Exercice I. (Cours, 6 points)

1. Enoncer et démontrer le théorème des restes chinois.

2. Montrer que $\mathbb{Z}$ est un anneau principal.

Exercice II. On se place dans $\mathbb{Z}/18\mathbb{Z}$.

1. a. Calculer l'inverse de 7.

On utilise l'algorithme d'Euclide : $18 = 7 \times 2 + 4$, $7 = 4 + 3$, $4 = 3 + 1$, ce qui montre que 7 et 18 sont premiers entre eux, on remonte ensuite l'algorithme : $1 = 4 - 3 = 4 - (7 - 4) = 4 \times 2 - 7 = (18 - 7 \times 2) \times 2 - 7 = 18 \times 2 - 7 \times 5$. Ce qui montre que $7 \times (-5) \equiv 1 \mod 18$ et donc que l'inverse de 7 modulo 18 est $-5 = 13$.

b. Résoudre l'équation $5x + 3 = 0$.

En multipliant l'équation par $-7 = 11$ (qui est l'inverse de 5 d'après la question précédente), l'équation est équivalente à $x + 33 = 0$ et donc $x = 3$. 3 est l'unique solution de l'équation.

c. Résoudre l'équation $4x + 10 = 0$.

4 n'est pas inversible modulo 18 car 4 et 18 ne sont pas premiers entre-eux. Résolvons dans $\mathbb{Z}$ l'équation $4x + 10 = 0 \mod 18$. En factorisant par 2, cette équation est équivalente à $2x + 5 = 0 \mod 9$. Maintenant 2 et 9 sont premiers entre eux et $2 \times 5 \equiv 1$ mod 9. En multipliant l'équation par 5 dans $\mathbb{Z}/9\mathbb{Z}$ elle est équivalente à $x + 25 \equiv 0$ mod 9 et donc à $x \equiv 2 \mod 9$. En revenant à l'équation initiale, les deux solutions sont donc 2 et $2 + 9 = 11$.

2. a. Montrer que l'application $f : x \mapsto 7x + 3$ est bijective.

$f : \mathbb{Z}/18\mathbb{Z} \to \mathbb{Z}/18\mathbb{Z}$, l'ensemble de départ et l'ensemble d'arrivée on le même cardinal, 18. Il suffit donc de montrer que f est injective pour montrer qu'elle est bijective.
Soit x, x' dans $\mathbb{Z}/18\mathbb{Z}$ tels que $f(x) = f(x')$. Alors $7x+3 = 7x'+3$ et donc $7(x-x') = 0$. En multipliant par 11 qui est l'inverse de 7 on obtient $x = x'$. Ceci montre que f est injective et donc bijective.

b. Trouver tous les x tels que $f(x) = x$.

Résolvons l'équation $f(x) = 7x + 3 = x$ dans $\mathbb{Z}/18\mathbb{Z}$. Elle est équivalente à $6x + 3 = 0$. 6 n'est pas inversible dans $\mathbb{Z}/18\mathbb{Z}$, 6 est même un diviseur de 18 ! Mais si x est un éléments de $\mathbb{Z}$ tel que 18 divise $6x + 3$ alors 6 divise a fortiori $6x + 3$ et 6 divise 3 ce qui est une contradiction. L'équation $f(x) = x$ n'a donc pas de solutions.

3. Donner le cardinal du groupe multiplicatif $(\mathbb{Z}/18\mathbb{Z})^\times$.

Les inversibles de $(\mathbb{Z}/18\mathbb{Z})$ sont les éléments premiers avec 18 c'est-à-dire $1, 5, 7, 11, 13, 17$, il y en a 6. Le cardinale de $(\mathbb{Z}/18\mathbb{Z})^\times$ est donc 6. *Autre méthode :* L'indicatrice d'Euler de 18 est $\varphi(18) = \varphi(2) \times \varphi(3^2) = 1 \times 3(3 - 1) = 6$. C'est le cardinal de $(\mathbb{Z}/18\mathbb{Z})^\times$.

4. a. Calculer 5^2, 5^3 et 5^6.

$5^2 = 7$, $5^3 = -1$ et $5^6 = 1$.

b. En déduire l'ordre de 5 dans le groupe multiplicatif $(\mathbb{Z}/18\mathbb{Z})^\times$.

Comme $5^6 = 1$ l'ordre de 5 divise 6, et comme 5^2 et 5^3 sont différents de 1, l'ordre de 5 est 6.

5. Donner explicitement un isomorphisme entre $(\mathbb{Z}/6\mathbb{Z}, +, 0)$ et $((\mathbb{Z}/18\mathbb{Z})^{\times}, \times, 1)$.

D'après la question précédente $f : \begin{array}{ccc} \mathbb{Z}/6\mathbb{Z} & \to & (\mathbb{Z}/18\mathbb{Z})^{\times} \\ k & \mapsto & 5^k \end{array}$ est un isomorphisme de groupes.

Exercice III. Dans S_4 on considère les éléments $\alpha = (12)(34)$ et $\beta = (13)(24)$, et N le sous-groupe qu'ils engendrent.

1. Déterminer les quatre éléments de N et dresser sa table de CAYLEY. Montrer que les éléments de N commutent.

En effectuant les calculs on trouve :

	id	$(12)(34)$	$(13)(24)$	$(14)(23)$
id	id	$(12)(34)$	$(13)(24)$	$(14)(23)$
$(12)(34)$	$(12)(34)$	id	$(14)(23)$	$(13)(24)$
$(13)(24)$	$(13)(24)$	$(14)(23)$	id	$(12)(34)$
$(14)(23)$	$(14)(23)$	$(13)(24)$	$(12)(34)$	id

On remarque que le tableau est symétrique par rapport à la diagonale principale, ce qui montre que N est commutatif (et cela justifie que l'on ne précise pas dans quel sens on effectue les multiplications).

2. Montrer que tous les éléments de N sont pairs et qu'ils sont d'ordre 1 ou 2.

Les transpositions sont impaires et donc les produits de deux transpositions sont pairs. L'identité est paire. Les quatre éléments de N sont donc pairs. L'identité est d'ordre 1 et les trois autres éléments sont d'ordre 2 (l'ordre d'un produit de cylcles à supports disjoints est le ppcm des longueurs des cycles).

3. Donner tous les éléments de S_4 qui sont pairs et d'ordre 1 ou 2.

L'ordre d'une permutation est le ppcm de la longueur des cycles de sa décomposition en cycles à supports disjoints. La seule permutation d'ordre 1 est l'indentité.
Les éléments de S_4 d'ordre 2 se décomposent donc en un produit de transpositions à supports disjoints, ils sont donc de la forme (12) ou $(12)(34)$. Les transpositions sont impaires. Les permutations paires de S_4 d'ordre 1 ou 2 sont donc exactement les éléments de N.

4. Soit $\rho, \sigma \in S_4$, montrer que $\sigma\rho\sigma^{-1}$ et ρ ont même ordre

Calculons les puissances successives de $\sigma\rho\sigma^{-1}$: $(\sigma\rho\sigma^{-1})^2 = \sigma\rho\sigma^{-1}\sigma\rho\sigma^{-1} = \sigma\rho^2\sigma^{-1}$, $(\sigma\rho\sigma^{-1})^3 = \sigma\rho^2\sigma^{-1}\sigma\rho\sigma^{-1} = \sigma\rho^3\sigma^{-1}$. Par récurrence nous montrerions que pour tout entier k,

$$(\sigma\rho\sigma^{-1})^k = \sigma\rho^k\sigma^{-1}.$$

Ainsi pour tout entier k, nous avons les équivalences suivantes :

$$(\sigma\rho\sigma^{-1})^k = id \iff \sigma\rho^k\sigma^{-1} = id \iff \rho^k = id.$$

La dernière équivalence étant obtenue en multipliant à gauche et à droite par σ^{-1} et σ respectivement.
Ceci montre que les idéaux annulateurs de ρ et $\sigma\rho\sigma^{-1}$ sont égaux et donc que leurs ordres (qui sont les générateurs positifs des idéaux annulateurs) sont égaux.

5. Soit $\rho, \sigma \in S_4$, montrer que $\sigma\rho\sigma^{-1}$ et ρ ont même signature.

La signature est un homomorphisme de groupes à valeur dans $\{\pm 1\}$, qui est un groupe commutatif. Nous avons donc $\mathrm{sign}(\sigma\rho\sigma^{-1}) = \mathrm{sign}(\sigma)\mathrm{sign}(\rho)\mathrm{sign}(\sigma^{-1}) = \mathrm{sign}(\sigma)\mathrm{sign}(\sigma)^{-1}\mathrm{sign}(\rho) = \mathrm{sign}(\rho)$.

6. En déduire que pour $\sigma \in S_4$ et $\rho \in N$, $\sigma\rho\sigma^{-1} \in N$.

D'après les questions précédentes pour toute permutation ρ de N, ρ est paire et d'ordre 1 ou 2, donc $\sigma\rho\sigma^{-1}$ est aussi une permutation paire et d'ordre 1 ou 2 et donc un élément de N. On dit que N est un sous-groupe distingué de S_4.

7. Déterminer une permutation $\sigma \in S_4$ telle que $\sigma\alpha\sigma^{-1} = \beta$ et $\sigma\beta\sigma^{-1} = \alpha$

Après plusieurs essais au brouillon, j'ai trouvé :

$$(132)(12)(34)(132)^{-1} = (132)(12)(34)(123) = (31)(24) = (13)(24).$$

Le cycle de longueur 3, $\sigma = (132)$ vérifie donc $\sigma\alpha\sigma^{-1} = \beta$.

Exercice IV. Soit G un groupe commutatif et x et y des éléments de G d'ordres finis respectifs m et n.

1. Donner la définition de l'ordre de x.

L'ordre d'un élément x d'un groupe G, est le plus petit entier $m > 0$ tel que $x^m = e$ où e est l'élément neutre du groupe. Alternativement l'ordre de x est le générateur strictement positif de l'idéal annulateur de x : $I_x = \{k \in \mathbb{Z} \mid x^k = e\}$. Si $I_x = \{0\}$ on dit que x est d'ordre infini.

2. a. Soit d un diviseur de m déterminer l'ordre de x^d dans G.

Comme d divise m, il existe $m' \in \mathbb{N}$ tel que $m = dm'$. Soit $k \in \mathbb{Z}$. $(x^d)^k = e \iff x^{dk} = e \iff m|dk \iff m'|k$. Par définition de l'ordre de x^d nous en déduisons que l'ordre de x^d et $m' = \frac{m}{d}$.

b. Pour $a \in \mathbb{Z}$, donner l'ordre de x^a en fonction de m et $\mathrm{pgcd}(a, m)$.

Soit k tel que $x(^a)^k = x^{ak} = e$. Par définition de l'ordre de x, on a l'équivalence $(x^a)^k = e \iff m|(ak)$. Soit d le pgcd de a et m. Alors il existe $a', m' \in \mathbb{N}$, tels que $a = da'$, $m = dm'$ et a' et m' sont premiers entre-eux. La condition précédente nous donne donc $(x^a)^k = e \iff (dm')|da'k \iff m'|a'k$ et d'après le lemme de Gauss, ceci est équivalent à $m'|k$. Par définition de l'ordre d'un élément nous avons montré que x^a est d'ordre $m' = \frac{m}{\mathrm{pgcd}(a,m)}$.

c. Soit d un diviseur de m, donner un élément de G d'ordre d.

D'après la question précédente $x^{\frac{m}{d}}$ est d'ordre d.

3. a. Montrer que si m et n sont premiers entre eux et si m et n divisent $a \in \mathbb{Z}$ alors mn divise a.

Comme m divise a il existe $a' \in \mathbb{Z}$ tels que $a = ma'$. Ainsi n divise ma' et d'après le lemmme de Gauss, n divise a'. Donc mn divise $ma' = a$.

b. Si m et n sont premiers entre eux montrer que l'ordre de $z = xy$ est mn.

Soit $k \in \mathbb{Z}$ tel que $z^k = e$. Comme G est commutatif nous avons $z^k = (xy)^k = x^k y^k = e$. En passant à la puissance m nous obtenons $e = e^m = (x^k y^k)^m = x^{km} y^{km} = (x^m)^k y^{km} = e^k y^{km} = y^{km}$. Par définition de l'ordre de y, ceci est équivalent à $n|km$ et d'après le lemme de GAUSS nous obtenons $z^k = e \Rightarrow n|k$. De même en passant à la puissance n nous montrerions que $z^k = e \Rightarrow n|k$. D'après la question précédente nous obtenons donc $z^k = e \Rightarrow (mn)|k$. L'implication réciproque est facile : $z^{mn} = (xy)^{mn} = x^{mn} y^{mn} = (x^m)^n (y^n)^m = e^n e^m = e$. Par définition de l'ordre de z nous avons donc montré que $z = xy$ est d'ordre mn dans G.

4. Soit $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $n = p_1^{\beta_1} \cdots p_r^{\beta_r}$ les décompositions en facteurs premiers de m et n, où $p_1, \ldots, p_r$ sont des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r \geq 0$ sont des entiers positifs.

a. Donner la décomposition en facteurs premiers du pgcd et du ppcm de m et n.

Pour tout i soit $\gamma_i = \max\{\alpha_i, \beta_i\}$ et $\delta_i = \min\{\alpha_i, \beta_i\}$. Alors

$$\mathrm{pgcd}(m, n) = {p_1}^{\delta_1} {p_2}^{\delta_2} \cdots {p_r}^{\delta_r} \text{ et } \mathrm{ppcm}(m, n) = {p_1}^{\gamma_1} {p_2}^{\gamma_2} \cdots {p_r}^{\gamma_r}.$$

b. Montrer que pour chaque i il existe un élément z_i de G d'ordre $p_i^{\max(\alpha_i, \beta_i)}$.

Soit i parmi $1, \ldots, r$.
<u>Premier cas</u> : si $\alpha_i \leq \beta_i$, alors $\beta_i = \max(\alpha_i, \beta_i) = \gamma_i$, et soit $n_i = \frac{n}{{p_i}^{\beta_i}}$. D'après les questions précédentes, $z_i = y^{n_i}$ est d'ordre $\frac{n}{n_i} = {p_i}^{\beta_i}$.
<u>Deuxième cas</u> : si $\alpha_i > \beta_i$, alors $\alpha_i = \max(\alpha_i, \beta_i) = \gamma_i$, et soit $m_i = \frac{m}{{p_i}^{\alpha_i}}$. D'après les questions précédentes, $z_i = x^{m_i}$ est d'ordre $\frac{m}{m_i} = {p_i}^{\alpha_i}$.
Dans tous les cas nous avons trouvé un élément z_i de G d'ordre $p_i^{\max(\alpha_i, \beta_i)}$.

c. Donner l'ordre de $z = z_1 \cdots z_r$.

En généralisant les questions précédentes, puisque les ordres des z_i sont deux à deux premiers entre eux, l'ordre de z est le produit des ordres c'est-à-dire $p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_r^{\max(\alpha_r, \beta_r)} = \mathrm{ppcm}(m, n)$.
Nous avons donc montré que pour tous éléments x et y dans G d'ordres respectifs m et n il existe un élément z de G d'ordre $\mathrm{ppcm}(m, n)$.