School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet V: Finite Fields (Solutions)

1. **(a) Find an irreducible polynomial of degree 3 over $\mathbb{F}_2$ and hence construct the addition and multiplication tables of the field $\mathbb{F}_8$ of order 8.**

   (b) Find an irreducible polynomial of degree 2 over $\mathbb{F}_3$ and hence construct the addition and multiplication tables of the field $\mathbb{F}_9$ of order 9.

Solution: (a) Let $f(X) = X^3 + X + 1$. Then

$$f(0) = 1 \qquad \text{and} \qquad f(1) = 1,$$

so $f(X)$ has no roots in $\mathbb{F}_2$, hence no linear factors over $\mathbb{F}_2$, and therefore $f(X)$ is irreducible over $\mathbb{F}_2$. Adjoin a root α to $\mathbb{F}_2$ to construct the field $\mathbb{F}_2(\alpha)$ with $|\mathbb{F}_2(\alpha) : \mathbb{F}_2| = 3$. Therefore $|\mathbb{F}_2(\alpha)| = 8$ and so $\mathbb{F}_2(\alpha) \cong F_8$. Then $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{F}_2(\alpha)$ over $\mathbb{F}_2$ and the eight elements are

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

Then the addition table is constructed from the vector space structure of $\mathbb{F}_2(\alpha)$ and is:

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

We calculate products by exploiting the fact that $f(\alpha) = 0$; that is,

$$\alpha^3 = -(\alpha+1) = \alpha+1.$$

Products involving 0, 1, α and $\alpha+1$ are straightforward. The others are as follows:

$$\begin{aligned}
\alpha \cdot \alpha^2 &= \alpha^3 = \alpha+1 \\
\alpha(\alpha^2+1) &= \alpha^3 + \alpha = (\alpha+1) + \alpha = 1 \\
\alpha(\alpha^2+\alpha) &= \alpha^3 + \alpha^2 = (\alpha+1) + \alpha^2 = \alpha^2+\alpha+1 \\
\alpha(\alpha^2+\alpha+1) &= \alpha^3 + \alpha^2 + \alpha = (\alpha+1) + \alpha^2 + \alpha = \alpha^2+1 \\
(\alpha+1)\alpha^2 &= \alpha^3 + \alpha^2 = \alpha^2+\alpha+1 \\
(\alpha+1)(\alpha^2+1) &= \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^2 \\
(\alpha+1)(\alpha^2+\alpha) &= \alpha^3 + \alpha = (\alpha+1) + \alpha = 1
\end{aligned}$$

$$
\begin{aligned}
(\alpha+1)(\alpha^2+\alpha+1) &= \alpha^3+1 = (\alpha+1)+1 = \alpha \\
\alpha^2\cdot\alpha^2 &= \alpha^4 = \alpha(\alpha+1) = \alpha^2+\alpha \\
\alpha^2(\alpha^2+1) &= \alpha^4+\alpha^2 = (\alpha^2+\alpha)+\alpha^2 = \alpha \\
\alpha^2(\alpha^2+\alpha) &= \alpha^4+\alpha^3 = (\alpha^2+\alpha)+(\alpha+1) = \alpha^2+1 \\
\alpha^2(\alpha^2+\alpha+1) &= \alpha^4+\alpha^3+\alpha^2 = (\alpha^2+\alpha)+(\alpha+1)+\alpha^2 = 1 \\
(\alpha^2+1)^2 &= \alpha^4+1 = \alpha^2+\alpha+1 \\
(\alpha^2+1)(\alpha^2+\alpha) &= \alpha^4+\alpha^3+\alpha^2+\alpha = (\alpha^2+\alpha)+(\alpha+1)+\alpha^2+\alpha = \alpha+1 \\
(\alpha^2+1)(\alpha^2+\alpha+1) &= \alpha^4+\alpha^3+\alpha+1 = (\alpha^2+\alpha)+(\alpha+1)+\alpha+1 = \alpha^2+\alpha \\
(\alpha^2+\alpha)^2 &= \alpha^4+\alpha^2 = (\alpha^2+\alpha)+\alpha^2 = \alpha \\
(\alpha^2+\alpha)(\alpha^2+\alpha+1) &= \alpha^4+\alpha = (\alpha^2+\alpha)+\alpha = \alpha^2
\end{aligned}
$$

and

$$(\alpha^2+\alpha+1)^2 = \alpha^4+\alpha^2+1 = (\alpha^2+\alpha)+\alpha^2+1 = \alpha+1.$$

Hence the multiplication table of $\mathbb{F}_2(\alpha)$ is:

$\times$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

(b) Let $f(X) = X^2+1$. Then

$$f(0)=1, \qquad f(1)=2, \qquad f(2)=2,$$

so $f(X)$ has no roots in $\mathbb{F}_3$, hence no linear factors over $\mathbb{F}_3$ and therefore $f(X)$ is irreducible over $\mathbb{F}_3$. Adjoin a root α to $\mathbb{F}_3$ to construct the field $\mathbb{F}_3(\alpha)$ with $|\mathbb{F}_3(\alpha):\mathbb{F}_3| = 2$. Therefore $|\mathbb{F}_3(\alpha)| = 9$ and so $\mathbb{F}_3(\alpha) \cong \mathbb{F}_9$. Then $\{1,\alpha\}$ is a basis for $\mathbb{F}_3(\alpha)$ over $\mathbb{F}_3$ and the addition table of $\mathbb{F}_3(\alpha)$ is determined by the vector space structure:

$+$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	0	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α
2	2	0	1	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$
α	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$	0	1	2
$\alpha+1$	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α	1	2	0
$\alpha+2$	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1
2α	2α	$2\alpha+1$	$2\alpha+2$	0	1	2	α	$\alpha+1$	$\alpha+2$
$2\alpha+1$	$2\alpha+1$	$2\alpha+2$	2α	1	2	0	$\alpha+1$	$\alpha+2$	α
$2\alpha+2$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1	$\alpha+2$	α	$\alpha+1$

The multiplication table is determined by $f(\alpha) = 0$; that is, $\alpha^2 = -1 = 2$. Hence we obtain:

$\times$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	2	$\alpha+2$	$2\alpha+2$	1	$\alpha+1$	$2\alpha+1$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$\alpha+2$	2α	1	$2\alpha+1$	2	α
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$2\alpha+2$	1	α	$\alpha+1$	2α	2
2α	0	2α	α	1	$2\alpha+1$	$\alpha+1$	2	$2\alpha+2$	$\alpha+2$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$\alpha+1$	2	2α	$2\alpha+2$	α	1
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$2\alpha+1$	α	2	$\alpha+2$	1	2α

2. **Let $F \subseteq K$ be an extension of finite fields.**
   - **(a) Show that K is a normal extension of F.**
   - **(b) Show that K is a separable extension of F.**

Solution: Throughout assume that F and K have characteristic p, with prime subfield $\mathbb{F}_p$ satisfying

$$\mathbb{F}_p \subseteq F \subseteq K.$$

Let $K \cong \mathbb{F}_{p^n}$ for some positive integer n.

(a) By our construction, K is the splitting field for $X^{p^n} - X$ over $\mathbb{F}_p$; it is therefore also the splitting field for $X^{p^n} - X$ over F. Hence K is a normal extension of F.

(b) Let $\alpha \in K$ and let $f(X)$ be the minimum polynomial of α over F. Now $\alpha^{p^n} - \alpha = 0$, so $f(X)$ divides $X^{p^n} - X$. The latter has distinct roots in K (in which it splits), namely the p^n elements of K. Thus $f(X)$ also has distinct roots in K (in which $f(X)$ splits). We conclude $f(X)$ is separable and hence K is a separable extension of F.

3. **Consider the Galois field $\mathbb{F}_{p^n}$ for order p^n where p is a prime number and n is a positive integer.**
   - **(a) If F is a subfield of $\mathbb{F}_{p^n}$, show that $F \cong \mathbb{F}_{p^d}$ for some divisor d of n. [Hint: Recall $|\mathbb{F}_{p^n} : \mathbb{F}_p| = n$.]**
   - **(b) Suppose that d is a divisor of n.**
     - **(i) Set $k = n/d$, $r = \sum_{i=0}^{k-1} p^{id} = (p^n - 1)/(p^d - 1)$ and**

       $$g(X) = \sum_{i=1}^{r} X^{p^n - i(p^d-1)-1}.$$

       Show that

       $$g(X)\,(X^{p^d} - X) = X^{p^n} - X.$$

     - **(ii) Show that $\mathbb{F}_{p^n}$ contains precisely p^d roots of $X^{p^d} - X$.**
     - **(iii) Show that $L = \{\, a \in \mathbb{F}_{p^n} \mid a^{p^d} = a \,\}$ is a subfield of $\mathbb{F}_{p^n}$ of order p^d.**
   - **(c) Conclude that $\mathbb{F}_{p^n}$ has a unique subfield of order p^d for each divisor d of n.**

Solution: (a) Let F be a subfield of $\mathbb{F}_{p^n}$. Then $\mathbb{F}_p \subseteq F \subseteq \mathbb{F}_{p^n}$, so F is a finite field of characteristic p, so $F \cong \mathbb{F}_{p^d}$ for some positive integer d. The Tower Law tells us $|F : \mathbb{F}_p| = d$ divides $|\mathbb{F}_{p^n} : \mathbb{F}_p| = n$. Hence $F \cong \mathbb{F}_{p^d}$ for some divisor d of n.

(b) Let d be a divisor of n.

(i) Put $k = n/d$,

$$r = \sum_{i=0}^{k-1} p^{id} = \frac{(p^d)^k - 1}{p^d - 1} = \frac{p^n - 1}{p^d - 1},$$

by the formula for a geometric progression, and

$$g(X) = \sum_{i=1}^{r} X^{p^n - i(p^d-1)-1}.$$

Observe

$$\begin{aligned} X^{p^n-i(p^d-1)-1}\,(X^{p^d} - X) &= X^{p^n-i(p^d-1)-1+p^d} - X^{p^n-i(p^d-1)} \\ &= X^{p^n-(i-1)(p^d-1)} - X^{p^n-i(p^d-1)}. \end{aligned}$$

Hence

$$\begin{aligned} g(X)\,(X^{p^d} - X) &= \sum_{i=1}^{r} X^{p^n-i(p^d-1)-1}\,(X^{p^d} - X) \\ &= \sum_{i=1}^{r} \left(X^{p^n-(i-1)(p^d-1)} - X^{p^n-i(p^d-1)} \right) \\ &= X^{p^n} - X^{p^n-r(p^d-1)}, \end{aligned}$$

since the first term of the ith summand cancels with the second term of the $(i-1)$th summand. As $r(p^d-1) = p^n - 1$, we conclude

$$g(X)\,(X^{p^d} - X) = X^{p^n} - X^{p^n-(p^n-1)} = X^{p^n} - X,$$

as claimed.

(ii) By construction, $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$ and this polynomial has distinct roots in $\mathbb{F}_{p^n}$. By part (i), $X^{p^d} - X$ divides $X^{p^n} - X$, hence this too splits in $\mathbb{F}_{p^n}$ and has distinct roots.

Thus $X^{p^d} - X$ has precisely p^d roots in $\mathbb{F}_{p^n}$.

(iii) Let $L = \{\, a \in \mathbb{F}_{p^n} \mid a^{p^d} = a \,\}$; that is, L is the set of roots of $X^{p^d} - X$ in $\mathbb{F}_{p^n}$. By (ii), $|L| = p^d$.

Note that 0 and 1 both satisfy $a^{p^d} = a$, so L is non-empty and contains non-zero elements. Let $a, b \in L$. Then

$$\begin{aligned} (a+b)^{p^d} &= a^{p^d} + b^{p^d} = a + b \\ (ab)^{p^d} &= a^{p^d}\,b^{p^d} = ab \\ (-a)^{p^d} &= (-1)^{p^d}\,a^{p^d} = -a^{p^d} = -a \end{aligned}$$

and, if $a \neq 0$,

$$(1/a)^{p^d} = 1/a^{p^d} = 1/a.$$

Here we use Freshman's Exponentiation in the first calculation and the fact that $(-1)^{p^d} = -1$ if p is odd and $(-1)^{p^d} = 1 = -1$ if $p = 2$ in the third. We conclude that L is a subfield of $\mathbb{F}_{p^n}$. This completes (iii).

(c) By (a), any subfield of $\mathbb{F}_{p^n}$ is isomorphic to $\mathbb{F}_{p^d}$ for some divisor d of n. Conversely, if d divides n, then by (b),

$$L = \{\, a \in \mathbb{F}_{p^n} \mid a^{p^d} = a \,\}$$

is a subfield of $\mathbb{F}_{p^n}$ of order p^d (hence isomorphic to $\mathbb{F}_{p^d}$). It remains to show that L is the *unique* subfield of $\mathbb{F}_{p^n}$ of order p^d.

However, if F is a subfield of $\mathbb{F}_{p^n}$ of order p^d, then $|F^*| = p^d - 1$, so

$$a^{p^d-1} = 1 \qquad \text{for all } a \in F^*.$$

Therefore

$$a^{p^d} = a \qquad \text{for all } a \in F$$

and we observe $F \subseteq L$. As $|F| = |L| = p^d$, we conclude $F = L$, as required.

4. **(a) Using information about the Galois field $\mathbb{F}_{16}$ of order 16, or otherwise, factorize $X^{15} - 1$ into a product of polynomials irreducible over $\mathbb{F}_2$.**

   [Hint: What are the subfields of $\mathbb{F}_{16}$? If an element lies in a particular subfield, what is the degree of its minimum polynomial?]

   (b) Using information about the Galois field $\mathbb{F}_{27}$ of order 27, or otherwise, find the degrees of the irreducible factors of $X^{26} - 1$ over $\mathbb{F}_3$. Find the number of irreducible factors of each degree.

Solution: (a) By Question 3, $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ has a unique subfield of order p^d for each divisor d of 4; that is, the subfields of $\mathbb{F}_{16}$ are $\mathbb{F}_2$, $\mathbb{F}_4$ and $\mathbb{F}_{16}$ itself.

If $\alpha \in \mathbb{F}_{16}$ and $\alpha \neq 0$, then $\alpha^{15} = 1$ (as $|\mathbb{F}_{16}^*| = 15$), so the minimum polynomial of α over $\mathbb{F}_2$ divides $X^{15} - 1$. Now if $\alpha \in \mathbb{F}_2$, then $\alpha = 1$ and $X - 1$ is the minimum polynomial of α over $\mathbb{F}_2$.

If $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$, then $\mathbb{F}_2(\alpha)$, the smallest subfield of $\mathbb{F}_{16}$ containing α, must be $\mathbb{F}_4$. Hence $|\mathbb{F}_2(\alpha) : \mathbb{F}_2| = |\mathbb{F}_4 : \mathbb{F}_2| = 2$ and the minimum polynomial of α over $\mathbb{F}_2$ must be of degree 2.

If $\alpha \in \mathbb{F}_{16} \setminus \mathbb{F}_4$, then $\mathbb{F}_2(\alpha) = \mathbb{F}_{16}$ (since α does not belong to the other alternative subfields $\mathbb{F}_2$ and $\mathbb{F}_4$) and the degree of the minimum polynomial of α over $\mathbb{F}_2$ is 4.

In Question 9 on Problem Sheet I we found the irreducible polynomials of degree at most 4 over $\mathbb{F}_2$. There is one irreducible polynomial of degree 2, namely

$$X^2 + X + 1,$$

and three irreducible polynomials of degree 4, namely

$$X^4 + X + 1, \qquad X^4 + X^3 + 1 \qquad \text{and} \qquad X^4 + X^3 + X^2 + X + 1.$$

The two elements in $\mathbb{F}_4 \setminus \mathbb{F}_2$ must have minimum polynomial $X^2 + X + 1$ and be the roots of this polynomial in $\mathbb{F}_{16}$. The twelve elements in $\mathbb{F}_{16} \setminus \mathbb{F}_4$ must be roots of the above three polynomials of degree 4. Each of these polynomials has precisely four roots in $\mathbb{F}_{16}$ since once they have one root, they then divide $X^{15} - 1$ and hence have distinct roots in $\mathbb{F}_{16}$. We conclude that the factorization of $X^{15} - 1$ over $\mathbb{F}_2$ is

$$X^{15} - 1 = (X - 1)\,(X^2 + X + 1)\,(X^4 + X + 1)\,(X^4 + X^3 + 1)\,(X^4 + X^3 + X^2 + X + 1).$$

(b) Since the multiplicative group $\mathbb{F}_{27}^*$ has order 26, every non-zero element of $\mathbb{F}_{27}$ is a root of $X^{26} - 1$. Now if $\alpha \in \mathbb{F}_{27}$, with $\alpha \neq 0$, then $\mathbb{F}_3(\alpha)$ is one of the subfields of $\mathbb{F}_{27}$. As $|\mathbb{F}_{27} : \mathbb{F}_3| = 3$, there are (by Question 3) precisely two subfields namely $\mathbb{F}_3$ and $\mathbb{F}_{27}$ itself. If $\alpha \in \mathbb{F}_3$ (that is, $\alpha = 1$ or 2), then $\mathbb{F}_3(\alpha) = \mathbb{F}_3$ and the minimum polynomial of α over $\mathbb{F}_3$ is $X - \alpha$ and this is a factor of $X^{26} - 1$ (as the minimum polynomial of α divides any polynomial over $\mathbb{F}_3$ having α as a root).

Otherwise, if $\alpha \in \mathbb{F}_{27} \setminus \mathbb{F}_3$, then α is one of 24 elements satisfying $\mathbb{F}_3(\alpha) = \mathbb{F}_{27}$. The minimum polynomial of α over $\mathbb{F}_3$ then has degree 3 and this is a factor of $X^{26} - 1$. There product of all such degree 3 minimum polynomials will then account for all roots α of $X^{26} - 1$ with $\alpha \notin \mathbb{F}_3$, so we conclude that there are eight degree 3 irreducible factors (covering between them three roots each to a total of 24 roots).

Hence $X^{26} - 1$ is a product of two irreducible factors of degree 1 and eight irreducible factors of degree 3 over $\mathbb{F}_3$.

5. **A *primitive nth root of unity* in a finite field F is an element x of order n in the multiplicative group F^*. [The terminology indicates that x satisfies $x^n = 1$ and that its powers $1, x, x^2, \dots, x^{n-1}$ are the n distinct roots of $X^n - 1$ in F.]**

   Let q be a power of a prime.

   (a) **Show that the Galois field $\mathbb{F}_q$ of order q contains a primitive nth root of unity if and only if $q \equiv 1 \pmod{n}$.**

   (b) **Suppose that n and q are coprime. Show that the splitting field of $X^n - 1$ over $\mathbb{F}_q$ is $\mathbb{F}_{q^m}$ where m is minimal subject to $q^m \equiv 1 \pmod{p}$.**

   (c) **For each value of n in the range $1 \leqslant n \leqslant 12$, determine the degree of the splitting field of $X^n - 1$ over $\mathbb{F}_5$.**

   (d) **Determine for which n in the range $1 \leqslant n \leqslant 12$ does the Galois field $\mathbb{F}_{5^{36}}$ of order 5^{36} contain a primitive nth root of unity?**

Solution: (a) Note that an element x of $\mathbb{F}_q^*$ is a primitive nth root of unity if and only if the cyclic subgroup $\langle x \rangle$ of $\mathbb{F}_q^*$ is of order n. Since $\mathbb{F}_q^*$ is cyclic of order $q-1$, it has a (unique) subgroup of order n if and only if n divides $q-1$; that is, $\mathbb{F}_q$ contains a primitive nth root of unity if and only if $q \equiv 1 \pmod{n}$.

(b) Consider a field extension L of $\mathbb{F}_q$ of degree m. Since $|L : \mathbb{F}_q| = m$, the order of L equals q^m, so $L \cong \mathbb{F}_{q^m}$. By part (a), L^* contains a primitive nth root of unity if and only if $q^m \equiv 1 \pmod{n}$. Now if L^* contains a primitive nth root of unity, then the powers of this root are n distinct roots of $X^n - 1$ and hence $X^n - 1$ splits in L.

Conversely, if $X^n - 1$ splits in L, then consider the set Z of roots of $X^n - 1$ in L. Since $D(X^n - 1) = nX^{n-1} \neq 0$ (as n is coprime to q and hence to the characteristic of L) and X does not divide $X^n - 1$, we observe $X^n - 1$ and its formal derivative are coprime. Thus the roots of $X^n - 1$ are distinct, so $|Z| = n$. If $\alpha, \beta \in Z$, then

$$(\alpha\beta)^n = \alpha^n \beta^n = 1,$$

and we conclude that Z is a multiplicative subgroup of L^*. Therefore Z is cyclic (as a subgroup of a cyclic group), so $Z = \langle x \rangle$ for some x of order n. This x is a primitive nth root of unity in L^* and so, by part (a), $q^m \equiv 1 \pmod{n}$.

In conclusion, $L = \mathbb{F}_{q^m}$ is a field over which $X^n - 1$ splits if and only if $q^m \equiv 1 \pmod{n}$. The splitting field of $X^n - 1$ is the smallest field over which $X^n - 1$ spits and hence is $\mathbb{F}_{q^m}$ where m is *smallest* such that $q^m \equiv 1 \pmod{n}$.

(c) By part (b), the spitting field of $X^n - 1$ over $\mathbb{F}_5$ is $\mathbb{F}_{5^m}$ where m is smallest such that $q^m \equiv 1 \pmod{n}$ *provided* n is coprime to 5. Thus we can, for $n \neq 5$, 10, determine the value m by calculating powers of $5 \mod n$. Indeed we seek the smallest value of m such that n divides $5^m - 1$ and we calculate this for each $n = 1, 2, \dots, 12$ except $n = 5$ or 10.

The values of m are as follows:

n	m
1	1
2	1
3	2
4	1
6	2
7	6
8	2
9	6
11	5
12	2

Hence the splitting field of $X^n - 1$ over $\mathbb{F}_5$ has degree 1 for $n = 1$, 2 and 4; has degree 2 for $n = 3$, 6, 8 and 12; has degree 5 for $n = 11$; and has degree 6 for $n = 7$ and 9.

It remains to consider $n = 5$ and $n = 10$. Since 5 is also the characteristic of our field,

$$X^5 - 1 = (X - 1)^5$$

and

$$\begin{aligned} X^{10} - 1 &= (X^2)^5 - 1 \\ &= (X^2 - 1)^5 \\ &= (X - 1)^5 (X + 1)^5. \end{aligned}$$

Thus both $X^5 - 1$ and $X^{10} - 1$ split over $\mathbb{F}_5$, so the degree of the splitting field of $X^n - 1$ over $\mathbb{F}_5$ is 1 for $n = 5$ and 10.

(d) As observed in part (b), the field $\mathbb{F}_{5^{36}}$ has a primitive nth root of unity, for n coprime to 5, when it contains the splitting field of $X^n - 1$ over $\mathbb{F}_5$. In part (c), we determined this splitting field as $\mathbb{F}_{5^m}$ for specific m. Thus, using Question 3, this splitting field is contained in $\mathbb{F}_{5^{36}}$ precisely when this degree m divides 36. Consequently, we know $\mathbb{F}_{5^{36}}$ contains a primitive nth root of unity for $n = 1$, 2, 3, 4, 6, 7, 8, 9 and 12, but not for $n = 11$.

The cases $n = 5$ and $n = 10$ must be handled separately, but are straightforward. The multiplicative group $\mathbb{F}_{5^{36}}^*$ has order $5^{36} - 1$ and this is not divisible by 5 or 10 (it is coprime to 5), so $\mathbb{F}_{5^{36}}^*$ has no element of order 5 or 10.

In conclusion, $\mathbb{F}_{5^{36}}$ contains a primitive nth root of unity for $n = 1$, 2, 3, 4, 6, 7, 8, 9 and 12 but not for $n = 5$, 10 or 11.

6. **Let F be a finite field with q elements where q is odd. Prove that the splitting field of $X^4 + 1$ over F has degree one or two and that $X^4 + 1$ factorizes in $F[X]$ either as a product of four distinct linear polynomials when 8 divides $q - 1$ or as a product of two distinct quadratic irreducible polynomials when 8 does not divide $q - 1$.**

[Hint: Consider the elements $-\alpha$, $1/\alpha$ and $-1/\alpha$ where α is a root of $X^4 + 1$ in some extension of F.]

Solution: Let α be a root of $X^4 + 1$ in an extension of F (for example, in a splitting field). Note

$$\begin{aligned} (-\alpha)^4 &= \alpha^4 = -1, \\ (1/\alpha)^4 &= 1/\alpha^4 = 1/(-1) = -1, \end{aligned}$$

and

$$(-1/\alpha)^4 = 1/\alpha^4 = 1/(-1) = -1,$$

so $-\alpha$, $1/\alpha$ and $-1/\alpha$ are roots of X^4+1 in $F(\alpha)$. Moreover, the formal derivative $D(X^4+1) = 4X^3 \neq 0$ is coprime to X^4+1, so these four roots are distinct. Thus $F(\alpha)$ is the splitting field of X^4+1 over F.

Suppose 8 divides $q-1$. Then F^* is cyclic of order $q-1$, so contains some element α of order 8. Note that F^* has a unique element of order 2, namely -1, since 1 and -1 are the only roots of X^2-1. Hence $\alpha^4 = -1$ and thus the element α of order 8 in F^* is a root of X^4+1. The previous paragraph now shows that X^4+1 splits as a product of linear factors in $F[X]$.

Conversely suppose 8 does not divide $q-1$. Let L be an extension of F of degree 2; that is, L is a field of order q^2. Now

$$q^2 - 1 = (q-1)(q+1)$$

is a product of two consecutive even integers, so one is divisible by 4. Hence q^2-1 is divisible by 8, so by the previous paragraph applied to L, X^4+1 splits over L. Let α be a root of X^4+1 in L. Then $F(\alpha)$ is the splitting field of X^4+1 over F and is some subfield of L. As $|L:F| = 2$, we conclude $F(\alpha) = F$ or L.

Note that $\alpha^4 = -1$, so $\alpha^8 = 1$. Thus α is an element of order 8 in L^* (since also $\alpha^4 = -1 \neq 1$). Since $8 \nmid (q-1)$, we conclude $\alpha \notin F$, so $L = F(\alpha)$ and the degree of the minimum polynomial over α is 2. This minimum polynomial divides X^4+1 and the same argument applies to all roots of X^4+1. We conclude that when $8 \nmid (q-1)$, the polynomial X^4+1 factorizes as a product of two distinct irreducible quadratic factors. (The factors are distinct as X^4+1 has four distinct roots in $F(\alpha)$.)

7. **Let G be a finite abelian group.**

   (a) If x_1 and x_2 are elements of G with coprime orders, show that x_1x_2 has order given by $o(x_1x_2) = o(x_1)\,o(x_2)$.

   (b) Suppose $p_1, p_2, \dots, p_k$ are distinct prime numbers and that $x_1, x_2, \dots, x_k \in G$ with $o(x_i) = p_i^{\alpha_i}$. Show that
   $$o(x_1x_2\dots x_k) = o(x_1)\,o(x_2)\dots o(x_k) = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}.$$

Solution: (a) Let $n = o(x_1)\,o(x_2)$. Since G is abelian,

$$(x_1x_2)^n = x_1^n x_2^n = 1$$

as $o(x_1)$ and $o(x_2)$ both divide n. Thus the order of x_1x_2 divides n.

Conversely, suppose $(x_1x_2)^k = 1$. Then

$$x_1^k = x_2^{-k},$$

so

$$x_1^{k\cdot o(x_2)} = (x_2^{o(x_2)})^{-k} = 1.$$

Hence $o(x_1)$ divides $k \cdot o(x_2)$. However, as $o(x_1)$ and $o(x_2)$ are coprime, we then conclude $o(x_1)$ divides k. By the same argument, we deduce $o(x_2)$ divides k. Thus, again using the fact that $o(x_1)$ and $o(x_2)$ are coprime, we establish that $o(x_1)\,o(x_2)$ divides k.

In conclusion, the smallest positive integer k such that $x^k = 1$ is $k = o(x_1)\,o(x_2)$; that is,

$$o(x_1x_2) = o(x_1)\,o(x_2).$$

(b) We proceed by induction on k, with the case $k=1$ being trivial. Suppose the result holds for $k-1$; that is,

$$o(x_1x_2\dots x_{k-1}) = o(x_1)\,o(x_2)\dots o(x_{k-1}) = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{k-1}^{\alpha_{k-1}}.$$

Thus $o(x_k) = p_k^{\alpha_k}$ and $o(x_1 x_2 \dots x_{k-1})$ are coprime, so by (a),

$$\begin{aligned} o(x_1 x_2 \dots x_k) &= o(x_1 x_2 \dots x_{k-1})\, o(x_k) \\ &= o(x_1)\, o(x_2) \dots o(x_{k-1}) \cdot o(x_k) \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}. \end{aligned}$$

This establishes the induction.

8. **Give an example of a finite group (necessarily non-abelian) which has no element of order equal to its exponent.**

Solution: Take $G = S_3$, the symmetric group of degree 3. Then G contains the identity (of order 1), transpositions (of order 2) and 3-cycles (of order 3). Hence the exponent of G is 6, but there are no elements of order 6 in $G = S_3$.