Mathematics 567						Final (50 points)	05/10/07, 13.30
Points (leave blank)							
1	2	3	4	5	$\sum$	Name:	
						(clearly, please)	

Time: 110 minutes. Explanations are a crucial part of a solution. If you are using a theorem from the course or the book, state so. You can work on the problems in any order you like.

1) 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)**

a) We know that char pol $= q_1 \cdot q_2 = (x-1)^4(x^2+1)^2$

and thus $\dim V = 2\cdot 2+4 = 8$

The min pol is the last invariant factor, $q_2 = (x-1)^3(x^2+1)$

b) The RCF is given by companion matrices for the invariant factors

$$\begin{bmatrix} C_{q_1} & 0 \\ 0 & C_{q_2} \end{bmatrix}$$

c) Over $\mathbb{C}$ we have $(x^2+1) = (x+i)(x-i)$. We thus have Jordan blocks for $1, i, -i$. The min pol yields the largest blocks for these factors. The sizes of the other blocks are given by the other invariant factors. Thus

1 Jordan block for -1, size 1
1 — " — , size 3
2 Jordan blocks for i, size 1
2 Jordan blocks for $-i$, size 1

Thus $J = \begin{pmatrix} -1 & & & & & & & \\ & -1 & 1 & 0 & & & & \\ & 0 & -1 & 1 & & & & \\ & 0 & 0 & -1 & & & & \\ & & & & i & & & \\ & & & & & i & & \\ & & & & & & -i & \\ & & & & & & & i \end{pmatrix}$

d) We can split coprime factors, thus there is a basis s.t. the matrix for T is

$$\begin{array}{cccc} \begin{pmatrix} C_{x-1} & & & 0 \\ & C_{x^2+1} & & \\ & & C_{(x-1)^3} & \\ 0 & & & C_{x^2+1} \end{pmatrix} \\ b_1 \quad b_2\, b_3 \quad b_4, b_5, b_6 \quad b_7, b_8 \end{array}$$

Then the subspaces spanned by each basis vector corresponding to blocks. (ie $\text{Span}(b_1)$, $\text{Span}(b_2, b_3)$, $\text{Span}(b_4, b_5, b_6)$ and $\text{Span}(b_7, b_8)$ are invariant.

2) For which n are there elements of order n in $\mathrm{GL}_2(\mathbb{Q})$? 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 $A^n = I$
then the minimal polynomial of A must divide $x^n - 1$.
Thus every irreducible factor of min pol$_A$ must divide $x^n - 1$
We know $x^n - 1 = \prod_{d | n} \Phi_d(x)$. For $A \in GL_2(\mathbb{Q})$ we need
that $\deg(\Phi_d(x)) = \varphi(d) \leq 2$ If $d = \prod p_i^{e_i}$ then

$\varphi(d) = \prod (p_i - 1) p_i^{e_i - 1}$ Thus $\varphi(d) \leq 2$ implies $p_i \leq 3$

$e_i \leq \begin{cases} 2 & \text{if } p_i = 2 \\ 1 & \text{if } p_i = 3 \end{cases}$ $\Rightarrow d \in \{1, 2, 3, 4, 6\}$ (and all these have $\varphi(d) \leq 2$)
$\varphi(d)$: 1 1 2 2 2

~~[illegible]~~

If $\varphi(d) = 2$ then minpol$(A) = \Phi_d$.
If $\varphi(d) = 1$ then minpol$(A) = \Phi_d \cdot$ another factor of deg 1

We now show that indeed these 5 order occur:

Order 1: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ order 2 $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, order 3 $[C_{x^2+x+1}] = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$

Order 4: $[C_{x^2+1}] = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ order 6: $[C_{x^2-x+1}] = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$

3) Let $F = \mathbb{F}_p$ be the finite field of order p and $F \leq K = \mathbb{F}_{p^a}$ for a natural number $a \geq 2$.
a) Show that $\mathrm{Gal}(K/F)$ is cyclic.
b) Let $f \in F[x]$ be irreducible of degree dividing a. Show that f must be a divisor of $x^{p^a} - x$.

(10 points)

a) We know that $[\mathbb{F}_{p^a} : \mathbb{F}_p] = a$. Now consider the map $\varphi : \mathbb{F}_{p^a} \to \mathbb{F}_{p^a}$, $x \mapsto x^p$. Then (Lecture, Frobenius automorphism) φ is a field automorphism. Note that $\mathbb{F}_{p^a} = \mathrm{Spl}(x^{p^a} - x)$, thus $\varphi^a = \mathrm{id}$. Vice versa for $b < a$ we have that $x^{p^b} - x$ $\boxed{\text{is separable } (\text{as } \gcd(x^{p^b}-x, (x^{p^b}-x)') = \gcd(x^{p^b}-x, -1) = 1)}$, thus has at most $p^b < p^a$ roots, thus not any element of $\mathbb{F}_{p^a}$ fulfills that $x^{p^b} = x$, thus $\varphi^b \neq \mathrm{id}$, thus the order of φ is a. Thus $\mathrm{Gal}(\mathbb{F}_{p^a}/\mathbb{F}_p) = \langle \varphi \rangle$

b) Suppose $\deg f \mid a$, ~~...~~ f irreducible. Then f defines a field $K = \mathbb{F}_p(\alpha)$, α a root of f with $[K : \mathbb{F}_p] = \deg f \mid a$

Because a) For any n there is up to isomorphism only one field of order p^n
b) The field of order p^b is a subfield of the field of order p^a if $b \mid a$

we have that $K \cong$ a subfield of $\mathbb{F}_{p^a}$ $\Rightarrow$ α is a root of $x^{p^a} - x$. This holds for any root α 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 $G = \mathrm{Gal}(K/\mathbb{Q})$. 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 $\mathrm{Fix}(U)$. (You may use without proof that $\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$.) **(10 points)**

a) We know from lecture: $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$

$\cong \mathbb{Z}_2 \times \mathbb{Z}_4$. Generators: 2 generates $(\mathbb{Z}/3\mathbb{Z})^\times$. By CRT we find that $11 \equiv 2\ (3)$, $\equiv 1\ (5)$. Similarly 2 generates $(\mathbb{Z}/5\mathbb{Z})^\times$ and $7 \equiv 2\ (5)$, $\equiv 1\ (3)$.

Thus let $\sigma: \zeta_{15} \mapsto \zeta_{15}^{11}$, $\tau: \zeta_{15} \mapsto \zeta_{15}^{7}$. Then we get the following lattice for $G \cong \mathbb{Z}_2 \times \mathbb{Z}_4$: (subgroups of order 2 must be cyclic, subgroups of order 4 is cyclic or $\mathbb{Z}_2 \times \mathbb{Z}_2$)

subgroup

$$\begin{tikzcd}
8 & & G \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
4 & \langle\tau\rangle \arrow[d, dash] & \langle\sigma\tau\rangle \arrow[dl, dash] & \langle\sigma,\tau^2\rangle \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \\
2 & \langle\tau^2\rangle \arrow[dr, dash] & \langle\sigma\tau^2\rangle \arrow[d, dash] & \langle\sigma\rangle \arrow[dl, dash] \\
1 & & \langle 1\rangle &
\end{tikzcd}$$

Now find subfields. We know that $\mathbb{Q}(\zeta_3) = \mathbb{Q}(i\sqrt{3})$, $\mathbb{Q}(\zeta_5)$ (and thus $\mathbb{Q}(\sqrt{5})$) and thus also $\mathbb{Q}(i\sqrt{15})$ are subfields. The subgroups of order 4 thus correspond to $\mathbb{Q}(i\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i\sqrt{15})$

We know that complex conj is: $\zeta_{15} \mapsto \zeta_{15}^{14}$, hence it is $\sigma\tau^2$, thus $\langle\sigma\tau^2\rangle$ corresponds to the real subfield. Also by construction σ does not act on ζ_5.

This follows: $\langle\sigma\tau^2\rangle \hat{=} \mathbb{Q}(\zeta_{15} + \overline{\zeta_{15}})$, $\langle\sigma,\tau^2\rangle \hat{=} \mathbb{Q}(\sqrt{5})$,
$\langle\sigma\rangle \hat{=} \mathbb{Q}(\zeta_5)$, $\langle\tau\rangle \hat{=} \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\zeta_3)$ (as τ does not act on ζ_3), thus $\langle\sigma\tau\rangle \hat{=}$ $\mathbb{Q}(i\sqrt{15})$ and $\langle\tau^2\rangle \hat{=} \mathbb{Q}(i\sqrt{3}, \sqrt{5})$

Thus the corresponding subfield diagram is

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{Q} \arrow[dl] \arrow[d] \arrow[dr] & & \\
\mathbb{Q}(i\sqrt{3}) \arrow[dr] & \mathbb{Q}(i\sqrt{15}) \arrow[d] & \mathbb{Q}(\sqrt{5}) \arrow[dl] \arrow[d] \arrow[dr] & \\
 & \mathbb{Q}(i\sqrt{3},\sqrt{5}) \arrow[dr] & \mathbb{Q}(\zeta_5+\overline{\zeta_{15}}) \arrow[d] & \mathbb{Q}(\zeta_5) \arrow[dl] \\
 & & \mathbb{Q}(\zeta_{15}) &
\end{tikzcd}$$

5) Let R be an ~~integral domain~~ PID 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 $a = x r_1 + y r_2$

Then the relation matrix for S is (x, y) which

has SNF $(\gcd(x,y), 0)$. Thus the structure

of R/S is (Fund. Thm!) $R/(\gcd(x,y)) \oplus R$, but

R is not a torsion module ($\forall$ $s \cdot r = 0 \Rightarrow s = 0$ as