Let $V$ be a $\mathbb{Q}$-vector space and $T : V \to V$ linear. Suppose that the invariant factors of $T$ are $q_1 := (x - 1)(x^2 + 1)$ and $q_2 := (x - 1)^3(x^2 + 1)$.

a) What is $\dim V$? Determine minimal polynomial and characteristic polynomial of $T$.

b) What is the rational canonical form for $T$?

c) Considering a matrix for $T$ over $\mathbb{C}$, what is the Jordan Canonical form?

d) Show that $V$ is the direct sum of four $T$-invariant subspaces. (10 points)
The \( J = \begin{pmatrix} -1 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \) is a basis.

We can split conjugate factors, that is, there is a basis \( \mathbf{v} \) such that for \( T \) is a block

\[
\begin{pmatrix} \mathbf{e}_{x-1} \\ \mathbf{e}_{x+1} \\ \mathbf{e}_{x-1}^2 \end{pmatrix} = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{pmatrix} \begin{pmatrix} \mathbf{b}_3 \\ \mathbf{b}_4 \end{pmatrix} \begin{pmatrix} \mathbf{b}_5 \\ \mathbf{b}_6 \end{pmatrix}
\]

so that \( \text{Span}(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4, \mathbf{b}_5, \mathbf{b}_6) \) is a basis.

\( \text{Span}(\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3) \) and \( \text{Span}(\mathbf{b}_4, \mathbf{b}_5, \mathbf{b}_6) \) are invariant.
2) For which $n$ are there elements of order $n$ in $GL_2(\mathbb{Q})$? For each possible order show
with an explicit matrix that such elements exists.

**Hint:** What can you tell about the minimal polynomial? (10 points)

Suppose $A \in GL_2(\mathbb{Q})$ has order $n$, then $A^n = I$

The minimal polynomial of a nilpotent $x^n - 1$.

The every irreducible factor of a nilpotent must divide $x^n - 1$.

We know $x^n - 1 = \prod d \phi_d(x)$. For $A \in GL_2(\mathbb{Q})$ we need

that $\deg(\phi_d(x)) = \deg(d) \leq 2$ if $d = \prod p_i^{e_i}$ the

$$\deg(d) = \prod (e_i - 1) p_i^{e_i - 1}$$

The $\deg(d) \leq 2$ implies $p_i \leq 3$

If $e_i = 2$ if $p_i = 2$

$$q_i \leq 1$$

if $p_i = 3$

We now show that which those 5 order occur:

**Order 1:** $(1,0)$  

**Order 2:** $(-1,0)$  

**Order 3:** $[C_{x^2 + x + 1}] = (0,-1)$

**Order 4:** $[C_{x^4}] = (0,-1)$  

**Order 6:** $[C_{x^6 - x + 1}] = (0,-1)$
3) Let $F = \mathbb{F}_p$ be the finite field of order $p$ and $F \leq K = \mathbb{F}_{p^n}$ for a natural number $n \geq 2$.

a) Show that $\text{Gal}(K/F)$ is cyclic.

b) Let $f \in F[x]$ be irreducible of degree dividing $n$. Show that $f$ must be a divisor of $x^{p^n} - x$.

(10 points)

a) We know that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Now consider $\psi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

\[ \psi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^p. \]

Let $\psi$ be a field automorphism. Note that $\mathbb{F}_{p^n} = \text{Gal}(x^{p^n} - x)$.

As $\psi^q = \text{id}$, we have for $b < n$ we have that

\[ x^{p^b} - x \] is separable (as $\gcd(x^{p^b} - x, (x^{p^b} - x)) = 1$)

is an extension of $\mathbb{F}_p = \mathbb{F}_p(x^{p^b} - x)$. This has at most $p^b - p$ roots.

The not every element of $\mathbb{F}_{p^n}$ fulfills that $x^{p^b} = x$. Hence $\psi^b = \text{id}$, i.e., the order of $\psi$ is $n$. Thus $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \left\{ \psi \right\}$.

b) Suppose $\alpha \in \mathbb{F}_{p^n}$ is irreducible. Then $\alpha$ defines a field $K = \mathbb{F}_p(\alpha)$, a subfield of $\mathbb{F}_{p^n}$ with $[K : \mathbb{F}_p] = b$ for $b < n$ because for any $\beta$ in $K$ is up to isomorphism only one field of order $p^b$.

b) The field of order $p^b$ is a subfield of the field of order $p^n$ if $b | n$. Hence we have that $K = \mathbb{F}_{p^b}$.

Thus $\alpha$ is a root of $x^{p^b} - x$. This holds for any root of $f$. 

4) Let $K = \mathbb{Q}(\zeta_{15})$ be the splitting field of $x^{15} - 1$ over $\mathbb{Q}$.

a) Determine the structure and generators for $G = \text{Gal}(K/\mathbb{Q})$. Express complex conjugation as a product of the generators.

b) Determine the subgroups of $G$ and for every subgroup $U \leq G$ the corresponding fixed field $\text{Fix}(U)$. (You may use without proof that $\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$.)

\[\begin{align*}
\text{Let } K &= \mathbb{Q}(\zeta_{15}) \\
\text{splitting field of } x^{15} - 1 \text{ over } \mathbb{Q}.
\end{align*}\]

\[\text{a) We know the lattice: } \text{Gal}(K/Q) = \langle \alpha, \beta \rangle, \quad \text{where } \alpha \text{ and } \beta \text{ generate } \mathbb{Q}(\zeta_{15}) \text{ over } \mathbb{Q}.\]

\[\text{Let } \mathbb{Q}(\zeta_{15}) = \mathbb{Q}(\zeta_5) \times \mathbb{Q}(\zeta_3), \text{ by CEA.}\]

\[\text{We find that } \mathbb{Q}(\zeta_{15}) \cong \mathbb{Q}(\zeta_5) \times \mathbb{Q}(\zeta_3) \text{ by ECA.}\]

\[\text{Let } \mathbb{Q}(\zeta_{15}) = \mathbb{Q}(\zeta_5) \times \mathbb{Q}(\zeta_3).\]

\[\text{Then we get the following subgroups of } G:\]

\[\begin{align*}
\mathbb{Q}(\zeta_{15}) &= \mathbb{Q}(\zeta_5) \times \mathbb{Q}(\zeta_3) \\
\text{and } \mathbb{Q}(\zeta_{15}) &= \mathbb{Q}(\zeta_5) \times \mathbb{Q}(\zeta_3).\]

\[\text{Now let subgroups. We know that } \mathbb{Q}(\zeta_{15}) = \mathbb{Q}(\zeta_5) \times \mathbb{Q}(\zeta_3) \text{ is }\]

\[\text{a subgroup of order } 2 \text{ in } G.\]

\[\text{Subgroups of } G \text{ of order } 2 \text{ are cyclic.}\]
The 16 correspondingly styled elements are: \( \mathbb{Q} \), \( \mathbb{Q}(i\sqrt{3}) \), \( \mathbb{Q}(i\sqrt{5}) \), \( \mathbb{Q}(i\sqrt{15}) \), \( \mathbb{Q}(3^{2/5}) \), \( \mathbb{Q}(3^{4/5}) \), \( \mathbb{Q}(3^{1/5}) \), \( \mathbb{Q}(i\sqrt{15}) \), and \( \mathbb{Q}(3^{2/5}) \).
5) Let \( R \) be an integral domain and \( F = R^2 \) a free module of rank 2. Let \( S = \langle a \rangle \ (a \in F) \) be a cyclic \( R \)-submodule of \( F \). Show that \( F/S \) cannot be a torsion module. (10 points)

Assume \( R = \langle r_1, r_2 \rangle \) and \( a = x r_1 + y r_2 \).

This is a torsion module if \( S = (x, y) \) which has \( SNF \ (gcd(xy), 0) \). Then the structure of \( R/S \) is \( \langle \text{gcd}(xy) \rangle \) \( R/(\text{gcd}(xy)) \oplus R \), but

\( R \) is not a torsion module (\( \langle x, y \rangle = 0 \Rightarrow s = 0 \)).