# Assignment 7, due March 23

**Corrections:**

- Exercise 5 added March 12. It is not required but please consider doing it – you will get extra credit. Make sure to read the Serre proof that $\left(\frac{2}{p}\right) = 1$ for $p = \pm 1 \bmod 8$.
- (March 21) Exercise 1 clarified that $\mathbb{E}$ is a finite degree extension of $\mathbb{Q}$.
- (March 21) Corrections to exercise 5b: replace $\alpha$ (incorrect) with $y = \alpha + \alpha^{-1}$, Replace $\overline{\mathbb{F}}_6$ (silly) with $\overline{\mathbb{F}}_p$.

1. Suppose $\omega \in \mathbb{C}$ is a primitive $p^{th}$ root of unity ($p$ being a rational prime) and $\mathbb{Q}[\omega]/\mathbb{Q}$ is the corresponding cyclotomic extension. Let $\sigma$ be a generator of the cyclic group $\mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$. This means that $\sigma^{p-1} = \mathrm{id}$ and $\sigma^k \neq \mathrm{id}$ for $1 \leq k < p-1$. Let $\mathbb{E}/\mathbb{Q}[\omega]$ finite degree be a field extension. We seek an extension $\widetilde{\sigma}$ that is an automorphism of $\mathbb{E}$ that fixes $\mathbb{Q}$ so that $\widetilde{\sigma}(x) = \sigma(x)$ if $x \in \mathbb{Q}[\omega]$.
   (a) Show that if $\mathbb{E}/\mathbb{Q}[\omega]$ is a normal extension, then there is such a $\widetilde{\sigma}$ with the property that $\widetilde{\sigma}^{p-1} = \mathrm{id}$.
   (b) Find an example of $\mathbb{E}/\mathbb{Q}[\omega]$ and a $\widetilde{\sigma}$ with $\widetilde{\sigma}^{p-1} \neq \mathrm{id}$.
   (c) Drop the hypothesis that $\mathbb{E}/\mathbb{Q}[\omega]$ is a normal extension. Is it still true that there is an extension $\widetilde{\sigma}$? Is it still possible to choose $\widetilde{\sigma}$ with $\widetilde{\sigma}^{p-1} = \mathrm{id}$?

2. Let $\mathbb{Z}_p$ be the $p-$adic integers from Assignment 6. Write any $x \in \mathbb{Q}$, in the form $x = p^n(a/b)$ where $a$ and $b$ are relatively prime to $p$. (It is OK for this definition if $a$ and $b$ are not relatively prime to each other.) Define the $p-adic$ valuation to be
$$|x|_p = p^{-n} \ .$$
   Show that the following definitions of $\mathbb{Q}_p$ are equivalent. In the process, show that $\mathbb{Q}_p$ is a field, with $\mathbb{Q} \subset \mathbb{Q}_p$ as a dense sub-field.
   (a) $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ in the $p-$adic norm $|x-y|_p$.
   (b) $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$.
   (c) $\mathbb{Q}_p$ is the field of fractions of the ring $\mathbb{Z}_p$ (in particular, $\mathbb{Z}_p$ has no zero-divisors).

3. A function $R(x, y)\colon \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$ (or any other metric space in place of $\mathbb{Q}_p$) is *continuous* at $(x, y)$ if for every $\epsilon > 0$ there is a $\delta(x, y) > 0$ so that if $|\xi|_p \leq \delta$ and $|\eta|_p \leq \delta$, then $|R(x+\xi, y+\eta) - R(x, y)|_p \leq \epsilon$. A function is *uniformly continuous* on $A \subseteq \mathbb{Q}_p$ if it is possible to find $\delta$ independent of $x$ and $y$ if $x \in A$ and $y \in A$.

   (a) Show that addition is uniformly continuous on $\mathbb{Q}_p$.

   (b) Show that multiplication is continuous but not uniformly continuous on $\mathbb{Q}_p$.

   (c) Show that multiplication is uniformly continuous on $\mathbb{Z}_p$.

   (d) Show that multiplication is uniformly continuous on any "ball" of the form $B_r = \left\{ x \in \mathbb{Q}_p \text{ with } |x|_p \leq r \right\}$.

   (e) Show that part (d) implies part (c) by showing that $\mathbb{Z}_p = B_1$.

   (f) Show that inversion ($x \to x^{-1}$) is continuous on $\mathbb{Q}_p - \{0\}$ (meaning $\mathbb{Q}_p$ with the "zero set", $\{0\}$, removed). Show that inversion is uniformly continuous on $B_r^c$ (the complement of $B_r$).

   (g) Show that the formal derivative on polynomials agrees with the limit definition
   $$f'(x) = \lim_{|h|_p \to 0} \frac{f(x+h) - f(x)}{h} .$$
   Is the monomial $f(x) = x^p$ special in this regard?

4. Let $\alpha \in \overline{\mathbb{F}}_p$ (this is the algebraic closure of the finite field) be a primitive $6^{th}$ root of unity.

   (a) Show that $\xi = e^{i\pi/3} \in \mathbb{C}$ (this is a primitive $6^{th}$ root of 1 in $\mathbb{C}$) satisfies the identities

   - $\xi + \xi^{-1} = 1$
   - $\xi^3 = -1$
   - $\xi^4 = -\xi$
   - $\xi^5 = -\xi^2$

   (b) Define $y = \alpha + \alpha^{-1} \in \overline{\mathbb{F}}_p$ and show that $y \in \mathbb{F}_p$.

   (c) Calculate $y^2$ and show that $y^2$ satisfies a quadratic equation with roots $y = 1$ and $y = -2$. *Hint*: Some of the part (a) relations may apply to $\alpha$.

   (d) Show by direct calculation that $y = 1$ in $\mathbb{F}_7$. *Hint*: You will find that there is only one possible $\alpha$.

   (e) Is there any $\mathbb{F}_p$ where $y = -2$?

5. (*Added late, do it as you have time*) Use the notation and results of Exercise 4. Assume that $\alpha + \alpha^{-1} = 1$ if you can't prove it. Use $z = \alpha - \alpha^{-1}$ to show that $-3$ is a square mod $p$ if $p = 1 \bmod 6$ ($p = 7, 13, 19, 31, \ldots$). Use the method that was used for showing 2 is a square mod $p$ if $p = 1$ or $p = -1 \bmod 8$ (page 7 of *A Course in Arithmetic*).

(a) Use trigonometry to show that in $\mathbb{C}$, $\xi - \xi^{-1} = \xi - \overline{\xi} = i\sqrt{3}$. Explain how this suggests $z^2 = -3$.

(b) Show that $z^2 = -3$ if $y = \alpha + \alpha^{-1} = 1$.

(c) Compute $z^6$ in $\overline{\mathbb{F}}_p$ to show that $z \in \mathbb{F}_p$ if $p = 1 \bmod 6$.

(d) Show that 3 is a square mod $p$ if $p = 1 \bmod 12$ but not if $p = 7 \bmod 12$.