These excercises are taken from the file Excercises 1.

Let Tr and N denote the trace and norm maps from $\mathbf{F}_{p^m}$ to $\mathbf{F}_p$.
By definition $Tr(x) = \sum_{i=0}^{m-1} \phi^i(x)$ and $N(x) = \prod_{i=0}^{m-1} \phi^i(x)$, where $\phi : \mathbf{F}_{p^m} \longrightarrow \mathbf{F}_{p^m}$ denotes the Frobenius automorphism.

8. (a) *Show that for every $a \in \mathbf{F}_{p^m}$ we have $Tr(a) = a+a^p+...+a^{p^{m-1}}$ and $N(a) = a^{1+p+\dots+p^{m-1}}$.*
   (b) Show that the trace is a surjective homomorphism of additive groups. (Hint: estimate the size of the kernel).
   (c) Show that the Norm map is a surjective homomorphism of multiplicative groups $\mathbf{F}_{p^m}^*$ to $\mathbf{F}_p^*$. (Hint: estimate the size of the kernel).

Sol.: (a) The Frobenius automorphism of $\mathbf{F}_{p^m}$ is given by $\phi(a) = a^p$ and its i^{th} iterate is given by $\phi^i(a) = a^{p^i}$. Now the formulas for Tr and N are immediate. Recall that ϕ generates the automorphism group of $\mathbf{F}_{p^m}$, which is cyclic of order m. Hence $\phi^m = Id$. From this it follows that indeed Tr and N take value in $\mathbf{F}_p$, as $Tr(a)$ and $N(a)$ are fixed by ϕ for all $a \in \mathbf{F}_{p^m}$.
(b) It is easy to check that $Tr\colon \mathbf{F}_{p^m} \to \mathbf{F}_p$ is a linear map of $\mathbf{F}_p$-vector spaces. If $Tr(a) = 0$, then a lies in the set of zeros of a polynomial of degree p^{m-1} in $\mathbf{F}_p[x]$. Such a set has cardinality at most p^{m-1}. Hence $\mathbf{F}_{p^m}/\ker(Tr)$ has cardinality at least $p^m/p^{m-1} = p = \#\mathbf{F}_p$ and Tr is surjective.
(c) It is easy to check that $N\colon \mathbf{F}_{p^m}^* \to \mathbf{F}_p^*$ is a homomorphism of multiplicative groups. Write $N(a) = a^{\frac{1-p^m}{1-p}}$. If $N(a) = 1$, then a lies in the set of zeros of a polynomial of degree $\frac{1-p^m}{1-p}$ in $\mathbf{F}_p[x]$. Such a set has cardinality at most $\frac{1-p^m}{1-p}$. Hence $\mathbf{F}_{p^m}^*/\ker(N)$ has cardinality at least

$$(p^m - 1)/\left(\frac{1-p^m}{1-p}\right) = p - 1 = \#\mathbf{F}_p^*$$

and N is surjective.

Remark. Note that if $\mathbf{F}_{p^n} \cong \mathbf{F}_p[x]/(f)$, with $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ irreducible etc...and $\alpha \in Zero(f)$, then $Tr(\alpha) = -a_{n-1}$ and $N(\alpha) = (-1)^n a_0$.

6. *Let p and r be distinct primes. Show that p is a primitive root modulo $r \Leftrightarrow \Phi_r(x) := \frac{x^r-1}{x-1}$ is irreducible in $\mathbf{F}_p[X]$.*

Sol.: Since p and r are distinct primes, we can apply [MILNE], Lemma 5.9, p.63:
Φ_r is irreducible in $\mathbf{F}_p[x]$ if and only if for any root ζ of Φ_r the degree $[\mathbf{F}_p[\zeta] : \mathbf{F}_p] = \varphi(r) = r - 1$. This means that $r - 1$ is the smallest positive integer d for which ζ lies in $\mathbf{F}_{p^d}$ or, equivalently, the smallest positive integer d for which ζ satisfies $\zeta^{p^d-1} = 1$. Since in addition ζ is primitive r^{th} root of unity (it satisfies $\zeta^r = 1$ and has order r), it follows that $\zeta^{p^d-1} = 1$ if and only if $r \mid p^d - 1$ if and only if $p^d \equiv 1 \bmod r$. In conclusion $r - 1$ the smallest integer d for which $p^d \equiv 1 \bmod r$. This means that p is a primitive root modulo r.

7. *(a) Factor $x^7 - 1$ and $x^{11} - 1$ in $\mathbf{F}_2[x]$.*
   (b) Factor $x^{16} - 1$ and $x^{16} - x$ in $\mathbf{F}_2[x]$.

Sol.: (a) Write

$$x^7 - 1 = (x-1)\frac{x^7-1}{x-1} = (x-1)(x^6 + \ldots + x + 1).$$

Since 2 has order 3 in $\mathbf{Z}_7^*$, by the previous excercise, we know that $\frac{x^7-1}{x-1}$ is not irreducible. Now write

$$x^8 - x = x(x^7 - 1) = x(x-1)(x^6 + \ldots + x + 1).$$

Recall that $\mathbf{F}_{2^3}$ is the splitting field of $x^8 - x$, that $\mathbf{F}_{2^3}$ is a degree three extension of $\mathbf{F}_2$, that it contains no proper subfields other than $\mathbf{F}_2$, and that for every $\alpha \in \mathbf{F}_{2^3} \setminus \mathbf{F}_2$, the subfield $\mathbf{F}_2[\alpha]$ is equal to $\mathbf{F}_{2^3}$ itself. Consequently $x^6 + \ldots + x + 1$ is the product of all irreducible degree 3 polynomials in $\mathbf{F}_2[x]$, namely $x^3 + x^2 + 1$ and $x^3 + x + 1$. In conclusion, in $\mathbf{F}_2[x]$

$$x^7 - 1 = (x-1)(x^3 + x^2 + 1)(x^3 + x + 1).$$

We can reason in a similar way for $x^{11} - 1$:

$$x^{11} - 1 = (x-1)\frac{x^{11}-1}{x-1} = (x-1)(x^{10} + \ldots + x + 1).$$

This time 2 is a primitive root in $\mathbf{Z}_{11}^*$, hence $\frac{x^{11}-1}{x-1}$ is irreducible in $\mathbf{F}_2[x]$ and the above is the complete factorization of $x^{11} - 1$ in $\mathbf{F}_2[x]$.

(b) Over $\mathbf{F}_2$, we have

$$x^{16} - 1 = x^{2^4} - 1 = (x-1)^{2^4}.$$

Recall that $x^{16} - x$ has $\mathbf{F}_{16}$ as its splitting field: the elements of $\mathbf{F}_{16}$ are precisely the zeros of the polynomial $x^{16} - x$.
The field $\mathbf{F}_{16}$ contains $\mathbf{F}_2$, and a field of 4 elements (which is isomorphic to $\mathbf{F}_4$). For every $\alpha \in \mathbf{F}_{16} \setminus \mathbf{F}_4$, the subfield $\mathbf{F}_2[\alpha]$ is equal to $\mathbf{F}_{16}$ itself. Therefore the polynomial $x^{16} - x$ factors into the product of all irreducible polynomials of degree 1, of degree 2, and of degree 4 in $\mathbf{F}_2$. Hence

$$x^{16} - x = x(x-1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1).$$