

Exercices sur les groupes, anneaux

1 Groupes

ÉNONCÉ :

Soit $G \neq \{e\}$ un groupe fini tel que : $\forall a \in G, a^2 = 1$.

1. Prouver que G est commutatif.
2. Prouver que $\text{Card } G$ est pair.
3. Prouver que $G = (\mathbb{Z}/2\mathbb{Z})^p$, et donc que $\text{Card } G = 2^p$.

1. On a : $\forall (a, b) \in G^2, (ab)^2 = 1 = a^2b^2$. On a donc : $abab = a^2b^2 = aabb$. En simplifiant à gauche et à droite dans $aabb = abab$, on en déduit que $ab = ba$. Donc G est commutatif.

2. Supposons que $\text{Card } G$ est impair. Comme $G \neq \{e\}$, $\text{Card } G \geq 3$.

Soit $a \in G \setminus \{e\}$. Par hypothèse, a engendre un groupe d'ordre 2, d'après le théorème de Lagrange, 2 doit diviser $\text{Card } G$, ce qui est impossible. Donc $\text{Card } G = 2n$ est pair.

3. Notons $F = \{ \{a_1, \dots, a_m\} \subset G \mid \forall i \in \{1, \dots, m\}, a_i \notin \langle a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_m \rangle \}$.

Si $G \neq \{e\}$, alors $F \neq \emptyset$.

F est fini et ordonné par l'inclusion. Soit $\{a_1, \dots, a_p\}$ élément maximal de F . Ceci signifie que $\forall g \in G, g$ appartient au sous-groupe engendré par a_1, \dots, a_p . Donc $\{a_1, \dots, a_p\}$ engendrent G .

Considérons maintenant $\varphi : \begin{pmatrix} \{1, a_1\} \times \dots \times \{1, a_p\} \longrightarrow G \\ (u_1, \dots, u_p) \longmapsto u_1 u_2 \dots u_p \end{pmatrix}$.

φ est un morphisme de groupes car G est abélien. On vient de voir qu'il est surjectif. L'injectivité résulte de la définition même de $\{a_1, \dots, a_p\}$.

Donc G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^p$.

2 Anneaux

ÉNONCÉ :

Soit A un anneau unitaire et commutatif.

Prouver que : A est un corps $\iff A[X]$ est intègre, et tout idéal de A est principal.

\implies c'est du cours.

\impliedby Montrons d'abord que si $A[X]$ est intègre, alors A est intègre. Supposons que A n'est pas un corps, et prouvons que $A[X]$ n'est pas principal.

Soit $a \in A \setminus \{0\}$ tel que a soit non-inversible. Considérons alors l'idéal $I = a \cdot A[X] + X \cdot A[X]$. Supposons que I est principal, il existe $P \in A[X]$ tel que $I = P \cdot A[X]$.

Comme $a \in I$, il existe $Q \in A[X]$ tel que $a = P \times Q$. Comme $A[X]$ est intègre, on a : $\deg a = 0 = \deg P + \deg Q$, donc $P \in A$ et $Q \in A$.

Mais $X \in I$, donc il existe $R \in A[X]$ tel que $X = P \times R$. Soit r le coefficient dominant de R .

On a : $1 = P \cdot r$, et $\deg R = 1$ car A est intègre, donc P est inversible, donc $I = P \cdot A[X] = a \cdot A[X] + X \cdot A[X]$. Donc $1 \in I$, donc il existe $T_1, T_2 \in A[X]$ tels que : $1 = a \cdot T_1 + X \cdot T_2$. On en déduit alors que $1 = a \cdot T_1(0)$. Par suite, a est inversible. Ceci contredit l'hypothèse. D'où le résultat.

ÉNONCÉ :

