irréductibles de $K[X]$ degré d (i.e. les éléments de $\mathscr{I}_d(K)$) pour un $d \mid n$. On obtient ainsi la factorisation annoncée pour $X^{q^n} - X$. En prenant les degrés, on trouve $q^n = \sum_{d|n} d\,I(d,q)$.

3. (a) Il est clair que $\mu(1) = 1$.