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

Sol.: From $(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$ and $(x+y)^4 = x^4 - 4x^3y + 6x^2y^2 - 4xy^3 + y^4$, which in charcteristic 3 become $x^4 + x^3y + xy^3 + y^4$ and $x^4 - x^3y - xy^3 + y^4$ respectively, we obtain

$$(x+y)^4 + x^4 + (x-y)^4 + y^4 = 3x^4 + 3y^4 = 0.$$

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

Sol.: Let $f(x) = ax^2 + bx + c$ be a degree 2 polynomial in $\mathbf{F}_p[x]$. If f is reducible in $\mathbf{F}_p[x]$, i.e. the product of two degree 1 polynomials with coefficients in $\mathbf{F}_p$, there is nothing to show since $\mathbf{F}_p \hookrightarrow \mathbf{F}_{p^2}$.
Assume now that f is irreducible and let ζ be one of its roots. Then $\mathbf{F}_p(\zeta)$ is an extension of $\mathbf{F}_p$ of degree 2, and therefore isomorphic to $\mathbf{F}_{p^2}$. It remains to show that the second root of f lies in $\mathbf{F}_p(\zeta)$ as well: this is immediate from the fact the roots of an arbitrary irreducible polynomial in $\mathbf{F}_p[x]$ are obtained from a given root by iterating the Frobenius automorphism. In this case, the second root is $\zeta^p \in \mathbf{F}_p(\zeta)$.

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

Sol.: The polynomial $f(x) = x^3 + x^2 + 1$ is irreducible in $\mathbf{Z}_2[x]$ because it has no zeros in $\mathbf{Z}_2$ (if it were reducible, it would necessarily have a linear factor). The field $\mathbf{F}_8$ is isomorphic to $\mathbf{Z}_2[x]/(f)$, and can be identified with the degree 2 polynomials with coefficients in $\mathbf{Z}_2$

$$0,\ 1,\ x,\ x^2,\ 1+x,\ 1+x^2,\ x+x^2,\ 1+x+x^2,$$

with sum and product modulo f, i.e. using the relation $x^3 = x^2 + 1$. For example

$$(1+x^2)\ +\ (x+x^2) = 1 + x + 2x^2 = 1 + x;$$

$$(1+x)(x+x^2) = x + 2x^2 + x^3 = x - (x^2+1) = x^2 + x + 1;$$

$$(x^2)^2 = x^4 = x(x^3) = x(x^2+1) = x^3 + x = x^2 + x + 1$$

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

Its multiplicative group $\mathbf{F}_8^*$ is cyclic of order 7. Every element, which is not the identity, is a generator of $\mathbf{F}_8^*$. The elements $\{0,\ 1\}$ form the subfield $\mathbf{F}_2 \hookrightarrow \mathbf{F}_8$, which is also the only subfield.
Let's check that x generates $\mathbf{K}^*$:

$$x, \quad x^2, \quad , x^3 = x^2+1, \quad x^4 = x^3+x = x^2+x+1, \quad x^5 = x^3+x^2+x = x+1, \quad x^6 = x^2+x, \quad x^7 = x^3+x^2 = 1.$$

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

Sol.: The first set consists of the elements of $\mathbf{F}_{16}$ minus those in the subfield $\mathbf{F}_{2^2}$: hence it has cardinality $16 - 4 = 12$.

Alternatively: the first set consists of the zeros of degree 4 irreducible polynomials with coefficients in $\mathbf{F}_2$. There are 3 of them. Hence the cardinality of the first set is equal to $3 \times 4 = 12$.

Similarly, the second set consists of the elements of $\mathbf{F}_{64}$ minus those in the subfields $\mathbf{F}_{2^2}$ and $\mathbf{F}_{2^3}$, keeping into account that $\mathbf{F}_{2^2} \cap \mathbf{F}_{2^3} = \mathbf{F}_2$: hence it has cardinality $64 - 4 - 8 + 2 = 54$.

Alternatively: the second set consists of the zeros of degree 6 irreducible polynomials with coefficients in $\mathbf{F}_2$. There are 9 of them. Hence the cardinality of the second set is equal to $9 \times 6 = 54$.

Note that the above sets properly contain the generators of the respective multiplicative groups: given one such a, the field $\mathbf{F}_2(a)$ contains all the powers of a, which fill the non-zero elements in the field.

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

Sol.: The number of irreducible polynomials of degree d in $\mathbf{F}_q[X]$ is $q - 1$ times the number of the monic irreducible polynomials of degree d in $\mathbf{F}_q[X]$.
So we count the *monic* ones: an irreducible polynomial of degree d in $\mathbf{F}_q[X]$ determines a degree d extension $\mathbf{F}_{q^d}$ of $\mathbf{F}_q$. Any zero of one such polynomial lies in $\mathbf{F}_{q^d}$ but in no proper subfield of $\mathbf{F}_{q^d}$. The number of such zeros, divided by the degree, is the number of irreducible monic polynomials of degree d in $\mathbf{F}_q[X]$:

$d = 1$: $\quad \#\{x - b,\ b \in \mathbf{F}_q\} = q$

$d = 2$: $\quad \frac{1}{2}\#(\mathbf{F}_{q^2} \setminus \mathbf{F}_q) = \frac{1}{2}(q^2 - q)$.

$d = 3$: $\quad \frac{1}{3}\#(\mathbf{F}_{q^3} \setminus \mathbf{F}_q) = \frac{1}{3}(q^3 - q)$.

$d = 4$: $\quad \frac{1}{4}\#(\mathbf{F}_{q^4} \setminus \mathbf{F}_{q^2}) = \frac{1}{4}(q^4 - q^2)$.

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 $\mathbf{F}_p[X]$.*

See Solutions of Lecture 2.

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

See Solutions of Lecture 2.

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)

See Solutions of Lecture 2.

9. (a) *For which of the following primes p the ring $\mathbf{F}_p[x]/(x^2+1)$ is a field?* $\quad p = 3,\ 5,\ 7,\ 11,\ 13,\ 19,\ 23.$

(b) Show that x^2+1 is irreducible in $\mathbf{Z}_p[x]$ if and only if $p \equiv 3 \bmod 4$.

Sol.: (a) We can construct a field of p^2 elements by using the polynomial $f(x) = x^2+1$ if and only if f is irreducible in $\mathbf{F}_p[x]$. Since it is quadratic, this is true if and only f has no linear factors, if and only if $f(0), \ldots, f(p-1) \not\equiv 0 \bmod p$.

One can check the values of $f(x) = x^2+1$ on $\mathbf{Z}_p$:

$p = 3$: $f(0) \equiv 1$, $f(1) \equiv 2$, $f(2) \equiv 2$; f irreducible;

$p = 5$: $f(0) \equiv 1$, $f(1) \equiv 2$, $f(2) \equiv 0$. f reducible;

$p = 7$: $f(0) \equiv 1$, $f(1) \equiv f(6) \equiv 2$, $f(2) \equiv f(5) \equiv 5$, $f(3) \equiv f(4) \equiv 3$; f irreducible;

etc...

(b) Proving that f is irreducible in $\mathbf{Z}_p[x]$ if and only if $p \equiv 3 \bmod 4$, is equivalent to proving that f is reducible in $\mathbf{F}_p[x]$ if and only if $p \equiv 1 \bmod 4$.
Indeed f is reducible in $\mathbf{F}_p[x]$ if and only if it has a zero in $\mathbf{Z}_p$ if and only if $x^2 \equiv -1 \bmod p$, which means that -1 is a square modulo p. An element z in the cyclic group $\mathbf{Z}_p^*$ is a square if and only if $z^{(p-1)/2} \equiv 1 \bmod p$. So we have to solve the equation

$$(-1)^{(p-1)/2} \equiv 1 \bmod p, \qquad (*)$$

in p. Recall that -1 has order 2 in $\mathbf{Z}_p^*$, for $p \neq 2$. Hence (*) holds if and only if $(p-1)/2$ is even, if and only if $p \equiv 1 \bmod 4$.

Checking the above list of primes, we find that for p=3, 7, 11, 19, 23 the polynomial x^2+1 is irreducible in $\mathbf{F}_p[x]$, while it is not for p=5,13.

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 $\gcd(d, q-1)$.

Sol.: (a) It is easy to check that the squares form a subgroup of $\mathbf{F}_q^*$.
If p is prime, then $q = p^k$ is odd if and only if p is an odd prime (and even if and only if $q = 2^k$). So assume that $q = p^k$, with p an odd prime, and let a be a primitive root in $\mathbf{F}_q^*$ (we know that $\mathbf{F}_q^*$ is cyclic!). Then $z \in \mathbf{F}_q^*$ is a square if and only if $z^{(q-1)/2} = 1$ if and only if $z = a^{2m}$, for some $m \in \mathbf{Z}$: one implication follows directly from Lagrange Theorem. For the converse, write $z = a^s$, for some integer s. If $z^{(q-1)/2} = (a^s)^{(q-1)/2} = a^{s(q-1)/2} = 1$, then the fact that a is a primitive root forces $s/2$ to be an integer, and s to be even.
Now it is clear that half of the elements in $\mathbf{F}_q^*$ are squares and the squares form a subgroup of index 2 in $\mathbf{F}_q^*$.
(b) Recall that in characteristic 2, $\phi(z) = z^2$ is an automorphism of $\mathbf{F}_{2^k}$, namely the Frobenius automorphism. As ϕ is surjective, every element of $\mathbf{F}_{2^k}$ is a square and therefore admits a square root. In particular the index of the squares in $\mathbf{F}_{2^k}^*$ is 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.

Sol.: (a) The polynomial $f(x) = x^2 + 2x + 2$ is irreducible since it has no zero in $\mathbf{F}_3$. Hence it determines a degree 2 extension of $\mathbf{F}_3$ isomorphic to $\mathbf{F}_3[x]/(x^2 + 2x + 2)$. If α is a root of f, then one can also write $\mathbf{F}_3[x]/(x^2 + 2x + 2) \cong \mathbf{F}_3[\alpha]$. Then α generates the multiplicative group of $\mathbf{F}_3[\alpha]^*$ if and only x generates $\mathbf{F}_3[x]/(x^2+2x+2)$. Computing the powers of x modulo the relation $x^2 = -2x - 2 = x + 1$, we find

$$x, \quad x^2 = x + 1, \quad x^3 = x(x + 1) = 2x + 1, \quad x^4 = x(2x + 1) = 2, \quad x^5 = 2x,$$
$$x^6 = 2x^2 = 2x + 2, \quad x^7 = x(2x + 2) = x + 2, \quad x^8 = x(x + 2) = 1.$$

(b) The polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbf{F}_2[x]$: it has no linear factor nor degree 2 factors. The splitting field of f is $\mathbf{F}_2[x]/(f) = \{ax^3 + bx^2 + cx + d \mid a, b, c, d \in \mathbf{F}_2\} \cong \mathbf{F}_{16}$. Computing the powers of x we find

$$x, \quad x^2, \quad x^3, \quad x^4 = x^3 + x^2 + x + 1, \quad x^5 = x(x^3 + x^2 + x + 1) = x^4 + x^3 + x^2 + x = 1.$$

Hence its roots do not generate the multiplicative group of $\mathbf{F}_{16}^*$.
(c) Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_{n-1}x + 1$ be a degree n symmetric polynomial in $\mathbf{F}_p[x]$, for some prime p. One easily verifies that if α is a root of f, then $\frac{1}{\alpha}$ is a root as well:

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_{n-1}\alpha + 1 = 0 \quad \Leftrightarrow \quad \frac{1}{\alpha^n}(1 + a_{n-1}\alpha + \ldots + \alpha^n) = 0.$$

Recall that the roots of f are of the form α, α^p, $\ldots$, $\alpha^{p^{n-1}}$. Hence $\alpha^{-1} = \alpha^{p^i}$, for $0 \leq i \leq n - 1$. Equivalently, $\alpha^{p^i+1} = 1$ and the order of α in $F_{p^n}^*$ is less or equal than $p^i + 1$, which is strictly smaller than $p^n - 1$.

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 $\zeta + 1$).*

Sol.: Assume that $\zeta^p - \zeta + a = 0$. Since $a \neq 0$, also $\zeta \neq 0$. In $\mathbf{F}_p[x]$, one has

$$(\zeta + 1)^p - (\zeta + 1) + a = \zeta^p + 1 - \zeta - 1 + a = 0.$$

This says that the roots of $\zeta^p - \zeta + a = 0$ are given by

$$\zeta, \quad \zeta + 1, \ldots, \zeta + p - 1.$$

Hence they are all distinct and lie in the same extension of $\mathbf{F}_p$, say a field isomorphic to $\mathbf{F}_{p^k}$, with k a divisor of $p = deg(x^p - x + a)$. But $k > 1$. Therefore $k = p$ and $x^p - x + a$ is necessarily irreducible.

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

Sol.: Fix $a \neq \pm 1$ a generator of $\mathbf{F}^*$. Then $a^m = -a$, for some $m \in \mathbf{Z}$, which implies $a^{2m-2} = 1$.
If $m > 1$, then F^* is finite and also F is finite.
If $m = 1$, then $a = -a \Leftrightarrow 2a = 0 \Leftrightarrow \text{char}(\mathbf{F}) = 2$. Write $a + 1 = a^n$, for some $n \neq 0, 1$. Then a is a zero of the polynomial $f(a) = x^n + x + 1 \in \mathbf{Z}_2[x]$.
Consider the map

$$\psi\colon \mathbf{F}_2[x]/(x^n + x + 1) \to \mathbf{F}, \quad \bar{f}(x) \mapsto \bar{f}(a).$$

Since $\mathbf{F}^*$ is cyclic, the map

$$\mathbf{F}_2[x] \to \mathbf{F}, \quad f(x) \mapsto f(a)$$

is surjective and its kernel contains the ideal (x^n+x+1). Then it factors through $\mathbf{F}_2[x]/(x^n+x+1)$. Consequently also ψ is surjective. Since $\mathbf{F}_2[x]/(x^n + x + 1)$ is finite, so is $\mathbf{F}$.