MA 741: Algebra I / Fall 2020
Homework assignment #9
Due before 8pm on Monday, December 14

Hint for (3a) edited 2:15pm 12/14/2020.
To turn in your work, please email your well-titled document (title should identify you, this course, and the HW set number) to `buma741fall2020@gmail.com` with "HW 9" in the subject line. Please indicate with whom you worked on the problem set.

(1) **Separability:** Let K be a field. Recall that a polynomial $f \in K[x]$ is *separable* if it has no repeated roots in any algebraic extension of K. This is equivalent to $\gcd(f, f') = 1$ (see 4(b) on HW #8).

(a) Show that if f is irreducible then f is not separable if and only if $f' = 0$; and in this case, $\operatorname{char} K = p$ for some prime p and $f(x) = g(x^p)$ for some polynomial $g \in K[x]$.

(b) Suppose $\operatorname{char} K = p$. Show that if the Frobenius endomorphism $\alpha \mapsto \alpha^p$ of K is surjective (in other words, if every element of K has a p^{th} root in K; equivalently, Frobenius is an automorphism) then for any polynomial $g \in K[x]$, we have $g(x^p) = h(x)^p$ for some polynomial $h \in K[x]$. Conclude that in this case every irreducible polynomial in $K[x]$ is separable.

A field K is usually said to be *perfect* if either $\operatorname{char} K = 0$ or $\operatorname{char} K = p$ and the Frobenius endomorphism $\alpha \mapsto \alpha^p$ is surjective. Parts (1a) and (1b) above show that this is equivalent to the definition given in class: K is perfect if and only if every algebraic extension L/K is separable. In particular, $\mathbb{Q}$ and $\mathbb{F}_p$ are perfect.

(c) Let K be a field of positive characteristic p and $f \in K[x]$ an irreducible polynomial. Prove that there exists an integer $d \geq 0$ and a *separable* irreducible polynomial $h \in K[x]$ so that

$$f(x) = h(x^{p^d}).$$

If f is the minimal polynomial of α in some extension L of K, show that α is separable over K if and only if $d = 0$. In general, show that α^{p^d} is separable over K.

For a finite extension L/K, let $[L : K]_s$ be the number of embeddings of L into an algebraic closure $\overline{K}$ over K. In class we explained why $[L : K]_s$ is multiplicative in towers (Aluffi Lemma VII.4.23) and asserted that $[L : K]_s \leq [L : K]$, with equality if and only if L/K is separable (Aluffi Prop. VII.4.24). As a corollary, separability transfers in towers: if $L/E/K$ is a tower of finite extensions of fields, then L/K is separable if and only if L/E and E/K is separable.

(d) Suppose L/K is an algebraic extension in positive characteristic p. An element α of L is said to be *purely inseparable* if $\alpha^{p^d} \in K$ for some $d \geq 0$. The extension L/K is then *purely inseparable* if every $\alpha \in L$ is purely inseparable over K.

Prove that α is purely inseparable if and only if $[K(\alpha) : K]_s = 1$.

(e) Suppose L/K is a field extension. Let $\alpha, \beta \in L$ be separable over K. Show that $K(\alpha, \beta)$ is a separable extension of K. Deduce that

$$L_{\text{sep}} := \{\gamma \in L : \gamma \text{ is separable over } K\}$$

is a subfield of L, the *separable closure of K in L*.

(f) Let L/K be an finite extension in positive characteristic and L_{sep} as above the separable closure of K in L. Show that the extension L/L_{sep} is purely inseparable. Show that $[L : L_{\text{sep}}]_s = 1$. Conclude that

$$[L_{\text{sep}} : K] = [L_{\text{sep}} : K]_s = [L : K]_s.$$

This explains why $[L : K]_s$ is called the *separable degree* of the extension L/K. As a corollary $[L : K]_s$ divides $[L : K]$.

(2) For each of the following extensions, determine whether it is Galois. If it is not Galois, determine the degree of the extension and whether the extension is normal or separable. If it is Galois, identify the Galois group, and describe the Galois correspondence completely explicitly (list the subgroups and the intermediate fields, show how they correspond, which ones are normal, etc.).

(a) $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

(b) $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}(\sqrt{2})$.

(c) $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}$.

(d) $\mathbb{Q}(\sqrt[4]{2}, i)$ over $\mathbb{Q}(i)$.

(e) $\mathbb{Q}(\sqrt[4]{2}, i)$ over $\mathbb{Q}$.

(*Hint:* One of the subfields of one of the extensions above is $\mathbb{Q}(\zeta_8 2^{\frac{1}{4}})$, where $\zeta_8 = e^{\frac{\pi i}{4}}$ is a primitive 8^{th} root of unity. Note also that $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8)$.)

(3) Consider the field $\mathbb{Q}(\zeta)$, where $\zeta = \zeta_7$ is a primitive 7^{th} root of unity.

(a) Show that $K/\mathbb{Q}$ is a Galois extension of degree 6.

(To show that $\frac{x^7-1}{x-1}$ is irreducible in $\mathbb{Q}[x]$, replace x by $x+1$ to get a polynomial $f(x) \in \mathbb{Z}[x]$. If f factors in $\mathbb{Z}[x]$, show by reducing f modulo 7 that the constant coefficient of each factor must be divisible by 7. Explain why this is impossible. This is a special case of the *Eisenstein criterion* for irreducibility.)

(b) Show that the Galois group is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^\times$. How many generators does this group have? Explain what each generator does to α. Which element of the Galois group corresponds to complex conjugation?

(c) List all the subfields of K, giving a primitive element and its minimal polynomial for each. If a subfield E is Galois over $\mathbb{Q}$, identify its Galois group and explain how it acts on your primitive element.

(d) A *totally real* field is an extension of $\mathbb{Q}$ all of whose embeddings to $\mathbb{C}$ land in $\mathbb{R}$. For example, $\mathbb{Q}(\sqrt{2})$ is a totally real field, but $\mathbb{Q}(\sqrt[3]{2})$ is not. Does $\mathbb{Q}(\zeta)$ have a totally real subfield? Explain.

(e) Show that $\sqrt{-7}$ is in $\mathbb{Q}(\zeta)$. Express $\sqrt{-7}$ as a polynomial in ζ.

(4) Read and understand DF Theorem 7 on p. 569: linear independence of characters.

(a) Show that every finite-dimensional irreducible complex representation of an abelian group is one-dimensional. (Come talk to me if you get stuck.)

Recall that you have shown (4(e) HW #7) that a finite-dimensional complex representation of G is totally decomposable.

(b) Now let G be a finite abelian groups. Give this total decomposition into irreducibles explicitly for the left regular representation $\mathbb{C}[G]$.

Problems 5(e) on HW #7 and 5(c) on HW #3 may be helpful.

(c) **Optional:** Do the same for $\mathbb{C}[S_3]$ as a representation of S_3.