MODERN ALGEBRA II SPRING 2019:
SEVENTH PROBLEM SET

1. Consider the field \( \mathbb{Q}(\sqrt[3]{2}) \), viewed as a vector space of dimension 3 over \( \mathbb{Q} \). Let \( a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2}) \), and define the multiplication map \( M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2} : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}) \) by

\[
M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2}(\alpha) = (a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) \cdot \alpha.
\]

In other words, \( M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2} \) is multiplication by \( a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \).

(i) Using the basis \( \{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\} \) of \( \mathbb{Q}(\sqrt[3]{2}) \), express the \( \mathbb{Q} \)-linear map \( M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2} \) as a 3 \( \times \) 3 matrix with entries in \( \mathbb{Q} \).

(ii) If \( A \in M_3(\mathbb{Q}) \) (i.e. \( A \) is a 3 \( \times \) 3 matrix with entries in \( \mathbb{Q} \)), what is the condition that \( A = M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2} \) (with respect to the basis \( \{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\} \)) for some \( a, b, c \in \mathbb{Q} \)?

(iii) What is \( \det M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2} \)? Argue without any computation that

\[
\det M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2} \neq 0
\]

as long as \( a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \neq 0 \).

(iv) (If you know Cramer’s rule for the inverse of a 3 \( \times \) 3 matrix.) Calculate the inverse matrix \( M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2}^{-1} \), and show that it is of the form \( M_{d+e\sqrt[3]{2}+f(\sqrt[3]{2})^2} \) for some \( d, e, f \in \mathbb{Q} \). Use this to give an explicit formula for \( (a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2)^{-1} \).

2. Let \( E \) be an extension field of a field \( F \), and let \( \alpha, \beta \in E \). Suppose that \( \alpha + \beta \) and \( \alpha\beta \in F \). Show that \( \alpha \) and \( \beta \) are both algebraic over \( F \), that \( F(\alpha) = F(\beta) \), and that \( [F(\alpha) : F] \leq 2 \). (Hint: find a degree two polynomial \( f \in F[x] \) such that \( \alpha \) and \( \beta \) are both roots of \( f \).)

3. Let \( F \) be a field and let \( n \) be a positive integer. Show that, if the characteristic of \( F = p > 0 \) and \( p \) divides \( n \), then \( x^n - 1 \) has a multiple root in some extension field \( E \) of \( F \). In fact, show that \( x^n - 1 \) is the \( p \)th power of a polynomial. Show however that if the characteristic of \( F = p \) and \( p \) does not divide \( n \), or if the characteristic of \( F \) is 0, then the polynomial \( x^n - 1 \) does not have a multiple root in any extension field \( E \) of \( F \).
4. (Derivatives via formal difference quotients). Let $F$ be a field.

(i) By direct computation, show that \( \frac{y^n - x^n}{y - x} \in F(x, y) \) is a polynomial in $x$ and $y$, i.e. is an element of $F[x,y]$.

(ii) Let $f \in F[x]$. Using (i), show that \( \frac{f(y) - f(x)}{y - x} \) is a polynomial $Q_f(x,y)$ in $x$ and $y$.

(iii) Show that, for all $c \in F$ and $f, g \in F[x]$, $Q_{cf}(x,y) = cQ_f(x,y)$ and that $Q_{f+g}(x,y) = Q_f(x,y) + Q_g(x,y)$. By the usual trick of adding and subtracting an appropriate term, show that $Q_{fg}(x,y) = f(y)Q_g(x,y) + Q_f(x,y)g(x)$.

(iv) Viewing $Q_f(x,y)$ as an element of $F[x,y]$, evaluate $Q_f(x,x)$ in case $f(x) = x^n$. Conclude that the formal derivative $Df$, as we have defined it in class, is equal to $Q_f(x,x)$ for every $f \in F[x]$. Use (iii) to prove the sum and product rules.

5. Let $F$ be a field of characteristic $p > 0$.

(i) Suppose that every element of $F$ is a $p^{th}$ power, i.e. for all $a \in F$, there exists an element $b \in F$ such that $b^p = a$. Equivalently, the Frobenius homomorphism $\sigma_p: F \to F$ is surjective. Such a field is called perfect. Show that, if $f \in F[x]$ is irreducible, then $f$ does not have multiple roots. (Hint: if it did, then $f$ would have derivative zero and hence be of the form $\sum_{i=0}^na_ix^{ip}$ for some $a_i \in F$. Since $F$ is perfect, there exist $b_i \in F$ such that $a_i = b_i^p$. Now show that the polynomial $f = \sum_{i=0}^na_ix^{ip} = \sum_{i=0}^nb_i^px^{ip}$ is a $p^{th}$ power and hence is not irreducible, a contradiction.)

(ii) Show that a finite field is perfect. (Hint: consider the Frobenius homomorphism $\sigma_p: F \to F$. Then $\sigma_p$ is injective. Now using the fact that $F$ is finite, conclude that $\sigma_p$ is surjective.)

(iii) For $\mathbb{F}_3$ and $k = 2$, show that the function $\sigma_2: \mathbb{F}_3 \to \mathbb{F}_3$ defined by $\sigma_2(\alpha) = \alpha^2$ is neither injective nor surjective. $\sigma_2(\alpha) = \alpha^2$. Thus, not every element of a finite field is a $k^{th}$ power. Where does the argument in (ii) break down?

(iv) More generally, let $F$ be a finite field with $\#(F) = q$. For every positive integer $k$, define $\sigma_k: F \to F$ by: $\sigma_k(\alpha) = \alpha^k$. Using the fact that $F^*$ is cyclic, show that $\sigma_k$ is a bijection $\iff$ $k$ and $q - 1$ are relatively prime.