Corrigé du contrôle final du vendredi 10 janvier 2014

Exercice 1.

Parmi les polynômes suivants lesquels sont irréductibles ?

1. $X^{12} + \pi^2 X^9 + \sqrt{7}X^6 + 15$ dans $\mathbb{R}[X]$;
   Ce polynôme est réductible dans $\mathbb{R}[X]$ car les seuls polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant négatif.
2. $X^3 + 3X^2 - 9X - 1$ dans $\mathbb{Q}[X]$;
   Comme ce polynôme est unitaire et a pour coefficient constant -1 , on vérifie facilement que les seuls racines rationnels possibles sont 1 et -1. Or, 1 et -1 ne sont pas des zéros de ce polynôme. Ce polynôme est donc irréductible car il est de degré 3 et n'a pas de racine dans $\mathbb{Q}$.
3. $X^3 - 6X^2 + 12X - 8$ dans $\mathbb{Q}[X]$;
   On remarque que 2 est racine de ce polynôme (en fait $X^3 - 6X^2 + 12X - 8 = (X-2)^3$) ; ce polynôme est donc réductible.
4. $20X^{17} + 27X^{13} - 15X^4 + 30X - 12$ dans $\mathbb{Q}[X]$;
   Ce polynôme satisfait le critère d'Eisenstein pour $p = 3$. Il est donc irréductible.
5. $5X^9 + 25X^7 - 75X^4 + 125X^2 - 25$ dans $\mathbb{Q}[X]$;
   On a $5X^9 + 25X^7 - 75X^4 + 125X^2 - 25 = 5(X^9 + 5X^7 - 15X^4 + 25X^2 - 5)$ et $X^9 + 5X^7 - 15X^4 + 25X^2 - 5$ vérifie le critère d'Eisenstein pour $p = 5$. On en déduit que $5X^9 + 25X^7 - 75X^4 + 125X^2 - 25$ est irréductible.
6. $X^6 - X^5 + X^4 - X^3 + X^2 - X + 1$ dans $\mathbb{Z}/7\mathbb{Z}[X]$.
   -1 est racine évidente, donc ce polynôme est réductible.

Exercice 2. Soit G un groupe. On note multiplicativement la loi de groupe et e l'élément neutre de G. On suppose qu'il existe un élément a d'ordre $n > 1$.

1. On fixe un nombre premier p divisant n et on pose $m = n/p$.
   Montrer que a^m est d'ordre p.
   On a d'une part $(a^m)^p = a^n = e$ et d'autre part, pour tout $k \in \mathbb{N}$, si $(a^m)^k = e$ alors $n = mp$ divise mk et donc p divise k. Cela signifie que a^m est d'ordre p.
2. Soit $b \in G$ un élément conjugué à a (c.à.d. tel que $b = gag^{-1}$ pour un $g \in G$). Montrer que b est également d'ordre n.
   Soit $g \in G$ tel que $b = gag^{-1}$. On vérifie facilement que pour tout $k \in \mathbb{N}$,
   $$b^k = ga^k g^{-1}$$
   et en particulier
   $$b^k = e \text{ si et seulement si } a^k = e.$$
   Ainsi, a et b ont même ordre.

Pour toute la suite, on suppose que tous les éléments de $G \setminus \{e\}$ sont conjugués à a.

3. En utilisant les deux questions précédentes, montrer que $x^p = e$ pour tout $x \in G$ et en particulier que $n = p$.
   Par la question (1.) a^m est d'ordre p et en particulier non trivial. Il est donc conjugué à a et par la question (2.) a même ordre que a. Donc $n = p$. Par la question (2.) tous les éléments non triviaux ont également même ordre que a, c'est-à-dire ordre p. Il suit que $x^p = e$ pour tout $x \in G$.

4. Soit $x \neq e$ dans G.

   (a) Montrer qu'il existe $g \in G$ tel que
   $$x^{-1} = gxg^{-1}.$$
   x et x^{-1} sont tous deux conjugués à a par hypothèse. Comme la relation de conjugaison est une relation d'équivalence, donc en particulier transitive et symétrique, on a immédiatement que x^{-1} est conjugué à x.

   (b) Vérifier que
   $$x = gx^{-1}g^{-1} \text{ puis que } x = g^2x(g^{-1})^2.$$
   $$x = (x^{-1})^{-1} = (gx^{-1}g^{-1})^{-1} = (g^{-1})^{-1}(x^{-1})^{-1}g^{-1} = gx^{-1}g^{-1}$$
   et en remplaçant dans cette dernière équation x^{-1} par gxg^{-1}, on obtient
   $$x = gx^{-1}g^{-1} = g(gxg^{-1})g^{-1} = g^2x(g^{-1})^2.$$

   (c) Montrer que pour tout entier positif k impair,
   $$x^{-1} = g^kx(g^{-1})^k.$$
   Pour $k = 1$, l'équation est vérifiée par le choix de g dans la question (a). Supposons l'équation vérifiée pour un entier positif k impair, alors par la question (b), on a
   $$x^{-1} = g^kx(g^{-1})^k = g^k(g^2x(g^{-1})^2)(g^{-1})^k = g^{k+2}x(g^{-1})^{k+2}$$
   et l'équation est donc également vérifiée pour $k + 2$. Par récurrence, cette équation est ainsi vérifiée pour tout entier positif k impair.

   (d) En déduire que $x^{-1} = x$ et $p = 2$.
   Si p était impair, alors par les questions (c) et (3.), $x^{-1} = g^px(g^{-1})^p = x$ et donc x est d'ordre 2, mais également d'ordre p par la question (3.). On a donc nécessairement $p = 2$ et $x^{-1} = x$.

5. Conclure que G est commutatif.
   Par la question (4.) tous les éléments non triviaux sont d'ordre 2. Soient $x, y \in G$. Alors
   $$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$
   Ainsi, G est commutatif.

Exercice 3. On dit qu'un nombre complexe est *algébrique* s'il est racine d'un polynôme non nul à coefficients rationnels.

Soit $\alpha \in \mathbb{C}$ un nombre algébrique et soit $I = \{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\}$.

1. Montrer I est un sous-groupe de $(\mathbb{Q}[X], +)$.
   Le polynôme nul est évidemment nul en α donc $0 \in I$.
   Soit $P, Q \in I$. Alors $(P+Q)(\alpha) = P(\alpha) + Q(\alpha) = 0 + 0 = 0$ et $(-P)(\alpha) = -P(\alpha) = 0$ donc $P + Q \in I$ et $-P \in I$. On a donc vérifié que I était un sous-groupe de $(\mathbb{Q}[X], +)$.

2. Montrer que pour tout $P \in I$ et tout $Q \in \mathbb{Q}[X]$, on a $QP \in I$.
   Soit $P \in I$ et $Q \in \mathbb{Q}[X]$. Alors $(QP)(\alpha) = Q(\alpha)P(\alpha) = Q(\alpha) \times 0 = 0$, donc $QP \in I$. (Remarque : une partie d'un anneau commutatif vérifiant (1.) et (2.) est appelée un idéal.)

3. Montrer qu'il existe un unique polynôme unitaire P_α qui engendre I (c.à.d. tel que $I = \{QP_\alpha \in \mathbb{Q}[X] \mid Q \in \mathbb{Q}[X]\}$).
   Montrons l'existence : $I \neq \{0\}$ car α est algébrique. On considère alors un polynôme non nul P_α de I de degré minimal, que l'on peut supposer unitaire. Comme $P_\alpha \in I$, on a évidemment
   $$\{QP_\alpha \in \mathbb{Q}[X] \mid Q \in \mathbb{Q}[X]\} \subset I.$$
   Pour l'inclusion inverse, considérons $P \in I$. Par division euclidienne de P par P_α dans $\mathbb{Q}[X]$, ils existent $Q, R \in \mathbb{Q}[X]$ tels que $P = P_\alpha Q + R$ avec R nul ou de degré strictement inférieur à celui de P_α. Comme $R = P - P_\alpha Q$, on a $R \in I$ et par minimalité du degré de P_α, le polynôme $R = 0$ et donc $P = QP_\alpha$. (Remarque : la preuve ci-dessus correspond à la preuve générale du fait qu'un anneau euclidien est principal, c'est-à-dire que ses idéaux sont engendrés par un seul élément.)
   Pour l'unicité, considérons un second polynôme unitaire P qui engendre I. Alors P_α et P se divisent réciproquement et comme ils sont unitaires, ils sont égaux.

4. Montrer que P_α est l'unique polynôme irréductible unitaire de $\mathbb{Q}[X]$ qui annule α.
   Si $P_\alpha = Q_1 Q_2$ alors $Q_1(\alpha) = 0$ ou $Q_2(\alpha) = 0$ et ainsi P_α divise Q_1 ou Q_2, ce qui signifie que Q_2 ou Q_1 sont des constantes. Le polynôme P_α est donc irréductible.
   Vérifions maintenant l'unicité (attention : l'unicité ne porte pas sur les mêmes propriétés que la question précédente).
   Soit P un polynôme irréductible unitaire tel que $P(\alpha) = 0$. Alors P_α divise P et par irréductibilité de P, ils sont associés, donc égaux car tous deux unitaires.

5. On considère $\mathbb{Q}[\alpha] = \{P(\alpha) \in \mathbb{C} \mid P \in \mathbb{Q}[X]\}$. Montrer que $\mathbb{Q}[\alpha]$ est un sous-anneau de $\mathbb{C}$.
   On vérifie facilement que l'application $\phi : \mathbb{Q}[X] \to \mathbb{C}$ définie par $\phi(P) = P(\alpha)$ pour tout $P \in \mathbb{Q}[X]$, est un morphisme d'anneaux. On en déduit que $\operatorname{Im}\phi = \mathbb{Q}[\alpha]$ est un sous-anneau de $\mathbb{C}$.

6. Soit $d = \deg P_\alpha$. Montrer que pour tout polynôme $P \in \mathbb{Q}[X]$, il existe un polynôme $R \in \mathbb{Q}[X]$ qui est soit nul, soit de degré strictement inférieur à d, et tel que
   $$P(\alpha) = R(\alpha).$$

Soit $P \in \mathbb{Q}[X]$. De même qu'à la question (3.), par division euclidienne ils existent $Q, R \in \mathbb{Q}[X]$ tels que $P = P_\alpha Q + R$ avec R nul ou de degré strictement inférieur à d. Alors, $P(\alpha) = P_\alpha(\alpha)Q(\alpha) + R(\alpha) = R(\alpha)$.

7. En déduire que

$$\mathbb{Q}[\alpha] = \{\lambda_0 + \lambda_1\alpha + \ldots + \lambda_{d-1}\alpha^{d-1} \in \mathbb{C} \mid \lambda_0, \ldots, \lambda_{d-1} \in \mathbb{Q}\}.$$

L'inclusion $\{\lambda_0 + \lambda_1\alpha + \ldots + \lambda_{d-1}\alpha^{d-1} \in \mathbb{C} \mid \lambda_0, \ldots, \lambda_{d-1} \in \mathbb{Q}\} \subset \mathbb{Q}[\alpha]$ est immédiate. Réciproquement, si $a \in \mathbb{Q}[\alpha]$ alors $a = P(\alpha)$ pour un polynôme $P \in \mathbb{Q}[X]$. Par la question précédente, $a = R(\alpha)$ où R est nul ou de degré strictement inférieur à d ; ce qui permet de conclure.

8. Soit $P \in \mathbb{Q}[X]$ un polynôme non nul de degré strictement inférieur à d. Montrer qu'il existe des polynômes $U, V \in \mathbb{Q}[X]$ tel que $PU + P_\alpha V = 1$.
   Comme P_α est irréductible et P est de degré strictement inférieur à celui de P_α, on a P et P_α premiers entre-eux et on peut donc appliquer le théorème de Bezout qui donne l'identité demandée.

9. En déduire que $\mathbb{Q}[\alpha]$ est un sous-corps de $\mathbb{C}$.
   On a vérifié en (5.) que $\mathbb{Q}[\alpha]$ est un sous-anneau. Il reste donc à vérifier la stabilité par inverse : soit $a \in \mathbb{Q}[\alpha] \setminus \{0\}$. Par (7.), il existe $P \in \mathbb{Q}[X]$ non nul de degré strictement inférieur à d tel que $a = P(\alpha)$. Par (8.), il existe des $U, V \in \mathbb{Q}[X]$ tel que $PU + P_\alpha V = 1$. Ainsi, $P(\alpha)U(\alpha) + P_\alpha(\alpha)V(\alpha) = 1$ et $aU(\alpha) = 1$. D'où $a^{-1} = U(\alpha) \in \mathbb{Q}[\alpha]$.

10. Montrer que $\mathbb{Q}[\alpha]$ est un espace vectoriel sur $\mathbb{Q}$ de dimension d.
    Comme $\mathbb{Q}[\alpha]$ est un corps contenant $\mathbb{Q}$, c'est en particulier un espace vectoriel sur $\mathbb{Q}$. Par la question (7.), la famille $(1, \alpha, \ldots, \alpha^{d-1})$ est une famille génératrice de $Q[\alpha]$. Montrons qu'elle est également libre : soient $\lambda_0, \ldots, \lambda_{d-1} \in \mathbb{Q}$ tel que $\lambda_0 + \lambda_1\alpha + \ldots + \lambda_{d-1}\alpha^{d-1} = 0$. Alors, le polynôme $P = \lambda_0 + \lambda_1 X + \ldots + \lambda_{d-1}X^{d-1}$ est dans I et donc divisible par P_α, qui est de degré d. Ainsi, $P = 0$ et $\lambda_0 = \lambda_1 = \ldots = \lambda_{d-1} = 0$; ce qui permet de conclure.

11. Supposons que $d = 2$ et $\alpha \in \mathbb{R}$. Montrer qu'il existe alors un rationnel positif a tel que $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{a}]$.
    Dans ce cas $P_\alpha = X^2 + bX + c$ avec $b, c \in \mathbb{Q}$. Comme $\alpha \in \mathbb{R}$ et P_α irréductible, le discriminant $\Delta = b^2 - 4c \in \mathbb{Q}$ vérifie $\Delta > 0$. Soit $a = \sqrt{\Delta}$, alors $\alpha = (-b \pm a)/2$ et donc $\mathbb{Q}[\alpha] \subseteq Q[\sqrt{a}]$. De même $a = \pm(2\alpha + b)$ donc $Q[\sqrt{a}] \subseteq \mathbb{Q}[\alpha]$.