Math 343 - Intro. Modern Algebra **Homework 6** **Due: March 15th, 2019**

Note: A random subset of these problems will be graded for credit.

(1) Recall that for an extension field E of a field F, an element $a \in E$ is algebraic over F if it is a root of some polynomial $f(x) \in F[X]$. Furthermore, the degree of an element $a \in E$ that is algebraic over F is the degree of a polynomial of minimal degree such that a is a root of the polynomial.

(a) Show $\sqrt{2} + \sqrt{3}$ algebraic over $\mathbb{Q}$. Find its degree over $\mathbb{Q}$. Prove your answer. Hint: For any monic poly. f with integer coefficients, if it has a rational root r then r is an integer divisor of $f(0)$.

(b) Show $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a simple extension field of $\mathbb{Q}$.

(2) Let $n \in \mathbb{N}$. Let E be an extension field of F that as a vector space over F has dimension n. Let $a \in E$. Prove that a is algebraic of degree at most n over F.

(3) Let $n \in \mathbb{N}$, $n \geq 2$, and $q \in \mathbb{N}$ be a positive integer power of a prime number. Let $\mathbb{F}_q$ be a field with q elements.

(a) How many non-zero vectors does $(\mathbb{F}_q)^n$ contain?

(b) Let $\mathbf{x} \in (\mathbb{F}_q)^n$ be a non-zero vector. How many vectors are there in $(\mathbb{F}_q)^n$ that DO NOT lie in the Span$(\mathbf{x})$?

(c) Let $\mathbf{x}, \mathbf{y} \in (\mathbb{F}_q)^n$ be a pair of linearly independent vectors. How many vectors are there in $(\mathbb{F}_q)^n$ that DO NOT lie in the Span$(\mathbf{x}, \mathbf{y})$?

(d) Consider the group $G = \mathrm{GL}_n(\mathbb{F}_q)$ consisting of invertible $n \times n$ matrices over a finite field with q elements. Find the order of G.

Hint: Each column (after the first) of an invertible matrix must not lie in the span of the previous columns.

(4) We know that $f(x) = x^3 + x^2 + 1$ is irreducible over $\mathbb{Z}_2$. Let α be a root of $f(x)$ is some extension field E of $\mathbb{Z}_2$. Show that $f(x)$ factors into the product of 3 linear factors in $\mathbb{Z}_2(\alpha)$.

Hint: Every element of $\mathbb{Z}_2(\alpha)$ looks like $a_0 + a_1\alpha + a_2\alpha^2$ where $a_0, a_1, a_2 \in \mathbb{Z}_2$. Divide $x^3 + x^2 + 1$ by $x - \alpha$ using long division and show that the quadratic quotient has a root in $\mathbb{Z}_2(\alpha)$.

(5) Let F be a field. Let i, j, k satisfy $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$ and $ik = -j$. Then assume that for any $a \in F$, $ab = ba$ for all $b \in \{i, j, k\}$. Let $Q_F = \{a + bi + cj + dk | a, b, c, d \in F\}$. Addition in Q_F is done by combining "like" terms (involving the linearly independent quantities $1, i, j, k$) and multiplication is done with the distributive property and the rules given for multiplying i, j, k amongst themselves and with field elements. It turns out that Q_F is a noncommutative ring, called the *quaternions*.

(a) Compute $(1 + i + j + 2k)(1 + 2i + 2j + k)$ if F is of characteristic 3.

(b) Compute $(1 + i + 2j + 3k)(1 - i - 2j - 3k)$ if F is of characteristic 0.

(c) Show that $\phi : Q_F \to \mathrm{M}_2(\mathbb{C})$ given by the rule below is a monomorphism.

$$\phi(a + bi + cj + dk) = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} + d\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

(d) If the characteristic of F is 5 then show that $1 + 2i + 3j - k$ is a zero divisor in Q_F.

(6) Let E be an extension field of F. Let $\alpha \in E$ be algebraic of odd degree over F. Show that α^2 is algebraic of odd degree over F and $F(\alpha) = F(\alpha^2)$.

Hint: If $F(\alpha^2) \neq F(\alpha)$ then $F(\alpha)$ must be an extension field of $F(\alpha^2)$ of degree 2 since α is a zero of $x^2 - \alpha^2$.

(7) Let E be an extension field of a field F.

(a) If $[E : F]$ is a prime, show that $E = F(\alpha)$ for all $\alpha \in E \setminus F$.

(b) Show that if $a, b \in E$ are algebraic over F of degrees m, n respectively, and m, n are relatively prime then $[F(a, b) : F] = mn$.

(8) Show that if F is a finite field of odd characteristic then F is not algebraically closed.

Hint: Consider that $1 \neq -1$ since the characteristic is odd. However, $1^2 = (-1)^2$, so the squares of elements in F run through at most $|F| - 1$ elements of F. So there is an element $\alpha \in F$ that is not a square of any element of F...

(9) Let $p \in \mathbb{N}$ be prime. Construct a field of order p^2.

Hint: Consider two cases, $p = 2$ and $p \neq 2$. In the case $p \neq 2$, use the preceding exercise. In either case, construct the field as a quotient of $\mathbb{Z}_p[x]$.

(10) Let $p \in \mathbb{N}$ be a prime and F be a finite field of characteristic p. Show that every element of F is algebraic over the subfield $\mathbb{Z}_p$.

Hint: Apply group theory to the multiplicative group F^* to show that every element $\alpha \in F$ is the root of some $x^k - 1 \in \mathbb{Z}_p[x]$ for some $k \in \mathbb{N}$.