Some of these excercises are similar to the ones we did today in class. Others will be discussed in the next lectures.

1. Show that in a field of characteristic 3 we have $(x+y)^4 + x^4 + (x-y)^4 + y^4 = 0$.

2. Show that any quadratic polynomial in $\mathbf{Z}_p[x]$ can be written as the product of two linear polynomials with coefficients in $\mathbf{F}_{p^2}$.

3. Prove that $f = x^3 + x^2 + 1$ is irreducible in $\mathbf{Z}_2[x]$. Let $K = \mathbf{Z}_2[x]/(f)$. Show hat K is a field of 8 elements. Show that x generates K^*.

4. Determine $\#\{a \in \mathbf{F}_{16} \ : \ \mathbf{F}_{16} = \mathbf{F}_2(a)\}$ and $\#\{a \in \mathbf{F}_{64} \ : \ \mathbf{F}_{64} = \mathbf{F}_2(a)\}$.

5. Let $\mathbf{F}_q$ be a finite field. Count the number of irreducible polynomials of degree d in $\mathbf{F}_q[X]$ for $d = 1, \ldots, 4$.

6. Let p and r be distinct primes. Show that p is a primitive root modulo r $\Leftrightarrow$ the polynomial $(X^r - 1)/(X-1)$ is irreducible in $\mathbf{F}_p[X]$.

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 $\mathbf{F}_2[X]$.

Let N and Tr denote the norm and trace 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 $N(a) = a^{1+p+\ldots+p^{m-1}}$ and $Tr(a) = a + a^p + \ldots + a^{p^{m-1}}$.
   (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 $\mathbf{F}_{p^m}^*$ to $\mathbf{F}_p^*$. (Hint: estimate the size of the kernel)

9. (a) For which of the following primes p the ring $\mathbf{F}_p[x]/(x^2+1)$ is a field? $p = 3, 5, 7, 11, 13, 19, 23$.
   (b) Show that $x^2 + 1$ is irreducible in $\mathbf{Z}_p[x]$ if and only if $p \equiv 3 \bmod 4$.

10. (a) Show that the squares form subgroup of $\mathbf{F}_q^*$ and that its index is 2 if q is odd and 1 if q is even.
    (b) Show that if $q = 2^k$, then every element of $\mathbf{F}_q$ has a square root in $\mathbf{F}_q$.
    (c) For any $d > 0$, show that the set of d-th powers form subgroup of $\mathbf{F}_q^*$ and that its index is $\gcd(d, q-1)$.

11. (a) Show that x^2+2x+2 is an irreducible polynomial in $\mathbf{F}_3[x]$ and that its roots are generators of the multiplicative group of its splitting field.
    (b) Show that $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbf{F}_2[x]$ but its roots do not generate the multiplicative group of its splitting field.
    (c) Show that the roots of a degree n irreducible polynomial with symmetric coefficients ($a_i = a_{n-i}$, for $1 \leq i \leq n/2$) do not generate the multiplicative group of its splitting field.

12. Let p be a prime and let $a \in \mathbf{F}_p$ be a non-zero element. Show that $x^p - x + a$ is irreducible in $\mathbf{F}_p[x]$. (Hint: if ζ is a root, then so is $\zeta + 1$).

13. Show that if $\mathbf{F}$ is a field whose multiplicative group is cyclic, then $\mathbf{F}$ must be finite.