École Polytechnique 2022-2023

Algèbre et théorie de Galois

Corrigé de la Feuille d'exercices 2

Exercice 1

1. Soit $H =< x >$ le sous-groupe engendré par x. On a $H = \{x^k, k \in \mathbf{Z}\} = \{e, x, x^2, \ldots, x^{n-1}\}$. Le cardinal de H est donc égal à l'ordre de x. La relation $|G| = |H||G/H|$ montre que cet entier divise le cardinal de G.

2. Soit $x \in G\backslash\{e\}$. Il est d'ordre supérieur ou égal à 2, et divise $|G| = p$. On en déduit que x est d'ordre p, et que $G = \{e, x, \ldots, x^{p-1}\}$. Le groupe G est donc cyclique, isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

Exercice 2

1. L'action isométrique de G sur le tétraèdre préserve les sommets, notamment parce qu'ils sont à distance maximale du centre. Le morphisme est injectif car les quatre vecteurs joignant l'origine aux sommets engendrent $\mathbf{R}^3$: une application *linéaire* est donc déterminée par l'image de ces vecteurs.

2. Soient z le milieu du segment xy et P le plan contenant l'arête opposée à xy, passant par z. La symétrie orthogonale s est la symétrie associée à P. (En effet, xy est bien perpendiculaire à P.) Il en résulte que s préserve les 4 sommets (et donc le tétraèdre). Par construction, $\phi(s)$ est la transposition qui échange x et y.

3. Le groupe $\mathfrak{S}(T)$ est engendré par les transpositions donc φ est aussi surjective (d'après 2.).

4. L'ensemble des paires d'arêtes opposées est en bijection avec les décompositions de T en $E_1 \cup E_2$, avec $|E_1| = |E_2| = 2$. Fixant $x \in T$, le choix d'une telle paire revient à choisir une arête contenant x et il y a $|T \setminus \{x\}| = 3$ telles arêtes. C'est un fait général que les permutations préservent ce type de partitions et on obtient donc un morphisme $f : \mathfrak{S}_4 \simeq G \to \mathfrak{S}(S) \simeq \mathfrak{S}_3$. De plus, les rotations d'angle $2\pi/3$ d'axe passant par un sommet et le centre de gravité du triangle opposé s'envoient sur les deux 3-cycles de $\mathfrak{S}(S)$ tandis que les symétries de la question 2. induisent les trois transpositions, f est donc surjective. (Remarque: Pour montrer la surjectivité, il aurait aussi suffit d'exhiber des générateurs dans l'image de f; le groupe $\mathfrak{S}_3$ n'ayant que 6 éléments, cela ne simplifierait pas notablement la démonstration.)

5. Indépendamment de l'interprétation géométrique, le morphisme f étant surjectif, on a $|K| = |\mathfrak{S}_4||\mathfrak{S}_3|^{-1} = 4$. De plus, puisque K est contenu dans le noyau de la signature (qui se factorise à travers $f : \mathfrak{S}_4 \to \mathfrak{S}_3$), c'est un sous-groupe de A_4. Nécessairement, c'est $(\mathbf{Z}/2\mathbf{Z})^2$ (en effet, A_4 ne contient aucun élément d'ordre 4 donc, d'après l'exercice 1, tous les éléments de K sont d'ordre 2). Géométriquement, on constate que les éléments de K sont l'identité et les rotations d'angle π d'axe passant par les milieux de deux arêtes opposées.

   Alternativement, cette description peut se démontrer directement de la façon suivante. Soit $r \in K$ un élément non trivial. Alors il existe $x \in T$ tel que $y = r(x)$ soit différent de x (d'après la question 1.). Notons $w, z \in T$ les deux sommets différents de x et y. Comme r préserve les paires d'arêtes opposées $\{[x, y], [w, z]\}$ et $\{[x, w], [y, z]\}$ on en déduit immédiatement que $r(y) = x$, $r(w) = z$ et $r(z) = w$. Il s'ensuit que r est la rotation d'angle π d'axe passant par les milieux de $[x, y]$ et $[w, z]$.

On peut montrer que les seuls sous-groupes distingués propres non triviaux de $\mathfrak{S}_4$ sont K et A_4.

Exercice 3

1. Ici encore, les orbites forment une partition de X : elles recouvrent X car $x \in G \cdot x$ et si $z \in G \cdot x \cap G \cdot y \neq \emptyset$, on a $z = g_1 \cdot x = g_2 \cdot y$ donc $y = g_2^{-1} \cdot z = (g_2^{-1} g_1) \cdot x \in G \cdot x$ d'où $G \cdot y \subseteq G \cdot x$. Par symétrie, $G \cdot x = G \cdot y$. L'égalité sur les cardinaux est alors triviale.

2. L'équation aux classes résulte de 1. et de la formule $|G| = |G \cdot x||G_x|$. Pour établir cette dernière, il suffit de vérifier que les fibres de l'application surjective $\pi : G \to G \cdot x$, $g \to g \cdot x$, sont toutes de même cardinal $|G_x|$. (Par 'fibre' d'une application $f : X \to Y$ on entend les sous-ensembles $f^{-1}(y)$, $y \in Y$. On dit que $f^{-1}(y)$ est la *fibre au-dessus de y*.) Or, si $g_1 \cdot x = g_2 \cdot x$, on a $g_1^{-1} g_2 \in G_x$, c'est-à-dire $g_2 \in g_1 G_x$: la fibre au-dessus de $g \cdot x$ est égale à $g \cdot G_x$, lui-même en bijection avec G_x.

3. Si G est un p-groupe, c'est-à-dire un groupe de cardinal une puissance de p, il en est de même de ses sous-groupes (Lagrange), en particulier les stabilisateurs G_x, pour $x \in X$. Les orbites $G \cdot x$ sont, on l'a vu, de cardinal l'*indice* de G_x dans G $[|G|/|G_x|]$ qui est lui-aussi une puissance de p. Deux cas sont donc possibles : soit l'orbite est ponctuelle (de cardinal 1, correspondant à un point fixe), soit elle est de cardinal > 1, nécessairement divisible par p (car c'est une puissance de p). En considérant l'égalité $|X| = \sum_{x \in \Theta} |G \cdot x|$ modulo p, on obtient bien la congruence $|X| \equiv |X^G| \pmod{p}$.

4. L'ensemble des points fixes de l'action de G sur lui-même par conjugaison est, tautologiquement, le centre $Z(G)$ de G. D'après ce qui précède, $Z(G)$ est donc un [sous-]groupe de cardinal divisible par p, donc de cardinal > 1.

Exercice 4

1. La projection $X \to G^{p-1}$, $(x_1, \ldots, x_p) \mapsto (x_2, \ldots, x_p)$ sur les $p-1$ dernières coordonnées induit une bijection: poser $x_1 := (x_2 \cdots \cdots x_p)^{-1}$. En particulier, $|X| = |G|^{p-1}$.

2. Il est évident que l'on a bien une action par permutation des indices sur l'ensemble G^p ; reste à vérifier que le sous-ensemble $X \subseteq G^p$ est stable. Cela revient à voir que si $x_1 x_2 \ldots x_{p-1} x_p = 1$, on a également $x_2 \ldots x_{p-1} x_p x_1 = 1$. La première égalité dit, comme on l'a vu, que x_1 est un inverse à gauche de $x_2 \ldots x_{p-1} x_p$; il l'est également à droite.

3. D'après l'exercice précédent, l'ensemble des points fixes de cette action est congru modulo p à $|G|^{p-1} \equiv 0$. Or, l'ensemble des points fixes de $\mathbf{Z}/p\mathbf{Z}$ sur G^p n'est autre que la diagonale $\{(x, x, \ldots, x) : x \in G\}$. Les points fixes dans X correspondent donc au sous-ensemble des $x \in G$ tels que $x^p = 1$ (éléments d'ordre 1 ou p). Comme cet ensemble est non vide — il contient $1 \in G$ — il contient également un élément $\neq 1$, d'ordre exactement p.

Exercice 5

1. Par définition, D_n^+ est le noyau du morphisme composé $D_n \to O_2(\mathbf{R}) \xrightarrow{det} \{\pm 1\}$; il est donc distingué. D'autre part, un élément de $D_n^+ = D_n \cap SO_2(\mathbf{R})$ est une rotation ; si elle préserve P son angle est nécessairement un multiple de $2\pi/n$, et réciproquement.

2. Tout élément de $O_2(\mathbf{R})\backslash SO_2(\mathbf{R})$ est une symétrie axiale [=réflexion] ; c'est en particulier vrai des éléments de $D_n\backslash D_n^+$. Notons que si s est une symétrie d'axe Δ, la symétrie conjuguée $\tau s\tau^{-1}$ est d'axe $\tau(\Delta)$. On vérifie alors immédiatement que si n est pair, il y deux classes de conjugaison (de même cardinal) : celles d'axe passant par des sommets (opposés) et celles d'axe passant par le milieu de côtés opposés. Si n est impair, il n'y a qu'une classe de conjugaison : tout axe de symétrie passe par un sommet et le milieu du côté opposé.

3. Le groupe D_n^+, de cardinal n, est le noyau du morphisme $D_n \to \{\pm 1\}$ induit par le déterminant. Le groupe D_n est donc de cardinal $2n$ si et seulement si ce morphisme est non trivial, c'est-à-dire s'il existe un élément dans $D_n\backslash D_n^+$. On a vu que c'est le cas.

Exercice 6

1. Soit $\pi : A \to A/I$ la surjection canonique. Si $\overline{J}$ est un idéal de A/I, alors $\pi^{-1}(\overline{J})$ est un idéal de A contenant I. Si J est un idéal de A contenant I, alors $\pi(J) = J/I$ est un idéal de A/I. On vérifie que ces applications sont inverses l'une de l'autre.

2. L'élément 0 est dans N. Soient $x, y \in N$; il existe $n, m \geq 1$ avec $x^n = 0$, $y^m = 0$. La formule du binôme donne $(x+y)^{n+m} = 0$, donc $x + y \in N$. Si $a \in A$, alors $(ax)^n = a^n x^n = 0$, donc $ax \in N$. Cela prouve que N est un idéal.

3. Soit $x \in A$ tel que l'image de x soit nilpotente dans A^{red}. Il existe $n \geq 1$ tel que $x^n \in N$. Il existe alors $m \geq 1$ tel que $(x^n)^m = x^{nm} = 0$, donc $x \in N$, et l'image de x est nulle dans A^{red}. L'anneau A^{red} est donc réduit.

4. Soit I un idéal premier de A. L'anneau A/I est donc intègre. Soit $x \in N$: il existe $n \geq 1$ avec $x^n = 0$. Cette égalité dans A/I implique que $x = 0$ dans A/I, donc $x \in I$. Les idéaux premiers de A contiennent tous N, et induisent donc des idéaux de A^{red} Si J est un idéal de A contenant N, on note $\overline{J} = J/N$. On a un isomorphisme

$$A/J \simeq A^{red}/\overline{J}$$

ce qui prouve que J est premier si et seulement si $\overline{J}$ est premier. Puisque les idéaux premiers contiennent tous N, on en déduit la bijection demandée.

Exercice 7

1. Dire que p ne divise pas tous les coefficients de f revient à dire que $f_p := f \pmod p \in \mathbf{Z}/p\mathbf{Z}[T]$ est non nul. La conclusion résulte alors du fait que $(fg)_p = f_p g_p$ et que le produit de deux polynômes non nuls à coefficients dans un corps est non nul. (L'anneau quotient $\mathbf{Z}/p\mathbf{Z}$ est bien un corps car p est premier ; on le note souvent $\mathbf{F}_p$.)

2. Résulte de 1. et du fait qu'un polynôme f est primitif si et seulement si $f_p \neq 0$ pour tout nombre premier p.

3. Il s'agit d'une question de pure arithmétique : on veut montrer que donné un élément de $\mathbf{Q}^n\backslash\{0\}$, c'est-à-dire un n-uplet de fractions (non toutes nulles), on peut factoriser un unique nombre rationnel > 0 pour obtenir un n-uplet d'*entiers* relatifs globalement premiers entre eux. Pour chaque nombre premier p, il faut et il suffit de factoriser la plus grande puissance de p (positive ou négative) permettant obtenir des fractions sans p au dénominateur. (En symboles, on peut introduire la valuation p-adique $v_p(r) \in \mathbf{Z} \cup \{+\infty\}$ d'un rationnel r et poser $c(f) = \prod_p p^{\min_i v_p(a_i)}$, où $f = \sum_i a_i T^i$.) Si les coefficients sont entiers, il en est de même du contenu, qui est le pgcd des coefficients.

4. On utilise 2. et l'unicité du 3. : si $f = c(f)F$, $g = c(g)G$ on a $fg = c(f)c(g)FG$, et FG est primitif. Donc $c(f)c(g)$ est le contenu de fg.

5. Soient $f \in \mathbf{Z}[T]$ irréductible et $f = gh$ une factorisation *dans* $\mathbf{Q}[T]$. On a $g = c(g)G$, de même pour h, d'où une réécriture $f = c(g)c(h)GH$, avec $c(g)c(h) = c(f)$. Or, f est irréductible dans $\mathbf{Z}[T]$ donc son contenu est égal à 1 ; on a donc une factorisation dans $\mathbf{Z}[T]$: $f = GH$. Ceci n'est possible que si $G = \pm 1$ (c'est-à-dire g constant) ou $H = \pm 1$ (c'est-à-dire h constant). CQFD.

Exercice 8

1. D'après le lemme de Gauß (exercice précédent), il suffit de montrer que f est irréductible dans $\mathbf{Z}[T]$. Soit $f = gh$ une factorisation avec $g, h \in \mathbf{Z}[T]$. Quitte à les multiplier tous les deux par -1, on peut supposer g et h unitaires. Notant f_p, g_p et h_p les réductions modulo p de f, g et h respectivement, on a alors dans $\mathbf{F}_p[T]$ la factorisation $f_p = g_p h_p$. Or, le terme de gauche est, par hypothèse, T^n. Il en résulte que $g_p = T^a$ et $h_p = T^b$ pour a, b deux entiers de somme n. Nécessairement, $a = deg(g)$, $b = deg(h)$; si a et b sont > 0 on a $p|g(0)$ et $p|h(0)$, d'où $p^2|f(0) = a_0$, ce qui est absurde. On a donc par exemple $a = 0$, d'où $g = 1$ et f est bien irréductible.

2. Le polynôme $T^n - 2$ convient : il satisfait le critère d'Eisenstein pour $p = 2$ et est donc irréductible.

De même, on pourrait établir un analogue du critère d'Eisenstein pour l'anneau $\mathbf{C}[X]$ (plutôt que $\mathbf{Z}$), de corps des fractions $K = \mathbf{C}(X)$ l'ensemble des fractions rationnelles à coefficients dans $\mathbf{C}$, et en déduire que le polynôme $T^n - X \in K[T]$ est irréductible pour tout entier $n \geq 1$.