Assignment 6, due March 9

Corrections: March 3: Exercise 3 edited to say "integrally closed" instead of "algebraically closed", Exercise 9 edited to change $x+n$ to x_n.

1. Choose an integer $n > 2$ and let $\Phi_n \subseteq \mathbb{Z}/(n)$ be the set of equivalence classes k mod n so that $\gcd(k,n) = 1$. The *Euler function* ϕ is defined by $\phi(n) = |\Phi_n|$.
   (a) Show that Φ_n is an abelian group of order $\phi(n)$ under multiplication. [This is a well known fact that you may have seen and is in many books. Please try to find a proof on your own.]
   (b) Find an n so that you can show that Φ_n is not a cyclic group. I don't know how to do this except by trying examples. You don't have to try primes (why not?).
   (c) Let $\mathbb{F}/\mathbb{Q}$ be a splitting field of $f(x) = x^n - 1$. Let $\omega_1, \ldots, \omega_n$ be the roots of p in $\mathbb{F}$. Show that the ω_k are distinct and closed under multiplication. Show that there is an ω_* so that if $a^n = 1$ in $\mathbb{F}$, then $a = \omega_*^k$ for some integer k (which is not unique). [Any such ω_* is a *primitive* root of unity.] *Hint*: It is possible to take $\mathbb{F} \subset \mathbb{C}$. Why?
   (d) Let $G = \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ be the Galois group and take $\sigma \in G$. Show that if ω_* is a primitive root of unity, then $\sigma(\omega_*)$ also is a primitive root of unity. *Hint*: You can characterize primitive roots of unity by what ω_*^k cannot be for $k < n$.
   (e) A polynomial p_n is defined by
   $$p_n(x) = \prod_{\omega_k \text{primitive}} (x - \omega_k) \; .$$
   Show that $p \in \mathbb{Q}[x]$ and that p is separable. Show that $\mathbb{F}$ is the splitting field of p.
   (f) Show that if ω_* is a primitive root of unity, then the map on primitive roots $\omega_k \to \omega_* \omega_k$ defines an element $\sigma \in G$.
   (g) Show that $\mathrm{Gal}(\mathbb{F}/\mathbb{Q}) = \Phi_n$. A field $\mathbb{F}$ of this type (roots of unity) is called *cyclotomic*.

2. Show that if $f(a) = 0$ and $a \neq 1$ in a cyclotomic field of roots of unity of order n, then a is a primitive root of unity a cyclotomic field of order n/d. Use this to show that the prime factorization of $f_n(x) = x^n - 1$ is
$$x^n - 1 = \prod_{k|n} p_k(x) \; .$$

Define the product to include the "trivial factor" $(x-1)$. Use this to verify the Euler ϕ function formula:

$$n = \sum_{k|n} \phi(k) \; .$$

[And try to say "famous ϕ function formula" five times quickly.]

3. Let R be a ring that is a unique factorization domain and an integral domain (redundant?). Let K be the field of fractions. Let $\mathbb{E}$ be a finite degree extension field of K. We say $a \in \mathbb{E}$ is *algebraic* over R if there is a monic polynomial $f \in R[x]$ with $f(a) = 0$ (a generalization of the definition from Assignment 5, which was for $R = \mathbb{Z}$). We say that R is *integrally closed* in $\mathbb{E}$ if there is no $a \in \mathbb{E}$ that is algebraic over R except $a \in R$. We say that R is *integrally closed* if it is integrally closed in K (the fraction field). Show that R is integrally closed. *Hint*: An element of K may be written

$$a \; = \; \frac{\displaystyle\prod_i p_i^{\alpha_i}}{\displaystyle\prod_j q_j^{\beta_j}}$$

Here $\{p_i\}$ and $\{q_j\}$ are disjoint finite sets of irreducibles in R and the α_i and β_j are positive integers. If a is the root of a monic polynomial of degree n, (show that) there is a $y \in R$ with

$$\prod_i p_i^{n\alpha_i} = y \prod_j q_j^{\beta_i} \; .$$

[The giveaway hint is because this fact is called *Gauss' lemma* and the proof is in most books. A harder theorem, also called Gauss' lemma but not part of this exercise, is that a monic $f \in R[x]$ is irreducible in $R[x]$ if it is irreducible in $K[x]$. This exercise shows that f has a linear factor in $R[x]$ only if it has a linear factor in $K[x]$.]

4. Suppose $a > 1$ is a positive integer that is not of the form $a = b^n$ for an integer b. Show that $f(x) = x^n - a$ is irreducible in $\mathbb{Q}$.

5. Suppose p is a rational prime and $a > 1$ is an integer that is not of the form $a = b^p$ for an integer b. Let $\mathbb{E}/\mathbb{Q}$ be the splitting field of $x^p - a$. Show that $\deg(\mathbb{E}/\mathbb{Q}) = p(p-1)$ and describe the Galois group. *Hint*: If you adjoin $a^{\frac{1}{p}}$ first (look at $\mathbb{Q}[a^{\frac{1}{p}}]/\mathbb{Q}$), you learn p divides $\deg(\mathbb{E}/\mathbb{Q})$. If you split $x^p - 1$ first, you get different information that suggests G has two generators. Compute the commutator. The example $x^3 - 2$ is a model for the general case.

6. (*Extra credit, don't work on this too long.*) Find an example of $f \in \mathbb{F}_p[x]$ that is irreducible but not separable.

7. Let $a \in \mathbb{Z}$ be a rational integer that may be written $a = p^n b$ where $p \not| b$ The $p-adic$ norm (more commonly called the $p-$adic *valuation*) of a is

$$\left|a\right|_p = p^{-n} \ .$$

Integers x and y are close in the $p-$adic sense if they agree to a high power of p. Show that this satisfies the *ultra-metric* inequality

$$\left|x - y\right|_p \leq \max\Big(\left|x\right|_p , \left|y\right|_p \Big) \ .$$

Show that this implies the ordinary triangle inequality

$$\left|x - y\right|_p \leq \left|x\right|_p + \left|y\right|_p \ .$$

8. For any $f \in \mathbb{Z}[x]$, and any $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$, show that

$$\begin{aligned} \left|f(x+y) - f(x)\right|_p &\leq \left|y\right|_p \\ \left|f(x+y) - [f(x) + f'(x)y]\right|_p &\leq \left|y\right|_p^2 \ . \end{aligned}$$

[These are "familiar" from ordinary calculus. The first says that a polynomial is *Lipschitz continuous*, but here the Lipschitz constant is always 1. The second says that the first derivative approximation is accurate to $O(\left|y\right|_p^2)$, but again with a constant 1. This The derivative f' is the formal derivative.] Use the first inequality to show (or do it directly) that if $f'(x) \neq 0 \bmod p$, and $\left|y\right|_p < 1$, then $f'(x+y) \neq 0 \bmod p$.

9. *Newton's method* from ordinary calculus to solve the equation $f(x) = 0$ is the iteration scheme

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \ .$$

Suppose $f \in \mathbb{Z}[x]$ and that if there is an $x_0 \in \mathbb{Z}$ with $f(x_0) = 0 \bmod p$ and $f'(x_0) \neq 0 \bmod p$. Show that there is a sequence $x_n \in \mathbb{Z}$ with

$$\begin{aligned} \left|x_n - x_{n-1}\right|_p &\leq p^{-n} \\ \left|f(x_n)\right|_p &\leq p^{-n} \ . \end{aligned}$$

[The conclusion of this exercise, sometimes re-packaged using part (c) of exercise 10, is called *Hensel's lemma*.]

10. (*Extra credit. Do this only if you have time and have taken the right analysis class.*) The *$p-$adic inteegers*, written $\mathbb{Z}_p$, are the completion of $\mathbb{Z}$ in the $p-$adic valuation. Suppose x_n and y_n are Cauchy sequences in $\mathbb{Z}$ with respect to $\left|\cdot\right|_p$ that represent $x \in \mathbb{Z}_p$ and $y \in \mathbb{Z}_p$ respectively. The Cauchy sequences defining $x + y$ and xy are $x_n + y_n$ and $x_n y_n$.

    (a) Show that these operations are well defined, which means showing that $x + y$ and xy in $\mathbb{Z}_p$ are independent of which Cauchy sequences represent x and y.

(b) Show that $\mathbb{Z}_p$ is a ring with these operations.

(c) Show that if $f \in \mathbb{Z}[x]$ and there is an $x_0 \in \mathbb{Z}$ with $f(x_0) = 0 \bmod p$ and $f'(x) \neq 0 \bmod p$, then $f(x) = 0$ for some $x \in \mathbb{Z}_p$.

(d) Show that $\mathbb{Z}_p$ is compact. If $x_k \in \mathbb{Z}_p$ is any sequence, show that there is a subsequence $k_j \to \infty$ as $j \to \infty$ so that x_{k_j} is a Cauchy sequence.