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 9

Due: Thursday, April 21.

A cyclotomic example. A field extension $\mathbb{F}/\mathbb{Q}$ is *cyclotomic* if it is generated by roots of unity. They are also called *abelian* because the Galois group (to be defined) is abelian. Let $\zeta_n = e^{2\pi i/n}$ be our usual primitive n^{th} root of unity. We will see, in general, that $[\,\mathbb{Q}[\zeta_n] : \mathbb{Q}\,] = \phi(n)$, where ϕ is the Euler *totient* function that counts the number of residue classes mod n that are relatively prime to n. The minimal polynomial of ζ_n is denoted $\Phi_n(x)$ and is called a *cyclotomic* polynomial. As we will see, the other roots of Φ_n are the other primitive n^{th} roots ζ_n^k, where k is relatively prime to n. In gcd notation, this is $\gcd(k,n) = (k,n) = 1$.

$$\Phi_n(x) = \prod_{(k,n)=1} (x - \zeta_n^k) \; . \tag{1}$$

The product over k with $(k,n) = 1$ means a product over all such residue classes. This is equivalent to taking all k with $1 \leq k < n$ that are relatively prime to n. Galois theory gives a general way to show that $\Phi_n \in \mathbb{Q}[X]$, (a fancy way of saying it has rational coefficients), and Exercise 2 gives an ad hoc proof for this case. Galois theory also gives a quick proof that the Φ_n are irreducible over $\mathbb{Q}$. I don't know whether there is an ad hoc proof of that which does not use Galois theory. Maybe you can find one. Maybe you can show that the Φ_n have integer coefficients.

The roots of unity ζ_n^k, even the ones that are not primitive, are the n distinct roots of $f_n(x) = x^n - 1$. If ζ_n^k is not a primitive root n^{th} root, then it is a primitive m^{th} root, where m is some divisor of n. This in written as

$$\left(\zeta_n^k\right)^m = 1 \; , \quad \text{for some } m|n \; , \;\; \left(\zeta_n^k\right)^r \neq 1 \; , 0 < r < m \; .$$

The degree of Φ_n is the number of primitive roots, which is $\phi(n)$. If ζ_n^k is not a primitive root of unity, then it is a primitive root of some divisor of n (Exercise 1).

1. Let m be the smallest positive integer exponent with $(\zeta_n^k)^m = 1$. Show that if $m \neq n$ (so ζ_n^k is not a primitive root) then $m|n$ and $km = n$. Show ζ_n^k is a primitive m^{th} root of unity.

2. Prove two facts about cyclotomic polynomials using Fermat style induction on n. That means: show they are true for $n = 1$ and then look at the smallest n where one or both of them might not be true. The first is the factorization formula

$$x^n - 1 = \prod_{m|n} \Phi_m(x) \; . \tag{2}$$

In (2), you have to count $m = 1$ and $m = n$ as divisors of n. The second fact is that the coefficients in Φ_n are all rational. *Hint* (for the second part), The Euclidean and polynomial division algorithms for rational polynomials use only rational operations. Therefore, if f and g are "rational" (in $\mathbb{Q}[X]$), then $h = \gcd(f, g)$ is rational. If f and g are rational and $g|f$ in an extension field of $\mathbb{Q}$, then $g|f$ in $\mathbb{Q}$.

3. Find the cyclotomic polynomials Φ_m for $m|8$. Find the primitive 8^{th} roots, 4^{th} roots, 2^{nd}, roots, and 1^{st} root, and verify (1) by direct calculation. Verify (2) by direct calculation.

4. Find the "cartesian" formula for ζ_8 (that is, $\zeta_8 = a + bi$), and:
   (a) Show that $\mathbb{Q}[\zeta_8] = \mathbb{K}[\sqrt{2}]$, wth $\mathbb{K} = \mathbb{Q}[i]$.
   (b) Show that $[\,\mathbb{Q}[\zeta_8] : \mathbb{Q}\,] = 4$.
   (c) Find an explicit basis for $\mathbb{Q}[\zeta_8]$ over $\mathbb{Q}$.

Algebraic closure. A field $\mathbb{F}$ is *algebraically closed* if every $f \in \mathbb{F}[X]$ has a root in $\mathbb{F}$. We say that $\overline{\mathbb{F}}$ is an *algebraic closure* of $\mathbb{F}$ if $\overline{\mathbb{F}}$ is algebraically closed, $\mathbb{F} \subseteq \overline{\mathbb{F}}$, and every $\alpha \in \overline{\mathbb{F}}$ is algebraic over $\mathbb{F}$. We might say "the" algebraic closure, because any two algebraic closures are isomorphic over $\mathbb{F}$. Philosophers can debate saying "the" or "an" for something that is unique up to isomorphism. You can construct an algebraic closure by repeatedly adjoining roots. But it can be subtle to say this correctly when you have to adjoin uncountably many roots possibly in uncountably many stages. Therefore, this exercise is for countable fields only, such as $\mathbb{Q}$, finite fields, or fields of rational functions over countable fields.

1. A set is *countable* if it is possible to make a list of its elements, with the list being indexed by the positive integers, as in
$$A = \{a_1, a_2, \ldots\} = \{a_n \mid n \in \mathbb{Z}\ ,\ \ n > 0\}\ .$$
Repetition (i.e. $a_j = a_k$ with $j \neq k$) is allowed. Show that if $A_1, A_2, \cdots$ is a countable family of countable sets, then the "whole thing" is countable:
$$\left(\bigcup_{m>0} A_m \right) \text{ is countable.}$$

2. Show that if $\mathbb{F}$ is countable, then $\mathbb{F}[X]$ is countable.

3. (Read Section 15.2 before doing this Exercise.) Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[X]$ a polynomial of degree n. Show that there is an extension field $\mathbb{K}/\mathbb{F}$ that is a *splitting field* for f over $\mathbb{F}$. By definition, $\mathbb{K}$ is a splitting field if f factors (splits) into a product of linear factors in $\mathbb{K}$,
$$f(X) = \prod_{j=1}^{n} (X - \alpha_j)\ ,$$

and $\mathbb{K} = \mathbb{F}[\alpha_1, \ldots, \alpha_n]$. In other words, you get $\mathbb{K}$ from $\mathbb{F}$ by adjoining all the roots of f. Show that the splitting field is countable if the ground field $\mathbb{F}$ is countable. Take into account the possibility that f is reducible over $\mathbb{F}$, and might even split into linear factors in $\mathbb{F}$.

4. Let f_n be a list of all polynomials over $\mathbb{F}$, which means that $\mathbb{F}[X] = \{f_n | n > 0\}$. Define a tower of fields starting with $\mathbb{F}_0 = \mathbb{F}$. The tower is $\mathbb{F}_n \subseteq \mathbb{F}_{n+1}$, with $\mathbb{F}_{n+1}$ being a splitting field for f_n over $\mathbb{F}_n$. Now verify that

$$\overline{\mathbb{F}} = \bigcup_{n \geq 0} \mathbb{F}_n \tag{3}$$

is an algebraic closure of $\mathbb{F}$, and countable. Here is one possible sequence of steps, which you may or may not choose to follow:

   (a) Show that the union (3) is countable.

   (b) Show that the union (3) is a field – closed under field operations.

   (c) Show that if $\alpha \in \mathbb{F}_n$, for some n, then α is algebraic over $\mathbb{F}$. *Hint.* A trick from Thursday's class may help here.

   (d) Suppose $g \in \mathbb{F}_n[X]$. Show that g has a root in $\mathbb{F}_m$ for some $m \geq n$. *Hint.* g has a root α in some extension $\mathbb{K}$ of $\mathbb{F}_n$ (Section 15.2) and α is algebraic over $\mathbb{F}_n$, so it is algebraic over $\mathbb{F}$, so it is a root of a polynomial in $\mathbb{F}[X]$.

   (e) If $g \in \overline{\mathbb{F}}[X]$, then $g \in \mathbb{F}_n[X]$ for some n.