

Algèbre 1
Examen

Question de cours 1. Soient G un groupe abélien fini et p_1, \dots, p_ℓ les diviseurs premiers de $|G|$. Montrer que $G \simeq G_{p_1} \times \dots \times G_{p_\ell}$.

Question de cours 2. Soient $\varphi : A \rightarrow B$ un homomorphisme d'anneaux et I un idéal bilatère de A . Supposons que $I \subset \text{Ker}(\varphi)$. Montrer qu'il existe un unique homomorphisme $\psi : A/I \rightarrow B$ tel que $\varphi = \psi \circ \pi$, où $\pi : A \rightarrow A/I$ est la projection canonique.

Exercice 1. Soit G un groupe abélien fini et H un sous-groupe de G . Soit \mathcal{R} la relation sur G définie par

$$a\mathcal{R}b \iff b - a \in H.$$

- (1) Montrer que \mathcal{R} est une relation d'équivalence.
- (2) Soit C une classe d'équivalence et $c \in C$. Montrer que $C = \{c + h \mid h \in H\}$.
- (3) Montrer que le cardinal de toute classe de \mathcal{R} est $|H|$. En déduire que $|G| = |G/H| \times |H|$.

Exercice 2. Soit $V = \mathbb{R}^n$. Notons $\mathcal{B} = \{e_1, \dots, e_n\}$ la base canonique de V . Pour tout élément σ du groupe symétrique \mathfrak{S}_n on définit l'application linéaire $S_\sigma : V \rightarrow V$ par $S_\sigma(e_i) = e_{\sigma(i)}$ pour tout $i \in \{1, \dots, n\}$.

- (1) Montrer que l'application $S : \mathfrak{S}_n \rightarrow \text{GL}(V)$, $\sigma \mapsto S_\sigma$, est un homomorphisme de groupes injectif.
- (2) Soit $\sigma \in \mathfrak{S}_n$. Montrer que $\det(S_\sigma) = \epsilon(\sigma)$, où $\epsilon : \mathfrak{S}_n \rightarrow \{\pm 1\}$ désigne la signature.

Exercice 3. On considère le sous-ensemble A de \mathbb{C} constitué des éléments de la forme $a_1 + i\sqrt{2}a_2$, où a_1 et a_2 sont des entiers.

- (1) Montrer que A est un sous-anneau de \mathbb{C} .
- (2) Déterminer les éléments inversibles de A .
- (3) Démontrer que, pour tout $z \in \mathbb{C}$, il existe $a \in A$ tel que $|z - a| < 1$.
- (4) Montrer que A est un anneau euclidien.
- (5) Soit p un nombre premier impair. Montrer que, si l'équation $X^2 + 2Y^2 = p$ a une solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, alors -2 est un carré modulo p .
- (6) Soit p un nombre premier impair. Supposons que l'équation $X^2 + 2Y^2 = p$ a une solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Montrer que $x + i\sqrt{2}y$ et $x - i\sqrt{2}y$ sont premiers dans A . En déduire que l'ensemble des solutions de l'équation $X^2 + 2Y^2 = p$ est $\{(x, y), (-x, y), (x, -y), (-x, -y)\}$.