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

2nd exercise set - Answers

Exercise 1. Show that a finite integral domain is a field.

Answer. Let R be a finite integral domain and take some $a \in R \setminus \{0\}$. It suffices to show that there exists some $b \in R$, such that $ab = 1$. Take the map

$$\phi \;:\; R \to R,\; x \mapsto ax.$$

Clearly, ϕ is 1-1 and, since R is finite, it follows that it is also onto, hence a bijection. It follows that there exists some $b \in R$, such that $\phi(b) = 1$, i.e., $ab = 1$. □

Exercise 2. Let F be a field. Show that for every $f, g \in F[X]$ and $c \in F$:

1. $(f+g)' = f' + g'$.
2. $(cf)' = cf'$.
3. $(fg)' = f'g + fg'$.

Answer. Write $f(X) = \sum_{i=0}^{n} f_i X^i$ and $g(X) = \sum_{i=0}^{n} g_i X^i$, where $f_i, g_i \in F$. We have that

$$\begin{aligned}(f+g)' &= \left(\sum_{i=0}^{n}(f_i+g_i)X^i\right)' = \sum_{i=1}^{n} i(f_i+g_i)X^{i-1} \\ &= \sum_{i=1}^{n} i f_i X^{i-1} + \sum_{i=1}^{n} i g_i X^{i-1} = f' + g'.\end{aligned}$$

The other items follow similarly. □

Exercise 3. Let $\mathbb{F}_3$ be a finite field of 3 elements and take $f(X) = X^3 - X - 1 \in \mathbb{F}_3[X]$.

1. Show that f is irreducible over $\mathbb{F}_3$.
2. If α is a root of f, find the degree of the extension $\mathbb{F}_3(\alpha)/\mathbb{F}_3$ and two bases.
3. Show that $g(X) = X^3 - X + 1 \in \mathbb{F}_3[X]$ is irreducible over $\mathbb{F}_3$ and show that there exists a root of g in $\mathbb{F}_3(\alpha)$.
4. Show that $\mathbb{F}_3(\alpha)$ does not contain a root of $h(X) = X^2 + 1 \in \mathbb{F}_3[X]$.

Answer.
1. Check that f has no roots in $\mathbb{F}_3$ and is of degree 3. The result follows.
2. Since $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 3$, we have that an $\mathbb{F}_3$-basis of $\mathbb{F}_3(\alpha)$ is the polynomial basis, that is, $\{1, \alpha, \alpha^2\}$. Another basis would be $\{1, \alpha+1, \alpha^2\}$.

3. Check that g has no roots in $\mathbb{F}_3$ and is of degree 3, thus is irreducible over $\mathbb{F}_3$. Further, notice that $g(-\alpha) = 0$.
4. Check that h has no roots in $\mathbb{F}_3$ and is of degree 2, thus is irreducible over $\mathbb{F}_3$. If β is a root of h, then $\mathbb{F}_3(\beta) = \mathbb{F}_{3^2}$ and if $\beta \in \mathbb{F}_3(\alpha) = \mathbb{F}_{3^3}$, then $\mathbb{F}_{3^2} \subseteq \mathbb{F}_{3^3} \Rightarrow 2 \mid 3$, a contradiction. □

Exercise 4. Prove that if θ is algebraic over L and the extension L/K is algebraic, then θ is algebraic over K.

Answer. Since θ is algebraic over L, there exists some $f = \sum_{i=0}^{n} f_i X^i \in L[X]$, such that $f(\theta) = 0$. Now, we get the following tower of extensions:

$$K \subseteq K(f_1) \subseteq \ldots \subseteq K(f_1, \ldots, f_n).$$

Notice that each of these extensions is a simple algebraic extensions, hence finite. It follows that $[K(f_1, \ldots, f_n) : K] < \infty$. Now, notice that $f \in K(f_1, \ldots, f_n)[X]$ and θ is a root of f, that is, θ is algebraic over $K(f_1, \ldots, f_n)$, hence the extension $K(f_1, \ldots, f_n, theta)/K(f_1, \ldots, f_n)$ is a simple algebraic extension, hence a finite extension.

Now, we get that

$$[K(f_1, \ldots, f_n, \theta) : K] = [K(f_1, \ldots, f_n, \theta) : K(f_1, \ldots, f_n)] \cdot [K(f_1, \ldots, f_n) : K],$$

where all the numbers on the RHS of the above are finite, so

$$[K(f_1, \ldots, f_n, \theta) : K] < \infty.$$

It follows that the extension is algebraic. The result follows from the fact that $\theta \in K(f_1, \ldots, f_n, \theta)$. □

Exercise 5. Show that if $[L : K] = p$, where p is prime and $K \subseteq F \subseteq L$ are fields, then $F = K$ or $F = L$.

Answer. We have that

$$p = [L : K] = [L : F] \cdot [F : K].$$

Since p is prime, we have that $[L : F] = 1$ or $[F : K] = 1$. The result follows. □

Exercise 6. Determine all the primitive elements of $\mathbb{F}_7$ and $\mathbb{F}_9$.

Answer. We begin with $\mathbb{F}_7$. Since 7 is prime, we have that $\mathbb{F}_7^* = \{1, 2, 3, 4, 5, 6\}$ and there are $\phi(6) = 2$ primitive elements among them. We explicitly check that $\text{ord}(1) = 1$ and $\text{ord}(2) = 3$, so $1, 2$ are not primitive. Then, we check that $\text{ord}(3) > 3$, so (since the order should divide $|\mathbb{F}_7^*| = 6$), $\text{ord}(3) = 6$ and 3 is primitive. The other primitive element is $3^{-1} = 5$.

Now, notice that $9 = 3^2$, so we must first construct $\mathbb{F}_9$. Take α a root of the (irreducible) $X^2 + 1 \in \mathbb{F}_3[X]$. Then $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ and

$$\mathbb{F}_3(\alpha)^* = \{1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}.$$

Now, we have $\phi(8) = 4$ primitive elements. We explicitly check that $1, 2, \alpha$ and 2α are not primitive, so the remaining 4 elements should be all primitive. □

Exercise 7. Find all the subfields of $\mathbb{F}_{5^{20}}$.

Answer. We have that all the subfields of $\mathbb{F}_{5^{20}}$ are of the form $\mathbb{F}_{5^d}$, where $d \mid 20$. Since $5 = 2^2 \cdot 5$, the divisors of 20 are $1, 2, 4, 5, 10, 20$, thus the subfields of $\mathbb{F}_{5^{20}}$ are

$$\mathbb{F}_5, \mathbb{F}_{5^2}, \mathbb{F}_{5^4}, \mathbb{F}_{5^5}, \mathbb{F}_{5^{10}} \text{ and } \mathbb{F}_{5^{20}}.$$ □

Exercise 8. Let $q = p^n$, where p is a prime. Show that the algebraic closure of $\mathbb{F}_q$ is an infinite field of characteristic p.

Answer. Let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. Since $\overline{\mathbb{F}}_q$ is an extension of $\mathbb{F}_q$, we have that $\text{char}\overline{\mathbb{F}}_q = \text{char}\mathbb{F}_q = p$.

Now assume that $\overline{\mathbb{F}}_q$ is finite. It follows that it is a finite extension of $\mathbb{F}_q$. Let n be the degree of this extension. Then $\overline{\mathbb{F}}_q = \mathbb{F}_{q^n}$. However, we know that for every positive integer k, there exists some irreducible polynomial of degree k, hence there exists some $f \in \mathbb{F}_q[X]$ irreducible of degree $n + 1$. If α is a root of f, then, by definition, $\alpha \in \overline{\mathbb{F}}_q = \mathbb{F}_{q^n}$ and $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^{n+1}}$. It follows that $\mathbb{F}_{q^{n+1}} \subseteq \mathbb{F}_{q^n}$, a contradiction. □

Exercise 9. Let $q > 3$ be a prime power. Show that

$$\sum_{a \in \mathbb{F}_q} a^2 = 0.$$

Hint: Prove that

$$\sum_{a \in \mathbb{F}_q} a = 0 \quad \text{and} \quad \sum_{\substack{a,b \in \mathbb{F}_q \\ a \neq b}} ab = 0$$

and combine the above facts.

Answer. We have that

$$X^q - X = \prod_{a \in \mathbb{F}_q} (X - a).$$

Notice that in the LHS of the above, the coefficient of both X^{q-1} and X^{q-2} is zero (since $q > 3$). The corresponding coefficients on the RHS of the above are $\sum_{a \in \mathbb{F}_q} a$ and $\sum_{\substack{a,b \in \mathbb{F}_q \\ a \neq b}} ab$, hence both these sums are zero. Now, using the above, we get that

$$\sum_{a \in \mathbb{F}_q} a^2 = \left(\sum_{a \in \mathbb{F}_q} a \right) \cdot \left(\sum_{b \in \mathbb{F}_q} b \right) - 2 \sum_{\substack{a,b \in \mathbb{F}_q \\ a \neq b}} ab = 0.$$ □