Morning solutions

(1) Using elementary row operations we get

$$\begin{pmatrix} 5 & 4 \\ 2 & 7 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & -10 \\ 2 & 7 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & -10 \\ 0 & 27 \end{pmatrix}$$

Using elementary column operations we get

$$\begin{pmatrix} 1 & -10 \\ 0 & 27 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 27 \end{pmatrix}$$

and $\mathbb{Z}/^2M \cong \mathbb{Z}/(27)$. Since $\mathbb{Z}/(27)$ has a unique subgroup of index 9 (and order 3), there exists a unique subgroup of $\mathbb{Z}^2$ containing M that has index 9. This module M is generated by $(1, -10)$ and $(0, 9)$.

(2) Suppose that B be the Jordan normal form of A and let $J_n(\lambda)$ be a Jordan block of B of size $n \times n$ with eigenvalue λ. If $n > 1$ then $J_n(\lambda)^2 - \lambda^2 I$ is nonzero and nilpotent. This means that B has a generalized eigenvector with eigenvalue λ^2 that is not an eigenvector. This implies that B and A are not diagonalizable, which is a contradiction. Therefore $n = 1$. So all the Jordan blocks of B have size 1×1. Therefore, B is diagonal and A is diagonalizable.

(3) (a) Let $\phi : R \to \mathbb{Z}[x]/(2, x)$ be the homomorphism defined by $\phi(p(x)) = p(x)+(2, x)$. The homomorphism is surjective, and the kernel is $I := (2, 2x, 2x^2, 2x^3, ...)$. By the first isomorphism theorem, R/I is isomorphic to $\mathbb{Z}[x]/(2, x) \simeq \mathbb{F}_2$, which is a field; thus, I is maximal. It is also not hard to see that $2x^n$ does not lie in the R-ideal generated by $(2, 2x, \ldots, 2x^{n-1})$ because the coefficient of x^n of any polynomial in $(2, 2x, \ldots, 2x^{n-1})$ is divisible by 4. This shows that I is not finitely generated.

(b) Let $\psi : R \to \mathbb{Z}[x]/(3) \cong \mathbb{F}_3[x]$ be the homomorphism defined by $\phi(p(x)) = p(x) + (3)$. It is easy to see that ψ is surjective and that the kernel is (3). So $R/(3)$ is isomorphic to $\mathbb{F}_3[x]$. In particular, this ring is not finite.

(4) (a) To specify a 2-dimensional subspace, one must specify two linearly independent vectors, and then mod out by the choice of basis. The number of possibilities for the first vector is p^4-1 as it can be any nonzero vector; the second vector cannot lie in the line spanned by the first, so there are $p^4 - p$ possibilities. In all, there are $(p^4 - 1)(p^4 - p)$ possibilities. The group $\mathrm{GL}_2(\mathbb{F}_p)$ has size $(p^2 - 1)(p^2 - p)$ by a similar argument; this group acts freely and transitivity on the choice of basis vectors for a given 2-dimensional subspace of V. Thus, the number of two dimensional subspaces is the quotient $\frac{(p^4-1)(p^4-p)}{(p^2-1)(p^2-p)} = (p^2 + 1)(1 + p + p^2)$. In particular, this number is congruent to 1 modulo p, and thus not divisible by p.

(b) The number computed in the first part is congruent to 1 modulo p. Now, for any p-group G acting on a set X, we have the congruence $|X^G| \equiv |X| \mod p$: all orbits that are not singletons (i.e., not fixed points) must have size divisible by p since G is a p-group. Applying this to the set X considered in (a) shows that

$|X^G| \equiv 1 \mod p$, and thus X^G is non-empty. This translates to the existence of a 2-dimensional subspace fixed (setwise) by G.

(5) The splitting field of K over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, i)$. Since $X^4 - 2$ is irreducible (by Eisenstein), we have $[\mathbb{Q}(\sqrt[4]{2} : \mathbb{Q})] = 4$. Since $i \notin \mathbb{Q}(\sqrt[4]{2})$, we have $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$ and $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [Q(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] \cdot [Q(\sqrt[4]{2} : \mathbb{Q})] = 2 \cdot 4 = 8$. From $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)]] \cdot [\mathbb{Q}(i) : \mathbb{Q}]$ follows that $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)]] = 4$ and $x^4 - 2$ is irreducible over $\mathbb{Q}(i)$.

(a) There exists an automorphism σ fixing $\mathbb{Q}(i)$ such that $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$. Let τ be complex conjugation. On the set of roots $\{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$ the actions of the automorphisms are given by $\sigma = (1\ 2\ 3\ 4)$ and $\tau = (2\ 4)$. Together they generate the dihedral group D_8 with 8 elements. So this must be the whole Galois group.

(b) By the Galois correspondence these subfields correspond to subgroups of D_8 of order 2. The order 2 subgroups are $\langle(1\ 3)\rangle$, $\langle(2, 4)\rangle$, $\langle(1\ 3)(2\ 4)\rangle$, $\langle(1\ 2)(3\ 4)\rangle$ and $\langle(1\ 4)(2\ 3)\rangle$. The corresponding subfields are $\mathbb{Q}(i\sqrt[4]{2})$, $\mathbb{Q}(-\sqrt[4]{2})$, $\mathbb{Q}(i, \sqrt{2})$ $\mathbb{Q}((1 + i)\sqrt[4]{2})$ and $\mathbb{Q}((1 - i)\sqrt[4]{2})$. respectively.

Afternoon solutions

(1) We have $[M : \mathbb{F}_p] = 60$, $[K : \mathbb{F}_p] = 6$ and $[L : \mathbb{F}_p] = 10$. The Galois group G of the extension $M/\mathbb{F}_p$ is $\mathbb{Z}/(60)$. The group G_K fixing K has index 6 so it is generated by $10 + (60)$. Similarly, the Galois group G_L that fixes L is generated by $6 + (60)$. The intersection of G_K and G_L is generated by $30 + (60)$. This intersection is isomorphic to $\mathbb{Z}/2$. This implies that $[M : KL] = 2$. So $[KL : \mathbb{F}_p] = 60/2 = 30$ and KL has p^{30} elements. The group generated by G_K and G_L is generated by $2 + (60)$. This group is isomorphic to $\mathbb{Z}/30$. Therefore $[M : K \cap L] = 30$, $[K \cap L : \mathbb{F}_p] = 60/30 = 2$ and $K \cap L$ has p^2 elements.

(2) The Galois group of K over $\mathbb{F}_p$ is $\mathbb{Z}/(de)$ since the finite field $\mathbb{F}_p$ has a unique extension (necessarily Galois) of degree n for any integer $n \geq 1$. As $\mathbb{Z}/(de)$ has a unique quotient of size d (namely, $\mathbb{Z}/(d)$), there is a unique field L between $\mathbb{F}_p$ and K such that $L/\mathbb{F}_p$ is Galois with group $\mathbb{Z}/(d)$. But then L has degree d over $\mathbb{F}_p$, so L must have p^d elements.

(3) Let $f(x)$ be the characteristic polynomial of A. Its degree is n. Since $f(x)$ is rreducible, the ideal $(f(x))$ is maximal.

(a) Consider the ring homomorphism $\phi : K[x] \to \mathrm{Mat}_{n,n}(K)$ that sends the polynomial $p(x)$ to $p(A)$. For any polynomial $p(x)$ we can write $p(x) = q(x)f(x) + r(x)$ where $r(x)$ has degree $< n$ (or is equal to 0). We have $p(A) = q(A)f(A) + r(A) = r(A)$ which lies in the span of $I, A, A^2, \ldots, A^{n-1}$. So the image $\mathrm{im}(\phi)$ of ϕ is equal to the span of $I, A, \ldots, A^{r-1}$. The kernel of ϕ contains the maximal ideal $(f(x))$. Since $\ker(\phi)$ is clearly not equal to $K[x]$, we must have $\ker(\phi) = (f(x))$. By the first isomorphism theorem, we have $K[x]/(f(x)) \cong \mathrm{im}(\varphi)$. Because $(f(x))$ is maximal, $K[x]/(f(x))$ is a field.

(b) The map $\psi : \mathrm{Mat}_{n,n}(K) \to K^n$ defined by $\psi(p(x)) = p(A)v$ is a $K[x]$-module homomorphism. . The kernel is an submodule (hence an ideal) of $K[x]$ that contains the maximal ideal $(f(x))$. The kernel is not the whole ring, because v is nonzero. Because $(f(x))$ is maximal, the kernel of ψ must be equal to $(f(x))$. If $v, Av, \ldots, A^{n-1}v$ are linearly dependent, then there exists a nonzero polynomial $q(x)$ of degree $\leq n - 1$ with $q(A)v = 0$. Since $q(x) \in \ker(\psi) = (f(x))$ we have $f(x) \mid q(x)$ but this is a contradiction because $f(x)$ has degree n and $q(x)$ has degree $< n$. So $v, Av, \ldots, A^{n-1}v$ are linearly independent. Since K^n has dimension n, these vectors must form a basis.

(4) (a) 0. Because $\mathbb{Z}/(2) \otimes \mathbb{Z}/(3)$ is generated as a $\mathbb{Z}$-module by

$$(1 + (2)) \otimes (1 + (3)) = (3 + (2)) \otimes (1 + (3)) = \\ = (1 + (2)) \otimes (3 + (3)) = (1 + (2)) \otimes (0 + (3)) = 0.$$

(b) $\mathbb{Z}/(3)$. The map $\psi : \mathbb{Z}/(3) \times \mathbb{Z}/(9) \to \mathbb{Z}/(3)$ given by $\psi(a+(3), b+(9)) = ab+(3)$ is well defined, so there exists a surjective group homomorphism $\mathbb{Z}/(3) \otimes_{\mathbb{Z}} \mathbb{Z}/(9) \to$

$\mathbb{Z}/(3)$. On the other hand $\mathbb{Z}/(3) \times \mathbb{Z}/(9)$ is generated by $(1+(3)) \otimes (1+(9))$ which has order at most 3 in $\mathbb{Z}/(3) \otimes_{\mathbb{Z}} \mathbb{Z}/(9)$.
$\mathbb{Z}/(3)$.

(c) 0.This module is generated by elements of the form

$$(\tfrac{a}{b} + \mathbb{Z}) \otimes \tfrac{c}{d} = (\tfrac{a}{b} + \mathbb{Z}) \otimes (b \cdot \tfrac{c}{db}) = (a + \mathbb{Z}) \otimes \tfrac{c}{db} = (0 + \mathbb{Z}) \otimes \tfrac{c}{db} = 0.$$

(5)

(a) Define $\psi : V \times V \times V \to \bigwedge^2 V \otimes V$ by

$$\psi(a, b, c) = (a \wedge c) \otimes b - (b \wedge c) \otimes a.$$

For fixed c, this map is bilinear in a and b. It is also skew-symmetric: $\psi(a, b, c) = -\psi(b, a, c)$. By the universal property of $\bigwedge^2 V$, there exists a map $\theta : \bigwedge^2 \times V \to \bigwedge^2 \otimes V$ such that

$$\theta((a \wedge b), c) = \psi(a, b, c) = (a \wedge c) \otimes b - (b \wedge c) \otimes a.$$

It is easy to verify that this map is also linear in c, so φ is bilinear, and there exists a linear map $\varphi : \bigwedge^2 V \otimes V \to \bigwedge^2 V \otimes V$ with the property

$$\varphi((a \wedge b) \otimes c) = \theta(a \wedge b, c) = (a \wedge c) \otimes b - (b \wedge c) \otimes a.$$

(b) Restricting φ to the span of $(e_1 \wedge e_2) \otimes e_3$, $(e_1 \wedge e_3) \otimes e_2$ and $(e_2 \wedge e_3) \otimes e_1$ gives the matrix

$$\begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}$$

This matrix has eigen value -2 with multiplicity 1 and eigenvalue 1 with multiplicity 2. For $i \neq j$ $e_i \wedge e_j) \otimes e_j$ is an eigenvector with eigenvalue 1. There are 6 such vectors. Combined we have the eigenvalue 1 with multiplicity 8 and the eigenvalue -2 with multiplicity 1.

(6) Let $n = 2^r m$ be the order of n where $r > 0$ and m is odd. Suppose that S is the 2-Sylow subgroup of G. It has 2^r elements. Since S is a nontrivial 2-group, it has a nontrivial center, and this nontrivial center has an element of order 2, call it g. Consider the action of G on itself by conjugation. If H is the stabilizer, and C is the orbit, then H is the centralizer of g, C is the conjugacy class of g and $|H| \cdot |C| = |G|$. Since H contains S, $|H|$ is divisible by 2^r which implies that $|C|$ is odd.