# Week 6, Due Mon 5/7

1. Draw a diagram of all the subfields of $\mathbf{Q}(\zeta_{13})$, indicating all inclusions and degrees.

2. (**Gauss Sums**) Let $p > 2$ be prime, and let $G = \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^\times$, where $\zeta$ is a primitive $p$th root of unity, and where $a \in G$ sends $\zeta$ to $\zeta^a$.

   (a) Say that $a \not\equiv 0 \mod p$ is a quadratic residue if it is a square; that is, $a \equiv x^2 \mod p$. Prove that $G$ has a unique subgroup $H$ of consisting of quadratic residues.

   (b) For $a \not\equiv 0 \mod p$, define the quadratic residue symbol as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue,} \\ -1 & a \text{ is not quadratic residue.} \end{cases}$$

   Prove that the map $G \to \{\pm 1\} = \mathbf{Z}/2\mathbf{Z}$ sending $a$ to $(a/p)$ is a homomorphism with kernel $H$.

   (c) Prove that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$.

   (d) Let $\chi := \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a = \sum_{a \in G} \left(\frac{a}{p}\right) \zeta^a \in \mathbf{Q}(\zeta)$. Prove that, for $g \in G$, $g\chi = \left(\frac{a}{p}\right) \chi$.

   (e) Deduce that $\chi^2$ is fixed by $G$ and hence $\chi^2 \in \mathbf{Q}$. Deduce that either $\chi = 0$, or $\chi$ generates the unique quadratic subfield $K := \mathbf{Q}(\zeta)^H \subset \mathbf{Q}(\zeta)$.

   (f) Prove that if one chooses any embedding of $\mathbf{Q}(\zeta)$ into $\mathbf{C}$, then complex conjugation acts on $\mathbf{Q}(\zeta)$ by $-1 \in G$, that is, $\zeta \mapsto \zeta^{-1}$.

   (g) Prove that if one chooses any embedding of $\mathbf{Q}(\zeta)$ into $\mathbf{C}$, then the absolute value squared $|x|^2$ of the image of $x \in \mathbf{Q}(\zeta) \subset \mathbf{C}$ is equal to $x \cdot cx$. If $p \geq 5$, show that the absolute value of $|1+\zeta|$ depends on the choice of embedding $\mathbf{Q}(\zeta) \to \mathbf{C}$. In contrast, show that the absolute value of $|\chi^2|$ does not depend on the embedding. (use (2e))

   (h) Prove that $|\chi^2| = \chi \cdot c\chi = \left(\sum_{a \in G} \left(\frac{a}{p}\right) \zeta^a\right) \left(\sum_{b \in G} \left(\frac{b}{p}\right) \zeta^{-b}\right) = \sum_{a,b \in G} \left(\frac{ab}{p}\right) \zeta^{a-b}$.

   (i) By replacing $a$ by $ab$ in the sum above, show that

$$|\chi^2| = \sum_{a,b \in G} \left(\frac{a}{p}\right) \zeta^{(a-1)b}.$$

   (j) Prove that $\sum_{b \in G} \zeta^{(a-1)b}$ equals $p-1$ if $a = 1 \in G$ and equals $-1$ for all other $a \in G$.

   (k) Deduce that $|\chi^2| = \sum_{a,b \in G} \left(\frac{ab}{p}\right) \zeta^{a-b} = p + \sum_{a \in G} \left(\frac{a}{p}\right) (-1) = p$.

   (l) Show that complex conjugation $c = -1$ lies in $H$ if and only if $p \equiv 1 \mod 4$. (use (2c))

   (m) Show that $c\chi = \chi$ if $c \in H$ and $c\chi = -\chi$ if $c \notin H$. Deduce that if $\mathbf{Q}(\zeta) \subset \mathbf{C}$, then $\chi$ is either real or purely imaginary depending on whether $c \in H$. (use (2d))

   (n) Let $p^* = p$ if $p \equiv 1 \mod 4$ and $-p$ if $p \equiv -1 \mod 4$. Prove that $\chi^2 = p^*$, and deduce that the quadratic subfield $K$ of $\mathbf{Q}(\zeta)$ is equal to $\mathbf{Q}(\sqrt{p^*})$.

   (o) Now suppose that $\mathbf{Q}(\zeta) \to \mathbf{C}$ sends $\zeta$ to the very specific choice $e^{2\pi i/p} \in \mathbf{C}$. Let $\sqrt{p^*}$ denote the complex number which is either positive if $p^* > 0$ or has positive imaginary part if $p^* < 0$. We know that $\chi^2 = p^*$ so $\chi = \pm\sqrt{p^*}$. Determine the correct sign in this formula for $p = 3$, 5, 7, and 11.

   (p) (*) Determine the sign in part (2o) for all $p$.