MATH 4108
MIDTERM EXAMINATION 1

Name	

1	2	3	4	5	Total

- There are 5 problems on this exam. Problem 3 is double-length and problem 5 has 5 points of extra credit available.
- The maximum score on this exam (without extra credit) is 60 points.
- You have 80 minutes to complete this exam.
- There are no aids of any kind (notes, text, etc.) allowed.
- All answers must be justified unless otherwise noted, and all proofs must be written in clear and grammatical English.
- You may cite any theorem, lemma, proposition, etc. proved in class or in the sections we covered in the text, in addition to any assigned homework problem.
- Good luck!

Problem 1. [2 points each]

For each part, give an example of a field with the stated property. If no such field exists, write "none". No justifications are required.

i. A field of characteristic 3 which is not finite.

ii. A field of degree 3 over $\mathbf{Q}$ which is not Galois.

iii. A field of degree 2 over $\mathbf{Q}$ which is not Galois.

iv. A field of degree 2 over $\mathbf{Q}$ which is Galois.

v. A Galois extension of $\mathbf{F}_3$ whose Galois group is not cyclic.

Solution.

i. $\mathbf{F}_3(t)$

ii. $\mathbf{Q}(\sqrt[3]{2})$

iii. None

iv. $\mathbf{Q}(\sqrt{2})$

v. None

Problem 2. [10 points]

i. What is the degree $[\mathbf{F}_9 : \mathbf{F}_3]$?

ii. Find all elements of $G(\mathbf{F}_9/\mathbf{F}_3)$.

Solution.

i. As vector spaces, $\mathbf{F}_9 \cong \mathbf{F}_3^2$ because it has $3^2 = 9$ elements, so the degree is 2.

ii. $G(\mathbf{F}_9/\mathbf{F}_3) = \{1, \sigma\}$ where $\sigma(\alpha) = \alpha^3$ is the Frobenius automorphism.

Problem 3.

[5 points each]

Let K be the splitting field for $x^4 + 1$ over $\mathbf{Q}$.

i. Prove that $K = \mathbf{Q}(\sqrt{2}, i)$.

ii. Determine the Galois group $G = G(K/\mathbf{Q})$.

iii. Draw the lattice of intermediate fields.

iv. Find all primitive elements of K.

Solution.

i. Let $\zeta = e^{2\pi i/8} = \frac{1}{\sqrt{2}}(1+i)$. The roots of x^4+1 are the solutions to the equation $x^4 = -1$, so

$$x^4 + 1 = (x-\zeta)(x-\zeta^3)(x-\zeta^5)(x-\zeta^7).$$

Hence $K = \mathbf{Q}(\zeta)$. Clearly $\zeta \in \mathbf{Q}(\sqrt{2}, i)$, so $K \subset \mathbf{Q}(\sqrt{2}, i)$. On the other hand, $i = \zeta^2 \in K$, so $\sqrt{2} = (1+i)/\zeta \in K$, and hence $\mathbf{Q}(\sqrt{2}, i) \subset K$.

ii. It follows from (i) that G has four elements. We know $G(K/\mathbf{Q}(\sqrt{2})) = \{1, \sigma\}$, where $\sigma(\sqrt{2}) = \sqrt{2}$ and $\sigma(i) = -i$. Similarly, $G(K/\mathbf{Q}(i)) = \{1, \tau\}$, where $\tau(\sqrt{2}) = -\sqrt{2}$ and $\tau(i) = i$. Hence $G = \{1, \sigma, \tau, \sigma\tau\}$.

iii. The Galois group has three order-2 subgroups $\{1, \sigma\}$, $\{1, \tau\}$, and $\{1, \sigma\tau\}$, so there are three quadratic intermediate fields

$$\begin{tikzcd}[column sep=small]
 & K \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbf{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbf{Q}(\sqrt{-2}) \arrow[d, dash] & \mathbf{Q}(i) \arrow[dl, dash] \\
 & \mathbf{Q} &
\end{tikzcd}$$

iv. An element $\alpha \in K$ can be written uniquely as $\alpha = a + b\sqrt{2} + ci + d\sqrt{-2}$ for $a, b, c, d \in \mathbf{Q}$. If α is not primitive then it is contained in one of the intermediate fields $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(i)$. This is the case when at least two of b, c, d are zero.

Problem 4. [10 points]

Let $\sigma\colon \mathbf{C}(t) \to \mathbf{C}(t)$ be the automorphism defined by $\sigma(t) = \zeta t$, where $\zeta = e^{2\pi i/3}$ is a primitive cube root of unity. Let $H = \langle \sigma \rangle$ and $F = \mathbf{C}(t)^H$. Find the degree $[\mathbf{C}(t) : F]$ and the minimal polynomial $f(x) \in F[x]$ for t over F.

Solution.

We have $\sigma^2(t) = \zeta^2 t$ and $\sigma^3(t) = t$, so $H = \{1, \sigma, \sigma^2\}$ and therefore $[\mathbf{C}(t) : F] = 3$ by the fixed field theorem. The set of roots of the minimal polynomial over the fixed field of H is the orbit of t under the action of H, so

$$f(x) = (x - t)(x - \zeta t)(x - \zeta^2 t) = x^3 - t^3.$$

Problem 5. [10 points]

Prove that $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is Galois, where $\zeta_n = e^{2\pi i/n}$.

Extra credit [5 points]: Calculate the Galois group $G = G(\mathbf{Q}(\zeta_7)/\mathbf{Q})$. Justify your answer!

Solution.

The field $\mathbf{Q}(\zeta_n)$ is the splitting field for the polynomial $x^n - 1$.

Since 7 is prime, the degree $[\mathbf{Q}(\zeta_7) : \mathbf{Q}]$ is $7 - 1 = 6$. The minimal polynomial for ζ_7 is the 7-cyclotomic polynomial

$$\Phi_7(x) = \sum_{n=0}^{6} x^n = \prod_{n=1}^{6} (x - \zeta^n).$$

Since this polynomial is irreducible, there exists $\sigma \in G$ such that $\sigma(\zeta) = \zeta^3$. Then

$$\sigma^2(\zeta) = \zeta^2, \quad \sigma^3(\zeta) = \zeta^6, \quad \sigma^4(\zeta) = \zeta^4, \quad \sigma^5(\zeta) = \zeta^5, \quad \sigma^6(\zeta) = \zeta.$$

Hence $G = \langle \sigma \rangle$ is cyclic of order 6.

[Scratch work]