Théorie de Galois. Mat 3661

Non-Devoir 3. À ne pas remettre. Les réponses seront données dans le site web du cours au plus tard le 20 février 2019. Si vous désirez avoir les réponses avant, enverrez-moi un courriel.

1. Démontrez qu'il est impossible de construire un 36-gone (un polygone régulier avec 36 côtés).

2. Trouvez le corps de décomposition sur $\mathbb{Q}$ de $p(x) = x^4 - 2$. Trouvez le degré de ce corps.

3. Trouvez le corps de décomposition sur $\mathbb{Q}$ de $p(x) = x^4 + 2$. Trouvez le degré de ce corps.

4. Trouvez le corps de décomposition sur $\mathbb{Q}$ de $p(x) = x^4 + x^2 + 1$. Trouvez le degré de ce corps. (Factoriser est une bonne idée).

5. Démontrez que
$$x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (x - \alpha).$$
Conclure que
$$\prod_{\alpha \in \mathbb{F}_{p^n}^*} \alpha = (-1)^{p^n},$$
alors, le produit des éléments non nuls d'un corps fini est $+1$ si $p = 2$ et -1 si p est impair. Le cas de p impair et $n = 1$ est le Théorème de Wilson: $(p-1)! \equiv -1 \bmod p$.

6. Démontrez que si p premier et $a \in \mathbb{F}_p$ avec $a \neq 0$, alors $x^p - x + a$ est un polynôme irréductible et séparable sur $\mathbb{F}_p$. (Piste : Montrez que si α est racine, alors, $\alpha + 1$ est racine.)

7. (a) Démontrez que $d|n$ si et seulement si $x^d - 1 | x^n - 1$. (Idée: écrire $n = qd + r$, alors $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$.)

   (b) Soit $a > 1$ un nombre éntier. Démontrez que $d|n$ si et seulement si $a^d - 1 | a^n - 1$.

   (c) Démontrez que $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$ si et seulement si $d|n$.

8. (a) Trouvez les polynômes irréductibles de degré 1, 2, et 4 sur $\mathbb{F}_2$, et démontrer que le produit est $x^{16} - x$.

   (b) Soit p premier et $n \geq 1$ entier. Démontrez que
$$\prod_{d|n} \prod_{\substack{f \in \mathbb{F}_p[x] \\ \text{irreductible, unitaire} \\ \deg f(x) = d}} f(x) = x^{p^n} - x.$$

9. (a) Montrez que $F = \bigcup \mathbb{F}_{p^n}$ est un corps et qu'il est la clôture algébrique de $\mathbb{F}_p$.

   (b) Trouvez $\mathbb{F}_{p^m} \cdot \mathbb{F}_{p^n} \subset \overline{\mathbb{F}_p}$.