Question 1

Construct the field of 9 elements. Write out the addition and multiplication tables.

Solution: Consider the set $\{0, 1, 2, i, 1+i, 2+i, 2i, 2+i, 2+2i\}$ of 9 elements with the following tables.

+	0	1	2	i	1+i	2+i	2i	1+2i	2+2i
0	0	1	2	i	1+i	2+i	2i	1+2i	2+2i
1	1	2	0	1+i	2+i	i	1+2i	2+2i	2i
2	2	0	1	2+i	i	1+i	2+2i	2i	1+2i
i	i	1+i	2+i	2i	1+2i	2+2i	0	1	2
1+i	1+i	2+i	i	1+2i	2+2i	2i	1	2	0
2+i	2+i	i	1+i	2+2i	2i	1+2i	2	0	1
2i	2i	1+2i	2+2i	0	1	2	i	1+i	2+i
1+2i	1+2i	2+2i	2i	1	2	0	1+i	2+i	i
2+2i	2+2i	2i	1+2i	2	0	1	2+i	i	1+i

and

×	0	1	2	i	1+i	2+i	2i	1+2i	2+2i
0	0	0	0	0	0	0	0	0	0
1	0	1	2	i	1+i	2+i	2i	1+2i	2+2i
2	0	2	1	2i	2+2i	1+2i	i	2+i	1+i
i	0	i	2i	2	2+i	2+2i	1	1+i	1+2i
1+i	0	1+i	2+2i	2+i	2i	1	1+2i	2	i
2+i	0	2+i	1+2i	2+2i	1	i	1+i	2i	2
2i	0	2i	i	1	1+2i	1+i	2	2+2i	2+i
1+2i	0	1+2i	2+i	1+i	2	2i	2+2i	i	1
2+2i	0	2+2i	1+i	1+2i	i	2	2+i	1	2i

Since the field is unique up to isomorphism, the field of 9 elements is as described in the table.

Question 2

Determine whether or not two fields $\mathbb{F}_3[x]/(x^2-2)$ and $\mathbb{F}_3[x]/(x^2-2x-1)$ are isomorphic. If they are isomorphic, find an isomorphism.

Solution: Notice that since there are 3 irreducible linear polynomials over $\mathbb{F}_3$ which are x, $x-1$, and $x+1$, and $x^3 - x = x(x+1)(x-1)$ Next, since

$$\gcd(x^2-2, x^3-x) = \gcd(x^2-2, x^2-1) = 1$$

and

$$\gcd(x^2-2x-1, x^3-x) = \gcd(x^2-2x-1, x^2-1) = \gcd(x^2-2x-1, 2x) = \gcd(x^2-1, 2x) = 1$$

it follows that, x^2-2 and x^2-2x-1 are both irreducible, thus

$$\mathbb{F}_{3^2} \simeq \mathbb{F}_3[x]/(x^2-2) \simeq \mathbb{F}_3[x]/(x^2-2x-1)$$

Note that since the polynomials are irreducible, these two are fields.

Now, for the isomorphism, consider that for any $f(x) \in \mathbb{F}_3[x]$, there exists $r(x)$ such that $f(x) = q(x)(x^2-2x-1) + r(x)$ where $\deg(r) \le 1$ by the euclidean algorithm. Thus, for any $f(x) \in \mathbb{F}_3[x]/(x^2-2x-1)$, $f(x) = r(x)$ for some linear or constant $r(x)$. Moreover, there exists $r'(x) \in \mathbb{F}_3[x]/(x^2-2)$ such that $\phi(r') = r$ when

$$\phi : \mathbb{F}_3[x]/(x^2-1) \hookrightarrow \mathbb{F}_3[x] \twoheadrightarrow \mathbb{F}_3[x]/(x^2-2x-1)$$

by the natural embedings.

And if $\phi(r)(x) = 0 \in \mathbb{F}_3[x]/(x^2-2x-1)$, then the corresponding polynomial in $\mathbb{F}_3[x]$ (in the middle step of ϕ) should only be $q(x)(x^2-2x-1)$ for some $q(x)$. Then, as the $\mathbb{F}_3[x]/(x^2-2) \hookrightarrow \mathbb{F}_3[x]$ is the natural embeding, we have that $r = 0$, as there is no polynomial of degree greater than 1 in $\mathbb{F}_3[x]/(x^2-2)$ and the natural embeding preserves degree.

Therefore, ϕ is injective and surjective, thus it is an isomorphism.

Question 3

Let $\mathbb{F}_q$ be a finite field and let n be a positive integer. Show that there exists an irreducible polynomial over $\mathbb{F}_q$ of degree n.

Solution:

Claim 1 Existence of $\mathbb{F}_{q^n}$

$\mathbb{F}_q$ must have characteristic p for some prime p as it is finite. Thus, $\mathbb{F}_p \subset \mathbb{F}_q$. Then, the degree $[\mathbb{F}_q : \mathbb{F}_p] = k$ for some integer, so $q = p^k$. Therefore, there exists a field $\mathbb{F}_{q^n} = \mathbb{F}_{p^{kn}}$.

Since there is such field, consider $E = \mathbb{F}_{q^n}$ and that $[E : \mathbb{F}_q] = n$ and E is a finite extension, thus $E = \mathbb{F}_q(\alpha)$ for some $\alpha \in E$. But since the degree of $[E : \mathbb{F}_q] = n$, then the minimal polynomial $m_\alpha \in \mathbb{F}_q[x]$ is of degree n. Since m_α is minimal, it is irreducible.

Question 4

Find a splitting field of $x^6 - 3$ over $\mathbb{F}_7$ and the degree of the splitting field.

Solution: Notice that if there is a linear or quadratic irreducible element that divides $x^6 - 3$, then it must divides $x^{7^2} - x$ since $x^{7^2} - x$ is the product of all irreducible polynomial degree 1 and 2.

Note that over a field of characteristic 7,

$$(x^6 - 3)^7 = x^{6^7} - 3^7$$

and

$$((x^6 - 3)^7 + 3^7)(x^6 - 3) = (x^{42})(x^6 - 3) = (x^{48} - 3x^{42})$$

Then, if something divides $x^6 - 3$ and $x^{7^2} - x$, then it must divides $\gcd(x^6 - 3, x^{49} - x)$. But

$$\begin{aligned}
\gcd(x^6 - 3, x^{49} - x) &= \gcd(x^6 - 3, x^{48} - 1) \\
&= \gcd(x^6 - 3, x^{48} - 1 - x^{48} + 3x^{42}) \\
&= \gcd(x^6 - 3, 3x^{42} - 1 - 3(x^{42} - 3^7) \\
&= \gcd(x^6 - 3, 3^8 - 1) \\
&= 1
\end{aligned}$$

Thus, there is none.

Next, if there is a cubic irreducible polynomial dividing $x^6 - 3$, then it must divides $x^{7^3} - x$ since $x^{7^3} - x$ is the product of all irreducible polynomial degree dividing 3.

Note that $7^3 = 343$,

$$((x^6 - 3)^7)^7 = (x^{42} - 3^7)^7 = (x^{294} - 3^{49})$$

and

$$(x^{48})(x^6 - 3)^{49} = (x^{48})(x^{294} - 3^{49}) = x^{342} - 3^{49}x^{48}$$

So,

$$\begin{aligned}
\gcd(x^6 - 3, x^{343} - x) &= \gcd(x^6 - 3, x^{342} - 1) \\
&= \gcd(x^6 - 3, x^{342} - 1 - x^{342} + 3^{49}x^{48}) \\
&= \gcd(x^6 - 3, 3^{49}(x^{48} - 1) + 3^{49} - 1) \\
&= \gcd(x^6 - 3, 3^{49}(3^8 - 1) + 3^{49} - 1) \\
&= 1
\end{aligned}$$

Thus, there is none.

If there is no irreducible divisor of degree less than 4, there is no irreducible divisor. Thus, $x^6 - 3$ is irreducible. Let E be the splitting field of f over $\mathbb{F}_7$. Then since $\mathbb{F}_7 \subset E$, $E = \mathbb{F}_{7^k}$ for some k. If $k \leq 5$, it is already shown that $x^6 - 3$ is irreducible, thus, does not divide $x^{7^k} - x$ which is the product of irreducible degree dividing k. As $\mathbb{F}_{7^k}$ is the splitting field of $x^{7^k} - x$, then it is not the splitting field of f.

However, $x^6 - 3$ divides $x^{7^6} - x$ since it is the product of all irreducible polynomials degree dividing 6. So, $\mathbb{F}_{7^6}$ splits $x^{7^6} - x$, thus it splits f. Therefore, the spliting field of f over $\mathbb{F}_7$ is $\mathbb{F}_{7^6}$, which gives that $[\mathbb{F}_{7^6} : \mathbb{F}_7] = 6$.

Question 5

Let $f \in \mathbb{F}_q[x]$. Show that if f is irreducible, then f divides $x^{q^{\deg(f)}} - x$.

Solution: Let α be a root of f, then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg(f) = n$. As $q = p^k$ and there exists a field $\mathbb{F}_{q^n} = \mathbb{F}_{p^{nk}}$ (as per claim 1). Then, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n} = \mathbb{F}_{p^{nk}}$.

Now, $\mathbb{F}_{p^{nk}}$ is the splitting field of $x^{p^{nk}} - x$ over $\mathbb{F}_p$ and α is an element in the splitting field with $\alpha \notin \mathbb{F}_q$. (because $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$). Therefore, α is a root of x^{q^n}. Hence, it follows that $f \mid x^{q^n} - x$.

Question 6

Let p be a prime integer. Find the smallest integer n such that $\mathbb{F}_{p^n}$ contains two subfields isomorphic to $\mathbb{F}_{p^r}$ and $\mathbb{F}_{p^s}$.

Solution: Notice that $\mathbb{F}_{p^r} \subset \mathbb{F}_{p^n}$ if and only if $r \mid n$ and similarly for s. If $n = \operatorname{lcm}(r, s)$ be the smallest integer that is divisible by r and s, then, $\mathbb{F}_{p^r} \subset \mathbb{F}_{p^n}$ and $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^n}$. And by definition, $\operatorname{lcm}(r, s)$ is the least number, thus $n = \operatorname{lcm}(r, s)$.

Question 7

Prove that every finite extension of a finite field is normal.

Solution: Let $F = \mathbb{F}_q$ be an arbitrary finite field and E/F be a finite extension with $[E : F] = n$. Then, $q = p^k$ and that there exists $\mathbb{F}_{q^n}$ as from claim 1.

Since $[E : F] = [\mathbb{F}_{q^n} : F]$ is finite over finite field F, then $|E| = |\mathbb{F}_{q^n}|$, which means that they are isomorphic due to the uniqueness of finite fields.

Now, as $\mathbb{F}_{q^n}$ is the splitting field of $x^{p^{nk}} - x$ over $\mathbb{F}_p$, then it is normal over $\mathbb{F}_p$. Moreover, ad $\mathbb{F}_q$ is an extension of $\mathbb{F}_p$, then $\mathbb{F}_{q^n}$ is also normal over $\mathbb{F}_q$. Lastly, as $E \simeq \mathbb{F}_{q^n}$, E is normal over $\mathbb{F}_q = F$.

Question 8

Let F be a field of $\operatorname{char}(F) = p$. Prove that the quotient field of the polynomial ring $F[x]$ over $F(x^p)$ is normal.

Solution: Consider that x^p is transcendental in F because if not, then there is a polynomial $a_0 + a_1x^p + \cdots + a_nx^{pn} = 0$ where $a_i \in F$. But that means x is also algebraic over F, which contradicts that $F[x]$ is a polynomial ring.

Therefore, $F[x^p]$ is a polynomial ring. Consider that x^p is irreducible $F[x^p]$, so the Eisenstein criterion applies for the $f(t) = t^p - x^p$ in $F[x^p][t]$. Hence, $f(t)$ is irreducible over $F(x^p)$. Since x is a root of the polynomial, then $[F(x) : F(x^p)] = p$ as f is the minimal polynomial of x and $F(x) = F(x^p)(x)$. Note also that p is a prime integer.

Next, notice that $f(t) = t^p - x^p = (t - x)^p$ over any field F of characteristic p. Therefore, $f(t)$ splits over $F(x)$. Moreover, if there is another field $F(x)/E/F(x^p)$, then $[E : F(x^p)] = 1$, which is $E = F(x^p)$ or $[F(x) : E] = 1$, which is that $E = F(x)$. Therefore, $F(x)$ is the splitting field of $f(t)$ over $F(x^p)$. Therefore, $F(x)$, the quotient field of $F[x]$, is normal over $F(x^p)$.

Question 9

Show that the polynomial $x^4 + 1$ is not irreducible over any field of nonzero characteristic.

Solution: For $p = 2$, consider that $1 + 1 = 0$. This implies that

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

which means $(x^4 + 1)$ is not irreducible over any field of characteristic 2.

Otherwise p is odd. Then there are 4 cases for p, which is $p \equiv 1, 3, 5, 7 \pmod 8$.

For the case that $p \equiv 1$ or $7 \pmod 8$, there exist a number r such that $r^2 \equiv 2 \pmod p$. In other words, in the field with characteristic $p \equiv \pm 1 \pmod 8$, there is an element r such that $r \cdot r = 2$. Then, as

$$(x^2 - rx + 1)(x^2 + rx + 1) = (x^2 + 1)^2 - (rx)^2 = x^4 + 2x^2 + 1 - r^2x^2 = x^4 + 1$$

the polynomial is reducible.

Lastly, if $p \equiv 3$ or $5 \pmod 8$, there exist a number r such that $r^2 \equiv -2 \pmod p$, which means that in the field of characteristic $p \equiv \pm 3 \pmod 8$, there must be an element r such that $r \cdot r = -2$. Then, similarly,

$$(x^2 - rx - 1)(x^2 + rx - 1) = (x^2 - 1)^2 - (rx^2) = x^4 - 2x^2 + 1 - r^2x^2 = x^4 + 1$$

. This implies that the polynomial is not irreducible.

Thus, the polynomial $x^4 + 1$ is not irreducible over any field of non-zero characteristic.

Question 10

Let F be a field. Show that if $a \in F \backslash F^p$ for a prime p, then $x^p - a$ is an irreducible polynomial over F.

Solution: Consider that F^p is the set $\{\, x^p \mid x \in F \,\}$, then let $a \in F$ and assume that $x^p - a$ is reducible. There must be some polynomial $g \in F[x]$ with $\deg(g) = k$ such that $k < r$ and $g \mid f$. Let E be the splitting field of g over F, so that

$$g(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$

As $g \in F[x]$, then g_0, the constant term of g must be an element of F, therefore,

$$\alpha_1 \alpha_2 \cdots \alpha_k = g_0 \in F$$

Since α_i is a root of g, then it is of f, so $f(\alpha_i) = 0$ for any i. This means that ${\alpha_i}^p = a$ for all i. Next, consider that

$$a^k = {\alpha_1}^p {\alpha_2}^p \cdots {\alpha_k}^p = (\alpha_1 \alpha_2 \cdots \alpha_k)^p = {g_0}^p$$

Since $k < p$ and p is prime, then there exists integer n, m making $nk + mp = 1$. From $a^k = {g_0}^p$, it could be infer that

$$a = a^{nk+mp} = a^{nk} a^{mp} = g_0^{np} a^{mp} = (g_0^n a^m)^p$$

Since $g_0^n a^m \in F$, then $a \in F^p$.

Hence, by contraposition, if $a \in F \backslash F^p$ for a prime p, then $x^p - a$ is an irreducible polynomial over F.