UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
APPLIED ALGEBRA - MEM244 (FALL SEMESTER 2019-20)
LECTURER: G. KAPETANAKIS

3rd set - Answers

Exercise 1. For a finite field $\mathbb{F}_q$, with q odd, show that an element $a \in \mathbb{F}_q^*$ has a square root in $\mathbb{F}_q$ if and only if $a^{(q-1)/2} = 1$.

Answer. Take some $a \in \mathbb{F}_q^*$ and let ζ be a primitive element of $\mathbb{F}_q$. It follows that there exists some $1 \leq k \leq q-1$, such that $a = \zeta^k$. We have that

$$\begin{aligned} a^{(q-1)/2} = 1 &\iff \operatorname{ord}(a) \mid \frac{q-1}{2} \iff \operatorname{ord}(\zeta^k) \mid \frac{q-1}{2} \\ &\iff \frac{\operatorname{ord}(\zeta)}{\gcd(k, \operatorname{ord}(\zeta))} \mid \frac{q-1}{2} \iff \frac{q-1}{\gcd(k, q-1)} \mid \frac{q-1}{2} \\ &\iff 2 \mid \gcd(k, q-1) \iff 2 \mid k. \end{aligned}$$

The result follows. $\square$

Exercise 2. 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 $\mathbb{F}_3$.

Answer. Recall the formula $\pi_q(n) = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{n/d}$.

1. Using the above, we compute $\pi_3(1) = 3$ and $\pi_3(2) = 3$.
2. All polynomials of degree one are irreducible, hence
$$\mathbb{I}_3(1) = \{x, x+1, x+2\}.$$
Using the root criterion (as for polynomials of degree 2 or 3), we get that
$$\mathbb{I}_3(2) = \{x^2+1, x^2+x+2, x^2+2x+2\}.$$
3. Recall that, over $\mathbb{F}_q$, $x^{q^n} - x = \prod_{d \mid n} \prod_{f \in \mathbb{I}_q(d)} f$. Here, we have that
$$\begin{aligned} x^9 - x &= \prod_{f \in \mathbb{I}_3(1) \cup \mathbb{I}_3(2)} f \\ &= x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2). \end{aligned}$$ $\square$

Exercise 3. How many elements does $\mathbb{F}_{5^6}$ have, that do not belong in any of its proper subfields? How many of them are non-primitive?

Answer. An element of $\mathbb{F}_q$, where $q = p^n$ does not belong to any of $\mathbb{F}_q$'s proper subfields iff its minimum polynomial over $\mathbb{F}_p$ is of degree n. Also, since such polynomials have exactly n roots in $\mathbb{F}_q$, it follows that the number of such elements is exactly n times the number of monic irreducible polynomials of degree n over $\mathbb{F}_p$.

In particular, the number of elements of $\mathbb{F}_{5^6}$, that do not belong in any of its proper subfields is

$$6 \cdot \pi_5(6) = \sum_{d|6} \mu(d) 5^{6/d} = 5^6 - 5^3 - 5^2 + 5 = 15480.$$

Moreover, a primitive element of $\mathbb{F}_q$ cannot belong to any proper subfield of $\mathbb{F}_q$, so all the primitive elements of $\mathbb{F}_{5^6}$ are found among the aforementioned 15480 elements. So,

$$15480 - \phi(5^6 - 1) = 15480 - \phi(15624) = 15480 - 4320 = 11160$$

of them are non-primitive. □

Exercise 4.

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 $\mathbb{F}_3$.

Answer.

1. $D = \{1, 2, 5, 10\}$.
2. $\Psi_1 = X - 1$, which is irreducible.
   $\Psi_2 = (X^2 - 1)/\Psi_1 = X + 1$, which is irreducible.
   $\Psi_5 = (X^5 - 1)/\Psi_1 = X^4 + X^3 + X^2 + X + 1$. Since $\mathrm{ord}_5(3) = 4 = \phi(5)$, we get that Ψ_5 is irreducible.
   $\Psi_{10} = (X^{10} - 1)/\Psi_1\Psi_2\Psi_5 = X^4 - X^3 + X^2 - X + 1$. Since $\mathrm{ord}_{10}(3) = 4 = \phi(10)$, we get that Ψ_{10} is irreducible.
3. Recall that if $(q, n) = 1$, then $X^n - 1 = \prod_{d|n} \Psi_d$. Here, we have that

$$X^{30} - 1 = (X^{10} - 1)^3 = (\Psi_1\Psi_2\Psi_5\Psi_{10})^3.$$ □

Exercise 5.

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 $\mathbb{F}_7$?

Answer.

1. Notice that the polynomial in question is $\Psi_{23}(X) = (X^{23} - 1)/(X - 1)$. We are looking for the smallest prime $p \neq 23$, such that $\mathrm{ord}_{23}(p) = \phi(23) = 22$. After a quick computation, we get that $\mathrm{ord}_{23}(2) = \mathrm{ord}_{23}(3) = 11$, but $\mathrm{ord}_{23}(5) = 22$.

2. Notice that $f(X) = \Psi_7(X)$, which factors into linear factors over $\mathbb{F}_p$, with $p \neq 7$, iff $p \equiv 1 \bmod 7$. The least prime satisfying the latter is $p = 29$. Over $\mathbb{F}_7$, we have that

$$\Psi_7(X) = \frac{X^7 - 1}{X - 1} = \frac{(X-1)^7}{X-1} = (X-1)^6. \qquad \square$$

Exercise 6. Show that for $a \in \mathbb{F}_q$ and $n \in \mathbb{N}$ the polynomial $x^{q^n} - x + na$ is divisible by $x^q - x + a$ over $\mathbb{F}_q$.

Answer. Let β be a root of $f(x) = x^q - x + a$, i.e., $\beta^q = \beta - a$. If $g(x) = x^{q^n} - x + na$, then

$$\begin{aligned} g(\beta) &= \beta^{q^n} - \beta + na \\ &= (\beta - a)^{q^{n-1}} - \beta + na \\ &= \beta^{q^{n-1}} - a^{q^{n-1}} - \beta + na \\ &= \beta^{q^{n-1}} - \beta + (n-1)a \\ &= \dots \\ &= \beta - \beta = 0. \end{aligned}$$

In other words, all the roots of f are also roots of g. Also, since $\gcd(f, f') = 1$, all the roots of f are simple. It follows that $f \mid g$. $\square$

Exercise 7. Let $q = p^k$, for some k. Prove that $\mathrm{Tr}(a^{p^n}) = (\mathrm{Tr}(a))^{p^n}$ for all $a \in \mathbb{F}_q$ and $n \in \mathbb{N}$.

Answer. We have that

$$\mathrm{Tr}(a^{p^n}) = \mathrm{Tr}(a^{p^{n-1}})^p = \dots = (\mathrm{Tr}(a))^{p^n}. \qquad \square$$

Exercise 8. Let $q = p^m$. Prove that if $\{a_1, \dots, a_m\}$ is an $\mathbb{F}_p$-basis of $\mathbb{F}_q$, then $\mathrm{Tr}(a_i) \neq 0$ for at least one $1 \leq i \leq m$.

Answer. Suppose that $\mathrm{Tr}(a_i) = 0$, for all $1 \leq i \leq m$. Then, for every $x \in \mathbb{F}_q$, there exist some $x_1, \dots, x_m \in \mathbb{F}_p$, such that

$$x = \sum_{i=1}^{m} x_i a_i,$$

which implies

$$\mathrm{Tr}(x) = \mathrm{Tr}\left(\sum_{i=1}^{m} x_i a_i\right) = \sum_{i=1}^{m} x_i \mathrm{Tr}(a_i) = 0.$$

The latter contradicts to the fact that $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is onto. $\square$