Algebraic Structures

1. The subgroups of $(\mathbb{Z}_{10}, +)$ are $\{\overline{0}\}$, $< \overline{2} >$, $< \overline{5} >$ and $< \overline{1} > = \mathbb{Z}_{10}$. The only subgroups of $(\mathbb{Z}_{11}, +)$ are $\{\overline{0}\}$ and $\mathbb{Z}_{11}$. One has an isomorphism $\mathbb{Z}_{10} \cong \mathbb{Z}_{11}^*$. Since $\overline{2}$ is a generator of $\mathbb{Z}_{11}^*$, the map $f(k \bmod 10) = 2^k \bmod 11$ is an isomorphism. The subgroups of $\mathbb{Z}_{11}^*$ are $\{\overline{1}\}$, $< \overline{4} >$, $< \overline{10} >$ and $< \overline{2} > = \mathbb{Z}_{11}^*$.
2. The possible orders are $1, 2, 3, 6, 9, 18, 27, 54$.
3. Homomorphism: $f(x_1 + x_2) = 5(x_1 + x_2) = 5x_1 + 5x_2 = f(x_1) + f(x_2)$. f is an isomorphism since f has an inverse map $f^{-1}(x) = 4x \bmod 19$.
4. Suppose $m \in \mathbb{Z}_n^*$. Since $\operatorname{ord}(\mathbb{Z}_n^*) = (p-1)(q-1)$, the congruence follows from Euler's Theorem for the group $\mathbb{Z}_n^*$. By reducing modulo p or modulo q, the statement follows for any $m \in \mathbb{Z}_n$.
5. $\operatorname{ord}(\mathbb{Z}_{23}^*) = 22$. We have $2^{11} \bmod 23 \equiv 1$ and hence $\operatorname{ord}(\overline{2}) = 11$. Since $5^{11} \bmod 23 \equiv 22$ and $5^2 \bmod 23 \equiv 2$, we obtain $\operatorname{ord}(\overline{5}) = 22$ (maximal) so that $\overline{5}$ is a generator of $\mathbb{Z}_{23}^*$.
6. $\operatorname{ord}(\overline{2}) = 18$ (a generator of $\mathbb{Z}_{19}^*$) and $\operatorname{ord}(\overline{5}) = 9$ (not a generator).
7. The order of any element in $\mathbb{Z}_n \times \mathbb{Z}_n$ is less than or equal to n. Since $\operatorname{ord}(\mathbb{Z}_n \times \mathbb{Z}_n) = n^2$, this group cannot be cyclic.
8. $\mathbb{Z}_2^3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ and $\mathbb{Z}_8$. Only $\mathbb{Z}_8$ is a cyclic group.
9. $\operatorname{ord}(\mathbb{Z}_{12}^*) = 4$. There is no element of order 4 and therefore $\mathbb{Z}_{12}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. $\operatorname{ord}(\mathbb{Z}_{23}^*) = 22$ and $\mathbb{Z}_{23}^* \cong \mathbb{Z}_{22} \cong \mathbb{Z}_{11} \times \mathbb{Z}_2$ by the Chinese Remainder Theorem.
10. $a \bmod n$ is a generator of the additive group $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$.
11. $p = 13$ and $q = 19$. The Extended Euclidean Algorithm gives $1 = 3p - 2q$ and hence $k = 7 \cdot (-2)q + 2 \cdot 3p = 59$.
12. $(1, 0)$ and $(0, 1)$ are nonzero and not invertible in $R_1 \times R_2$.
13. Since D is linear it suffices to show that $D(x^n x^m) = D(x^n)x^m + x^n D(x^m)$. The left side of this equation is $(n+m)x^{n+m-1}$ and the right side is $nx^{n-1+m} + mx^{n+m-1} = (n+m)x^{n+m-1}$.
14. a) 16 elements. It is not a field since $1 + x^2 + x^4 = (1 + x + x^2)^2$ is reducible in $GF(2)[x]$.
    b) 9 elements. It is a field since $1 + x^2$ is irreducible in $GF(3)[x]$; the polynomial does not have zeros over $GF(3)$.
    c) 2^n elements. It is not a field since $x^n - 1$ is reducible; $x = 1$ is a zero and $(x - 1)$ a linear factor of $x^n - 1$.
15. $x^3 \equiv x + 1$, $x^4 \equiv x^2 + x$, $x^5 \equiv x^2 + x + 1$, $x^6 \equiv x^2 + 1$, $x^7 \equiv 1$ modulo $1 + x + x^3$.
16. For example, $h(x) = 1 + x + x^6$ or $h(x) = 1 + x^3 + x^6$. Both polynomials have no zeros over $GF(2)$. One can manually check that they are not divisible by any polynomial of degree 2 and 3. They are therefore irreducible. We may also use Sage.

```
sage: R.<x> = PolynomialRing(GF(2), 'x')
sage: h=1+x+x^6; h.is_irreducible()
True
sage: h=1+x^3+x^6; h.is_irreducible()
True
```

17. We factorize $x^{256} - x$ over $GF(2)$.

```
sage: R.<x> = PolynomialRing(GF(2), 'x')
sage: R(x^256-x).factor()
x * (x + 1) * (x^2 + x + 1) * (x^4 + x + 1) * (x^4 + x^3 + 1) *
(x^4 + x^3 + x^2 + x + 1) * (x^8 + x^4 + x^3 + x + 1) *
(x^8 + x^4 + x^3 + x^2 + 1) * (x^8 + x^5 + x^3 + x + 1) *
(x^8 + x^5 + x^3 + x^2 + 1) *
(x^8 + x^5 + x^4 + x^3 + 1) *
(x^8 + x^5 + x^4 + x^3 + x^2 + x + 1) *
(x^8 + x^6 + x^3 + x^2 + 1) *
(x^8 + x^6 + x^4 + x^3 + x^2 + x + 1) *
(x^8 + x^6 + x^5 + x + 1) *
(x^8 + x^6 + x^5 + x^2 + 1) * (x^8 + x^6 + x^5 + x^3 + 1) *
(x^8 + x^6 + x^5 + x^4 + 1) *
(x^8 + x^6 + x^5 + x^4 + x^2 + x + 1) *
(x^8 + x^6 + x^5 + x^4 + x^3 + x + 1) *
(x^8 + x^7 + x^2 + x + 1) *
(x^8 + x^7 + x^3 + x + 1) * (x^8 + x^7 + x^3 + x^2 + 1) *
(x^8 + x^7 + x^4 + x^3 + x^2 + x + 1) *
(x^8 + x^7 + x^5 + x + 1) * (x^8 + x^7+ x^5 + x^3 + 1) *
(x^8 + x^7 + x^5 + x^4 + 1) *
(x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1) *
(x^8 + x^7 + x^6 + x + 1) *
(x^8 + x^7 + x^6 + x^3 + x^2 + x + 1) *
(x^8 + x^7 + x^6 + x^4 + x^2 + x + 1) *
(x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1) *
(x^8 + x^7 + x^6 + x^5 + x^2 + x + 1)*
(x^8 + x^7 + x^6 + x^5 + x^4 + x + 1) *
(x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1) *
(x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1)
```

The seventh factor is $x^8 + x^4 + x^3 + x + 1$.

18. The subfields of $GF(2^8)$ are $GF(2^4) = GF(2)[x](x^4 + x + 1)$, $GF(2^2) = GF(2)[x]/(x^2 + x + 1)$ and $GF(2)$.

19. $f(x) = x$, $h(x) = x^7 + x^3 + x^2 + 1$. Then $f(x) \cdot h(x) \equiv x^8 + x^4 + x^3 + x \equiv 1 \bmod (x^8 + x^4 + x^3 + x + 1)$. $h(x)$ corresponds to `8D`.

20. f^{-1} is given by the bit permutation (2 4 1 6 5 7 8 3). The 8×8 matrices A and A^{-1} corresponding to f and f^{-1} have exactly one entry equal to 1 in each row and column and the other entries are 0. The columns are the images of the unit vectors. For example, the first column of A is $(01000000)^T$ and the first column of A^{-1} is $(00100000)^T$.

21. The conjugate transpose of A is

$$A^* = \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}.$$

Since $A^* \cdot A = I_2$, the matrix A is unitary and $A^{-1} = A^*$.

22. f is bijective if and only if A is regular, i.e., an invertible matrix. Then

$$f^{-1}(x) = A^{-1}(x - b) = A^{-1}x - A^{-1}b.$$

23. f is the sum of a $GF(2)$-linear map and a constant translation. The linear map is given by the regular matrix $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$. The constant translation is given by the vector $b = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$. We have $A^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ and
$$f^{-1}(x_1, x_2, x_3) = A^{-1}x - A^{-1}b = (x_1 + x_3,\, x_1 + x_2 + x_3,\, x_1 + x_2 + 1).$$

24. Suppose V and W have the column vectors v_1, v_2, v_3 and w_1, w_2, w_3, respectively. Then $AV = W$ and $A = WV^{-1}$.
$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

25. A $GF(2^8)$-linear map on $V = GF(2^8)$ is a multiplication by an element of $GF(2^8)$ since V has dimension 1 over $GF(2^8)$. Hence there are 256 different $GF(2^8)$-linear maps. On the other hand, a $GF(2)$-linear map on V is given by a 8×8 matrix over $GF(2)$ since V has dimension 8 over $GF(2)$. Such a matrix has 64 binary entries and there are thus 2^{64} different matrices and associated $GF(2)$-linear maps.

26. The adversary chooses $m = 0$. If the oracle returns $c = 0$, then the output is most likely computed by the linear function family F_k. Linear functions map zero to zero whereas the output of a random function (for any input) is almost certainly not zero. Hence the prf-advantage is close to 1.