UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
APPLIED ALGEBRA - MEM244 (FALL SEMESTER 2018-19)
LECTURER: G. KAPETANAKIS

3rd set

Exercise 1. Set $\mathbb{I}_q(n) := \{f \in \mathbb{F}_q[X] \mid f \text{ monic and irreducible of degree } n\}$ and $\pi_q(n) := |\mathbb{I}_q(n)|$.

1. Compute the numbers $\pi_3(1)$ and $\pi_3(2)$.
2. Find the sets $\mathbb{I}_3(1)$ and $\mathbb{I}_3(2)$.
3. Factor $X^9 - X$ over $\mathbb{F}_3$.

Exercise 2.
1. Find the set $D := \{d \in \mathbb{N} : d \mid 30 \text{ and } (d, 3) = 1\}$.
2. For every $d \in D$, write Ψ_d over $\mathbb{F}_3$ and describe its factorization, where Ψ_n stands for the n-th cyclotomic polynomial.
3. Factor $X^{30} - 1$ over $\mathbb{F}_3$.

Exercise 3.
1. Find the least prime p, such that $X^{22} + X^{21} + \cdots + X + 1$ is irreducible over $\mathbb{F}_p$.
2. Find the least prime $p > 7$ such that $f(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_p[X]$ factors into linear factors. How does it factor over $\mathbb{F}_7$?

Exercise 4. Let N be the norm function from $\mathbb{F}_q$ to $\mathbb{F}_p$, where $q = p^n$. Prove the following:

1. N is well-defined.
2. $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{F}_q$.
3. $N(a) = a^n$ for all $a \in \mathbb{F}_p$.
4. $N(\alpha^p) = N(\alpha)$ for all $\alpha \in \mathbb{F}_q$.

Hint: Look at the corresponding proof of the trace function.

Exercise 5. Let N be as in Exercise 4.

1. Show that $N(\alpha) = 0$ if and only if $\alpha = 0$.
2. Show that $N \mid_{F_q^*}$ defines a group homomorphism $\mathbb{F}_q^* \to \mathbb{F}_p^*$.
3. Show that $N \mid_{F_q^*} : \mathbb{F}_q^* \to \mathbb{F}_p^*$ is onto and deduce that N is onto.

Hint: Look at the corresponding proof of the trace function.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΕΦΑΡΜΟΣΜΕΝΗ ΑΛΓΕΒΡΑ - ΜΕΜ244 (ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2018-19)
ΔΙΔΑΣΚΩΝ: Γ. ΚΑΠΕΤΑΝΑΚΗΣ

3ο σετ ασκήσεων

Άσκηση 1. Θέτουμε $\mathbb{I}_q(n) := \{f \in \mathbb{F}_q[X] \mid f \text{ μονικό και ανάγωγο βαθμού } n\}$ και $\pi_q(n) := |\mathbb{I}_q(n)|$.

1. Υπολογίστε τους αριθμούς $\pi_3(1)$ και $\pi_3(2)$.
2. Βρείτε τα σύνολα $\mathbb{I}_3(1)$ και $\mathbb{I}_3(2)$.
3. Αναλύστε σε ανάγωγους παράγοντες το $X^9 - X$ υπέρ του $\mathbb{F}_3$.

Άσκηση 2. 1. Βρείτε το σύνολο $D := \{d \in \mathbb{N} : d \mid 30 \text{ and } (d, 3) = 1\}$.
2. Για κάθε $d \in D$, γράψτε το Ψ_d υπέρ του $\mathbb{F}_3$ και περιγράψτε την παραγοντοποίησή του, όπου Ψ_n το n-στο κυκλοτομικό πολυώνυμο.
3. Παραγοντοποιείστε το $X^{30} - 1$ υπέρ του $\mathbb{F}_3$.

Άσκηση 3. 1. Βρείτε τον ελάχιστο πρώτο p, τέτοιο ώστε το $X^{22} + X^{21} + \cdots + X + 1$ να είναι ανάγωγο υπέρ του $\mathbb{F}_p$.
2. Βρείτε τον ελάχιστο πρώτο $p > 7$ τέτοιον ώστε το $f(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_p[X]$ αναλύεται σε γραμμικούς (πρωτοβάθμιους) όρους. Πώς παραγοντοποιείται στο $\mathbb{F}_7$?

Άσκηση 4. Έστω N η νόρμα από το $\mathbb{F}_q$ στο $\mathbb{F}_p$, όπου $q = p^n$. Αποδείξτε τα ακόλουθα:

1. Η N είναι καλά ορισμένη.
2. $N(\alpha\beta) = N(\alpha)N(\beta)$ για κάθε $\alpha, \beta \in \mathbb{F}_q$.
3. $N(a) = a^n$ για κάθε $a \in \mathbb{F}_p$.
4. $N(\alpha^p) = N(\alpha)$ για κάθε $\alpha \in \mathbb{F}_q$.

Υπόδειξη: Δείτε την αντίστοιχη απόδειξη για το ίχνος.

Άσκηση 5. Έστω N όπως στην Άσκηση 4.

1. Δείξτε ότι $N(\alpha) = 0$ αν και μόνο αν $\alpha = 0$.
2. Δείξτε ότι η $N\mid_{F_q^*}$ ορίζει έναν ομομορφισμό ομάδων $\mathbb{F}_q^* \to \mathbb{F}_p^*$.
3. Δείξτε ότι η $N\mid_{F_q^*} : \mathbb{F}_q^* \to \mathbb{F}_p^*$ είναι επί και καταλήξτε ότι η N είναι επί.

Υπόδειξη: Δείτε την αντίστοιχη απόδειξη για το ίχνος.