Corps finis : l'artisèche.

Théorème principal : a) Tout corps fini est de caractéristique $p>0$ (p premier) et a un cardinal de la forme p^n ($n\geq 1$).

b) Réciproquement si $p>0$ est premier et $q=p^n$ ($n\geq 1$), il existe un corps, unique à isomorphisme près, de cardinal q et noté $\mathbb{F}_q$.

Evidemment $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$, mais pour $n\geq 2$ prendre garde que $\mathbb{F}_q=\mathbb{F}_{p^n}$ n'a pas de description explicite simple : $\mathbb{F}_q \neq \frac{\mathbb{Z}}{q\mathbb{Z}}$, $\mathbb{F}_q \neq \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^n$! (pas d'iso. d'anneaux)

Exemples : $\mathbb{F}_4=\frac{\mathbb{F}_2[X]}{(X^2+X+1)}$, $\mathbb{F}_8=\frac{\mathbb{F}_2[X]}{(X^3+X+1)}$, $\mathbb{F}_9=\frac{\mathbb{F}_3[X]}{(X^2+1)}$, ...

Quelques résultats :

a) $\mathbb{F}_q^*$, $\cdot$ est un groupe cyclique, donc isomorphe à $\frac{\mathbb{Z}}{(q-1)\mathbb{Z}}$, $+$.

b) Il existe un morphisme $\mathbb{F}_q \to \mathbb{F}_r$ de corps $\Leftrightarrow$ $r=q^f$ avec $f\geq 1$.
On écrit alors souvent $\mathbb{F}_q \subset \mathbb{F}_r$. Par exemple $\mathbb{F}_p \subset \mathbb{F}_{p^n}$.

Il n'y a aucun morphisme ~~$\mathbb{F}_4 \to \mathbb{F}_8$~~ ni ~~$\mathbb{F}_{25} \to \mathbb{F}_{125}$~~ ni...

c) $\mathbb{F}_q$ est le corps des racines (= splitting field) de $X^q-X \in \mathbb{F}_p[X]$.
Si on dispose d'une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$, on a
$\mathbb{F}_q=\{x\in\overline{\mathbb{F}_p} \mid x^q=x\}$. [Il est étrange que l'ensemble des zéros d'un polynôme forme un corps !]

d) $X^{p^n}-X=\prod_{f\in\mathcal{J}_n} f(X)$ où $\mathcal{J}_n$ désigne l'ensemble des polynômes unitaires irréductibles de $\mathbb{F}_p[X]$ de degré d divisant n.

Et il existe $f\in\mathcal{J}_n$ de degré n.