Honors Algebra II, Courant Institute, Spring 2021
http://www.math.nyu.edu/faculty/goodman/teaching/HonorsAlgebraII2021/HonorsAlgebraII.html
Check the class forum for corrections and hints

Assignment 6, due March 16 (before class starts).

Instructions

- Do not hand in a rough draft. Copy or type answers neatly and clearly. Points may be deducted for writing that is sloppy, has excessive cross-outs, or is hard to read.
- State facts precisely in clear language or notation. Put assertions in logical order. State clearly what the hypotheses and conclusions. Put the steps of an argument in logical order, including definitions. Points may be deducted for an incorrectly stated argument even if you seen to understand it. Clear mathematical exposition is an important goal for the class.
- Learn the Greek letters used in math. Learn their mathematical names and write them clearly.

Assigned Exercises, to hand in

1. Let $\mathbb{F}_q$ be the extension of $\mathbb{F}_p$ generated by all the l^{th} roots of unity. To say this another way, let $f(t) = t^l - 1$ and let $\mathbb{K}$ be an extension of $\mathbb{F}_p$ so that f splits into a product of linear factors in $\mathbb{K}$. Let $\alpha_1, \cdots, \alpha_m$ be the roots of f in $\mathbb{K}$ and define the possibly intermediate field $\mathbb{F}_q = \mathbb{F}_p[\alpha_1, \cdots, \alpha_m] \subseteq \mathbb{K}$. Assume l is a rational prime.
   (a) Show that f has l distinct roots in $\mathbb{K}$.
   (b) Show that if $f(\alpha) = 0$ and $\alpha \notin \mathbb{F}_p$, then α is a primitive l^{th} root of unity in $\mathbb{F}_q$.
   (c) Let α be as in part (b). Show that f splits in $\mathbb{F}_p[\alpha] \subseteq \mathbb{K}$.
   (d) Show that $q = p^l$. *Hint.* Find the degree of the extension $[\mathbb{F}_p[\alpha] : \mathbb{F}_p]$.
   (e) Let g be a generator of the multiplicative group $\mathbb{F}_q^*$ with $q = p^l$. Use the little Fermat theorem and the Chinese remainder theorem to give a direct elementary proof that if $g^{p^l - 1} = 1$, there is a k so that $\alpha = g^k$ is a primitive l^{th} root of unity.
2. It is a general theorem that any two fields of order p^r are isomorphic. Consider the polynomials $f(t) = t^2 - 3$ and $g(t) = t^2 + 1$.
   (a) Show that both f and g are irreducible in $\mathbb{F}_7[t]$.
   (b) Let x and y be non-squares mod p, which is written using the Legendre symbol as $\left(\frac{x}{p}\right) = \left(\frac{y}{p}\right) = -1$. There is no z with $z^2 = x$ or $z^2 = y \bmod p$. Show that there is a z with $x = z^2 y \bmod p$.

(c) Let α be the image of t in $\mathbb{F}_7[t]/(f)$ and β the image of t in $\mathbb{F}_7[t]/(g)$. Define fields $\mathbb{K} = \mathbb{F}_7[\alpha]$ and $\mathbb{L} = \mathbb{F}_7[\beta]$. Construct an explicit isomorphism $\phi\colon \mathbb{K} \to \mathbb{L}$. Find $a + b\beta$ with $a, b \in \mathbb{F}_7$ so that $\phi(\alpha) = a + b\beta$ works. *Hint.* Part (b) suggests a way.

(d) Construct a second isomorphism $\psi \neq \phi$.

3. This exercise is a variation on the proof in *A Course in Arithmetic* linked to the `Resources and Assignments` page (above the link to this assignments) that 2 is a square mod p if and only if $p = \pm 1 \bmod 8$. The primitive 12^{th} root of unity in $\mathbb{C}$ is $\omega = e^{i\pi/6}$. This unit length complex number makes a 30° angle with the $x-$axis.

(a) Find the cartesian coordinate representation $\omega = x + iy$, and use this to calculate that $\omega + \omega^{-1} = \sqrt{3}$.

(b) Let $\mathbb{K}$ be a finite extension field of $\mathbb{F}_p$ that contains a primitive 12^{th} root of unity, β. Define $x = \beta + \beta^{-1}$ in $\mathbb{K}$. Show that $x^2 = 3$. *Hint.* The geometry of powers of ω in $\mathbb{C}$ suggest calculations that reveal properties of β in $\mathbb{K}$. A drawing shows that the six elements ω^{2k} form vertices of a regular hexagon. These add up to zero. The even numbered vertices, k even, are the three cube roots of unity. They add up to zero, so sum over the odd numbered vertices also is zero. This sum includes ω^2 and ω^{-2}.

There are algebraic proofs for these facts that apply also to sums involving β^{2k}. For example, the six distinct elements β^{2k} are the six distinct roots of the polynomial $f \in \mathbb{K}[t]$ with $f(t) = t^6 - 1$, which reveals the sum over the six elements.

(c) Show that $x \in \mathbb{F}_p$ if $p = \pm 1 \bmod 12$.

(d) Use quadratic reciprocity to verify that this is true for $p = 11$ ($p = -1 \bmod 12$) and $p = 61$ ($p = 1 \bmod 12$).

4. Use quadratic reciprocity and the multiplicative property of the Legendre symbol to determine whether 200 is a square mod 101.

5. Show that every finite degree extension of a finite field has a primitive element (Textbook Exercise 8.1). *Hint.* You may see the idea if you look for a primitive element for the smallest extension, say, $\mathbb{F}_{25}$ over $\mathbb{F}_5$.