Question 1

Show that an algebraically closed field is infinite.

Solution: Assume that there is a finite field that is algebraically closed. Let the field be $\mathbb{F}_q$ where $q = p^n$ for some prime n. Then, there exists a field extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$ such that it is the splitting field of $x^{q^2} - x$. As $\mathbb{F}_{q^2}$ is a finite extension of $\mathbb{F}_q$ such that $\mathbb{F}_q \neq \mathbb{F}_{q^2}$, then $\mathbb{F}_q$ is not algebraically closed by definition.

Question 2

Let $\bar{F}$ be an algebraic closure of the finite field $\mathbb{F}_q$. Show that $\bar{F}$ is the union of all finite subfields.

Solution: Notice that the splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$ is $\mathbb{F}_q^n$. Therefore, for any n, $\mathbb{F}_{q^n}$ must be contained by the algebraic closure $\bar{F}$. This means that $\bigcup_{n\geq 1} \mathbb{F}_{q^n} \subset \bar{F}$.

Then, since any irreducible polynomial over $\mathbb{F}_q$ must have finite degree, say m, it follows that the splitting field of that polynomial is $\mathbb{F}_{q^m}$. As the splitting of any irreducible polynomial is a finite field, then it must split in $\bigcup_{n\geq 1} \mathbb{F}_{q^n}$. Thus, $\bar{F} \subset \bigcup_{n\geq 1} \mathbb{F}_{q^n}$.

This gives that $\bar{F} = \bigcup_{n\geq 1} \mathbb{F}_{q^n}$.

For any n, as $\mathbb{F}_{q^n}/\mathbb{F}_q$ is an algebraic extension, then $\mathbb{F}_{q^n}$ is a finite subfield of $\bar{F}$. Thus, $\bar{F}$ is the union of all of its finite subfields as needed.

Question 3

Let E/F be a Galois extension. Show that if the quotient group $E^\times/F^\times$ has an element of order n, then $E^\times$ has an element of order n.

Solution: Since there is an element of order n, then, let that element be α. So, $\alpha^n \in F^\times$ and α^k for any $k < n$ is not a member of $F^\times$. Let $f = x^n - \alpha^n$. As f has a root in E and E is normal and separable, then f must split in E So, $f = (x - \beta_1)\cdots(x - \beta_n)$, where each of the β_i is an element in $E^\times$ and $\beta_i \neq \beta_j$ for all $i \neq j$.

Then, create a set of elements $\{\gamma_1, \dots, \gamma_n\}$ such that $\gamma_i = \beta_i/\alpha$, then $\gamma_i^n = \frac{\beta_i^n}{\alpha^n} = 1$. Moreover, as $\beta_i \neq \beta_j$ for $i \neq j$, then $\gamma_i \neq \gamma_j$ for $i \neq j$.

Since there are at least n roots of 1, which are $\gamma_1, \dots, \gamma_n$ in the field E, then $\mu_n \in E^\times$. Therefore, there is an element of order n, which is the primitive nth root in $E^\times$.

Question 4

Find $\mathrm{Gal}(E/\mathbb{F}_9)$ where E denotes the splitting field of $x^{16} - 1$ over $\mathbb{F}_9$.

Solution: Notice that $f(x) = x^{16} - 1$ is separable as $f'(x) \neq 0$ and E is a splitting field, thus normal, therefore, $E/\mathbb{F}_9$ is galois.

Consider that the degree of a primitive root of $x^{16} - 1 = (x^8 - 1)(x^8 + 1)$ is 16, then as μ_{16}, the group of roots, is a subgroup of $E^\times$, the splitting field E must be such that $16 \mid |E^\times|$, which, the smallest such E is $|E| = 81$, as E must also be of order 3^n. This means that the splitting field E contains $\mathbb{F}_{81}$.

Now, $\mathbb{F}_{81}$ is the splitting field of

$$x^{81} - x = x(x^{80} - 1) = x(x^{16} - 1)(x^{64} + x^{48} + x^{32} + x^{16} + 1)$$

Thus, $E = \mathbb{F}_{81}$, which implies the degree $[E : \mathbb{F}_9] = 2$.

As the field extension is galois, then $|\mathrm{Gal}(E/\mathbb{F}_9)| = 2$. Therefore, $\mathrm{Gal}(E/\mathbb{F}_9) \simeq \mathbb{Z}/2\mathbb{Z}$.

Question 5

Let μ_n be the group of nth root of 1. Let $r = \mathrm{lcm}(m, n)$ and $s = \gcd(m, n)$. Show that $\mathbb{Q}(\mu_n)\mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_r)$ and $\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_s)$.

Solution: Since $n \mid r$, then $\mathbb{Q}(\mu_n) \subset \mathbb{Q}(\mu_r)$ and since $m \mid r$, $\mathbb{Q}(\mu_m) \subset \mathbb{Q}(\mu_r)$. As two fields are contained in $\mathbb{Q}(\mu_r)$, the composition, which is the smallest field containing both field, must also be contained in $\mathbb{Q}(\mu_r)$.

Let η_n be the primitive nth root of unity and η_m be the primitive mth root. Then, as there exists a, b such that $an + bm = \gcd(n, m)$, then there exist $an + bm \equiv 1 \pmod{\operatorname{lcm}(n, m)}$. Hence, $\eta^{an}\eta^{bm}$ is a primitive rth root of unity. Thus, $\mu_r \subset \mathbb{Q}(\mu_n)\mathbb{Q}(\mu_m)$, and therefore, $\mathbb{Q}(\mu_r) \subset \mathbb{Q}(\mu_n)(\mu_m)$

Next, as $s \mid n$ and $s \mid m$, then $\mathbb{Q}(\mu_s) \subset \mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m)$ as $x^s - 1 \mid x^n - 1$ and similarly for $x^m - 1$.

Now, as cyclotomic extensions are galois, then

$$\operatorname{Gal}(\mathbb{Q}(\mu_n)\mathbb{Q}(\mu_m)/\mathbb{Q}(\mu_n)) \simeq \operatorname{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m))$$

which gives that

$$\phi(\operatorname{lcm}(n, m)) = [\mathbb{Q}(\mu_n)\mathbb{Q}(\mu_m) : \mathbb{Q}] = [\mathbb{Q}(\mu_m) : \mathbb{Q}][\mathbb{Q}(\mu_n) : \mathbb{Q}][\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) : \mathbb{Q}]$$

Thus, $[\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) : \mathbb{Q}] = \frac{\phi(n)\phi(m)}{\phi(r)}$. As

$$\frac{\phi(n)\phi(m)}{\phi(r)} = \frac{n\prod_{p|n}(1 - 1/p) \cdot m\prod_{p|m}(1 - 1/p)}{\operatorname{lcm}(n, m)\prod_{p|\operatorname{lcm}(n,m)}(1 - 1/p)} = \gcd(n, m) \prod_{p|\gcd(n,m)} (1 - 1/p) = \phi(\gcd(n, m))$$

Then, $\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_d)$

Question 6

Prove that $\mathbb{Q}(\mu_n) \subseteq \mathbb{Q}(\mu_m)$ if and only if $n \mid m$ or $n = 2r$ for some odd divisor r of m.

Solution:
($\Longrightarrow$):

Since $\mathbb{Q}(\mu_n) \subset \mathbb{Q}(\mu_m)$, then $\mathbb{Q}(\mu_{\gcd(n,m)}) = \mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_n)$. Let $d = \gcd(n, m)$, then $\phi(d) = \phi(n)$.

If $d = 1$, then $\phi(d) = \phi(n)$ means $\phi(n) = \phi(1) = 1$. Thus, $n = 1$ or $n = 2$, because if $n \geq 3$, then $\phi(n) \geq \phi(p)$ for some odd prime divisor p of n. Thus, $\phi(n) \geq p - 1 > 1$. In the case that $n = 1$, $n \mid m$. In the case that $n = 2$, $n = 2 \cdot 1$ where 1 is an odd divisor of m.

Otherwise, $d > 1$ and as $d \mid n$, then it can be written as $d = 2^{a_0}p_1^{a_1} \cdots p_n^{a_n}$ and $n = 2^{b_0}p_1^{b_1} \cdots p_n^{b_n}q$ for some odd number q not divisible by any p_i for odd primes p_i such that $a_i \geq 1$ except for $a_0 \geq 0$ and $b_i \geq a_i$ for all i.

Since $\phi(d) = \phi(n)$, then

$$\phi(2^{a_0})\phi(p_1^{a_1}) \cdots \phi(p_n^{a_n}) = \phi(2^{b_0})\phi(p_1^{b_1}) \cdots \phi(p_n^{b_n})\phi(q)$$

as for all any odd prime p and $n \geq 1$, $\phi(p^{n+1}) = p \cdot \phi(p^n)$, then it must be the case that $b_i = a_i$ for all $i \geq 1$ and that $q = 1$. Thus, it follows that $\phi(2_0^a) = \phi(2_0^b)$. As $\phi(1) = \phi(2) = 1$ and $\phi(2^{n+1}) = 2\phi(2^n)$ for $n > 1$, then either $a_0 = b_0$ or $a_0 = 0$ and $b_0 = 1$ must hold.

This means that $d = n$ in the first case, and $2d = n$ for an odd d in the latter case. If $d = n$, then $n \mid m$ and otherwise, $n = 2d$ for some $d \mid m$ such that d is odd.

($\Longleftarrow$):

If $n \mid m$, then let $dn = m$. Now, $x^m - 1 = x^{dn} - 1 = (x^n - 1)(x^{(d-1)n} + x^{(d-2)n} + \cdots + 1)$. Thus, $x^n - 1 \mid x^m - 1$. This means that any root of $x^n - 1$ is a root of $x^m - 1$, thus $\mu_n \subseteq \mu_m$. Therefore, $\mathbb{Q}(\mu_n) \subseteq \mathbb{Q}(\mu_m)$.

Otherwise, if $n = 2r$ but $n \nmid m$ for some odd divisor r of m, then m is odd, so $-1 \notin \mu_m$. However, $\mathbb{Q}(\mu_n) \subseteq \mathbb{Q}(\mu_{2m})$ as $n \mid m$, and $\mu_{2m} = \mu_m \cup \{ -\eta \mid \eta \in \mu_m \}$ As $(-\eta)^{2m} = (-\eta)^{m^2} = -1^2 = 1$. Therefore, $\mathbb{Q}(\mu_{2m}) = \mathbb{Q}(\mu_m)$, which gives that $\mathbb{Q}(\mu_n) \subseteq \mathbb{Q}(\mu_m)$.

Question 7

Find all roots of unity which are contained in $\mathbb{Q}(\sqrt{-3})$

Solution: As $\mathbb{Q}(\sqrt{-3})$ is the splitting field of $f(x) = x^2 + 3$, and $\sqrt{-3} \notin \mathbb{Q}$ then $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2$. Since the field group μ_n is cyclic, if $\mathbb{Q}(\sqrt{-3})$ contains a primitive n root of unity, then it must contain all the nth root of unity, which means that it must the splits $x^n - 1$, and therefore have degree $\phi(n)$.

Notice that $\phi(3) = \phi(4) = \phi(6) = 2$ are the only numbers with this property because for a prime $p > 3$, $\phi(p) = p-1 > 2$, which means that for $n > 6$, $\phi(n) > \phi(2)\phi(3) > 2$.

Consider

$$\frac{\sqrt{-3}+1}{2}^3 = \frac{\sqrt{-3}^3 + 3\sqrt{-3}^2 + 3\sqrt{-3} + 1}{8} = 1$$

with $\frac{\sqrt{-3}+1}{2} \neq 1$, therefore $\mu_3 \subset \mathbb{Q}(\sqrt{-3})$. As $\mu_6 = \mu_3 \cup \{ -x \mid x \in \mu_3 \}$, then $\mathbb{Q}(\mu_6) = \mathbb{Q}(\mu_3)$, so $\mu_6 \subset \mathbb{Q}(\sqrt{-3})$. Lastly, as 6 is the largest integer n in which $\phi(n) = 2$, then there is no other root of unity in $\mathbb{Q}(\sqrt{-3})$.

Question 8

Let F be a field of characteristic $p \neq 0$ and let L/F be a field extension. Show that if $\alpha \in L$ is separarble over F, then $F(\alpha) = F(\alpha^p)$

Solution: Generally, $F(\alpha^p) \subset F(\alpha)$, leaving only to show that $F(\alpha) \subset F(\alpha^p)$. Let $m_{\alpha,F}$ be the minimal polynomial of α over F and $m_{\alpha,F(\alpha^p)}$ be the minimal polynomial of α over $F(\alpha^p)$. Then, as $F(\alpha^p)$ is an extension of F, then

$$m_{\alpha,F(\alpha^p)} \mid m_{\alpha,F}$$

From the assumption, α is separable over F, thus $m_{\alpha,F}$ is separable. This implies that $m_{\alpha,F(\alpha^p)}$ as it divides a separable polynomial.

However, notice that $x^p - \alpha^p$ has α as a root, and

$$x^p - \alpha^p = (x-\alpha)^p$$

This means that $m_{\alpha,F(\alpha^p)} = (x-\alpha)^k$ for some $k < p$. However, as $m_{\alpha,F(\alpha^p)}$ is separable, then $m_{\alpha,F(\alpha^p)} = x - \alpha$, otherwise, there is a root with multiplicity greater than 1, thus not separable.

As $m_{\alpha,F(\alpha^p)} = x - \alpha$, then $F(\alpha^p, \alpha) = F(\alpha)$ is a field extension of degree 1 over $F(\alpha^p)$. This lead to a conclusion that, $F(\alpha^p) = F(\alpha)$.

Question 9

Let A be the sum of all elements of a finite field $\mathbb{F}_q$ and let B be the product of all non-zero elements of $\mathbb{F}_q$. Compute $A + B$.

Solution: Let $\text{char}(\mathbb{F}_q) = p > 0$. It is possible to label the elements of $\mathbb{F}_q$ as $a_1, \dots, a_q$ such that $a_q = 0$ and for all i, $a_i + a_{q-i} = 0$ as every element in a field has a additive inverse. Then, if $p = 2$, then there will be one element in which $i = q - i$, which is $i = \frac{q}{2}$, and $a_{q/2} + a_{q/2} = 0$ gives that $a_{q/2} = q/2$

For $p \neq 2$, the elements can be label in another way, which is $m_1, \dots, m_q$ where $m_q = 0$, $m_1 = 1$, $m_{q-1} = -1$ and for other i, $m_i \cdot m_{q-i} = 1$. This is because any element of a field, apart from 0 has an inverse. And as for $p \neq 2$, there is only 2 roots of $x^2 - 1$, which are $x = 1$ and $x = -1$, then every element apart from $0, 1, -1$ has inverse that is differred from itself.

For $p = 2$, there is only 1 root of $x^2 - 1 = (x-1)^2$, which is 1, thus, the other $q - 2$ elements apart from 1 and 0 has an inverse that is distinct from itself. So the label is set such that $m_i \cdot m_{q-i+1} = 1$ for all $2 \leq i < q$ instead.

If $p \neq 2$, there are $q - 1$ non-zero elements, which is even. Therefore,

$$\sum_{a\in\mathbb{F}_q} a = \sum_{i=1}^{q} a_i = a_1 + a_q + \sum_{i=2}^{q-1} a_i = a_1 + a_q + \sum_{i=2}^{\frac{q}{2}} a_i + a_{q-i} = 1 + 0 + \sum_{i=2}^{\frac{q}{2}} 0 = 1$$

$$\prod_{m\in\mathbb{F}_q^\times} m = \prod_{i=1}^{q-1} m_i = m_1 \cdot m_{q-1} \cdot \prod_{i=2}^{q-2} m_i = -1 \cdot \prod_{i=2}^{\frac{q-1}{2}} m_i \cdot m_{q-i} = -\prod_{i=2}^{\frac{q-1}{2}} 1 = -1$$

So $A + B = 0$.

Otherwise if $p = 2$, then

$$\sum_{a\in\mathbb{F}_q} a = \sum_{i=1}^{q} a_i = a_q + \sum_{i=1}^{q-1} a_i = a_q + a_{q/2} \sum_{i=1}^{\frac{q}{2}-1} a_i + a_{q-i} = 0 + \frac{q}{2} + \sum_{i=1}^{\frac{q}{2}-1} 0 = \frac{q}{2}$$

$$\prod_{m\in\mathbb{F}_q^\times} m = \prod_{i=1}^{q-1} m_i = q_1 \prod_{i=2}^{q-1} m_i = \prod_{i=2}^{\frac{q}{2}} m_i \cdot m_{q-i+1} = \prod_{i=2}^{\frac{q}{2}} 1 = 1$$

So, $A + B = \frac{q}{2} + 1$

Question 10

Assume that $\text{char}(\mathbb{F}_q) \neq 2$. Prove that $\left|\left\{ x^2 \mid x \in \mathbb{F}_q \right\}\right| = (|\mathbb{F}_q| + 1)/2$.

Solution: Since $\text{char}(\mathbb{F}_q) \neq 2$, then q is odd. As there is q elements, then $x^2 = (q-x)^2$ for all $0 \leq x < q$. Thus, $\left|\left\{ x^2 \mid x \in \mathbb{F}_q \right\}\right| \leq (|\mathbb{F}_q| + 1)/2$.

Now, if consider that the polynomial $x^2 - a$ where $a \in \left\{ x^2 \mid x \in \mathbb{F}_q \right\}$ is reducible to $x^2 - a = (x-\alpha)(x+\alpha)$ as $x^2 - a$ is monic. This means that no other element, apart from α and $-\alpha$, can be the root of $x^2 - a$, and thus, no other element β would satisfy $\beta^2 = a$.

Thus, each of the element of $\left\{ x^2 \mid x \in \mathbb{F}_q \right\}$ corresponds to 2 mutually exclusive elements of $\mathbb{F}_q$, namely, x and $-x$ (and no other elements).

This means that $\left|\left\{ x^2 \mid x \in \mathbb{F}_q \right\}\right| \geq |\mathbb{F}_q|/2$ Hence, $\left|\left\{ x^2 \mid x \in \mathbb{F}_q \right\}\right| = (|\mathbb{F}_q| + 1)/2$