INF 240 - Exercise problems - 7
Solutions

Nikolay Kaleyski

Exercise 1. *Let a be some non-zero element of $\mathbb{F}$. If we multiply all elements of $\mathbb{F}$ by a, we will once again obtain all elements of $\mathbb{F}$ (but in a different order). Formally, this is due to the function $f_a : x \mapsto a \cdot x$ being a permutation, and this is because a has an inverse a^{-1} and so f_a is invertible (that is, if we know that the output of the function is y and we want to find x such that $a \cdot x = y$, we simply have to multiply y by a^{-1}). For example, if we consider $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ and $a = 3$, we get the mapping $x \mapsto 3x$ given in Table 1.*

x	$3x$
0	0
1	3
2	6
3	2
4	5
5	1
6	4

Table 1: Example of a mapping $x \mapsto ax$

Since we get the same set of elements, their sum must also be the same, i.e. for any $a \neq 0$, we have

$$\sum_{x \in \mathbb{F}} x = \sum_{x \in \mathbb{F}} ax.$$

Therefore

$$0 = \sum_{x \in \mathbb{F}} x - \sum_{x \in \mathbb{F}} ax = \sum_{x \in \mathbb{F}} x(1-a) = (1-a) \sum_{x \in \mathbb{F}} x.$$

If $\mathbb{F} \neq \mathbb{F}_2$, we can always select an element a such that $a \neq 0$ and $a \neq 1$. Then $(1-a) \neq 0$, and since finite fields have no zero divisors, the equality $(1-a)\sum_{x \in \mathbb{F}} x = 0$ implies $\sum_{x \in \mathbb{F}} x = 0$.

Exercise 2. *Suppose we have $a^2 + ab + b^2 = 0$. Assume that $b \neq 0$; this will lead us to a contradiction which will prove that $b = 0$ and hence also $a = 0$. If $b \neq 0$, we can divide both sides of the equation by b^2 to get*

$$\left(\frac{a}{b}\right)^2 + \frac{a}{b} + 1 = 0.$$

If we denote $c = a/b$, this becomes

$$c^2 + c + 1 = 0.$$

It is easy to see that the polynomial $f(x) = x^2 + x + 1$ *is irreducible over* $\mathbb{F}_2$ *since* $f(0) = f(1) = 1$ *and hence it has no roots. Since* $\deg(f) = 2$*, its roots lie in the extension field* $\mathbb{F}_{2^2}$*. Thus, if* $f(c) = c^2 + c + 1 = 0$*, i.e. if* c *is a root of* f*, then* c *must be in* $\mathbb{F}_{2^2}$ *(but not in* $\mathbb{F}_2$*). However, this is impossible, since* n *is odd and* $\mathbb{F}_{2^2}$ *is a subfield of* $\mathbb{F}_{2^n}$ *if and only if* 2 *divides* n*, i.e. if* n *is even. We thus get a contradiction with our assumption that* $b \neq 0$*. From* $a^2 + ab + b^2 = 0$ *and* $b = 0$*, we then get* $a^2 = 0$ *which implies* $a = 0$*.*

Exercise 3.

1. *The structure of* $\mathbb{F}_7$ *is simply* $\mathbb{F}_7 = \{0, \ldots, 6\}$*. To check whether some* $a \in \mathbb{F}_7$ *is a primitive element, i.e. to check whether* a *generates the multiplicative group* $\mathbb{F}_7^*$*, we simply keep computing powers* a*,* a^2*,* a^3*, ... of* a *until we loop, and we check to see whether these powers encompass all elements of* $\mathbb{F}_7$*. Clearly,* 1 *cannot generate anything other than itself. For the remaining elements, we get:*

   - $2^0 = 1 \to 2^1 = 2 \to 2^2 = 4 \to 2^3 = 1$;
   - $3^0 = 1 \to 3^1 = 3 \to 3^2 = 2 \to 3^3 = 6 \to 3^4 = 4 \to 3^5 = 5 \to 3^6 = 1$;
   - $4^0 = 1 \to 4^1 = 4 \to 4^2 = 2 \to 4^3 = 1$;
   - $5^0 = 1 \to 5^1 = 5 \to 5^2 = 4 \to 5^3 = 6 \to 5^4 = 2 \to 5^5 = 3 \to 5^6 = 1$;
   - $6^0 = 1 \to 6^1 = 6 \to 6^2 = 1$.

   Thus, 3 *and* 5 *are the primitive elements of* $\mathbb{F}_7$*.*

2. *In the same way as for* $\mathbb{F}_7$*, we find that the primitive elements of* $\mathbb{F}_{17}$ *are* $3, 5, 6, 7, 10, 11, 12, 14$.

3. *Since* $\mathbb{F}_9 = \mathbb{F}_{3^2}$ *is not a prime field, its structure is more complicated and we need an irreducible polynomial to represent its elements. Let us take say* $p(x) = x^2 + x + 2$*, which is easily seen to be irreducible in* $\mathbb{F}_3[x]$ *since it has no roots. Taking* α *to be a root of* $p(x)$*, i.e.* $p(\alpha) = \alpha^2 + \alpha + 2 = 0$*, we want to check whether* α *is a primitive element of* $\mathbb{F}_9$*. To do this, we keep multiplying* α *with itself until we loop; in the multiplication process, we reduce powers* α^k *of* α *with* $k > 1$ *using the identity* $\alpha^2 = -\alpha - 2 = 2\alpha + 1$*. We obtain the following Table 2.*

i	α^i
0	1
1	α
2	$\alpha^2 = 2\alpha + 1$
3	$2\alpha^2 + \alpha = 2(2\alpha + 1) + \alpha = 2\alpha + 2$
4	$2\alpha^2 + 2\alpha = 2(2\alpha + 1) + 2\alpha = 2$
5	2α
6	$2(2\alpha + 1) = \alpha + 2$
7	$\alpha^2 + 2\alpha = 2\alpha + 1 + 2\alpha = \alpha + 1$
8	$\alpha^2 + \alpha = 2\alpha + 1 + \alpha = 1$

Table 2: Generating all elements of $\mathbb{F}_7^*$ as powers of α

Since we obtain 8 distinct elements, we have obtained all non-zero elements of $\mathbb{F}_9$ and have thus generated $\mathbb{F}_9^*$; hence, α is a primitive element.

Since, as we have seen above, all non-zero elements of $\mathbb{F}_9$ can be represented as powers of α, it remains to check whether these remaining powers are primitive elements themselves. We can simplify our work a bit by applying Theorem 2.18 and Corollary 2.19 (as indexed in Lidl & Niederreiter). Since $\mathbb{F}_9 = \mathbb{F}_{3^2}$, we have that $a \in \mathbb{F}_9^*$ is primitive if and only if a^3 is primitive. Thus, we immediately have that α^3 is primitive (applying this again would tell us that α^9 is primitive, but since $\alpha^8 = 1$, this is simply $\alpha^9 = \alpha$). If we consider all powers of α^2, we have $(\alpha^2)^2 = \alpha^4$, $(\alpha^2)^3 = \alpha^6$, and $(\alpha^2)^4 = \alpha^8 = 1$, so that we loop before generating all elements. Thus. α^2 (and also α^6 by Theorem 2.18) is not primitive. Similarly, since $(\alpha^4)^2 = \alpha^8 = 1$, α^4 is not primitive. Finally, for α^5, we have $(\alpha^5)^2 = \alpha^2$, $(\alpha^5)^3 = \alpha^7$, $(\alpha^5)^4 = \alpha^4$, $(\alpha^5)^5 = \alpha$, $(\alpha^5)^6 = \alpha^6$, $(\alpha^5)^2 = \alpha^3$, $(\alpha^6)^6 = 1$. Thus, α^5 is primitive, and so is $(\alpha^6)^3 = \alpha^7$.

Exercise 4. *This can be shown in the same way as in the proof of Theorem 2.8 in Lidl & Niederreiter. Suppose that M is a finite sub-group of the multiplicative group $\mathbb{F}^*$ of some field $\mathbb{F}$, and let $h = p_1^{r_1} \dots p_m^{r_m}$ be its prime factorization. For every i in the range $1 \leq i \leq m$, observe that the polynomial $x^{h/p_i} - 1$ has at most $h/p_i < h$ roots, and so we can pick some $a_i \in M$ which is not a root of that polynomial, i.e. such that $a_i^{h/p_i} \neq 1$. If we take $b_i = a_i^{h/p_i^{r_i}}$, then $b_i^{p_i^{r_i}} = a_i^h = 1$, and thus the order of b_i is a divisor of $p_i^{r_i}$. Since p_i is prime, this divisor can only be of the form $p_i^{s_i}$ for some $s_i \leq r_i$. On the other hand, $b_i^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1$ by the choice of a_i, so that the order of b_i must be precisely $p_i^{r_i}$.*

Having defined such b_i for all i in $1 \leq i \leq m$, we now take $b = b_1 b_2 \dots b_m$, and claim that b generates M. If it does not, then its order must be a divisor of h strictly less than h itself. Thus, the order of b must be a divisor of h/p_i for some i, say of h/p_1. This means that $b^{h/p_1} = b_1^{h/p_1} \dots b_m^{h/p_m} = 1$. For all other i, i.e. for $i \neq 1$, we have that $p_i^{r_i}$ divides h/p_1, and so $b_i^{h/p_i} = 1$. Thus $b_1^{h/p_1} = 1$. But we know that the order of b_1 is $p_1^{r_1}$, and this cannot be a divisor of b_1^{h/p_1} since h/p_1 contains one power of p_1 less in its factorization. We have thus obtained a contradiction to the assumption that the order of b is strictly less than h, and so b must indeed be a generator of M.

Exercise 5. *Suppose $\mathbb{F}^*$ is cyclic and generated by α. Let $\beta = \alpha^{-1}$ be the inverse of this generator. Since F^* is cyclic, there exists some positive integer k such that $\alpha^k = \beta$. Then $\alpha^{k+1} = \alpha \cdot \alpha^{-1} = 1$, so α^{k+1}, α^{k+2}, $\dots$ simply repeats the sequence α, α^2, $\dots$. Therefore, all elements of $\mathbb{F}^*$ can be expressed as powers α^i with $i \leq k$, and since k is a concrete and fixed number, there can only be finitely many elements in $\mathbb{F}^*$.*

Exercise 6. *We know that $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if m divides n, and that all subfields of $\mathbb{F}_{p^n}$ are of this form. Therefore, the subfields of $\mathbb{F}_{5^{42}}$ are precisely all finite fields of the form $\mathbb{F}_{5^m}$ with m dividing 42; thus, we just have to find all the divisors of 42. Since $42 = 2 \cdot 3 \cdot 7$, we can easily see that $K = \{1, 2, 3, 6, 7, 14, 21, 42\}$ are precisely all divisors of 42, and so $\mathbb{F}_{5^k}$ with $k \in K$ are precisely all subfields of $\mathbb{F}_5^{42}$.*