Now, an important comment about counting the number of irreducible polynomials.

Remark 5: As Theorem 9 shows us, $x^{p^n} - x$ is the product of all the irreducible polynomials over $\mathbb{F}_p$ of degree d, taken over all the divisors d of n. If $N(d)$ denotes the number of irreducible polynomials of degree d over $\mathbb{F}_p$, then on comparing degrees we get

$$p^n = \sum_{d \mid n} d\, N(d).$$

Using this equation, we can recursively determine the numbers $N(d)$.

Let us consider some examples of the application of Theorem 9 and Remark 5.

Example 7: Find all the irreducible polynomials over $\mathbb{F}_2$ with roots in $\mathbb{F}_4$.

Solution: You know that $\mathbb{F}_4$ is the splitting field of $x^4 - x$ over $\mathbb{F}_2$, and has the factorisation $x^4 - x = x(x-1)(x^2 + x + 1)$.
Here the factors x and $x-1$ are distinct irreducible polynomials over $\mathbb{F}_2$ of degree 1, corresponding to the divisor 1 of 2.
The factor $x^2 + x + 1$ is the irreducible polynomial of degree 2 over $\mathbb{F}_2$, corresponding to the divisor 2 of 2.

***

Example 8: Obtain all the irreducible polynomials over $\mathbb{F}_2$, which divide $x^8 - x$. Hence obtain all the elements of $\mathbb{F}_8$.

Solution: As in Example 7, x and $(x-1)$ are the two irreducible polynomials over $\mathbb{F}_2$ of degree 1. Since $|\mathbb{F}_8| = 2^3$, any other irreducible polynomials have to be of degree 3.
By Remark 5, $2^3 = N(1) + 3N(3)$, and you know that $N(1) = 2$. Hence, $N(3) = 2$.
Therefore, $x^8 - x$ has two irreducible cubic factors.
Now $x^8 - x = x(x-1)(x^6 + x^5 + \cdots + x + 1)$.
You can check that $x^6 + x^5 + \cdots + x + 1$ is factored over $\mathbb{F}_2$ as $(x^3 + x^2 + 1)(x^3 + x + 1)$. You should also verify that both these cubic factors are irreducible over $\mathbb{F}_2$. So their roots are the elements of $\mathbb{F}_8 \setminus \{0, 1\}$.
Suppose α is a root of $x^3 + x^2 + 1$. Then $\{1, \alpha, \alpha^2\}$ is an $\mathbb{F}_2$-basis of $\mathbb{F}_8$. So $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$. Note that $\alpha^3 + \alpha^2 + 1 = 0$.

***

Example 9: Write $x^{16} - x$ as a product of distinct irreducible polynomials over $\mathbb{F}_2$.

Solution: $\mathbb{F}_{2^4}$ is the splitting field of $x^{16} - x$ over $\mathbb{F}_2$. As $[\mathbb{F}_{2^4} : \mathbb{F}_2] = 4$, an irreducible factor of $x^{16} - x$ can have degree 1, 2 or 4. Now, the only linear factors possible over $\mathbb{F}_2$ are x and $x-1$. Also

$$x^{16} - x = x(x^{15} - 1) = x(x^5 - 1)(x^{10} + x^5 + 1)$$
$$= x(x-1)(x^4 + x^3 + x^2 + x + 1)(x^{10} + x^5 + 1).$$

Since the polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$ has no roots in $\mathbb{F}_2$, it is either irreducible over $\mathbb{F}_2$ or has an irreducible factor of degree 2. But the only irreducible polynomial of degree 2 over $\mathbb{F}_2$ is $x^2 + x + 1$, which does not divide $f(x)$. So $f(x)$ must be irreducible over $\mathbb{F}_2$.

On dividing $x^{10} + x^5 + 1$ by $x^2 + x + 1$, we have the factorisation

$$x^{10} + x^5 + 1 = (x^2 + x + 1)(x^8 + x^7 + x^5 + x^4 + x^3 + x + 1). \quad \ldots(3)$$

On adding $2x^4 (= 0 \text{ in } \mathbb{F}_2)$ to the second factor on the right hand side of (3), we get

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

Arguing as before, you can check that both the factors on the right hand side of (4) are irreducible over $\mathbb{F}_2$. Hence, the irreducible factorisation of $x^{16} - x$ over $\mathbb{F}_2$ is $x(x-1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x + 1)$.

***

Try some exercises now.

E12) Write $x^{27} - x$ as a product of irreducible factors over $\mathbb{F}_3$. Is this also the irreducible factorisation over $\mathbb{Q}$ of $x^{27} - x$? Give reasons for your answer.

E13) With reference to Example 8, let $K = \mathbb{F}_2(\alpha)$ and $L = \mathbb{F}_2(\beta)$, where β is a root of $x^3 + x + 1$. Give an explicit isomorphism from K to L.

E14) i) Show that $x^p - x - a$ is irreducible over $\mathbb{F}_p$, where $a \neq 0$.

ii) Show that $x^p - x - a$ is irreducible over $\mathbb{F}_{p^n}$, $n \geq 1$, iff it has no linear factor.

With this we come to the end of this discussion on finite (splitting) fields and irreducible polynomials over $\mathbb{F}_p$. Let us take a brief look at what you have studied in this unit.

12.5 SUMMARY

In this unit, we have covered the following points.

1. The existence, and uniqueness, of a splitting field of a given polynomial over a given field.

2. Every finite field is a splitting field over $\mathbb{F}_p$, for some prime p.

3. For every prime p, and $n \in \mathbb{N}$, there is a unique field (up to isomorphism) of order p^n, which is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. These are the only finite fields.

4. How to explicitly construct a finite field of order p^n.

5. Every finite extension of a finite field is simple.

6. $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ iff $m \mid n$.

7. Given a prime p and $n \in \mathbb{N}$, there is an irreducible polynomial of degree d over $\mathbb{F}_{p^n}$ $\forall\, d \in \mathbb{N}$.

8. Given a prime p and $n \in \mathbb{N}$, $x^{p^n} - x$ is the product of all the distinct irreducible polynomials over $\mathbb{F}_p$ of degree d, where d varies over all the divisors of n.

9. $p^n = \sum_{d \mid n} d\, N(d)$, where $N(d)$ is the number of irreducible polynomials of degree d over $\mathbb{F}_p$.

12.6 SOLUTIONS / ANSWERS

E1) Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ be two arbitrary polynomials over k. We can assume, without loss of generality, that $n \le m$. Then

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_m x^m$$

and

$$f(x)g(x) = (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + \cdots + \left(\sum_{i+j=k} a_i b_j\right)x^k + \cdots + (a_n b_m)x^{n+m}.$$

Now, on applying $\tilde{\sigma}$, we get

$$\tilde{\sigma}(f(x) + g(x))$$
$$= \sigma(a_0 + b_0) + \sigma(a_1 + b_1)x + \cdots + \sigma(a_n + b_n)x^n + \sigma(b_{n+1})x^{n+1} + \cdots + \sigma(b_m)x^m$$
$$= (\sigma(a_0) + \sigma(b_0)) + (\sigma(a_1) + \sigma(b_1))x + \cdots + (\sigma(a_n) + \sigma(b_n))x^n + \cdots + \sigma(b_m)x^m$$
$$= [\sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n] + [\sigma(b_0) + \sigma(b_1)x + \cdots + \sigma(b_m)x^m]$$
$$= \tilde{\sigma}(f(x)) + \tilde{\sigma}(g(x)),$$

and

$$\tilde{\sigma}(f(x)g(x))$$
$$= \sigma(a_0 b_0) + \sigma(a_0 b_1 + a_1 b_0)x + \cdots + \sigma\left(\sum_{i+j=k} a_i b_j\right)x^k + \cdots + \sigma(a_n b_m)x^{n+m}$$
$$= \sigma(a_0)\sigma(b_0) + (\sigma(a_0)\sigma(b_1) + \sigma(a_1)\sigma(b_0))x + \cdots + \left(\sum_{i+j=k} \sigma(a_i)\sigma(b_j)\right)x^k + \cdots + \sigma(a_n)\sigma(b_m)x^{n+m}$$

$= [\sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n][(\sigma(b_0) + \sigma(b_1)x + \cdots + \sigma(b_m)x^m]$
$= \tilde{\sigma}(f(x))\tilde{\sigma}(g(x)).$
Thus, $\tilde{\sigma}$ is a ring homomorphism.

Next, if $\tilde{\sigma}(f(x)) = \tilde{\sigma}(g(x))$, then
$\tilde{\sigma}(a_0 + a_1x + \cdots + a_nx^n) = \tilde{\sigma}(b_0 + b_1x + \cdots + b_mx^m)$
$\Rightarrow \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n = \sigma(b_0) + \sigma(b_1)x + \cdots + \sigma(b_m)x^m$
$\Rightarrow n = m,$ and $\sigma(a_i) = \sigma(b_i)\ \forall\ i \in \{0, 1, \ldots, n\}.$
Since σ is one-one on k and $a_i, b_i \in k$, $a_i = b_i\ \forall$ i.
$\therefore f(x) = g(x)$
$\therefore \tilde{\sigma}$ is 1-1.

To show surjectivity, let $f'(x) = a'_0 + a'_1x + \cdots + a'_nx^n$ be an arbitrary polynomial in $k'[x]$. Since $a'_0, a'_1, \ldots, a'_n \in k'$ and $\sigma : k \to k'$ is surjective, there exist $a_0, a_1, \ldots, a_n \in k$ such that $\sigma(a_i) = a'_i$, $0 \le i \le n$.
Thus, $\exists\ f(x) = a_0 + a_1x + \cdots + a_nx^n \in k[x]$ such that
$\tilde{\sigma}(f(x)) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n = f'(x).$

Finally, let $f(x)$ be an irreducible polynomial over k and assume that its image $f'(x) = \tilde{\sigma}(f(x))$ is reducible over k'. Then there exist non-constant polynomials $g'(x), h'(x) \in k'[x]$ such that $f'(x) = g'(x)h'(x)$.
By the surjectivity of $\tilde{\sigma}$ on $k[x]$, there exist $g(x), h(x) \in k[x]$ such that $\tilde{\sigma}(g(x)) = g'(x)$ and $\tilde{\sigma}(h(x)) = h'(x)$.
Since σ preserves degree, $g(x)$ and $h(x)$ must be non-constant. Also
$\tilde{\sigma}(f(x)) = f'(x) = g'(x)h'(x) = \tilde{\sigma}(g(x))\tilde{\sigma}(h(x))$
$\Rightarrow f(x) = g(x)h(x)$, as $\tilde{\sigma}$ is 1-1.
This contradicts the irreducibility of $f(x)$.
Hence $f'(x)$ is irreducible in $k'[x]$.

E2) Let $f(x), g(x) \in k[x]$ have a common factor over some extension field F of k. Suppose they are relatively prime in $k[x]$, then there exist polynomials $a(x), b(x)$ in $k[x]$ such that $a(x)f(x) + b(x)g(x) = 1$. Since $k \subseteq F$, this relation will also hold over F, i.e., $f(x)$ and $g(x)$ must be relatively prime in $F[x]$, which is a contradiction.
Hence $f(x)$ and $g(x)$ have a common factor over k also.

E3) i) The roots of $f(x)$ are $2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2, \omega, \omega^2$, where ω is a non-real cube root of unity.
Thus, the splitting field of $f(x)$ over $\mathbb{Q}$ is
$\mathbb{Q}(2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2, \omega, \omega^2) = \mathbb{Q}(2^{1/3}, \omega).$

ii) $\mathbb{Q}(5^{1/3}, 5^{1/3}\omega, 5^{1/3}\omega^2) = \mathbb{Q}(5^{1/3}, \omega).$

iii) The roots of $f(x)$ are $1 + \omega, 1 + \omega^2 \in \mathbb{Q}(\omega)$.
Hence $\mathbb{Q}(\omega)$ is the splitting field over itself.

iv) Over $\mathbb{Z}_2$, $x^6+1 = x^6-1 = (x^3-1)^2 = (x+1)^2(x^2+x+1)^2$.
The roots are $1, 1, \alpha, \alpha, 1+\alpha, 1+\alpha$, where α is a root of the irreducible polynomial x^2+x+1 over $\mathbb{Z}_2$.
Hence, the splitting field of $f(x)$ over $\mathbb{Z}_2$ is $\mathbb{Z}_2(\alpha)$.

E4) i) The splitting field of x^2+1 over $\mathbb{Q}$ is $\mathbb{Q}(i)$, which is a degree 2 extension of $\mathbb{Q}$.

ii) The polynomial $f(x) = x^4+x^2+1$ factors over $\mathbb{Q}$ as $x^4+x^2+1 = (x^2+1)^2 - x^2 = (x^2-x+1)(x^2+x+1)$, so that the roots of $f(x)$ are $\pm\omega, \pm\omega^2$. Hence the splitting field of x^4+x^2+1 over $\mathbb{Q}$ is $\mathbb{Q}(\omega, \omega^2) = \mathbb{Q}(\omega)$, which is a degree 2 extension of $\mathbb{Q}$, since ω satisfies the irreducible polynomial x^2+x+1 over $\mathbb{Q}$.

iii) The splitting field of x^4+2 over $\mathbb{Q}$ is $\mathbb{Q}(2^{1/4}, i)$. Now, $[\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}] = [\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}(2^{1/4})][\mathbb{Q}(2^{1/4}) : \mathbb{Q}] = 2\times 4 = 8$, since i satisfies the irreducible polynomial $x^2+1 \in \mathbb{Q}(2^{1/4})$ and $2^{1/4}$ satisfies the irreducible polynomial $x^4+2 \in \mathbb{Q}$ (irreducible by Eisenstein's criterion).
Hence $4 < [\mathbb{Q}(2^{1/4}, i) : \mathbb{Q}] < 4!$.

iv) Consider the polynomial $f(x) = x^3-2$. You can check it is irreducible over $\mathbb{Q}$. Its roots are $2^{1/3}$, $2^{1/3}\omega$, $2^{1/3}\omega^2$. So the splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(2^{1/3}, \omega)$. Hence, $[\mathbb{Q}(2^{1/3}, \omega) : \mathbb{Q}] = [\mathbb{Q}(2^{1/3})(\omega) : \mathbb{Q}(2^{1/3})][\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 2\cdot 3 = 6 = 3!$.

E5) Let F be a finite field. The multiplicative group $F^* = F\setminus\{0\}$ is a finite group of order p^n-1. So $a^{p^n-1} = 1$ for every non-zero element a in F. Therefore, the polynomial $x^{p^n}-x$ has p^n distinct roots in F. Hence the field F is the splitting field of $f(x)$ over $\mathbb{F}_p$.

E6) i) The field is $\mathbb{F}_9$, the splitting field of x^9-x, over $\mathbb{F}_3$.
Now $x^9-x = x(x-1)(x^7+x^6+\cdots+x+1)$
$= x(x-1)(x-2)(x^2+1)(x^2-x-1)(x^2+x-1)$ as a product of irreducible polynomials over $\mathbb{Z}_3$.
If α is a root of x^2+1 over $\mathbb{Z}_3$, then $\{1, \alpha\}$ is an $\mathbb{F}_3$-basis of $\mathbb{F}_9$.
So $\mathbb{F}_9 = \{0, 1, 2, \alpha, 2\alpha, 1+\alpha, 1+2\alpha, 2+\alpha, 2+2\alpha\}$.

ii) $0, 1, 2$ satisfy $x, x-1, x-2$, respectively.
$\alpha, 2\alpha$ satisfy x^2+1,
$1+\alpha, 1+2\alpha$ satisfy x^2+x-1
$2+\alpha, 2+2\alpha$ satisfy x^2-x-1.

E7) Let $|K| = p^n$. Then $x^{p^n-1}-1 = \prod_{\alpha_i \in K^*}(x-\alpha_i)$.

Putting $x = 0$ in this gives $(-1)^{p^n-1}\left(\prod_i \alpha_i\right) = -1.$

For $p \neq 2$, $p^n - 1$ is even, and hence the result.
If $p = 2$, $-1 = 1$, and hence the result.

E8) $3 \in \mathbb{F}_{13}^*$. Hence, $3^{12} = 1$, so that $3^{13} = 3$.
Thus, 3 is a 13^{th} root of 3 in $\mathbb{F}_{13}$.

E9) From E6, you see that $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$, where $\alpha^2 + 1 = 0$.
Thus, α is one primitive element.
Similarly, you can check that $\mathbb{F}_9 = \mathbb{F}_3(\beta)$, where $\beta = 1 + \alpha$.
Clearly, $\beta \neq \alpha$.

E10) Let $n = km + r, 0 \leq r < m$. Then

$$x^n - 1 = x^r(x^m)^k - 1 = x^r(x^{mk} - 1) + (x^r - 1)$$
$$= x^r(x^m - 1)\left(\sum_{i=0}^{k-1} x^{im}\right) + (x^r - 1).$$

Therefore, $x^m - 1$ divides $x^n - 1$ iff $x^r - 1 = 0$, i.e., iff $r = 0$, i.e., iff m divides n. On taking $x = p$, a prime number, we have $p^m - 1$ divides $p^n - 1$ if and only if m divides n.
Thus, $x^{p^m} - x$ divides $x^{p^n} - x$ iff $x^{p^m-1} - 1$ divides $x^{p^n-1} - 1$ iff $p^m - 1$ divides $p^n - 1$ iff m divides n.

E11) Since both the fields $\mathbb{F}_{p^8}, \mathbb{F}_{p^{12}}$ have characteristic p, they have the same prime field, $\mathbb{F}_p$. Now, by Theorem 7, $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if m divides n.
Therefore $\mathbb{F}_p, \mathbb{F}_{p^2}, \mathbb{F}_{p^4}$ are the only proper subfields of $\mathbb{F}_{p^8}$, corresponding to the divisors 1, 2 and 4 of 8.
Similarly, as 1, 2, 4 and 6 are the only divisors of 12, $\mathbb{F}_p, \mathbb{F}_{p^2}, \mathbb{F}_{p^4}, \mathbb{F}_{p^6}$ are the proper subfields of $\mathbb{F}_{p^{12}}$.

E12) $\mathbb{F}_{3^3}$ is the splitting field of $x^{27} - x$ over $\mathbb{F}_3$.
$x, x-1, x-2$ are the only linear factors, corresponding to the divisor 1 of 3. So $N(1) = 3$.
Now, by Theorem 9, any other irreducible factor has to be of degree 3.
Also, by Remark 5, $3^3 = N(1) + 3N(3)$, so that $N(3) = 8$.
Hence, we need to find 8 cubic irreducible polynomials over $\mathbb{F}_3$, with their roots in $\mathbb{F}_{27}$. You should check that these are
$x^3 + x + 1, x^3 - x + 1, x^3 + x - 1, x^3 - x - 1, x^3 + x^2 + 1, x^3 - x^2 + 1,$
$x^3 + x^2 - 1, x^3 - x^2 - 1.$
Thus, $x^{27} - x$ is the product of these 8 cubic polynomials and the 3 linear polynomials.

Over $\mathbb{Q}$, $x^{27} - x = x(x^{13} - 1)(x^{13} + 1)$

$= x(x-1)(x+1)(x^{12} + x^{11} + \cdots + x + 1)(x^{12} - x^{11} + x^{10} - \cdots - x + 1)$ …(5)

From Example 11, Unit 9, you know that $x^{12} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$. By a similar argument to that in the example, you can check that $x^{12} - x^{11} + x^{10} - \cdots + x^2 - x + 1$ is irreducible over $\mathbb{Q}$. Hence, the factorisation in (5) above is the required one, which is very different from the factorisation over $\mathbb{F}_3$.

E13) Since $\beta = 1 + \alpha$, $K = L$. Thus, the identity map is an explicit isomorphism from K to L.

E14) i) Let $f(x) = x^p - x - a$, $a \neq 0$. For any $b \in \mathbb{F}_p$, $b^p = b$. Therefore, $f(b) = b^p - b - a = -a \neq 0$, i.e., $f(x)$ has no roots in $\mathbb{F}_p$. So $f(x)$ has no linear factors over $\mathbb{F}_p$. Moreover, if α is a root of $f(x)$ in some extension of $\mathbb{F}_p$, then so is $\alpha + i$ for every $i \in \{0, 1, \ldots, p-1\}$.

So $f(x) = \prod_{i=0}^{p-1} [x - (\alpha + i)]$ in the splitting field K of $f(x)$.

Now, if $p(x)$ is an irreducible factor of $f(x)$ over $\mathbb{F}_p$ of degree m, then $p(x) \mid f(x)$.

$\therefore p(x) = (x - \alpha - i_1)(x - \alpha - i_2)\cdots(x - \alpha - i_m)$ in K.

But $p(x) \in \mathbb{F}_p[x]$, so that the coefficient of x^{m-1} belongs to $\mathbb{F}_p$,

i.e., $\sum_{k=0}^{m} (\alpha - i_k) \in \mathbb{F}_p$, i.e., $m\alpha - \sum_{k=0}^{m} i_k \in \mathbb{F}_p$.

As $\sum_{k=0}^{m} i_k \pmod p \in \mathbb{F}_p$. So $m\alpha \in \mathbb{F}_p$. Since $0 < m < p$, m and p are coprime. So $m^{-1} \in \mathbb{F}_p$, and hence $\alpha \in \mathbb{F}_p$, which contradicts the fact that $f(x)$ has no linear factor over $\mathbb{F}_p$.

ii) The second part follows on similar lines as (i) above.