Plaquette 1 – Groupes, idéaux, anneaux quotients et corps finis

Structures algébriques — Prépa MP / MPI (2e année)

Corrections détaillées

Boîte à outils

Groupes.

— **Ordre d'un élément** x : plus petit $n \geq 1$ tel que $x^n = e$; alors $\langle x \rangle$ est **cyclique** d'ordre n.

— **Théorème de Lagrange** : dans un groupe fini G, l'ordre de tout sous-groupe **divise** $|G|$. En particulier $x^{|G|} = e$.

— Un groupe d'ordre **premier** est cyclique, engendré par n'importe quel élément $\neq e$.

— **Sous-groupe distingué** $H \lhd G$: $\forall g,\ gHg^{-1} = H$. Le **quotient** G/H est alors un groupe.

— **Théorème d'isomorphisme** : si $f : G \to G'$ est un morphisme, $G/\ker f \simeq \mathrm{Im} f$.

Anneaux.

— **Idéal** I d'un anneau commutatif A : sous-groupe additif tel que $\forall a \in A,\ aI \subset I$.

— Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$; ceux de $\mathrm{K}[X]$ sont les (P) — ces anneaux sont **principaux**.

— pgcd et ppcm s'y lisent : $a\mathbb{Z} + b\mathbb{Z} = \mathrm{pgcd}(a,b)\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{ppcm}(a,b)\mathbb{Z}$.

— **Anneau quotient** A/I ; $\mathbb{Z}/n\mathbb{Z}$ est un **corps** $\Leftrightarrow$ n est premier.

— **Éléments inversibles** de $\mathbb{Z}/n\mathbb{Z}$: les $\overline{k}$ avec $\mathrm{pgcd}(k,n) = 1$; leur nombre est $\varphi(n)$ (**indicatrice d'Euler**).

— **Théorème d'Euler** : si $\mathrm{pgcd}(a,n) = 1$, alors

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

— **Théorème chinois** : si $m \wedge n = 1$, $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (isomorphisme d'anneaux).

Corps. Un corps fini a un cardinal p^k ; son groupe multiplicatif est **cyclique**.

Correction de l'exercice 1 – Ordre d'un élément et Lagrange

Lagrange : l'ordre de x est celui du sous-groupe $\langle x \rangle$, il **divise** $|G| = 15$.

— Les diviseurs de 15 sont 1, 3, 5, 15.

— $x \neq e$ exclut l'ordre 1.

— **Ordres possibles** : 3, 5 ou 15.

— **Conséquence** : $x^{15} = e$ pour tout $x \in G$.

— **Complément** : on démontre (théorèmes de Sylow) que tout groupe d'ordre 15 est en fait **cyclique**, donc isomorphe à $\mathbb{Z}/15\mathbb{Z}$; il possède alors des éléments de chacun de ces trois ordres.

Réponse. 3, 5 ou 15.

Correction de l'exercice 2 – Groupe d'ordre premier

— Comme $p \geq 2$, il existe $x \in G$ avec $x \neq e$.

— L'ordre d de x divise p (Lagrange) et vaut 1 ou p.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— $d = 1$ signifierait $x = e$: exclu. Donc $d = p$.
— Ainsi $\langle x \rangle$ est un sous-groupe de **cardinal** $p = |G|$, donc $\langle x \rangle = G$.
— **Conclusion** : G est cyclique, engendré par **n'importe lequel** de ses éléments distincts de e ; il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
— **Conséquence structurelle** : il n'existe, à isomorphisme près, **qu'un seul** groupe d'ordre premier — les groupes d'ordre 2, 3, 5, 7… sont tous déterminés.

Réponse. Tout $x \neq e$ est d'ordre p, donc $G = \langle x \rangle$.

Correction de l'exercice 3 – Idéaux de Z

$\mathbb{Z}$ est **principal** : tout idéal est de la forme $n\mathbb{Z}$.

— **Somme** : I est un idéal contenant 6 et 10, donc $6 - 10 = -4$, puis $6 - 4 = 2$. On a $I = 2\mathbb{Z}$.
— **Formule** : $a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$, et $\text{pgcd}(6, 10) = 2$ ✓
— **Intersection** : J est formé des multiples communs, donc $J = \text{ppcm}(6, 10)\mathbb{Z} = 30\mathbb{Z}$.
— **Contrôle** : $\text{pgcd} \times \text{ppcm} = 2 \times 30 = 60 = 6 \times 10$ ✓
— **Lecture Bézout** : $I = 2\mathbb{Z}$ signifie exactement qu'il existe u, v avec $6u + 10v = 2$ — par exemple $u = 2$, $v = -1$.

Réponse. $I = 2\mathbb{Z}$ et $J = 30\mathbb{Z}$.

Correction de l'exercice 4 – Idéaux de K[X]

$\mathbb{R}[X]$ est **principal** : l'idéal engendré est (D) où D est le **PGCD** des deux polynômes.

— **Factorisations** : $X^2 - 1 = (X - 1)(X + 1)$ et $X^2 - 3X + 2 = (X - 1)(X - 2)$.
— Le seul facteur commun est $X - 1$, donc $D = X - 1$.
— **Idéal** : $\left(X^2 - 1\right) + \left(X^2 - 3X + 2\right) = (X - 1)$.
— **Contrôle par Euclide** : la différence des deux polynômes vaut $3X - 3 = 3(X - 1)$, qui appartient à l'idéal ; donc $X - 1$ y est aussi.
— **Généralisation** : dans un anneau principal, « idéal engendré par une famille » = « idéal engendré par leur PGCD » — c'est la traduction algébrique de Bézout.

Réponse. L'idéal $(X - 1)$.

Correction de l'exercice 5 – Indicatrice d'Euler

— **Décomposition** : $36 = 2^2 \times 3^2$.
— **Multiplicativité** : $\varphi(36) = \varphi(4)\varphi(9) = 2 \times 6 = 12$.
— **Vérification par la formule** : $36\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 36 \times \frac{1}{2} \times \frac{2}{3} = 12$ ✓

Application. $\text{pgcd}(5, 36) = 1$, donc le **théorème d'Euler** donne $5^{12} \equiv 1 \pmod{36}$.

— $100 = 12 \times 8 + 4$, donc $5^{100} \equiv 5^4 \pmod{36}$.
— $5^2 = 25$, $5^4 = 625 = 17 \times 36 + 13$.
— **Reste** : 13.
— **Contrôle** : $625 - 612 = 13$ ✓

Réponse. $\varphi(36) = 12$ et $5^{100} \equiv 13 \pmod{36}$.

Correction de l'exercice 6 – Théorème chinois

7 et 9 sont premiers entre eux : le système a une unique solution modulo 63.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— De la première : $x = 3 + 7k$.
— Report : $3 + 7k \equiv 4 \pmod 9$, soit $7k \equiv 1 \pmod 9$.
— **Inverse de** 7 **modulo** 9 : $7 \times 4 = 28 = 27 + 1 \equiv 1$, donc $k \equiv 4 \pmod 9$.
— $x = 3 + 7(4 + 9m) = 31 + 63m$, soit $x \equiv 31 \pmod{63}$.
— **Vérification** : $31 = 4 \times 7 + 3$ ✓ et $31 = 3 \times 9 + 4$ ✓
— **Interprétation** : l'application $\overline{x} \mapsto (\overline{x}, \overline{x})$ est un **isomorphisme d'anneaux** $\mathbb{Z}/63\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$; résoudre le système, c'est calculer l'image réciproque de $(\overline{3}, \overline{4})$.

Réponse. $x \equiv 31 \pmod{63}$.

Correction de l'exercice 7 – Noyau et théorème d'isomorphisme

— **Morphisme** : $|zz'| = |z||z'|$, donc f est un morphisme de groupes multiplicatifs.
— **Noyau** : $|z| = 1$, donc $\ker f = \mathrm{U}$, le **cercle unité**.
— **Image** : tout réel $r > 0$ est le module de r lui-même, donc f est **surjective**.
— **Théorème d'isomorphisme** :

$$\mathbb{C}^* / \mathrm{U} \simeq \mathbb{R}_+^*$$

— **Lecture géométrique** : « oublier » le module revient à ne garder que l'argument, et réciproquement. Tout complexe non nul s'écrit de manière unique $re^{i\theta}$ avec $r > 0$: c'est la décomposition $\mathbb{C}^* \simeq \mathbb{R}_+^* \times \mathrm{U}$.

Réponse. $\ker f = \mathrm{U}$ et $\mathbb{C}^*/\mathrm{U} \simeq \mathbb{R}_+^*$.

Correction de l'exercice 8 – Sous-groupe distingué

Soient $H = \ker f$, $g \in G$ et $h \in H$.

— **Sous-groupe** : $f(e) = e'$, donc $e \in H$; et si $h, h' \in H$, $f(hh'^{-1}) = f(h)f(h')^{-1} = e'$.
— **Caractère distingué** : on calcule l'image du conjugué,

$$f\left(ghg^{-1}\right) = f(g)f(h)f(g)^{-1} = f(g)\,e'\,f(g)^{-1} = e'$$

— Donc $ghg^{-1} \in H$ pour tous $g \in G$, $h \in H$: $H \lhd G$.
— **Réciproque vraie** : tout sous-groupe distingué est le noyau d'un morphisme, à savoir la **projection canonique** $G \to G/H$.
— **Exemple** : dans S_n, le noyau de la signature est le groupe alterné A_n, distingué d'indice 2.

Réponse. $f(ghg^{-1}) = e'$: le noyau est distingué.

Correction de l'exercice 9 – Corps fini

Le groupe F_7^* est d'ordre 6 ; l'ordre de $\overline{3}$ divise 6.

— **Puissances** : $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$ (modulo 7).
— La première puissance égale à 1 est la sixième : $\overline{3}$ est d'**ordre 6**.
— Il engendre donc un sous-groupe de cardinal $6 = \left|\mathrm{F}_7^*\right|$: $\overline{3}$ est un **générateur** (on dit aussi une **racine primitive** modulo 7).
— **Contrôle** : les six puissances listées parcourent bien $\{1, 2, 3, 4, 5, 6\}$ sans répétition ✓
— **Théorème général** : le groupe multiplicatif de tout corps **fini** est cyclique.

Réponse. $\overline{3}$ est d'ordre 6 : c'est un générateur de F_7^*.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Correction de l'exercice 10 – Anneau quotient de polynômes

— X^2+1 est **irréductible** sur $\mathbb{R}$ (discriminant négatif).
— Dans un anneau principal, le quotient par un idéal engendré par un élément **irréductible** est un **corps**. Donc $\mathbb{R}[X]/(X^2+1)$ est un corps.
— **Isomorphisme explicite** : on considère $\Phi{:}\mathbb{R}[X]\to\mathbb{C}$, $P\mapsto P(\mathrm{i})$.
— C'est un morphisme d'anneaux **surjectif** ($a+bX\mapsto a+b\mathrm{i}$).
— Son **noyau** est l'ensemble des P tels que $P(\mathrm{i})=0$, c'est-à-dire (à coefficients réels) les multiples de X^2+1.
— Le théorème d'isomorphisme donne $\mathbb{R}[X]/\left(X^2+1\right)\simeq\mathbb{C}$.
— **Lecture** : « i » n'est rien d'autre que la classe de X — on **construit** ainsi $\mathbb{C}$ sans postuler l'existence d'une racine de -1.

Réponse. $\Phi(P)=P(\mathrm{i})$ a pour noyau (X^2+1) ; quotient $\simeq\mathbb{C}$.

Correction de l'exercice 11 – Groupe symétrique et signature

Décomposition en cycles : on suit les images.

— $1\to3\to4\to1$: cycle (1 3 4), de longueur 3.
— $2\to5\to2$: cycle (2 5), de longueur 2.
— Donc $\sigma=(1\ 3\ 4)(2\ 5)$, produit de cycles **disjoints** (ils commutent).
— **Signature** : un cycle de longueur ℓ a pour signature $(-1)^{\ell-1}$.

$$\varepsilon(\sigma)=(-1)^2\times(-1)^1=-1$$

— σ est donc une permutation **impaire**.
— **Ordre** : c'est le **ppcm** des longueurs, soit $\mathrm{ppcm}(3,2)=6$.
— **Contrôle** : σ^6 ramène chaque cycle à l'identité, et aucune puissance plus petite ne le fait pour les deux à la fois ✓

Réponse. $\sigma=(1\ 3\ 4)(2\ 5)$, signature -1, ordre 6.

Correction de l'exercice 12 – Groupe des inversibles : cyclique ou non

a) $(\mathbb{Z}/9\mathbb{Z})^\times=\{\overline{1},\overline{2},\overline{4},\overline{5},\overline{7},\overline{8}\}$ (les classes premières avec 9), de cardinal $\varphi(9)=6$. Puissances de $\overline{2}$: $\overline{2},\overline{4},\overline{8},\overline{16}=\overline{7},\overline{14}=\overline{5},\overline{10}=\overline{1}$. L'ordre de $\overline{2}$ est 6 :

$$(\mathbb{Z}/9\mathbb{Z})^\times=\langle\overline{2}\rangle\simeq\mathbb{Z}/6\mathbb{Z}$$

b) $(\mathbb{Z}/8\mathbb{Z})^\times=\{\overline{1},\overline{3},\overline{5},\overline{7}\}$ et $3^2=9$, $5^2=25$, $7^2=49$ sont tous $\equiv 1 \pmod 8$. Aucun élément n'est d'ordre 4 : pas cyclique. Chaque élément non neutre est d'ordre 2 : c'est le groupe de Klein $(\mathbb{Z}/2\mathbb{Z})^2$.

c) L'isomorphisme d'anneaux $\mathbb{Z}/15\mathbb{Z}\to\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ envoie les inversibles sur les inversibles du produit, qui sont les couples d'inversibles. Donc le groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, dont tout élément vérifie $x^4=e$: aucun élément d'ordre $8=\varphi(15)$, le groupe n'est pas cyclique. (Exemple : $\overline{2}$ est d'ordre 4 : $2,4,8,16\equiv1$.)

Réponse. $n=9$: cyclique, engendré par $\overline{2}$; $n=8$: Klein ; $n=15$: $\mathbb{Z}/2\times\mathbb{Z}/4$, non cyclique.

Correction de l'exercice 13 – Ordre d'un produit dans un groupe abélien

a) G est abélien, donc $(ab)^{mn}=a^{mn}b^{mn}=(a^m)^n(b^n)^m=e$.

b) $(ab)^d=e$ donne $a^d=b^{-d}$, puis en élevant à la puissance n : $a^{dn}=b^{-dn}=e$. L'ordre m

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

de a divise donc dn ; comme $m \wedge n = 1$, le **lemme de Gauss** donne $m \mid d$. Symétriquement, $n \mid d$.

c) $m \mid d$ et $n \mid d$ avec $m \wedge n = 1$: $mn \mid d$. Avec a), $d \mid mn$. Donc

$$\mathrm{ord}(ab) = mn$$

d) En notation additive, $\overline{1}$ et $\overline{3}$ sont d'ordre 4, mais $\overline{1} + \overline{3} = \overline{0}$ est d'ordre 1. L'hypothèse de coprimalité est indispensable.

Réponse. $\mathrm{ord}(ab) = mn$ si $m \wedge n = 1$ (Gauss) ; faux sinon ($\overline{1} + \overline{3} = \overline{0}$ dans $\mathbb{Z}/4$).

Correction de l'exercice 14 – Morphismes de Z/nZ dans Z/mZ

a) $f(\overline{k}) = f(k\overline{1}) = kf(\overline{1})$: f est déterminé par $\overline{a} = f(\overline{1})$. Et $n\overline{1} = \overline{0}$ impose $n\overline{a} = f(\overline{0}) = \overline{0}$, c'est-à-dire $m \mid na$.

b) Si $k \equiv k' \pmod{n}$, alors $k - k' = tn$ et $(k - k')a = tna$ est multiple de m : $\overline{ka} = \overline{k'a}$. La formule est bien définie, et additive.

c) Les $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ tels que $m \mid na$: avec $d = n \wedge m$, $n = dn'$, $m = dm'$, $m' \wedge n' = 1$, la condition s'écrit $m' \mid n'a$, soit $m' \mid a$. Les solutions dans $[\![0, m-1]\!]$ sont les multiples de m' :

$$\mathrm{card}\,\mathrm{Hom} = \frac{m}{m'} = d = n \wedge m$$

— $n = 12$, $m = 18$: 6 morphismes, $f(\overline{1}) \in \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\}$ ($m' = 3$).

Réponse. $f(\overline{1}) = \overline{a}$ avec $m \mid na$; $n \wedge m$ morphismes ; 6 pour $(12, 18)$.

Correction de l'exercice 15 – Synthèse : sous-groupes de Z/12Z

$\mathbb{Z}/12\mathbb{Z}$ est **cyclique** d'ordre 12 : ses sous-groupes sont **exactement** les $\langle\overline{d}\rangle$ pour $d \mid 12$, et il y en a un **et un seul** par diviseur.

— $d = 1$: $\langle\overline{1}\rangle = \mathbb{Z}/12\mathbb{Z}$, d'ordre 12.
— $d = 2$: $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$, d'ordre 6.
— $d = 3$: $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$, d'ordre 4.
— $d = 4$: $\{\overline{0}, \overline{4}, \overline{8}\}$, d'ordre 3.
— $d = 6$: $\{\overline{0}, \overline{6}\}$, d'ordre 2.
— $d = 12$: $\{\overline{0}\}$, d'ordre 1.
— **Règle** : le sous-groupe engendré par $\overline{d}$ est d'ordre $\dfrac{12}{\mathrm{pgcd}(d, 12)}$; il y a donc autant de sous-groupes que de **diviseurs** de 12, soit 6.
— **Contrôle de Lagrange** : 1, 2, 3, 4, 6, 12 divisent tous 12 ✓
— **Générateurs du groupe** : les $\overline{k}$ avec $k \wedge 12 = 1$, soit $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ — au nombre de $\varphi(12) = 4$.

Réponse. Six sous-groupes, un par diviseur de 12.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).