Advanced Algebra II HW3

Sean Eli

February 12, 2022

Problem 1a. Suppose A is a square complex matrix with $A^k = I$. A is diagonalizable.

Proof. If $A^k = I$ then the minimal polynomial of A divides $x^k - 1$, which is separable over $\mathbb{C}$. So the minimal polynomial of A has distinct roots. This means the elementary divisors for A are linear factors, so the Jordan form of A is diagonal.

Problem 1b. The matrix $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ over $\mathbb{F}_p$, with $\alpha \neq 0$, cannot be diagonalized even though $A^p = I$.

Proof. The characteristic polynomial of A is $c(x) = (x-1)^2$, so the only eigenvalue of A is 1. A basis for the nullspace of $A - 1I$ is $(1, 0)^t$, so the eigenspace E_1 is 1-dimensional. Thus there is no basis for $\mathbb{F}_p^2$ consisting of eigenvectors of A. ■

Problem 2. Find the rational canonical form of the Frobenius map $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$.

Proof. To do this, we need to find the minimal polynomial of ϕ. Recall from class that $a^{p^n} = a$ for all $a \in \mathbb{F}_{p^n}$, therefore $\phi^n = I$. Since $\mathbb{F}_{p^n}$ is a dimension n vector space over $\mathbb{F}_p$, the characteristic polynomial $c(x)$ of ϕ has degree n: it follows that $c(x) = x^n - 1$. Suppose the minimal polynomial for ϕ over $\mathbb{F}_p$ is $m(x) = \sum_{i=0}^{k} b_i x^i$ where $k < n$. Then, for each $a \in \mathbb{F}_{p^n}$,

$$0 = m(\phi)(a) = \sum_{i=0}^{k} b_i \phi(a)^i = \sum_{i=0}^{k} b_i a^{p^i}.$$

So each $a \in \mathbb{F}_{p^n}$ is a root of the polynomial $\sum_{i=0}^{k} b_i x^{p^i}$, which has degree p^k. There are at most p^k such roots, contradicting the order of $\mathbb{F}_{p^n}$. Thus, the minimal polynomial has degree n, and is $x^n - 1$. Snce the invariant factors of ϕ divide the minimal polynomial, and their product is the characteristic polynomial, it follows that there is only one invariant factor, $x^n - 1$. So the RCF is the companion matrix for $x^n - 1$:

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & \vdots & \vdots & \vdots & 0 \\ 0 & \dots & \dots & 1 & 0 \end{pmatrix}$$

■

Problem 3. There are only finitely many roots of unity in a finite extension $K/\mathbb{Q}$.

Proof. Let $[K:\mathbb{Q}] = n$, so any $\alpha \in K$ is the root of a degree $\leq n$ polynomial over $\mathbb{Q}$. If $\zeta \in K$ is a root of unity, then (since ζ generates some group of roots of unity), ζ is a primitive m-th root of unity for some m. This means ζ is the root of the m-th cyclotomic polynomial $\Phi_m(x)$. Since $\Phi_m(x)$ is irreducible over $\mathbb{Q}$ and has degree $\phi(m)$, we have $\phi(m) \leq n$.

There are finitely many cyclotomic polynomials with degree smaller than n. This is because Euler's phi-function satisfies $\phi(m) \to \infty$ as $m \to \infty$ (so there are finitely many m with $\phi(m) \leq n$). Since any root of unity $\zeta \in K$ is the root of a cyclotomic polynomial $\Phi_m(x)$ with $\phi(m) \leq n$, we conclude there are finitely many roots of unity in K.

■

Problem 4. Suppose d_1, d_2, and $d_1 d_2$ are not squares in $\mathbb{Q}^\times$. Show $K/F := \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})/\mathbb{Q}$ is Galois and its Galois group is the Klein four group. Is the converse true?

Proof. Since $\sqrt{d_1}$ and $\sqrt{d_2}$ are algebraic over F of degree 2 (and $d_1 \neq d_2$), $[K:F] \leq 4$. BWOC, if $\sqrt{d_2} \in \mathbb{Q}(\sqrt{d_1})$, then $\sqrt{d_2} = a + b\sqrt{d_1}$ for rational a, b, which implies $d_2 = a^2 + b^2 d_1 + 2ab\sqrt{d_1}$. Thus $\sqrt{d_1} \in \mathbb{Q}$ which is impossible. It follows that

$$[K:F] = [K:\mathbb{Q}(\sqrt{d_1})][\mathbb{Q}(\sqrt{d_1}):\mathbb{Q}] = 4.$$

Elements of $\mathrm{Aut}(K/F)$ permute the roots of $x^2 - d_1$ and of $x^2 - d_2$, so there are four automorphisms (the roots of $x^2 - d_1$ must be swapped or fixed. The same is true for the other polynomial. There are four possibilities). Therefore $[K:F]$ is Galois. The Galois group $\mathrm{Aut}(K/F)$ is the Klein four group $\{1, f, g, fg\}$, since f and g are automorphisms which swap the roots of precisely one of $x^2 - d_1$ or $x^2 - d_2$, and fg is their composition.

Next suppose $K/\mathbb{Q}$ is a Galois extension with $\mathrm{Aut}(K/\mathbb{Q}) \cong \{1, f, g, fg\}$. Consider the subgroups $\langle f \rangle, \langle g \rangle$, and $\langle fg \rangle$, which are all $\cong \mathbb{Z}/2\mathbb{Z}$. By the fundamental theorem of Galois theory, the corresponding fixed fields contained in K are all degree 2 (so the only intermediate fields are degree 2 extensions of $\mathbb{Q}$). Also there are no containments among these three intermediate fields. Since they are quadratic extensions, the intermediate fields are $\mathbb{Q}(\sqrt{d_1}), \mathbb{Q}(\sqrt{d_2})$, and $\mathbb{Q}(\sqrt{d_3})$ for rational numbers d_1, d_2, d_3 which are not squares in $\mathbb{Q}$. Then $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) \subset K$ and by considering degrees, these fields are the same. It follows that $d_3 = d_1 d_2$. ■

Problem 5. Determine all the subfields of the splitting field of $x^8 - 2 \in \mathbb{Q}[x]$ that are Galois extensions of $\mathbb{Q}$.

Proof. The splitting field of $x^8 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(i, \sqrt[8]{2})$, which is a Galois extension (splitting field of a separable polynomial) of degree 16 over $\mathbb{Q}$. The subgroup and intermediate field lattices of $\mathbb{Q}(i, \sqrt[8]{2})/\mathbb{Q}$ are given in section 14.2 of the textbook.

1. Since quadratic extensions of $\mathbb{Q}$ are Galois, the subfields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(i\sqrt{2})$ are Galois extensions of $\mathbb{Q}$.

2. $\mathbb{Q}(i\sqrt[4]{2})$ does not contain $\sqrt[4]{2}$, but it contains a root of the irreducible x^2-4. Thus, this is not a splitting field, and therefore not Galois. Similarly $\mathbb{Q}(\sqrt[4]{2})$ is not Galois. $\mathbb{Q}(i, \sqrt{2})$ is the splitting field of the separable polynomial $(x^2 + 1)(x^2 - 2)$ and is thus Galois. Notice, in the subgroup diagram, the subgroups $\langle \tau\sigma^3 \rangle$ and $\langle \tau\sigma \rangle$ are conjugate: thus, neither is normal, so their corresponding fields $\mathbb{Q}((1+i)\sqrt[4]{2})$ and $\mathbb{Q}((1-i)\sqrt[4]{2})$ are not Galois. Among degree 4 intermediate extensions, only $\mathbb{Q}(i, \sqrt{2})$ is Galois over $\mathbb{Q}$.

3. Next are degree 8 extensions. $\mathbb{Q}(i, \sqrt[4]{2})$ is the splitting field of the separable polynomial $x^4 - 2$ over $\mathbb{Q}$, and is thus Galois. $\mathbb{Q}(\sqrt[8]{2})$ contains exactly one root of the irreducible $x^8 - 2$ and is thus not Galois. Let ζ be a primitive eighth root of unity. Similarly, none of the fields $\mathbb{Q}(i\sqrt[8]{2}), \mathbb{Q}(\zeta^3\sqrt[8]{2})$, and $\mathbb{Q}(\zeta\sqrt[8]{2})$ contains all roots of $x^8 - 2$ and are therefore not Galois over $\mathbb{Q}$.

The only intermediate Galois extensions of $\mathbb{Q}$ are $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i\sqrt{2}), \mathbb{Q}(i, \sqrt{2}), \mathbb{Q}(i, \sqrt[4]{2})$, and $\mathbb{Q}(i, \sqrt[8]{2})$.

■

Problem 6a. Let K/F be a finite separable extension. Fix an algebraic closure $\overline{\mathbb{F}}$ and an embedding $\iota : F \hookrightarrow \overline{\mathbb{F}}$. Show there are exactly $[K : F]$ embeddings $\sigma : K \hookrightarrow \overline{\mathbb{F}}$ that extend ι.

Proof. Induct on $[K : F]$. If $[K : F] = 1$ then $K = F$ so there is exactly one embedding $K \hookrightarrow \overline{\mathbb{F}}$ extending ι, namely ι.

Suppose whenever E/F_2 is any separable extension with $1 \leq [E : F_2] < n$, and $\tau : F_2 \hookrightarrow \overline{\mathbb{F}}$ is an embedding, then there are exactly $[E : F_2]$ embeddings $E \hookrightarrow \overline{\mathbb{F}}$ extending τ. If $[K : F] = n$ then there exists $\alpha \in K \setminus F$ of degree ≥ 2. Notice $F(\alpha) \subset K$ so $F(\alpha)$ is a separable extension of F, and by the inductive hypothesis there are exactly $[F(\alpha) : F]$ embeddings $F(\alpha) \hookrightarrow \overline{\mathbb{F}}$ which extend $\iota : F \hookrightarrow \overline{\mathbb{F}}$. Call these $\sigma_1, ..., \sigma_k$. Also $K/F(\alpha)$ is a finite separable extension of degree $< n$, so by the inductive hypothesis, for each $\sigma_i : F(\alpha) \to \overline{\mathbb{F}}$, there are exactly $[K : F(\alpha)]$ embeddings $K \to \overline{\mathbb{F}}$ extending σ_i. This yields $[K : F]$ embeddings of K into $\overline{\mathbb{F}}$ which extend ι. (something must be wrong since "separable" was not really used ...)

Problem 6b. Suppose K/F is Galois. The restriction of an F-embedding $\sigma : K \hookrightarrow \overline{\mathbb{F}}$ to K gives an element of $\mathrm{Aut}(K/F)$.

Proof. I am not sure what to show: is the problem asking to show that for all n F-embeddings $\sigma_1, ..., \sigma_n$, their images are the same sets $\sigma_1(K) = .. = \sigma_n(K)$?