Leçons : 101, 103, 104.

Th de Wedderburn

Énoncé : un anneau à division fini est commutatif, cad un corps.

Preuve.

Soit A un anneau à division fini. Son centre, $Z = \{y\in A \mid \forall x\in A,\ yx = xy\}$, est un sous-anneau à division commutatif de A ; cad un corps. On note $q\geq 2$ son cardinal (car $\{0,1\}\subset Z$). A est alors un Z-ev de dim finie : $|A| = q^n$ avec $n\geq 1$. Le but est de montrer $n=1$: on va par l'absurde supposer $n\geq 2$.

$A^\times$ agit sur lui-même par conjugaison. Pour $x\in A$ on note $Z_x = \{y\in A\mid yx=xy\}$, c'est un sous anneau à division de A (non nécessairement commutatif) et $\mathrm{Stab}(x) = Z_x^\times$. Puisque Z_x est un Z-ev de dim finie, $|Z_x| = q^d$ avec $d\geq 1$. Mq $d\mid n$. $Z_x^\times \subset A^\times$ donc par le th de Lagrange, $q^d-1 \mid q^n-1$. On écrit la div euclidienne de n par d : $n = md + r$ avec $m\in\mathbb{N}$ et $0\le r<d$. D'une part $q^n\equiv 1\ [q^d-1]$; d'autre part $q^n = (q^d)^m\cdot q^r \equiv q^r\ [q^d-1]$: $q^r\equiv 1\ [q^d-1]$. Autrement dit $q^d-1 \mid q^r-1$; or $q^r-1 < q^d-1$ donc $q^r-1=0$, cad $r=0$. D'où $d\mid n$.

On écrit la formule des classes : soit $X\subset A^\times$ un système de représentants des orbites non triviales (les orbites triviales étant les $\{x\}$ pour $x\in Z^\times$). Alors : $q^n-1 = |A^\times| = \sum_{x\in Z^\times}|\{x\}| + \sum_{x\in X}\frac{|A^\times|}{|\mathrm{Stab}(x)|}$

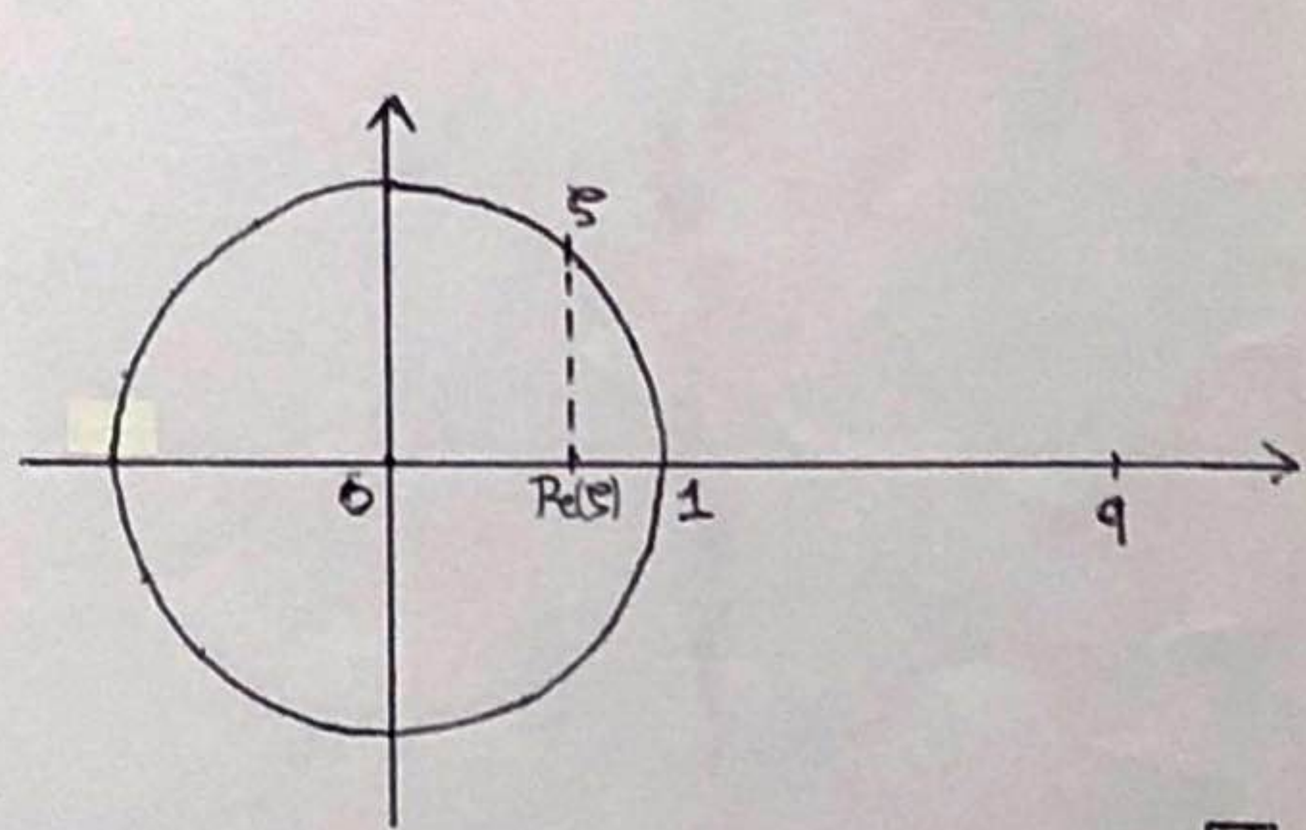
$= |Z^\times| + \sum_{x\in X}\frac{|A^\times|}{|Z_x^\times|} = q-1 + \sum_{d\in D} m_d \frac{q^n-1}{q^d-1}$ avec D inclus dans les diviseurs stricts de n

(car si $x\notin Z$, $|Z_x| = q^d$ avec $d\neq n$) et m_d le nb de $x\in X$ tq $|Z_x| = q^d$.

On va utiliser les polynômes cyclotomiques pour trouver une contradiction. Pour $k\geq 1$, $q^k-1 = \prod_{\ell\mid k}\Phi_\ell(q)$, donc pour d divisant strictement n, $\frac{q^n-1}{q^d-1} = \prod_{\substack{\ell\mid n\\ \ell\nmid d}}\Phi_\ell(q)$. En particulier, dans $\mathbb{Z}$:

$\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$. Puisque l'on a aussi $\Phi_n(q)\mid q^n-1$, $\Phi_n(q)\mid q-1$; ce qui implique $|\Phi_n(q)|\le q-1$.

Mais $\Phi_n(q) = \prod_{\zeta\in\mathbb{U}_n^*}(q-\zeta)$. Or pour $\zeta\in\mathbb{U}\setminus\{1\}$,
$|q-\zeta| = \sqrt{(\mathrm{Im}\,\zeta)^2 + (q-\mathrm{Re}\,\zeta)^2} \geq |q-\mathrm{Re}\,\zeta| > q-1$ puisque $\mathrm{Re}\,\zeta<1$. Donc $|\Phi_n(q)| > (q-1)^{\varphi(n)} \geq q-1$ car $q-1\geq 1$. Cela contredit ce qui précède !



□

Réf : Perrin : p 82.

↳ On prend la déf de corps qui comprend la commutativité. Un corps est ainsi un anneau à division commutatif.

↳ Si $|A| = q^n$ et $|Z_x| = q^d$, $d \mid n$. On l'a montré par de l'arithmétique élémentaire, cependant on peut aussi le justifier par le fait que A est un Z_x-ev à gauche (généralisation des ev aux anneaux à division), comme dans la théorie des corps finis. On l'esquive car on n'a pas étudié cette généralisation des ev.