MATH 7752 Final

James Harbour

May 6, 2022

Problem 1

Let F be a field, $n \in \mathbb{N}$ and $A \in Mat_n(F)$.

(a): (10 points) Assume that $\text{char}(F) = 0$. Prove that the matrix A is nilpotent if and only if $\text{Tr}(A^k) = 0$, for all $k \in \mathbb{N}$.

Proof.

$\underline{\implies}$: Suppose that A is nilpotent. Then there exists some $N \in \mathbb{N}$ such that $A^N = 0$. Let $k \in \mathbb{N}$. Then we have that $(A^k)^N = (A^N)^k = 0$, so by definition $\mu_{A^k} \mid x^N$ whence $\mu_{A^k}(x) = x^m$ for some $m \leq N$.

Now let $\alpha_1(x) \mid \alpha_2(x) \cdots \mid \alpha_s(x)$ be the invariant factors for A^k. As $\alpha_s(x) = \mu_{A^k}(x) = x^m$, it follows that each $\alpha_i = x^{m_i}$ for some $0 \leq m_i \leq m$. But then each companion matrix C_{α_i} has zeroes along its diagonal, whence $\text{Tr}(A^k) = \sum_{i=1}^{s} \text{Tr}(C_{\alpha_i}) = 0$.

$\underline{\impliedby}$: (*N.B. I was unable to complete this direction, however I have left my partial work here*) Fix an algebraic closure $\overline{F} \supseteq F$ and let

$$JCF(A) = \begin{pmatrix} J(d_1, \lambda_1) & & \\ & \ddots & \\ & & J(d_s, \lambda_s) \end{pmatrix}$$

where $\lambda_i \in \overline{F}$, $d_i \in \mathbb{N}$. As $\text{Tr}(JCF(A)^k) = \text{Tr}(A^k)$ for all $k \in \mathbb{N}$ and $JCF(A)$ is nilpotent if and only if A is nilpotent, we may assume without loss of generality that $A = JCF(A)$. For $1 \leq i \leq s$, write $J(d_i, \lambda_i) = D_i + N_i$ where $D_i = \text{diag}(\lambda_i, \ldots, \lambda_i) \in M_{d_i \times d_i}(\overline{F})$ and $N_i = \begin{pmatrix} 0 & 1 & & \\ & 0 & & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix} \in M_{d_i \times d_i}(F)$. Then, $A = D + N$ where

$$D = \begin{pmatrix} D_1 & & \\ & \ddots & \\ & & D_s \end{pmatrix}, \qquad N = \begin{pmatrix} N_1 & & \\ & \ddots & \\ & & N_s \end{pmatrix}.$$

Note that D is diagonal and N is nilpotent. Now we compute

$$DN = \begin{pmatrix} D_1 & & \\ & \ddots & \\ & & D_s \end{pmatrix} \begin{pmatrix} N_1 & & \\ & \ddots & \\ & & N_s \end{pmatrix} = \begin{pmatrix} D_1N_1 & & \\ & \ddots & \\ & & D_sN_s \end{pmatrix} = \begin{pmatrix} \lambda_1 I_{d_1} N_1 & & \\ & \ddots & \\ & & \lambda_s I_{d_s} N_s \end{pmatrix}$$
$$= \begin{pmatrix} N_1(\lambda_1 I_{d_1}) & & \\ & \ddots & \\ & & N_s(\lambda_s I_{d_s}) \end{pmatrix} = \begin{pmatrix} N_1 D_1 & & \\ & \ddots & \\ & & N_s D_s \end{pmatrix} = ND.$$

Thus by repeated transpositions, $D^iN^j = N^jD^i$ for all $i, j \in \mathbb{N}$. Fix $i, j \in \mathbb{N}$. As N is nilpotent, there exists some $t \in \mathbb{N}$ such that $N^t = 0$. Then

$$(D^iN^j)^t = \overbrace{D^iN^j \cdots D^iN^j}^{t \text{ times}} = (D^i)^t(N^j)^t = D^{it}(N^t)^j = 0,$$

so D^iN^j is nilpotent. Then by the forward direction, $\mathrm{Tr}(D^iN^j) = 0$. So, for all $m \in \mathbb{N}$,

$$0 = \mathrm{Tr}(J^m) = \mathrm{Tr}\left(\sum_{k=0}^{m} \binom{m}{k} D^{m-k}N^k\right) = \sum_{k=0}^{m} \binom{m}{k} \mathrm{Tr}(D^{m-k}N^k) = \mathrm{Tr}(D^m) = d_1 \cdot \lambda_1^m + \cdots d_s \cdot \lambda_s^m.$$

□

(b): (4 points) Show that the assertion of (a) is false if $\mathrm{char}(F) \neq 0$.

Solution. Let $p = \mathrm{char}(F) > 0$.

If $n \geq p$, then consider the matrix $A = \begin{pmatrix} I_p & \\ & 0_{n-p} \end{pmatrix}$. We have that $\mathrm{Tr}(A^k) = \mathrm{Tr}(A) = p \cdot 1 = 0$ for all $k \in \mathbb{N}$, but $A^k = A \neq 0$ for all $k \in \mathbb{N}$. Thus, the assertion is false for nonzero characteristic.

□

Problem 2

Let $A \in GL_n(\mathbb{F}_p)$, where p is a prime number and $n \in \mathbb{N}$.

(a): (6 points) Suppose that the matrix A is **diagonalizable over the algebraic closure** $\overline{\mathbb{F}}_p$. Show that the order of A in the group $GL_n(\mathbb{F}_p)$ is equal to the lcm of the orders of the eigenvalues of A in $\overline{\mathbb{F}}_p^{\times}$.

Proof. Let $\lambda_1, \cdots, \lambda_n \in \overline{\mathbb{F}}_p^{\times}$ be the eigenvalues of A counted with multiplicity, let $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, and let m be the order of A in $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$. Then by assumption there exists some $S \in \mathrm{GL}_n \overline{\mathbb{F}}_p$ such that $A = S^{-1}DS$. Set $l = \mathrm{lcm}\{o(\lambda_i) : 1 \leq i \leq n\}$ where $o(\lambda)$ denotes the order of λ in $\overline{\mathbb{F}}_p^{\times}$. Then $A^l = S^{-1}D^lS = I_n$, so $m \mid l$.

On the other hand, suppose for the sake of contradiction that $m < l$. Then $I_n = A^m = S^{-1}D^mS \implies D^m = I_n$, whence $\lambda_i^m = 1$ for all $1 \leq i \leq n$, contradicting that l is the least common multiple of the orders of the λ_i's. □

(b): (10 points) Prove that $GL_n(\mathbb{F}_p)$ has an element B of exact order $p^n - 1$.

Proof. Note that as $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, $\mathbb{F}_{p^n} \cong (\mathbb{F}_p)^n$ as $\mathbb{F}_p$-vector spaces. Motivated by this observation, recall that $\mathbb{F}_{p^n}^\times$ is cyclic of order $p^n - 1$, so let $\mathbb{F}_{p^n}^\times = \langle \omega \rangle$. Consider the $\mathbb{F}_p$-linear map $T_\omega : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by left multiplication by ω. Note that as $\omega \neq 0$, $T_\omega \in \mathrm{GL}(\mathbb{F}_{p^n})$. Moreover, $(T_\omega)^k = T_{\omega^k}$ for $k \in \mathbb{N}$, so $(T_\omega)^k = id$ if and only if $\omega^k = 1$, whence the order of T_ω is precisely the order of ω, i.e. $p^n - 1$. Now fix any $\mathbb{F}_p$-basis $\mathcal{B} = \{1, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_{p^n}$ and set $B = [T_\omega]_\mathcal{B} \in \mathrm{GL}_n(\mathbb{F}_p)$. Then the order of $B \in \mathrm{GL}_n(\mathbb{F}_p)$ equals the order $T_\omega \in \mathrm{GL}(\mathbb{F}_{p^n})$, so we have found an element of order $p^n - 1$. □

(c): (4 points) Construct explicitly an element $B \in GL_2(\mathbb{F}_3)$ of order 8.

Solution. To begin, we compute in $\mathbb{F}_3[x]$ that

$$(x+1)^2 = x^2 + 2x + 1 \qquad (x+2)^2 = x^2 + x + 1 \qquad (x+1)(x+2) = x^2 + 2.$$

As $x^2 + 1$ is clearly not divisible by x and does not appear as one of the products above, it is irreducible in $\mathbb{F}_3[x]$. Thus $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(x^2+1)$. In the following, we suppress the overbars when denoting elements of $\mathbb{F}_3$ identified inside of $\mathbb{F}_3[x]/(x^2+1)$ and write $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$. Let $\alpha = \overline{x} \in \mathbb{F}_9$ so $\alpha^2 = -1 = 2$. Then $\{1, \alpha\}$ is an $\mathbb{F}_3$-basis for $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$ and we have the following complete list of elements:

$$\begin{array}{c|c|c} 0 & \alpha & 2\alpha \\ 1 & \alpha+1 & 2\alpha+1 \\ 2 & \alpha+2 & 2\alpha+2. \end{array}$$

We claim that $\mathbb{F}_9^\times = \langle \alpha + 1 \rangle$. We compute

$$\begin{aligned} (\alpha+1)^2 &= \alpha^2 + 2\alpha + 1 = 2 + 2\alpha + 1 = 2\alpha \\ (\alpha+1)^3 &= (2\alpha)(\alpha+1) = 2\alpha^2 + 2 = 2\alpha + 1 \\ (\alpha+1)^4 &= (2\alpha+1)(\alpha+1) = 2\alpha^2 + 2\alpha + \alpha + 1 = 2 \\ (\alpha+1)^5 &= 2(\alpha+1) = 2\alpha + 2 \\ (\alpha+1)^6 &= (2\alpha+2)(\alpha+1) = 4\alpha = \alpha \\ (\alpha+1)^7 &= (\alpha)(\alpha+1) = \alpha^2 + \alpha = \alpha + 2 \\ (\alpha+1)^8 &= (\alpha+2)(\alpha+1) = \alpha^2 + 3\alpha + 2 = 1, \end{aligned}$$

so $\langle \alpha + 1 \rangle = \mathbb{F}_9 \setminus \{0\} = \mathbb{F}_9^\times$. Set $\omega = \alpha + 1$ and let $T_\omega : \mathbb{F}_9 \to \mathbb{F}_9$ be given by left multiplication by ω. For the $\mathbb{F}_3$-basis $\mathcal{B} = \{1, \alpha\}$ of $\mathbb{F}_9$, we have that

$$B := [T_\omega]_\mathcal{B} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

is an order 8 element of $\mathrm{GL}_2(\mathbb{F}_3)$. □

Problem 3

Let $f(x) = (x^2 - 2)(x^3 - 3) \in \mathbb{Q}[x]$, and let K be a splitting field of $f(x)$ over $\mathbb{Q}$.

(a): (10 points) Prove that $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_3 \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Let $\zeta \in \mathbb{C}$ be a primitive 3rd root of unity. We compute

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt[3]{3})(x - \zeta\sqrt[3]{3})(x - \zeta^2\sqrt[3]{3})$$

over $\mathbb{C}$, so $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \zeta)$. As $\mathbb{Q}(\sqrt[3]{3}) \subseteq \mathbb{R}$ and $\zeta \in \mathbb{C} \setminus \mathbb{R}$, it follows that $\mu_{\zeta,\mathbb{Q}(\sqrt[3]{3})} = \mu_{\zeta,\mathbb{Q}} = x^2 + x + 1$ so $[\mathbb{Q}(\sqrt[3]{3}, \zeta) : \mathbb{Q}(\sqrt[3]{3})] = 2$. By Eisenstein's criterion, $x^3 - 3$ is irreducible over $\mathbb{Q}$ so $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ whence $[\mathbb{Q}(\sqrt[3]{3}, \zeta) : \mathbb{Q}] = 6$. Hence $[\mathbb{Q}(\sqrt[3]{3}, \zeta) : \mathbb{Q}(\zeta)] = 3$. On the other hand, we clearly have that $[\mathbb{Q}(\zeta, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$, so $[\mathbb{Q}(\zeta, \sqrt{2}) : \mathbb{Q}] = 4$ whence $[\mathbb{Q}(\zeta, \sqrt{2}) : \mathbb{Q}(\zeta)] = 2$. Observe that

$$[K : \mathbb{Q}(\zeta, \sqrt{2})] \cdot 2 = [K : \mathbb{Q}(\zeta)] = [K : \mathbb{Q}(\sqrt[3]{3}, \zeta)] \cdot 3,$$

so $2, 3 \mid [K : \mathbb{Q}(\zeta)] \implies 6 \mid [K : \mathbb{Q}(\zeta)]$. On the other hand, $\deg(\mu_{\sqrt[3]{3},\mathbb{Q}(\sqrt{2},\zeta)}) \leq \deg(\mu_{\sqrt[3]{3},\mathbb{Q}(\zeta)}) = 3$ whence

$$6 \mid [K : \mathbb{Q}(\zeta)] = [K : \mathbb{Q}(\sqrt{2}, \zeta)][\mathbb{Q}(\sqrt{2}, \zeta) : \mathbb{Q}(\zeta)] = [K : \mathbb{Q}(\sqrt{2}, \zeta)] \cdot 2 \leq 6$$

so $[K : \mathbb{Q}(\zeta)] = 6$ and thus $|\operatorname{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 12$.

Let $K_1 = \mathbb{Q}(\sqrt{2})$ and $K_2 = \mathbb{Q}(\sqrt[3]{3}, \zeta)$. Note that K_1 is a splitting field for $x^2 - 2$ over $\mathbb{Q}$ and K_2 is a splitting field for $x^3 - 3$ over $\mathbb{Q}$, so $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ are Galois. We claim that K is the compositum of K_1 and K_2. One one hand, as $K_1, K_2 \subseteq K$ we have by minimality that $K_1K_2 \subseteq K$. On the other hand, suppose that $L/\mathbb{Q}$ is a field extension such that $K_1, K_2 \subseteq L$. Then $\zeta, \sqrt{2}, \sqrt[3]{3} \in L$ whence $K \subseteq L$. Thus $K = K_1, K_2$. Now, we obtain an embedding

$$\operatorname{Gal}(K/\mathbb{Q}) \hookrightarrow \operatorname{Gal}(K_1/\mathbb{Q}) \times \operatorname{Gal}(K_2/\mathbb{Q}).$$

As $|\operatorname{Gal}(K_1/\mathbb{Q}) \times \operatorname{Gal}(K_2/\mathbb{Q})| = 12 = |\operatorname{Gal}(K/\mathbb{Q})|$, it follows that this injection is actually a group isomorphism.

As $|\operatorname{Gal}(K_1/\mathbb{Q})| = 2$, we have that $\operatorname{Gal}(K_1/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. On the other hand, as $x^3 - 3$ is irreducible over $\mathbb{Q}$ and K_2 is a splitting of $x^3 - 3$, the action of $\operatorname{Gal}(K_2/\mathbb{Q})$ on K_2 induces transitive action on the roots of $x^3 - 3$ and thus an embedding $\operatorname{Gal}(K_2/\mathbb{Q}) \hookrightarrow S_3$. However, $|\operatorname{Gal}(K_2/\mathbb{Q})| = 6 = |S_3|$, so this embedding is actually an isomorphism i.e. $\operatorname{Gal}(K_2/\mathbb{Q}) \cong S_3$. Thus $\operatorname{Gal}(K/\mathbb{Q}) \cong \operatorname{Gal}(K_1/\mathbb{Q}) \times \operatorname{Gal}(K_2/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times S_3$.

□

(b): (8 points) Find a primitive element of K over $\mathbb{Q}$ (and prove your answer).

Proof. We claim that $\alpha := \sqrt{2} + \sqrt[3]{3} + \zeta$ is a primitive element of $K/\mathbb{Q}$. As $\alpha \in K$ and consequently $\mathbb{Q}(\alpha) \subseteq K$, it suffices to show that $|\operatorname{Gal}(K/\mathbb{Q}(\alpha))| = [K : \mathbb{Q}(\alpha)] = 1$, i.e. that $\operatorname{Gal}(K/\mathbb{Q}(\alpha)) \subseteq \operatorname{Gal}(K/\mathbb{Q})$ is trivial. Henceforth, it is enough to show that every nonidentity element of $\operatorname{Gal}(K/\mathbb{Q})$ does not fix α.

Note that the isomorphism $\operatorname{Gal}(K/\mathbb{Q}) \hookrightarrow \operatorname{Gal}(K_1/\mathbb{Q}) \times \operatorname{Gal}(K_2/\mathbb{Q})$ is given by restriction in each component and that, for any $\upsilon \in \operatorname{Gal}(K/\mathbb{Q})$,

$$\upsilon(\alpha) = \upsilon|_{K_1}(\sqrt{2}) + \upsilon|_{K_2}(\sqrt[3]{3} + \zeta).$$

Moreover, this being an isomorphism implies that $K_1 \cap K_2 = \mathbb{Q}$.

Suppose $\mu \in \operatorname{Gal}(K/\mathbb{Q})$ fixes α.

$$\sqrt{2} + \sqrt[3]{3} + \zeta = \mu(\sqrt{2}) + \mu(\sqrt[3]{3} + \zeta) \implies \mu(\sqrt{2}) - \sqrt{2} = \mu(\sqrt[3]{3} + \zeta) - \sqrt[3]{3} + \zeta.$$

As $\mu|_{K_1}(K_1) = K_1$ and $\mu|_{K_2}(K_2) = K_2$, it follows that

$$\mu(\sqrt{2}) - \sqrt{2} = \mu(\sqrt[3]{3} + \zeta) - \sqrt[3]{3} - \zeta \in K_1 \cap K_2 = \mathbb{Q}.$$

As $\mu|_{K_1} \in \operatorname{Gal}(K_1/\mathbb{Q})$ permutes $\{\pm\sqrt{2}\}$, it follows that $\mu(\sqrt{2}) - \sqrt{2} = 0$. As $\mu|_{K_2} \in \operatorname{Gal}(K_2/\mathbb{Q})$ permutes $\{\sqrt[3]{3}, \zeta\sqrt[3]{3}, \zeta^2\sqrt[3]{3}\}$ and $\{\zeta, \zeta^2\}$, it follows that

$$\mu(\sqrt[3]{3} + \zeta) - (\sqrt[3]{3} + \zeta) = 0$$

But then $\mu(\sqrt[3]{3}) = \sqrt[3]{3}$ and $\mu(\zeta) = \zeta$, so $\mu = id$. □

Problem 4

(a): (10 points) Let $F \subseteq K \subseteq L$ be a tower of algebraic extensions. Let $\alpha \in L$, and let $\mu_{\alpha,F}(x)$ be its minimal polynomial over F. Prove an isomorphism of K-algebras

$$K \otimes_F F(\alpha) \simeq K[x]/(\mu_{\alpha,F}(x)).$$

Proof. Define a map $\Psi : K[x] \to K \otimes_F F(\alpha)$ by $\Psi(\sum_{i=0}^n c_i x^i) = \sum_{i=0}^n c_i \otimes \alpha^i$. Suppose $f(x), g(x) \in K[x]$. Write $f(x) = \sum_{i=0}^n c_i x^i$ and $g(x) = \sum_{i=0}^n d_i x^i$, where we have made the number of summands in each sum agree by taking zeroes as extra coefficients if the degrees do not match. Then

$$\Psi(f(x)+g(x)) = \Psi\left(\sum_{i=0}^n (c_i+d_i)x^i\right) = \sum_{i=0}^n (c_i+d_i)\otimes\alpha^i = \sum_{i=0}^n c_i\otimes\alpha^i + \sum_{i=0}^n d_i\otimes\alpha^i = \Psi(f(x))+\Psi(g(x)),$$

and

$$\Psi(f(x)g(x)) = \Psi\left(\sum_{k=0}^n \left(\sum_{i=0}^k c_{k-i}d_i\right)x^k\right) = \sum_{k=0}^n \left(\sum_{i=0}^k c_{k-i}d_i\right)\otimes\alpha^k = \left(\sum_{i=0}^n c_i\otimes\alpha^i\right)\left(\sum_{j=0}^n d_j\otimes\alpha^j\right) = \Psi(f(x))\Psi(g(x$$

Lastly, for any $\lambda \in K$,

$$\Psi(\lambda f(x)) = \Psi(\sum_{i=0}^n \lambda c_i x^i) = \sum_{i=0}^n \lambda c_i \otimes \alpha = (\lambda\otimes 1)\Psi(f(x)) = \lambda\cdot\Psi(f(x)),$$

so Ψ is indeed a K-algebra homomorphism. Moreover, Ψ is surjective as the image of Ψ clearly contains all simple tensors $c\otimes f(\alpha)$ (take $\Psi(cf(x))$), whence by linearity the image of Ψ is all of $K\otimes_F F(\alpha)$.

Suppose that $f(x) \in K[x]$ and write $\mu_{\alpha,F}(x) = \sum_{i=0}^n a_i x^i$ for some $a_i \in F$. Then

$$\begin{aligned}\Psi(f(x)\mu_{\alpha,F}(x)) &= \Psi(f(x))\left(\sum_{i=0}^n a_i\otimes\alpha^i\right) = \Psi(f(x))\left(\sum_{i=0}^n 1\otimes a_i\alpha^i\right)\\ &= \Psi(f(x))\left(1\otimes\left(\sum_{i=0}^n a_i\alpha^i\right)\right) = \Psi(f(x))\left(1\otimes\mu_{\alpha,F}(\alpha)\right) = 0,\end{aligned}$$

so $(\mu_{\alpha,F}(x)) \subseteq \ker(\Psi)$. Hence, there exists a well-defined K-algebra homomorphism $\tilde{\Psi} : K[x]/(\mu_{\alpha,F}(x)) \to K\otimes_F F(\alpha)$ such that the diagram below commutes

$$\begin{array}{ccc} K[x] & \xrightarrow{\quad\Psi\quad} & K\otimes_F F(\alpha) \\ {\scriptstyle\pi}\big\downarrow & \nearrow_{\tilde{\Psi}} & \\ \frac{K[x]}{(\mu_{\alpha,F}(x))} & & \end{array}$$

where $\pi : K[x] \to K[x]/(\mu_{\alpha,F}(x))$ is the natural projection. On one hand, as Ψ is surjective it immediately follows that $\tilde{\Psi}$ is also surjective. On the other hand, as $K[x]$ is a PID and $(\mu_{\alpha,F}(x))$ is a prime ideal of $K[x]$, $(\mu_{\alpha,F}(x))$ is actually a maximal ideal of $K[x]$ so $K[x]/(\mu_{\alpha,F}(x))$ is a field. Thus, as $\ker(\tilde{\Psi})$ is an ideal of $K[x]/(\mu_{\alpha,F}(x))$ and $\tilde{\Psi}$ is not trivial, it follows that $\ker(\tilde{\Psi}) = 0$ i.e. $\tilde{\Psi}$ is injective. Hence $\tilde{\Psi}$ is a K-algebra isomorphism.

□

(b): (13 points) Let K_1, K_2 be two algebraic extensions (not necessarily finite) of a field F. Suppose that F has characteristic 0 and that we have F-embeddings $K_1, K_2 \hookrightarrow \overline{F}$, to a fixed algebraic closure of F. Prove that the F-algebra $K_1 \otimes_F K_2$ has no nonzero nilpotent elements. **Hint:** Reduce to the case when one of the extensions is finite over F.

Proof. Suppose first that K_2/F is finite. As $\mathrm{char}(F) = 0$, K_2/F is finite and separable whence by the primitive element theorem there exists some $\alpha \in K_2$ such that $K_2 = F(\alpha)$. By part(a) applied to the algebraic tower $F \subseteq K_1 \subseteq \overline{F}$, we have an isomorphism of K_1-algebras (and thus F-algebras),

$$K_1 \otimes_F K_2 = K_1 \otimes_F F(\alpha) \cong K_1[x]/(\mu_{\alpha,F}(x)).$$

Suppose that $f \in K[x]$ is such that $f^n \in (\mu_{\alpha,F}(x))$ for some $n \in \mathbb{N}$. Then $(f(\alpha))^n = 0$, whence $f(\alpha) = 0$ so $f \in (\mu_{\alpha,F}(x))$ and thus $\overline{f} \equiv 0$ in $K_1[x]/(\mu_{\alpha,F}(x))$. Thus, $K_1 \otimes_F K_2 \cong K_1[x]/(\mu_{\alpha,F}(x))$ has no nonzero nilpotents.

Now suppose that K_1, K_2 are just algebraic extensions of F. Suppose that $\gamma = \sum_{j=1}^m c_j\alpha_j \otimes \beta_j \in K_1 \otimes_F K_2$ is nilpotent. Note that the field $F(\beta_1, \cdots, \beta_m) \subseteq K_2$ is finite over F, so the by part (a) the sub-F-algebra $K_1 \otimes_F F(\beta_1, \cdots, \beta_m) \subseteq K_1 \otimes_F K_2$ contains no nonzero nilpotents. However, $\gamma = \sum_{j=1}^m c_j\alpha_j \otimes \beta_j \in K_1 \otimes_F F(\beta_1, \cdots, \beta_m)$, so γ being nilpotent implies that $\gamma = 0$. □

Problem 5

(a): (6 points) Let K/F be a finite Galois extension and let $G = \mathrm{Gal}(K/F)$. Assume that G is a simple group (recall: this means that G has no nontrivial proper normal subgroups). Let $\alpha \in K \setminus F$ and $\mu_{\alpha,F}(x) \in F[x]$ its minimal polynomial over F. Prove that K is a splitting field for $\mu_{\alpha,F}(x)$.

Proof. On one hand, as $\alpha \in K$ and $\mu_{\alpha,F}(\alpha) = 0$, the normality of K/F implies that $\mu_{\alpha,F}(x)$ splits over K. Hence, there exist $\alpha_1, \ldots, \alpha_n \in K$ (take $\alpha_1 = \alpha$) such that

$$\mu_{\alpha,F}(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in K[x].$$

Let $K_0 = F(\alpha_1, \cdots, \alpha_n)$, so $F \subseteq K_0 \subseteq K$. As K/F is Galois, it follows that K_0/F is separable. As K_0 is a splitting field of $\mu_{\alpha,F}$ over F, it follows that K_0/F is normal, and thus Galois. Hence, by the fundamental theorem of Galois theory $\mathrm{Gal}(K/K_0) \triangleleft G$. As $\alpha \in K_0 \setminus F$, we have that $[K_0 : F] > 1$ and thus

$$|\mathrm{Gal}(K/K_0)| = [K : K_0] = \frac{[K : F]}{[K_0 : F]} < [K : F] = |G|.$$

Now the simplicity of G implies that $\mathrm{Gal}(K/K_0)$ is trivial, so $K = K_0$ is a splitting field for $\mu_{\alpha,F}(x)$. □

(b): (8 points) Let $F \subseteq L \subseteq K$ be a tower of finite extensions. Suppose that both L/F and K/F are Galois and the Galois group $H = \mathrm{Gal}(K/L)$ of K/L is cyclic. Let M be any subfield of K/L. Prove that the extension M/F is Galois.

Proof. Let $\sigma \in H$ be such that $H = \langle\sigma\rangle$. As $\mathrm{Gal}(K/M) \subseteq \mathrm{Gal}(K/L) = H$, there exists some $d \in \{1, \ldots, |H|\}$ such that $\mathrm{Gal}(K/M) = \langle\sigma^d\rangle$. By the fundamental theorem of Galois theory, as L/F is Galois we have that $\langle\sigma\rangle = H \triangleleft \mathrm{Gal}(K/F)$.

Suppose that $\tau \in \mathrm{Gal}(K/F)$. By normality, there is some $k \in \mathbb{N} \cup \{0\}$ such that $\tau\sigma\tau^{-1} = \sigma^k$. For $s \in \mathbb{N}$ we compute,

$$\tau(\sigma^d)^s\tau^{-1} = \tau\sigma^{ds}\tau^{-1} = (\tau\sigma\tau^{-1})^{ds} = (\sigma^k)^{ds} = (\sigma^d)^{sk} \in \langle\sigma^d\rangle,$$

so $\tau\langle\sigma^d\rangle\tau^{-1} = \langle\sigma^d\rangle$. Thus $\mathrm{Gal}(K/M) = \langle\sigma^d\rangle \triangleleft \mathrm{Gal}(K/F)$, so by the fundamental theorem of Galois theory M/F is Galois. □

Problem 6

Let p be an odd prime. Consider the p^{th} cyclotomic field, $K = \mathbb{Q}(\zeta)$, where $\zeta \in \mathbb{C}$ is a primitive p^{th} root of unity.

(a): (6 points) Prove that K contains a unique subfield of the form $\mathbb{Q}(\sqrt{m})$, where $m \in \mathbb{Z}$ is a square-free integer.

Proof. Note that $K/\mathbb{Q}$ is Galois and $G = \mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ by such that $\sigma(\zeta) = \zeta^m$ for some $m > 1$ with $(m, p) = 1$. Then $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$. Consider the subgroup $H = \langle\sigma^2\rangle \subseteq G$. As $|H| = \frac{p-1}{2}$, $[G : H] = 2$ and thus $H \triangleleft G$. Letting $K_0 = K^H$, it follows by the fundamental theorem of Galois theory that $[K : K_0] = |H| = \frac{p-1}{2}$ and that $K_0/\mathbb{Q}$ is Galois with $[K_0 : \mathbb{Q}] = 2$. Note that this is the unique subgroup of index 2 by cyclicity of G, whence the Galois correspondence implies that K_0 is the unique subfield of K with $[K : \mathbb{Q}] = 2$. Now, by Kummer's theorem, there exists some $\alpha \in K_0 \setminus \mathbb{Q}$ such that $\alpha^2 \in \mathbb{Q}$ and $K_0 = \mathbb{Q}(\alpha)$. As such, we may write $\alpha = \sqrt{\frac{a}{b}}$ for some square-free $a, b \in \mathbb{Z}\setminus\{0\}$ with $(a, b) = 1$.

As a, b are square-free and (a, b), $x^2 - ab$ and $x^2 - \frac{a}{b}$ are irreducible in $\mathbb{Q}[x]$. Thus, the relation $\sqrt{ab} = b\sqrt{\frac{a}{b}}$ combined with the reverse direction of homework 11 problem 6 gives that $\mathbb{Q}(\sqrt{\frac{a}{b}}) = \mathbb{Q}(\sqrt{ab})$. As a,b are square-free and coprime, ab is square-free and we are done.

Now suppose that $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{m'})$ for some $m' \in \mathbb{Z}$ also square-free. By homework 11 problem 6 forward direction, $m' = c^2 m^r$ for some $r \in \mathbb{N}$ with $(r, 2) = 1$. By square-freeness, we have that $c = 1$ and $r = 1$, so $m = m'$. □

(b): (10 points) Now suppose $p = 5$. Find the integer m explicitly. **Hint:** Finding an explicit generator of the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ might be useful.

Proof. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be such that $\sigma(\zeta) = \zeta^2$. Then $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$. Let $H = \langle\sigma^2\rangle = \{id, \sigma^2\}$. We compute that $\sigma^2(\zeta) = \sigma(\zeta^2) = \zeta^4$. Consider $\alpha = id(\zeta) + \sigma^2(\zeta) = \zeta + \zeta^4$. By construction, $\alpha \in K^H$. Moreover,

$$\alpha = \zeta + \zeta^{-1} = \zeta + \overline{\zeta} = 2\cos(\frac{2\pi}{5}) = \frac{\sqrt{5} - 1}{2} \notin \mathbb{Q}$$

so $\mathbb{Q}(\alpha) = K^H$. As $\sqrt{5} = 2\alpha + 1$, $\sqrt{5} \in \mathbb{Q}(\alpha)$. On the other hand, the above identity shows that $\alpha \in \mathbb{Q}(\sqrt{5})$, so $K^H = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$ and thus $m = 5$. □

(c): (5 points) Do the same for $p = 7$. How is your answer different from (b)? What would you expect the general answer to be?

Proof. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be such that $\sigma(\zeta) = \zeta^2$. Then $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$. Let $H = \langle\sigma^2\rangle = \{id, \sigma^2, \sigma^4\}$. Let $\alpha = id(\zeta) + \sigma^2(\zeta) + \sigma^4(\zeta) = \zeta + \zeta^{2^2} + \zeta^{2^4} = \zeta + \zeta^2 + \zeta^4$. Again by construction it is clear that $\alpha \in K^H$. Note that $1 + \zeta + \zeta^2 + \zeta^4 + \zeta^{-1} + \zeta^{-2} + \zeta^{-4} = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0$, whence

$$\zeta + \zeta^2 + \zeta^4 = \alpha = -1 - \zeta^{-1} + \zeta^{-2} + \zeta^{-4}$$

For brevity, let $\beta = \zeta^{-1} + \zeta^{-2} + \zeta^{-4}$, so

$$2\alpha + 1 = \zeta + \zeta^2 + \zeta^4 - (\zeta^{-1} + \zeta^{-2} + \zeta^{-4}) = \alpha - \beta.$$

We compute (pain pain pain),

$$\begin{aligned}(2\alpha+1)^2 &= \zeta+\zeta^2+\zeta^4+2(\zeta^3+\zeta^5+\zeta^6)+\zeta^3+\zeta^5+\zeta^6+2(\zeta+\zeta^2+\zeta^4)-2\alpha\beta\\ &= 3(\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6)-2\alpha\beta = -3-2\alpha\beta\\ &= -3-2\left(\zeta^4+\zeta^6+\zeta^7+\zeta^5+\zeta^8+\zeta^7+\zeta^9+\zeta^10\right)\\ &= -3-2\left(3+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6\right) = -3-2(3-1) = -7,\end{aligned}$$

so $\alpha \in \{\frac{1}{2}(-1\pm\sqrt{-7})\} \notin \mathbb{Q}$, whence $K^H = \mathbb{Q}(\alpha)$. On one hand, we than have that $\alpha \in \mathbb{Q}(\sqrt{-7})$. On the other hand, the above relation implies that $2\alpha+1 \in \{\pm\sqrt{-7}\}$ so $\sqrt{-7} \in \mathbb{Q}(\alpha)$. Thus $K^H = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-7})$, so $m = -7$.

This answer is different from that in part (b) as it is $\sqrt{-p}$ as opposed to $\sqrt{p}$. I conjecture that the general answer is $\sqrt{\pm p}$ where the sign depends on whether $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$.

□