Colle du 16 octobre 2009

- Reprise du programme précédent sur l'arithmétique.
- Congruence. L'anneau $\mathbb{Z}/n\mathbb{Z}$
- Numération décimale, binaire. Algorithmes d'exponentiation rapide.
- Corps, sous-corps : définition, exemples : $\mathbb{Z}/p\mathbb{Z}$ ssi p est premier, le corps $\mathbb{Q}$ des rationnels. Caractéristique d'un corps.
- N.B. : l'existence du corps des fractions d'un anneau intègre a été admise.
- Structure de K-algèbre.

Exercice Montrer que $(p-1)! \equiv -1 \mod p \Leftrightarrow p$ est premier. En déduire une fonction $f : \mathbb{N}^* \to \mathbb{N}^*$ qui prend uniquement les valeurs 2 (une infinité de fois) et les nombres premiers impairs (une seule fois chacun).

Exercice En considérant un diviseur premier de $2^p - 1$ pour p premier, donner une nouvelle démonstration de l'infinité des nombres premiers.

Exercice Trouver tous les automorphismes de $\mathbb{R}$, puis tous les automorphismes de $\mathbb{C}$ laissant fixe $\mathbb{R}$.

Exercice Soit $d \in \mathbb{Z}$ sans facteur carré, $\sqrt{d} \in \mathbb{C}$ une racine carrée de d, et K le plus petit corps contenant $\mathbb{Q}$ et $\sqrt{d}$. Montrer que $K = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$.

Soit $A = \{z \in K | z \text{ est entier sur } \mathbb{Z}\}$. Montrer que $x \in A \Leftrightarrow 2a \in \mathbb{Z}$ et $a^2 - db^2 \in \mathbb{Z}$. En déduire que si $d \equiv 2, 3 \mod 4$, montrer qu'on a $A = \mathbb{Z}[\sqrt{d}]$, et si $d \equiv 1 \mod 4$ alors $A = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Exercice Soit K un corps de caractéristique $p > 0$. Montrer que $x \mapsto x^p$ est un endomorphisme de corps. Montrer que si K est fini, alors c'est un automorphisme, et que si K est $\mathbb{Z}/p\mathbb{Z}$, c'est l'identité.

Exercice Montrer qu'un anneau fini intègre est un corps.

Exercice Montrer qu'un anneau intègre est un corps si et seulement si ses seuls idéaux sont (0) et A.

Exercice Soit p un nombre premier, et $\mathbb{Z}_p$ le sous-ensemble de $\prod_{n \in \mathbb{N}^*} \mathbb{Z}/p^n\mathbb{Z}$ où les éléments $(x_n)_{n \geq 1}$ vérifient $x_{n+1} \equiv x_n \mod p^n$ pour tout n. Montrer que $\mathbb{Z}_p$ est un sous-anneau intègre de $\prod_{n \in \mathbb{N}^*} \mathbb{Z}/p^n\mathbb{Z}$. Quel est son corps de fractions ?

Question de cours Caractéristique d'un corps ?

Question de cours Montrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Question de cours Démontrer le théorème d'Euler (si a est premier avec n, $a^{\varphi(n)} \equiv 1 \mod n$).