Q1 (a) Give an example of an irreducible polynomial of degree 3 in $\mathbb{F}_2[x]$ and show how to use this to construct a field with 8 elements.

Let $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. (or $f(x) = x^3 + x^2 + 1$, the same argument will apply)

If $f(x) = g(x) \cdot h(x)$, then $\deg g + \deg h = 3$ so WLOG $\deg g \leq 1$.

If $\deg g = 0$ then g is a unit so the factorisation is trivial.

If $\deg g = 1$, $g(x) \in \mathbb{F}_2[x]$ then g has a root in $\mathbb{F}_2$. Thus f has a root in $\mathbb{F}_2$. But $f(0) = 1$, $f(1) = 1$, a contradiction.

Therefore $f(x)$ is irreducible in $\mathbb{F}_2[x]$.

Consider the ring $\mathbb{F}_2[x]/(f(x))$.

Since f is irreducible this ring is a field

Since $\deg f = 3$, this is a degree 3 field extension of $\mathbb{F}_2$.

Thus $\mathbb{F}_2[x]/(f(x))$ is a field with $2^3 = 8$ elements.

(b) Construct an element of order 7 in $GL_3(\mathbb{F}_2)$.

Write $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$. The multiplicative group $\mathbb{F}_8^\times$ has order seven so $x^7 = 1$.

Multiplication by x is a $\mathbb{F}_2$-linear transformation on the three-dimensional $\mathbb{F}_2$-vector space $\mathbb{F}_8$ that has order 7.

With respect to the basis $(1, x, x^2)$ of $\mathbb{F}_8$, the matrix of multiplication by x is $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

The element $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in GL_3(\mathbb{F}_2)$ thus has order 7 (which can also be checked by direct computation).

Q5: Let p be a prime number. Let G be a transitive subgroup of S_p containing a transposition. Prove that $G = S_p$.

Define a graph with vertices $1, 2, \dots, p$ and where i and j are connected by an edge if and only if $(i\ j) \in G$.

Lemma: All vertices of this graph have the same degree.

Proof: Let i and j be two vertices. Since G is transitive, there exists $\sigma \in G$ with $\sigma(i) = j$.

For any $k \neq i$:

$$\sigma \cdot (i\ k) \cdot \sigma^{-1} = (j\ \sigma(k))$$

Thus if $(i\ k) \in G$ then $(j\ \sigma(k)) \in G$.

This implies that the degree of i is less than or equal to the degree of j. (using $k \longmapsto \sigma(k)$ is injective).

Similarly the degree of j is less than or equal to the degree of i, so we must have equality, proving the Lemma.

Lemma: Every connected component of our graph is a complete graph.

Proof: We have to show that if i and j are joined by an edge, and if j and k are joined by an edge, then i and k are joined by an edge.

This is true since $(i\ k) = (j\ k)(i\ j)$.

The two lemmas imply that our graph is a disjoint union of complete graphs, each of the same size.

Since we have a prime number of vertices there are two possibilities

(i) disjoint union of p copies of complete graph on one vertex

(ii) complete graph on p vertices.

(i) is impossible since G is assumed to contain a transposition. So (ii) must hold. Thus all transpositions lie in G. Since the symmetric group is generated by transpositions, this implies $G = S_p$, as required.

Q6: Let H be a subgroup of S_n of index n. Let $g_1H, \dots, g_nH$ be the n left cosets of H in S_n. Define a homomorphism $\phi : S_n \to S_n$ by

$$\phi(\sigma)(i) = j \quad \text{where} \quad \sigma(g_iH) = g_jH.$$

Prove that ϕ is an inner automorphism if and only if H is the stabiliser of some $i \in \{1, 2, \dots, n\}$ under the natural action of S_n on $\{1, 2, \dots, n\}$.

First suppose that H is the stabaliser of $k \in \{1, 2, \dots, n\}$. Then the n left cosets of H are all of the form

$$(k\ j)H = \{\sigma \in S_n \mid \sigma(k) = j\}.$$

Therefore, there exists a permutation $\tau \in S_n$ such that

$$g_iH = \{\sigma \in S_n \mid \sigma(k) = \tau(i)\}.$$

We will show that $\phi(\sigma) = \tau^{-1}\sigma\tau$.

If $\sigma(g_iH) = g_j(H)$, then $(\sigma g_i)(k) = g_j(k)$,

ie $\sigma\tau(i) = \tau(j)$.

$\therefore (\tau^{-1}\sigma\tau)(i) = j$.

By definition of ϕ, $\phi(\sigma)(i) = j$, so we've shown $\phi(\sigma) = \tau^{-1}\sigma\tau$, hence $\phi(\sigma)$ is inner.

Conversely suppose that $\phi(\sigma)$ is an inner automorphism: $\phi(\sigma) = \tau^{-1}\sigma\tau$ for some $\tau \in S_n$.

One coset must be the trivial coset. Thus $g_\ell H = H$ for some ℓ.

Let $h \in H$. Then $h(g_\ell H) = hH = H = g_\ell H$

so $\phi(h)(\ell) = \ell$.

$\therefore (\tau^{-1}h\tau)(\ell) = \ell$

$\therefore h(\tau(\ell)) = \tau(\ell)$.

$\therefore H \subset$ Stabiliser of $\tau(\ell)$.

In this inclusion, both subgroups are subgroups of index n. Thus we must have equality, and hence H is a stabiliser as required.