Contrôle continu 3

Exercice 1

Soit K un corps fini de cardinal 8. On fixe $a \in K \setminus \{0_K, 1_K\}$. On note $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

1. Montrer que la caractéristique de K est 2.
2. Justifier l'existence d'un morphisme d'anneaux $f : \mathbb{F}_2[X] \to K$ tel que $f(X) = a$.
3. Montrer qu'il existe un polynôme non nul M tel que $\mathrm{Ker} f = M\mathbb{F}_2[X]$.
4. Montrer que $\mathrm{Im} f$ est un corps et que M est irréductible.
5. Montrer que $\mathrm{Im} f = K$. Indication : on admettra que si $K_1 \subset K_2$ sont deux corps finis, alors il existe $d \in \mathbb{N}^*$ tel que $|K_2| = |K_1|^d$.
6. En déduire que $\deg M = 3$, puis que M est égal soit à $M_1 = X^3 + X + \dot{1}$ soit à $M_2 = X^3 + X^2 + \dot{1}$.
7. À l'aide du morphisme d'anneaux $P \mapsto \overline{P(X + \dot{1})}$ de $\mathbf{F}_2[X]$ dans $\mathbf{F}_2[X]/(M_2)$, montrer qu'il existe un unique corps de cardinal 8 à isomorphisme près.

Exercice 2

Soit p un nombre premier p. On note K le corps $\mathbb{Z}/p\mathbb{Z}$ et A l'anneau $\mathbb{Z}/p^2\mathbb{Z}$. On cherche à construire des groupes d'ordre p^3 non abéliens à l'aide de produits semi-directs $K^2 \rtimes K$ et $A \rtimes K$ (dans lesquels on voit K^2, A et K comme des groupes additifs).

1. (a) Montrer que pour tout $z \in K$, l'application $\varphi_z : (x, y) \mapsto (x, y + zx)$ est dans $GL(K^2)$ et que l'application $\varphi : z \mapsto \varphi_z$ de K dans $GL(K^2)$ est un morphisme de groupes.
   (b) En déduire comment réaliser un produit semi-direct $K^2 \rtimes K$ non abélien.
   (c) On identifie tout élément $(x, y, z) \in K^3$ à $((x, y), z) \in K^2 \times K$. Montrer qu'on obtient un morphisme injectif de groupes de $K^2 \rtimes K$ dans $GL_3(K)$ en posant
   $$f((x, y, z)) = \begin{pmatrix} 1 & z & y \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}.$$
2. (a) Quel est l'ordre du groupe multiplicatif $A^\times$? En déduire que le groupe $A^\times$ possède au moins un élément a d'ordre p.
   (b) Montrer que l'application $f_a : k \mapsto a^k$ de $\mathbb{Z}$ dans $A^\times$ fournit un morphisme du groupe $(K, +)$ dans le groupe $(A^\times, \times)$, puis un morphisme ψ du groupe $(K, +)$ dans le groupe $(\mathrm{Aut}(A), \circ)$ des automorphismes du groupe $(A, +)$.
   (c) En déduire un comment réaliser un produit semi-direct $A \rtimes K$ non abélien.

Exercice 3

Soit G un groupe et p un nombre premier. On rappelle les faits suivants vus en cours ou en TD, qu'on pourra utiliser sans démonstration dans l'exercice.

1. Tout groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à$(\mathbb{Z}/p\mathbb{Z})^2$.
2. Le centre $Z(G)$ de G est un sous-groupe distingué de G.
3. Si G est p-groupe, $Z(G)$ n'est pas réduit à $\{1_G\}$.
4. Si le groupe $G/Z(G)$ est cyclique, alors G est abélien.
5. Si G est fini et si p est le plus petit nombre premier divisant $|G|$, alors tout sous-groupe d'indice p dans G est distingué.

On suppose désormais que p est impair, que G est d'ordre p^3 et non abélien. On se propose de montrer que G est le produit semi-direct d'un groupe d'ordre p^2 par un groupe d'ordre p. On note π la projection canonique de G sur $G/Z(G)$ et f l'application $x \mapsto x^p$ de G dans G.

1. Soient Γ un groupe, Λ un sous-groupe de Γ différent de Γ et $b \in \Gamma \setminus \Lambda$. Montrer que si l'ordre de b est égal à p, alors $\Lambda \cap \langle b \rangle = \{1_\Gamma\}$.
2. En déduire que si H est un sous-groupe de G d'ordre p^2 et si $k \in G \setminus H$ est un élement d'ordre p, alors $G = H \rtimes \langle k \rangle$.
3. Montrer que $|Z(G)| = p$ et que le groupe $G/Z(G)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.
4. En déduire que pour tous a et b dans G, les éléments a^p et $[a,b] := aba^{-1}b^{-1}$ sont dans $Z(G)$, et $[a,b]^p = 1_G$.
5. En déduire que pour tous a, b dans G et $n \in \mathbb{N}^*$, on a $[a,b^n] = [a,b]^n$ et $(ba)^n = b^n a^n [a,b]^{n(n-1)/2}$. Indication : on pourra calculer de deux façons différentes $aba^{-1}[a,b^n]b^{-1}$ et raisonner par récurrence.
6. En déduire que f est un morphisme de groupes.
7. Montrer que $\mathrm{Im}f \subset \mathrm{Ker}f$ et déduire que $|\mathrm{Ker}f| = p^2$ ou $|\mathrm{Ker}f| = p^3$.
8. On suppose ici que $|\mathrm{Ker}f| = p^3$. Soient $b \in G \setminus Z(G)$ et $B = \langle b \rangle$.
   (a) Soit $H = Z(G)B = \{xy : (x,y) \in Z(G) \times B\}$. Montrer que H est un sous-groupe de G d'ordre p^2. On pourra utiliser la question 1 pour reconnaître un produit semi-direct interne, ou bien trouver $|H|$ en regardant le noyau et l'image de $\pi_{|H}$.
   (b) Soit $k \in G \setminus H$. Pourquoi a-t-on $G = H \rtimes \langle k \rangle$?
9. On suppose ici que $|\mathrm{Ker}f| = p^2$.
   (a) Calculer $|\mathrm{Im}f|$ et en déduire que $\mathrm{Im}f = Z(G)$.
   (b) Soient $h \in G \setminus \mathrm{Ker}f$ et $k \in \mathrm{Ker}f \setminus \mathrm{Im}f$. Pourquoi a-t-on $G = \langle h \rangle \rtimes \langle k \rangle$?

Un corrigé

Exercice 1

1. Soit Θ_K l'unique morphisme d'anneaux de $\mathbb{Z}$ dans K. Alors $\Theta_K(\mathbb{Z})$ est un sous-anneau de K, donc intègre et fini, isomorphe à $\mathbb{Z}/\mathrm{car}(K)\mathbb{Z}$. Donc $\mathrm{car}(K)$ est un nombre premier. Mais $\mathrm{car}(K)$ est l'ordre de 1_K dans le groupe $(K,+)$ de cardinal 8, donc $\mathrm{car}(K)$ divise 8. Variante : $\Theta_K(\mathbb{Z})$ est un sous-corps du corps fini K donc $|K|$ est une puissance de $|\Theta_K(\mathbb{Z})| = |\mathrm{car}(K)|$. Ainsi, $\mathrm{car}(K) = 2$.

2. Par passage au quotient, Θ_K fournit un morphisme d'anneaux de $\mathbb{F}_2$ dans K. La propriété universelle permet de l'étendre en un morphisme d'anneaux f de $\mathbb{F}_2[X]$ dans K tel que $f(X) = a$.

3. Le noyau de f est un idéal de $\mathbb{F}_2[X]$, principal car l'anneau $\mathbb{F}_2[X]$ est principal. Comme $\mathbb{F}_2[X]$ est infini et K est fini, f n'est pas injectif, donc $\mathrm{Ker}f$ n'est pas réduit à $\{0_K\}$. Ainsi, il existe un polynôme non nul M tel que $\mathrm{Ker}f = M\mathbb{F}_2[X]$.

4. Comme $\mathrm{Im}f$ est un sous-anneau de K, il est fini et intègre, donc c'est un corps. En effet, pour tout $x \in K \setminus \{0_K\}$, l'application $y \mapsto xy$ de K dans K est un endomorphisme du groupe fini $(K,+)$, injectif car le noyau est réduit à $\{0_K\}$, donc bijectif ; en particulier, il existe $y \in K$ tel que $xy = 1_K$.

   Donc $\mathbb{F}_2[X]/(M)$ est aussi un corps et l'idéal (M) est maximal. Si un polynôme P divise M, l'idéal (P) contient (M) donc est égal à (M) ou à $\mathbb{F}_2[X]$, donc P est inversible ou associé à M. Ainsi, M est irréductible.

   Autre méthode : $\mathrm{Im}f$ est intègre comme sous-anneau de K, donc $\mathbb{F}_2[X]/(M)$ est intègre, donc l'idéal (M) est premier. On en déduit que le polynôme M est irréductible dans $\mathbb{F}_2[X]$. Comme l'anneau $\mathbb{F}_2[X]$ est principal, cela entraîne que l'idéal (M) est maximal, donc $\mathbb{F}_2[X]/(M)$ et $\mathrm{Im}f$ sont des corps.

5. Comme $\mathrm{Im}f$ est un sous-coprs de K, il existe d dans $\mathbb{N}^*$ tel que $8 = |K| = |\mathrm{Im}f|^d$. Mais $\mathrm{Im}f$ contient au moins trois éléments distincts, 0_K, 1_K et a. La seule possibilité est $|\mathrm{Im}f| = 8$ donc $\mathrm{Im}f = K$.

6. Par passage au quotient, le morphisme surjectif f (d'anneaux et de $\mathbb{F}_2$-espaces vectoriels) fournit un isomorphisme $\overline{f}$ de $\mathbb{F}_2[X]/M\mathbb{F}_2[X]$ vers K.

   Notons $m = \deg M$. On vérifie que $S := \mathrm{Vect}(\{\dot{1}, X, \ldots, X^{m-1}\})$ est un système de représentants du quotient $\mathbb{F}_2[X]/M\mathbb{F}_2[X]$ (en utilisant la division euclidienne par M). Donc $2^m = |S| = |K| = 8$ et $m = 3$.

   Parmi les huit polynômes de degré 3 dans $\mathbb{F}_2[X]$, les polynômes irréductibles sont ceux qui n'admettent ni 0_K ni 1_K comme racine, à savoir M_1 et M_2.

7. Comme M_1 et M_2 sont des polynômes irréductibles de degré 3 dans l'anneau principal $\mathbb{F}_2[X]$, les quotients $\mathbb{F}_2[X]/(M_1)$ et $\mathbb{F}_2[X]/(M_2)$ sont bien des corps à 8 éléments. De plus tout corps à 8 éléments est isomorphe à un de ces deux corps. Il reste à voir que ces deux corps sont isomorphes.

L'application $P \mapsto P(X+\dot{1})$ de $\mathbb{F}_2[X]$ dans $\mathbb{F}_2[X]$ est un isomorphisme d'anneaux (égal à son inverse car $\mathrm{car}(K)=2$), donc l'application $g : P \mapsto \overline{P(X+\dot{1})}$ de $\mathbb{F}_2[X]$ dans $\mathbb{F}_2[X]/(M_2)$ est un morphisme surjectif d'anneaux. Il suffit de vérifier que $\mathrm{Ker} g = (M_1)$ pour obtenir l'isomorphisme souhaité par passage au quotient. L'égalité $M_1 = M_2(X - 1_K)$ fournit justement l'équivalence

$$\forall P \in \mathbb{F}_2[X], \quad g(M_2) = \overline{0} \iff M_2 | P(X+\dot{1}) \iff M_1 | P.$$

Exercice 2

1. (a) Soit $z \in K$. L'application φ_z est l'application linéaire de matrice

$$M_z = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}$$

dans la base canonique de K^2. Comme $\det M_z = 1$, on a $\varphi_z \in GL(K^2)$. Or pour tout $(z, z') \in K^2$, $M_z M_{z'} = M_{z+z'}$ donc $\varphi_z \varphi_{z'} = \varphi_{z+z'}$. L'application $\varphi : z \mapsto \varphi_z$ de K dans $GL(K^2)$ est donc un morphisme de groupes.

(b) Tout élément de $GL(K^2)$ est un automorphisme du groupe additif K^2. Le morphisme non trivial φ fournit donc un produit semi-direct $K^2 \rtimes K$ non direct, donc non abélien. Sa loi $*$ est donnée par

$$\begin{aligned} ((x,y),z) * ((x',y'),z') &= ((x,y) + \varphi_z(x',y'), z+z') \\ &= ((x,y) + (x', y' + zx'), z+z') \\ &= ((x+x', y+y'+zx'), z+z'). \end{aligned}$$

Donc f est un morphisme de $K^2 \rtimes K$ dans $\mathrm{Aut}(K)$, injectif puisque pour tout $((x,y),z) \in K^2 \times K$, x, y, z sont des coefficients de $f(x,y,z)$.

(c) Soient (x,y,z) et (x',y',z') dans K^3. Alors

$$\begin{aligned} f((x,y,z))f((x',y',z')) &= \begin{pmatrix} 1 & z & y \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & z' & y' \\ 0 & 1 & x' \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & z'+z & y'+zx'+y \\ 0 & 1 & x'+x \\ 0 & 0 & 1 \end{pmatrix} \\ &= f((x,y,z) * (x',y',z')). \end{aligned}$$

2. (a) Comme $|A^\times| = \phi(p) = p(p-1)$. Comme p est premier et divise $|A^\times|$, le théorème de Cauchy assure que le groupe $A^\times$ possède au moins un élément d'ordre p. Variante : le théorème de Sylow fournit l'existence d'un sous-groupe S d'ordre p. Tout élément de $S \setminus \{1_A\}$ est d'ordre p. Remarque : on peut aussi vérifier que la classe de $1+p$ dans $A = \mathbb{Z}/p\mathbb{Z}$ est un élément d'ordre p dans le groupe multiplicatif $A^\times$.

(b) L'application $f_a : k \mapsto a^k$ de $\mathbb{Z}$ dans $A^\times$ est un morphisme de groupes, de noyau $p\mathbb{Z}$ puisque a est d'ordre p. Par passage au quotient, on obtient un morphisme de groupes injectif $\overline{f_a}$ de K dans $A^\times$. Pour tout $z = \overline{k} \in K$, l'application $\psi_z : h \to \overline{f_a}(z)h = a^k h$ de A dans A est un automorphisme du groupe $(A, +)$. De plus, pour tout $(z, z') \in K^2$, $\psi_{z+z'} = \psi_z \circ \psi_{z'}$.

(c) Comme $\psi : z \mapsto \psi_z$ est un morphisme de groupes non trivial de K dans $\mathrm{Aut}(A)$, on obtient donc un produit semi-direct $A \rtimes K$ non direct, donc non abélien en posant pour tout (h, k) et (h', k') dans $A \times \mathbb{Z}$,

$$(h, \overline{k}) * (h, \overline{k'}) = (h + \psi_{\overline{k}}(h'), \overline{k} + \overline{k'}) = (h + a^k h', \overline{k + k'}).$$

Exercice 3

1. Si le sous-groupe $\Lambda \cap \langle b \rangle$ n'était pas réduit à $\{1_\Gamma\}$, il contiendrait alors un élément de la forme b^k avec k entier non multiple de p. Comme p est premier, k serait premier avec p, donc il existerait deux entiers u et v tels que $ku + pv = 1$, d'où $b = b^{ku}b^{pv} = (b^k)^u \in \Lambda$, ce qui contredirait l'hypothèse. Donc $\Lambda \cap \langle b \rangle = \{1_\Gamma\}$. Autre méthode : comme $\Lambda \cap \langle b \rangle$ est un sous-groupe de $\langle b \rangle$, son ordre divise p, mais ce n'est pas p puisque $b \notin \Lambda$, donc $|\Lambda \cap \langle b \rangle| = 1$ et $\Lambda \cap \langle b \rangle = \{1_\Gamma\}$.
2. Soient H un sous-groupe H de G, d'ordre p^2, et $k \in G \setminus H$ d'ordre p. Alors :
   (a) $[G : H] = p$ est plus petit diviseur premier de $|G|$, donc $H \lhd G$.
   (b) $H \cap \langle k \rangle = \{1_\Gamma\}$ d'après la question 1.
   (c) $|H| \times |\langle k \rangle| = p^2 \times p = |G|$.

   Ainsi, $G = H \rtimes \langle k \rangle$.
3. D'après le théorème de Lagrange et les rappels, $|Z(G)|$ divise $|G| = p^3$ et $|Z(G)| > 1$. De plus, G est supposé non-abélien, donc le groupe $G/Z(G)$ n'est pas cyclique, donc $|G/Z(G)| \notin \{1, p\}$, autrement dit $|Z(G)| \notin \{p^3, p^2\}$. Ainsi, $|Z(G)| = p$ et le groupe $G/Z(G)$ est d'ordre p^2 et non cyclique, donc $G/Z(G)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.
4. Soient a et b dans G. D'après la question précédente, $G/Z(G)$ est abélien et tout élément de $G/Z(G)$ est d'ordre 1 ou p. Dans $G/Z(G)$, on a donc $\overline{a^p} = \overline{a}^p = \overline{1_G}$ et $\overline{[a, b]} = [\overline{a}, \overline{b}] = \overline{1_G}$. Donc a^p et $[a, b] := aba^{-1}b^{-1}$ sont dans $Z(G)$. Comme $Z(G)$ est d'ordre p, on a donc $[a, b]^p = 1_G$.
5. Fixons a, b dans G. Pour tout $n \in \mathbb{N}$, notons P_n et Q_n les égalités $[a, b^n] = [a, b]^n$ et $(ba)^n = b^n a^n [a, b]^{n(n-1)/2}$.

   Comme $g^0 = 1_G$ et $[g, 1_G] = 1_G$ pour tout $g \in G$, P_0 et Q_0 sont vraies.

   Soit $n \in \mathbb{N}$ tel que P_n et Q_n soit vérifiées. Alors d'une part

$$[a, b^{n+1}] = ab^{n+1}a^{-1}b^{-n-1} = aba^{-1}ab^n a^{-1}b^{-n}b^{-1} = aba^{-1}[a, b^n]b^{-1}.$$

D'autre part, comme $[a, b^n]$ est dans $Z(G)$ et d'après P_n

$$aba^{-1}[a, b^n]b^{-1} = aba^{-1}b^{-1}[a, b^n] = [a, b][a, b]^n = [a, b]^{n+1}.$$

Donc P_{n+1} est vérifiée. D'après Q_n, le fait que comme $[a, b^n] \in Z(G)$ et P_n,

$$\begin{aligned}(ba)^{n+1} = (ba)(ba)^n &= bab^n a^n [a, b]^{n(n-1)/2} \\ &= b([a, b^n]b^n a)a^n [a, b]^{n(n-1)/2} \\ &= b^{n+1}a^{n+1}[a, b]^{n(n-1)/2}[a, b]^n \\ &= b^{n+1}a^{n+1}[a, b]^{n(n+1)/2},\end{aligned}$$

donc Q_{n+1} est vérifiée, ce qui achève la récurrence.

6. Soient a, b dans G. Comme p est impair, $(ba)^p = b^p a^p ([a, b]^p)^{(p-1)/2} = b^p a^p$ car $[a, b]^p = 1_G$. Donc f est un morphisme de groupes.
7. La question 4 montre que $\mathrm{Im}f \subset Z(G) \subset \mathrm{Ker}f$, donc $|\mathrm{Im}f|$ divise $|\mathrm{Ker}f|$. Preuve directe : soit $y \in \mathrm{Im}f$. Alors $y = x^p$ avec $x \in G$, d'où $y^p = x^{p^2} = 1_G$ car l'ordre de x divise p^2. En effet, l'ordre de x divise $|G| = p^3$, et cette divisibilité est stricte, sans quoi G serait cyclique alors qu'il est supposé non abélien.
   Mais $|\mathrm{Im}f| \times |\mathrm{Ker}f| = |G| = p^3$, donc $(|\mathrm{Ker}f|, |\mathrm{Im}f|) = (p^2, p)$ ou $(p^3, 1)$.
8. On suppose ici que $|\mathrm{Ker}f| = p^3$. Soient $b \in G \setminus Z(G)$ et $B = \langle b \rangle$.
   (a) Comme $b^p = f(p) = 1_G$ et $b \neq 1_G$, l'élément b est d'ordre p. La question 1 montre que $Z(G) \cap B$ est réduit à $\{1_G\}$. Mais $Z(G) \triangleleft G$, donc $H = Z(G)B$ est le produit semi-direct interne de $Z(G)$ par B, qui sont d'ordre p (en fait, ce produit est direct car tout élément de $Z(G)$ commute avec tout élément de B). Donc $|H|$ est un sous-groupe de G, d'ordre p^2.
   Autre argument : $H = \pi^{-1}(\pi(B))$ car pour tout $g \in G$,

$$\begin{aligned}g \in H &\iff \exists y \in B, \exists x \in Z(G), g = yx \\ &\iff \exists y \in B : \pi(g) = \pi(y) \\ &\iff \pi(g) \in \pi(B).\end{aligned}$$

   Comme $\pi(B)$ est un sous-groupe de $G/Z(G)$, H est un sous-groupe de G. Mais $\mathrm{Ker}\pi|_B = Z(G) \cap B = \{1_G\}$ et $\mathrm{Ker}\pi|_H = Z(G) \cap H = Z(G)$, donc $|H|/|Z(G)| = |\pi(H)| = |\pi(B)| = |B|/|\{1_G\}| = p$ d'où $|H| = p^2$.
   (b) Soit $k \in G \setminus H$. Alors k est d'ordre p. Comme $|H| = p^2$, le résultat de la question 2 montre que $G = H \rtimes \langle k \rangle$.
9. On suppose ici que $|\mathrm{Ker}f| = p^2$.
   (a) Comme $\mathrm{Im}f \subset Z(G)$ (question 4) et $|\mathrm{Im}f| = p = |Z(G)|$, on a $\mathrm{Im}f = Z(G)$.
   (b) Soient $h \in G \setminus \mathrm{Ker}f$ et $k \in \mathrm{Ker}f \setminus \mathrm{Im}f$. Alors h est d'ordre p^2, et k est d'ordre p. Les éléments de $\langle h \rangle$ sont les éléments de la forme h^r pour $r \in \mathbb{Z}$. Mais $h^r \in \mathrm{Im}f$ si p divise r et h^r est d'ordre p^2 sinon. Donc $k \notin \langle h \rangle$ et le résultat de la question 2 montre que $G = \langle h \rangle \rtimes \langle k \rangle$.

Barème

	Exercice 1		**10,5**
1	$\mathrm{car}(K) = 2$		1
2	propriété universelle		1
3	idéal principal non nul		1
4	$\mathrm{Im}f$ est un corps		1
	M est irréductible		1
5	$\mathrm{Im}f = K$		0,5
6	$\deg M = 3$		1
	$M = M_1$ ou M_2		1
7	existence et au plus deux		1
	unicité		2

	Exercice 2		**7**
1a	$\varphi_z \in GL(K^2)$		0,5
	morphisme de groupes		0,5
1b	produit semi-direct non abélien		1
1c	morphisme injectif		1
2a	$\lvert A^\times \rvert = p(p-1)$		0,5
	élément d'ordre p		0,5
2b	morphisme de K dans $\mathrm{Aut}(A)$		2
2c	produit semi-direct non abélien		1

	Exercice 3		**14,5**
1	$\Lambda \cap \langle b \rangle = \{1_\Gamma\}$		1
2	produit semi-direct		1,5
3	$\lvert Z(G) \rvert = p$ et $G/Z(G) \sim (\mathbb{Z}/p\mathbb{Z})^2$		1
4	$a^p \in Z(G)$		0,5
	$[a,b] \in Z(G)$		0,5
	$[a,b]^p = 1_G$		0,5
5	récurrence pour $[a,b^n]$		1
	récurrence pour $(ba)^n$		1
6	f morphisme		1
7	$\mathrm{Im}f \subset \mathrm{Ker}f$ et ordres possibles		1,5
8a	H sous-roupe d'ordre p^2		1,5
8b	utiliser la question 2		0,5
9a	$\mathrm{Im}f = Z(G)$		1
9b	$G = \langle h \rangle \rtimes \langle b \rangle$		2

Remarques sur les copies

Exercice 1

1. Question souvent mal faite.

2. Justifier l'existence d'un morphisme d'anneaux de $\mathbb{F}_2$ dans K, ou d'un isomorphisme entre K et $\{0_K, 1_K\}$ pour appliquer la propriété universelle ou utiliser un morphisme d'évaluation.

3. Souvent, le fait que l'idéal n'est pas réduit à $\{0_K\}$ est mal justifié. Le polynôme X^8 n'est pas dans le noyau mais les polynôme $X^7 - 1$ y est. Il y a parfois confusion entre les groupes $(K, +)$ et $(K^\times, \times)$.

Exercice 2

1a. Penser à justifier la linéarité de φ_z sans perdre une page pour cette question !

1b. Les groupes K et K^2 sont additifs. Le morphisme non trivial φ de K dans $\mathrm{Aut}(K^2)$ fournit un produit semi-direct $K^2 \rtimes K$ non direct donc non abélien, sans qu'il soit nécessaire de vérifier qu'on a bien une loi de groupe non commutative.

1c. Rédaction souvent lourde.

2a. Quelques valeurs aberrantes pour $|A^\times|$.

2b. Justification incomplète.

2c. Mêmes remarques qu'au 1b.

Exercice 3

1. Des preuves variées, mais où il manque parfois un argument essentiel.

2. Fait correctement en général.

3. Le fait que $G/Z(G)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ est prfois non justifié.

4. Le lien avec la question précédente n'a pas été vu dans nombre de copies.

5. Question qui sort de l'ordinaire, la deuxième formule a rarement été établie.

6. Question facile que certains ont su repérer.

7. Trop de copies ne pensent pas à utiliser la relation $|G| = |\mathrm{Ker} f||\mathrm{Im} f|$ dans cette question.