Honors Algebra II, Courant Institute, Spring 2022
http://www.math.nyu.edu/faculty/goodman/teaching/HonorsAlgebraII2022/HonorsAlgebraII.html
Check the class forum for corrections and hints

Assignment 11

Due: Thursday, May 5.

1. (*Section 16.1 of the Michael Artin book is about elementary symmetric polynomials. This exercise gives a different approach to some of that material suggested by the book of Emil Artin. You may find this approach confusing at first because polynomials over rational function fields take time to get used to.*) Let $\mathbb{F}$ be a field and let $\mathbb{K}$ be the rational function fields in three variables over $\mathbb{F}$:

$$\mathbb{K} = \mathbb{F}(X, Y, Z) \ .$$

Define a polynomial $f \in \mathbb{K}[T]$ by

$$f(T) = (T - X)(T - Y)(T - Z) \ . \tag{1}$$

This formula gives a polynomial in T because X, Y, and Z are elements of $\mathbb{K}$. This can cause (has caused!) confusion, particularly in part (b).

(a) Define $A_1, A_2, A_3 \in \mathbb{K}$ by

$$f(T) = T^3 - A_1 T^2 + A_2 T - A_3 \ . \tag{2}$$

The A_1, A_2, and A_3 are elements of $\mathbb{F}[X, Y, Z]$ (i.e., polynomials). Find formulas for them. (They are the *elementary symmetric polynomials* in the variables X, Y, and Z.)

(b) Define the intermediate fields $\mathbb{L} \subset \mathbb{M} \subset \mathbb{K}$ by

$$\mathbb{L} = \mathbb{F}(A_1, A_2, A_3) \ , \ \ \mathbb{M} = \mathbb{L}[X] \ .$$

Show that:

- $[\,\mathbb{M} : \mathbb{L}] = 3$ *Hint.* (2) does not split in $\mathbb{K}$.
- $\mathbb{K} = \mathbb{M}[Y]$
- $[\,\mathbb{K} : \mathbb{M}] = 2$

(c) The permutation group S_3 acts on $\mathbb{K}$ by permuting the variables X, Y, Z. The *fixed field* of this action is the set of rational functions $r(X, Y, Z)$ that are *invariant* under permutation of variables (i.e., $r(X, Y, Z) = r(Z, X, Y) = r(Y, X, Z)$, etc.). The field-theoretic notation for the fixed field is $\mathbb{K}^{S_3}$. Show that $\mathbb{L} \subseteq \mathbb{K}^{S_3}$.

(d) We will prove next week that for any field extension $\mathbb{K}$ over $\mathbb{F}$,

$$|\text{Gal}(\mathbb{K}/\mathbb{F})| \leq [\,\mathbb{K} : \mathbb{F}\,] \ .$$

Assuming this and using the notation of part (c), show that

$$[\,\mathbb{K} : \mathbb{K}^{S_3}\,] \geq 6 \ .$$

Combine this with part (b) to show that $\mathbb{L} = \mathbb{K}^{S_3}$. (This is the basic fact of Michael Artin's Section 16.1: any symmetric function is a function of the elementary symmetric functions. Emil Artin does the theorem for rational functions while Michael Artin does it in a longer but more elementary way just for polynomials. Both of them do it for $n \geq 3$ variables, which is more or less the same as the argument here, but with more notation.)

2. (*Making the formal derivative look more like calculus*) Take a polynomial over a field, $f \in \mathbb{F}[X]$ and define a new polynomial $u \in \mathbb{F}[X, h]$ (the ring of polynomials in two variables) by $u(X, h) = f(X + h)$.

(a) Show that there are polynomials $f' \in \mathbb{F}[X]$ and $r \in \mathbb{F}[X, h]$ so that

$$f(X + h) = f(X) + hf'(X) + h^2 r(X, h) \ . \tag{3}$$

(The last term on the right is a version of $O(h^2)$.) The formula (3) defines a map $D \colon \mathbb{F}[X] \to \mathbb{F}[X]$ by $Df = f'$.

(b) Show that D is a linear map on $\mathbb{F}[X]$ as a vector space over $\mathbb{F}$, and a homomorphism of $\mathbb{F}[X]$ as an additive group, but is not a ring homomorphism.

(c) Use (3) to show that $(fg)' = f'g + fg'$ in $\mathbb{F}[X]$. (An additive group homomorphism on a ring is called a *derivation* if it satisfies $D(fg) = (Df)g + f(Dg)$. Formal differentiation is a derivation.)

(d) Identify $\ker(D)$. The answer depends on whether $\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) = p > 1$. (This is a restatement of an exercise from Assignment 10.)

(e) (*Do this only if you're interested. It's not important for the class.*) Show that if $c \in \mathbb{F}$ (a polynomial of degree zero) and D is a derivation on $\mathbb{F}[X]$ then $Dc = 0$. Show that if D is any derivation $\mathbb{F}[X]$ satisfying $\deg(Df) < \deg(f)$, then $Df = cf'$, for some $c \in \mathbb{F}$. Is this true without the hypothesis $\deg(Df) < \deg(f)$?

3. (*We described the splitting field of $X^3 - 2$ in class. Here's an example where (hint) the same ideas apply but the general structure is more clear.*) Let $\mathbb{K}/\mathbb{Q}$ be a splitting field of $X^5 - 2$ with $\mathbb{K} \subset \mathbb{C}$. Give an analysis of $\mathbb{K}/\mathbb{Q}$ that explains the following:

- $\mathbb{K} = \mathbb{Q}[\rho, \zeta_5]$, where $\rho \in \mathbb{R}$ has $\rho^5 = 2$ and $\zeta_5 = e^{2\pi i/5}$.

- Let G be the group of field automorphisms of $\mathbb{K}$ that fix $\mathbb{Q}$ (i.e., the *Galois group* $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$. Any $g \in G$ is uniquely specified by integers k and n so that $g(\rho) = \zeta_5^k \rho$ and $g(\zeta_5) = \zeta_5^n$.
- Define special elements $\sigma\colon (\rho \rightsquigarrow \zeta_5\rho,\ \zeta_5 \rightsquigarrow \zeta_5)$ and $\tau\colon (\rho \rightsquigarrow \rho,\ \zeta_5 \rightsquigarrow \zeta_5^2)$. These satisfy $\sigma^5 = \mathrm{id}$, $\tau^4 = \mathrm{id}$ (more precisely, σ has order 5 and τ has order 4) and the commutator relation $\tau\sigma\tau^{-1} = \sigma^2$. This is a "generators and relations" description of G.
- Every $g \in G$ may be represented as $g = \sigma^k \tau^n$, where k and n are uniquely defined mod 5 and mod 4 respectively. *Warning.* G is not a product group, not abelian, and $(\sigma^j\tau^m)(\sigma^k\tau^n) \neq \sigma^{j+k}\tau^{m+n}$.
- $|G| = [\mathbb{K} : \mathbb{Q}]$. (This is a general theorem, but please verify it explicitly by determining the order of G and the degree of $\mathbb{K}/\mathbb{Q}$)

4. A group G is a *reflection group* if every $g \in G$ has $g^2 = \mathrm{id}$ (every element has order two). Let $\mathbb{K} \subset \mathbb{C}$ be a finite degree extension of $\mathbb{Q}$ so that $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$ is not a reflection group. Show that $\mathbb{K}$ contains at least one nontrivial root of unity $e^{2\pi i/n}$ with $n > 2$. *Hint.* Let $\{\gamma_j\}$ be a basis of $\mathbb{K}$ over $\mathbb{Q}$. Let M be the matrix with rational coefficients that represents the action of g in the $\{\gamma_j\}$ basis. Why are there elements of $\mathbb{K}$ corresponding to eigenvalues and eigenvectors of M?