Corrigé de l'examen final

Problème 1

1. Trouver les facteurs invariants du groupe $\mathbb{Z}/54\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}$

Réponse : Comme

$$\begin{aligned} \mathbb{Z}/54\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z} \\ \mathbb{Z}/360\mathbb{Z} &\cong \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \ , \end{aligned}$$

les diviseurs élémentaires de $\mathbb{Z}/54\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}$ sont 2, 2^3, 3^2, 3^3, 5. Après les avoir ordonnés, nous obtenons

$$\begin{matrix} 2 & 3^2 & 5^0 \\ 2^3 & 3^3 & 5 \ . \end{matrix}$$

Alors, les facteurs invariants sont $2 \times 3^2 \times 5^0 = 18$ et $2^3 \times 3^3 \times 5 = 1080$. □

2. Classifier à isomorphisme prèsles groupes abéliens d'ordre 360.

Réponse : D'après le théorème de structure des groupes abéliens de type fini, il suffit de déterminer toutes les possibilités pour les diviseurs élémentaires de $\mathbb{Z}/360\mathbb{Z}$. Or,

$$360 \ = \ 2^3 \times 3^2 \times 5 \ ,$$

un groupe abélien d'ordre 8 est, à isomorphisme près, de la forme $\mathbb{Z}/8\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et un groupe d'ordre 9 est de la forme $\mathbb{Z}/9\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Par conséquent, tout groupe abélien d'ordre 360 est isomorphe à l'un des groupes suivants :

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z};$$

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z};$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z};$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z};$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z};$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \ .$$

□

Problème 2

1. Soit

$$f \ = \ X_1^2X_2^2 + X_1^2X_3^2 + X_1^2X_4^2 + X_2^2X_3^2 + X_2^2X_4^2 + X_3^2X_4^2 \in \mathbb{Z}[X_1, X_2, X_3, X_4] \ .$$

Exprimer le polynôme f *en fonction des polynômes symétriques élémentaires.*

Réponse : Notons que $f = S(X_1^2X_2^2)$. Alors, l'exercice 1.4 de la fiche 5 montre que

$$f \ = \ s_2^2 + b_{(2,1,1,0)}s_1s_3 + b_{(1,1,1,1)}s_4 \ .$$

Il est possible de faire les choix suivants de valeurs de $X_1, \ldots, X_4$ pour ensuite aboutir aux valeurs correspondantes des $s_1, \ldots, s_4$:

$$\begin{aligned} X_1 = X_2 = X_3 = 1, X_4 = 0 \quad &\Rightarrow \quad s_1 = 3, s_2 = 3, s_3 = 1, s_4 = 0 \\ X_1 = X_2 = -1, X_3 = X_4 = 1 \quad &\Rightarrow \quad s_1 = 0, s_2 = -2, s_3 = 0, s_4 = 1 \ . \end{aligned}$$

Il en découle que

$$b_{(2,1,1,0)} \ = \ -2 \quad , \quad b_{(1,1,1,1)} \ = \ 2 \ .$$

Ainsi,

$$f \;=\; s_2^2 - 2s_1s_3 + 2s_4 \;.$$

2. Soient α_1, α_2, α_3, α_4 les racines complexes du polynôme $X^4 - 2X^3 + 3X^2 - 4X + 5$. Sans chercher les valeurs des racines α_1, α_2, α_3, α_4, calculer

$$\frac{\alpha_1\alpha_2}{\alpha_3\alpha_4} + \frac{\alpha_1\alpha_3}{\alpha_2\alpha_4} + \frac{\alpha_1\alpha_4}{\alpha_2\alpha_3} + \frac{\alpha_2\alpha_3}{\alpha_1\alpha_4} + \frac{\alpha_2\alpha_4}{\alpha_1\alpha_3} + \frac{\alpha_3\alpha_4}{\alpha_1\alpha_2} \;.$$

Réponse : Appelons Q l'expression dont la valeur est recherchée. Après calcul du dénominateur commun, nous aboutissons à l'égalité

$$Q \;=\; \frac{S(\alpha_1^2\alpha_2^2)}{s_4(\alpha_1,\alpha_2,\alpha_3,\alpha_4)} \;.$$

Ainsi,

$$Q \;=\; \frac{s_2^2 - 2s_1s_3 + 2s_4}{s_4}(\alpha_1,\alpha_2,\alpha_3,\alpha_4) \;.$$

Or $s_1 = 2$, $s_2 = 3$, $s_3 = 4$, $s_4 = 5$, et nous trouvons après calcul

$$Q \;=\; \frac{3}{5} \;.$$

□

Problème 3

Réponse : (Le problème coïncide presque avec l'exercice 6, partie 2b de la fiche 4 de TD.)

D'apres un théorème du cours $Iso^+(C)$ est isomorphe à S_4, donc, $|Iso^+(C)| = 24$. (On peut aussi utiliser l'exercice 5.2 de la fiche 4.)

Notons aussi que $Iso^+(C) \cong Iso^+(O)$ (vu en cours). Donc, les réponses de 2 coïncident avec les réponces de 1.

Il nous reste à répondre aux questions 1b et 1c. Les axes de symétrie de C se répartissent en trois classes : (i) 6 axes réliants les milieux des arêtes opposées, (ii) 4 axes réliants les sommets opposés et (iii) 3 axes réliants les milieux des faces opposées. On sait que le stabilisateur dans $Iso^+(C)$ d'un axe l est un sous-groupe cyclique dont tous les éléments non-triviaux ont l comme axe de rotation. On voit facilement (faire un dessin !) que les stabilisateurs des axes de (i) (resp. (ii), resp.(iii)) sont des groupes cyclique d'ordre 2 (resp. 3, resp.4). Dans chaque groupe d'ordre 3 on a deux éléments d'ordre 3 et dans chaque groupe cyclique d'ordre 4 on a un élément d'ordre 2 et deux éléments d'ordre 4. Donc, on obtient $6 + 3 = 9$ éléments d'ordre deux, $4 \times 2 = 8$ éléments d'ordre trois et $3 \times 2 = 6$ éléments d'ordre quatre. Au total, on obtient 23 éléments *distincts* différents de 1. Puisque $|Iso^+(C)| = 24$, la réponse à 1b est $9, 8$ et 6, respectivement.

Pour trouver la réponse de 1c, notons que les axes de chaque classe sont deux à deux conjugués dans $Iso^+(C)$ et deux axes de deux classes différentes ne le sont pas. On sait que si deux axes sont conjugués alors leurs stabilisateurs sont conjugués aussi. En particulier, les éléments d'ordre deux sont réparti en deux classes de conjugaisons : une de 6 éléments (correspondant à (i)) et une autre de 3 éléments (correspondant à (iii)). La classe (ii) donne quatre 3-groupes conjugués (ici on découvre pour S_4 et $p = 3$ le théorème de Sylow) et dans chaque 3-groupe les deux éléments d'ordre 3 sont conjugués. (Pour voir le dernier, notez que les deux éléments d'ordre 3 dans A_3 sont conjugués par un élément de S_3 et que S_3 est plongé dans S_4.) Donc, les éléments d'ordre trois sont conjugués. Finalement, puisque on a trois groupes cyclique conjuqués d'ordre quatre et dans chacun les éléments d'ordre 4 sont conjugués (notons que $(1234)^{-1} = (4321) = ((14)(23))(1234)((14)(23))^{-1}$) tous les éléments d'ordre quatre sont conjugués. Donc les nombres des classes de conjugaison qu'on cherche sont 2, 1 et 1, respectivement. □

Problème 4 *Soit G un groupe d'ordre* 2009 $(= 7^2.41)$.

1. Montrer que $G \cong P \times Q$, où P est un groupe d'ordre 41*, et Q est un groupe d'ordre* 49*. En déduire que chaque groupe d'ordre* 2009 *est abélien.*

Réponse : D'après le théorème de Sylow G a un 41-Sylow d'ordre 41 et un 7-Sylow d'ordre 49. Appelons ces sous-groupes P et Q respectivement.

Le nombre de 41-Sylow de G est congru à 1 modulo 41 et divise 49 selon le théorème de Sylow. Il en découle que ce nombre est 1 et que donc P est distingué dans G. Un raisonnement similaire de comptage s'applique à Q, et permet de conclure.

Nous constatons aussi que $P \cap Q = \{1\}$, que $G = PQ$ et que les deux sous-groupes dans le produit sont distingués. Tout ceci revient à dire que $G \cong P \times Q$.

Il reste alors à montrer que G est abélien. Notons que P et Q sont abéliens puisque P est d'ordre premier et que Q est d'ordre premier au carré. Par ailleurs, les éléments de P commutent avec ceux de Q. Ainsi, G est commutatif. □

2. Classifier à isomorphisme près tous les groupes d'ordre 2009*.*
Réponse : Puisque, d'après le point 1, tous les groupes d'ordre2009 sont abéliens, il suffit pour répondre à cette question d'appliquer le théorème de structure pour les groupes abéliens de type fini. Ce théorème montre qu'il y a deux groupes non isomorphes d'ordre 2009 :

$$\mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z} \ ,$$

soit encore,

$$\mathbb{Z}/2009\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/287\mathbb{Z} \ .$$

□

3. Soient P et Q comme dans la partie 1. Montrer que $\mathrm{Aut}(G) \cong \mathrm{Aut}(P) \times \mathrm{Aut}(Q)$*.*
Réponse : Commençons par une remarque qui guidera le reste des raisonnements. Si σ est un automorphisme de G, alors $\sigma(P) = P$ et $\sigma(Q) = Q$. En effet, comme dans tout groupe et pour tout p premier, l'image homomorphique d'un p-élément est un p-élément et que P et Q sont les seuls 41- et 7-Sylow de G respectivement, $\sigma(P) \subset P$ et $\sigma(Q) \subset Q$. Comme σ est une bijection, ces deux inclusions sont en fait des égalités.

Il découle du paragraphe précédent que la restriction de tout automorphisme $\sigma \in \mathrm{Aut}(G)$ au sous-groupe P (resp. Q) est un automorphisme qu'on appellera σ_P (resp. σ_Q) de P (resp. Q). Les automorphismes de σ_P et σ_Q ainsi définis sont uniquement définis puisqu'ils sont les restrictions d'un même automorphisme aux sous-groupes P et Q respectivement.

Les conclusions du dernier paragraphe permettent d'établir l'application suivante :

$$\begin{array}{rccc} \Sigma & : & \mathrm{Aut}(G) & \longrightarrow & \mathrm{Aut}(P) \times \mathrm{Aut}(Q) \\ & & \sigma & \longmapsto & (\sigma_P, \sigma_Q) \end{array}$$

Si $\sigma,\ \tau \in \mathrm{Aut}(G)$ alors

$$\begin{aligned} (\sigma \circ \tau)_P(P) &= (\sigma \circ \tau)(P) \\ &= \sigma(\tau(P)) \\ &= \sigma_P(\tau_P(P)) \\ &= (\sigma_P \circ \tau_P)(P) \ , \end{aligned}$$

et les mêmes égalités prévalent après avoir remplacé P par Q. Par conséquent, Σ est un homomorphisme.

Nous montrerons maintenant que Σ est un isomorphisme, ce qui achévera la réponse au point 3. Commençons par la propriété injective. Un automorphisme σ de $\mathrm{Aut}(G)$ appartient à $\ker(\Sigma)$ si et seulement si σ_P et σ_Q sont les applications identiques. Or, tout élément de G s'écrit sous forme $xy \in$ avec $x \in P$ et $y \in Q$. Ainsi,

$$\sigma(xy) = \sigma(x)\sigma(y) = \sigma_P(x)\sigma_Q(y) = xy \ .$$

Maintenant, montrons la surjectivité de Σ. Soient $\sigma_1 \in \mathrm{Aut}(P)$ et $\sigma_2 \in \mathrm{Aut}(Q)$. Nous définissons l'application suivante :

$$\begin{array}{rccc} \sigma & : & G & \longrightarrow & G \\ & & xy & \longmapsto & \sigma_1(x)\sigma_2(y) \end{array}$$

avec $x \in P$ et $y \in Q$. L'application σ est définie sans ambiguïté puisque, G étant la somme directe de P et de Q, chacun de ses éléments s'écrit de manière unique comme produit d'un élément de P et d'un autre de Q. Notre objectif dans le reste de la preuve sera de montrer que σ est un automorphisme de G dont l'image sous l'action de Σ est (σ_1, σ_2).

La propriété homomorphique de σ découle de celles de σ_1 et de σ_2. Il en est de même pour la surjectivité de σ. Maintenant, supposons $\sigma(xy) = 1$ pour $x \in P$ et $y \in Q$. D'après la définition de σ, $\sigma_1(x)\sigma_2(y) = 1$. Or $\sigma_1(x) \in P$, $\sigma_2(y) \in Q$ et $P \cap Q = \{1\}$. Par conséquent, $\sigma_1(x) = \sigma_2(y) = 1$. Comme σ_1 et σ_2 sont des automorphismes de P et de Q respectivement, $x = y = 1$. Comme $G = PQ$, tout élément de $\ker(\sigma)$ s'écrit comme produit d'un $x \in P$ et d'un $y \in Q$. Ainsi notre raisonnement montre que $\ker(\sigma) = \{1\}$.

Les deux derniers paragraphes montrent que σ est un automorphisme de G. Il s'ensuit de la définition de σ que $\sigma_P = \sigma_1$ et $\sigma_Q = \sigma_2$. Par conséquent, $\Sigma(\sigma) = (\sigma_1, \sigma_2)$. Nous avons donc montré que Σ est une surjection. La preuve est terminée. □

4. Montrer que :

(*a*) *Si Q est cyclique, alors* $\mathrm{Aut}(Q)$ *est cyclique aussi. Quel est l'ordre de* $\mathrm{Aut}(Q)$ *quand Q est cyclique ?*

(*b*) *Si Q n'est pas cyclique, alors* $\mathrm{Aut}(Q)$ *est isomorphe à* $\mathrm{GL}(2, \mathbb{F}_7)$ *où* $\mathbb{F}_7$ *est le corps de* 7 *éléments. Quel est l'ordre* $\mathrm{GL}(2, \mathbb{F}_7)$ *?*

Réponse : (a) Si Q est cyclique, il est isomorphe à $(\mathbb{Z}/49\mathbb{Z}, +)$. D'après les exercices 8 et 9 de la première fiche, le groupe d'automorphismes de Q est alors de cardinal $\phi(49) = 7 \times 6 = 42$ où ϕ est la fonction indicatrice d'Euler. Comme $42 = 2 \times 3 \times 7$, le théorème chinois montre que le groupe d'automorphismes de Q est cyclique d'ordre 42.

(b) Supposons maintenant Q non cyclique. Alors, $Q \cong (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, +)$. Ce dernier groupe peut être aussi considéré comme l'espace vectoriel de dimension 2 sur le corps $\mathbb{F}_7$ avec la base canonique $e_1 = (1, 0)$ et $e_2 = (0, 1)$. La loi externe induite par $\mathbb{F}_7$ est décrite par les identités

$$\lambda e_1 = \underbrace{(1,0) + \ldots + (1,0)}_{\lambda \text{ fois}} \quad \text{et} \quad \lambda e_2 = \underbrace{(0,1) + \ldots + (0,1)}_{\lambda \text{ fois}} ,$$

avec $\lambda \in \mathbb{F}_7$ qui sont ensuite étendues au groupe tout entier par linéarité. Cette action est définie sans ambiguïté.

Si $\sigma \in \mathrm{Aut}(Q)$, alors

$$\begin{aligned} \sigma(\lambda e_1) &= \sigma(\underbrace{(1,0) + \ldots + (1,0)}_{\lambda \text{ fois}}) \\ &= \underbrace{\sigma(1,0) + \ldots + \sigma(1,0)}_{\lambda \text{ fois}} \\ &= \lambda\sigma((1,0)) \\ &= \lambda\sigma(e_1) . \end{aligned}$$

Le même raisonnement s'applique à λe_2. Nous avons donc montré que σ est une application linéaire. Etant bijectif, $\sigma \in \mathrm{GL}(2, \mathbb{F}_7)$. Ainsi, $\mathrm{Aut}(Q) \leq \mathrm{GL}(2, \mathbb{F}_7)$. L'autre inclusion est claire puisque chaque bijection linéaire de $\mathbb{F}_7 \times \mathbb{F}_7$ est aussi un automorphisme du groupe $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

Finalement, l'ordre de $\mathrm{GL}(2, \mathbb{F}_7)$ est

$$(7^2 - 1)(7^2 - 7) .$$

Problème 5

1. Soient A un anneau commutatif non nul et A^* l'ensemble de ses éléments inversibles. Montrer que les conditions suivantes équivalentes :

(*i*) *A a un seul idéal maximal ;*

(*ii*) *il existe un idéal $M \neq A$ qui contient l'ensemble $A \setminus A^*$;*

(*iii*) *$A \setminus A^*$ est un idéal ;*

(*iv*) *pour tous a et b dans A, si $a+b=1$ alors soit a soit b est inversible.*

Réponse : ((i)⇒(ii)) Soit M le seul idéal maximal de A. Si $x \in A \setminus A^*$ alors l'idéal engendré par x, notamment (x), est un idéal propre et contenu dans un idéal maximal de A d'après des résultats généraux sur les anneaux. Or M est le seul idéal maximal de A. Ainsi, $A \setminus A^* \subset M$.

((ii)⇒(iii)) Un idéal propre, en l'occurrence M, ne peut pas contenir d'inversible. Par conséquent, $M \subset A \setminus A^*$. L'hypothèse (ii) implique alors que $M = A \setminus A^*$. En particulier, $A \setminus A^*$ est un idéal.

((iii)⇒(iv)) Soient a et b comme dans l'énoncé de la condition (iv). Si aucun de ces deux éléments n'est inversible, alors, d'après l'hypothèse (iii) leur somme est dans l'idéal $A \setminus A^*$. Or 1 est inversible.

((iv)⇒(i)) Si M_1 et M_2 sont deux idéaux maximaux distincts de A, alors $A = M_1 + M_2$. En particulier, il existe $a \in M_1$ et $b \in M_2$ tels que $a+b=1$. Or ni a ni b n'est inversible. □

2. Soit p un entier premier. On pose

$$A = \left\{ \frac{a}{b} \ : \ a,\ b \in \mathbb{Z} \text{ tels que } p \not| b \right\} .$$

Montrer que A est local et déterminer son idéal maximal.

Réponse : Il découle de la définition de A que

$$A^* = \left\{ \frac{a}{b} \in A \ : \ p \not| a \right\} .$$

Si $\frac{a_1}{b_1}$ et $\frac{a_2}{b_2} \in A$ sont tels que

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = 1$$

alors

$$b_2 a_1 + b_1 a_2 = b_1 b_2 .$$

Si p divise a_1 et a_2, alors $p | b_1 b_2$. Comme p est premier, $p | b_1$ ou $p | b_2$. Cette conclusion contredit la définition de A. La condition (iv) du premier point du problème montre alors que A est local.

La réponse à la deuxième question de ce point a déjà été donnée. □

3. Soit p un entier premier et $n \in \mathbb{N}$, $n \neq 0$. Montrer que l'anneau quotient $\mathbb{Z}/p^n\mathbb{Z}$ est local. Quel est son idéal maximal ?

Réponse : Tout idéal maximal de $(\mathbb{Z}, +, .)$ est de la forme (q) avec q premier. Si $q \wedge p = 1$, alors l'image de q dans le quotient $\mathbb{Z}/p^n\mathbb{Z}$ est un générateur du groupe abélien $(\mathbb{Z}/p^n\mathbb{Z}, +)$ et donc de l'anneau quotient $(\mathbb{Z}/p^n\mathbb{Z}, +, .)$. Si $q = p$, alors l'image de (p) après passage au quotient $(\mathbb{Z}/p^n\mathbb{Z}, +, .)$ est un idéal propre et par conséquent toujours maximal. Comme tout idéal maximal du quotient $(\mathbb{Z}/p^n\mathbb{Z}, +, .)$ est l'image d'un idéal maximal de $(\mathbb{Z}, +, .)$, (p) est le seul idéal maximal de $(\mathbb{Z}/p^n\mathbb{Z}, +, .)$. Ainsi, l'anneau quotient est local avec le seul idéal maximal (p). □