Assignment 5, due March 2

Corrections: [none yet]

1. Show that if $\mathbb{E}/\mathbb{Q}$ is the splitting field of a polynomial of degree n, then $\deg(\mathbb{E}/\mathbb{Q})$ divides $n!$.

2. Find the Galois group of the splitting field of $x^3 - 3x^2 + 1$ over $\mathbb{Q}$.

3. (*Quick introduction for some, quick review for others*). Let R be a ring. A *module* V over R is an abelian group (written additively) together with an "R action", written as multiplication. We assume everything is associative and distributive. For example, if $x \in R$ and $y \in R$ and $u \in V$, then $(x+y)u = (xy) + (yu)$. On the left is addition in R then action of $x + y \in R$ on $u \in V$. On the right is $xu \in V$ (x acting on u) added (in V) to yu. Also, $x(u_1 + u_2) = xu_1 + xu_2$, etc. If R were a field then this would make V a vector space, but there is more variety in modules than in vector spaces.

   (a) Show that if $I \subset R$ is an ideal, addition in I and multiplication by $x \in R$ makes I a module over R.

   (b) Show that if $I \subset R$ is an ideal, then R/I is a module in a natural way.

   (c) A set $g_1 \in V$, ..., $g_n \in V$ is a set of *generators* of V (or *generates* V) if every $u \in V$ may be written as

   $$u = \sum_{j=1}^{m} x_j g_j \ , \quad x_j \in R \ .$$

   The representation need not be unique and m need not be minimal. Give an example of a module generated by one generator that is not isomorphic to R in the category of modules over R. [Note, this can't happen for vector spaces.]

   (d) Give an example of a module $V \subset R$ that cannot be generated by a single generator. *Hint*: $\mathfrak{p} \subset \mathbb{Z}[i\sqrt{5}]$. [A proper subspace of a vector space requires fewer generators (basis vectors), never more.]

4. Suppose $\mathbb{E}/\mathbb{Q}$ is a finite degree normal extension. An $\alpha \in \mathbb{E}$ is an *algebraic integer* if $f(\alpha) = 0$ where $f \in \mathbb{Z}[x]$ is a *monic* polynomial (*monic* means f has leading coefficient 1, so $f(x) = x^n + b_{n-1}x^{n-1} + \cdots$.)

(a) Show that the module over $\mathbb{Z}$, V, generated by powers of α is finitely generated if α is an algebraic integer. Show that $\alpha V \subset V$.

(b) Suppose $\alpha \in \mathbb{E}$ and $V \subset \mathbb{E}$ is a finitely generated $\mathbb{Z}$ module with $\alpha V \subset V$. Show that α is an algebraic integer. *Hint*: Write the action of multiplication of α in terms of the generators g_k of V and show that α is an eigenvalue of the resulting matrix.

(c) Show that the set of algebraic integers in $\mathbb{E}$ forms a ring. *Hint*: If g_k generate the α module and h_j generate the β module, then the elements $g_k h_j$ generate a module for $\alpha + \beta$ and $\alpha\beta$.

(d) Show that $\mathbb{Z}[i]$ (the Gaussian integers) are the algebraic integers in $\mathbb{Q}[i]/\mathbb{Q}$.

5. The field $\mathbb{F}$ is algebraically closed if any $g \in \mathbb{F}[x]$ splits in $\mathbb{F}$. A field $\mathbb{E}/\mathbb{F}$ is an *algebraic closure* of $\mathbb{F}$ if $\mathbb{E}$ is algebraically closed and no proper subfield $\mathbb{B} \subset \mathbb{E}$ that contains $\mathbb{F}$ is algebraically closed. For example, $\mathbb{C}$ is algebraically closed (the "fundamental theorem of algebra") and $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. This exercise gives a construction of an algebraic closure of finite or countable fields. The construction for fields that are not countable involves fancier set theory, the *axiom of choice* in the form of *Zorn's lemma*. Our version will be enough for our class. It is not hard to prove, but not part of this exercise, that all algebraic closures of $\mathbb{F}$ are isomorphic. We call any one of them "the" algebraic closure.

(a) Suppose $\mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots$ is an infinite sequence of fields. Show that $\overline{\mathbb{K}}$ is a field, where
$$\overline{\mathbb{K}} = \cup_{n=1}^{\infty} \mathbb{K}_n \ .$$
Assume $\mathbb{K}_{n+1}/\mathbb{K}_n$ is a field extension for each n.

(b) Suppose $\mathbb{E}/\mathbb{F}/\mathbb{K}$ is a three element tower of finite index algebraic field extensions. Show that every $\alpha \in \mathbb{E}$ satisfies a polynomial equation $f(\alpha) = 0$ where $f \in \mathbb{K}[x]$. This is the main idea behind this exercise.

(c) A set S is *countable* if it is possible to put the elements into an enumerated list
$$S = \{s_1, s_2, \ldots\} \ .$$
It's OK to have repeats. For example, the positive rational numbers are countable because you can make the list $\frac{0}{1}, \frac{1}{1}, \frac{0}{2}, \frac{1}{2}, \frac{2}{2}, \frac{3}{2}, \frac{4}{2}, \frac{0}{3}, \cdots$. Show that if $\mathbb{K}$ is a finite or countable field, then the set of polynomials $\mathbb{K}[x]$ is also countable.

(d) Call the list from part (c) $f_1(x), f_2(x), \cdots$. Let $\mathbb{K}_{n+1}$ be an extension field of $\mathbb{K}_n$ where f_n splits. Show that each of the polynomials f_n splits inthe union $\overline{\mathbb{K}}$.

(e) Suppose $g \in \mathbb{K}_n[x]$. Show that g splits in some K_m for $m \geq n$.

(f) Suppose $g \in \overline{\mathbb{K}}[x]$. Show that g splits in $\mathbb{K}_n$.

(g) Let $\overline{\mathbb{Q}}$ be "the" algebraic closure of $\mathbb{Q}$. Show that $\overline{\mathbb{Q}}$ is countable. In particular, $\mathbb{C}$ is not the algebraic closure of $\mathbb{Q}$.

(h) Show that $\overline{\mathbb{F}_p}$ is an infinite field of characteristic p.