CYCLOTOMIC FIELDS PROBLEM SHEET 1

TOM LOVERING (LOVERING@FAS.HARVARD.EDU)

(1) A *basic Pythagorean triple* is a triple (x, y, z) of positive integers that are pairwise coprime and satisfy

$$x^2 + y^2 = z^2.$$

By putting different numbers into the general solution to this equation, write down five different basic Pythagorean triples [regard (x, y, z) and (y, x, z) as the same triple].

(2) (Fermat's Last Theorem for $n = 4$) Show that $x^4 + y^4 = z^2$ has no solutions in positive integers.[1]

(3) Give an example of a non-abelian Galois extension $K/\mathbb{Q}$. Compute its Galois group and all its subextensions. Is it possible to embed K in a cyclotomic field $\mathbb{Q}(\zeta_n)$?

(4) Find all the subfields of $\mathbb{Q}(\zeta_{11})$. For each embedding $\tau : \mathbb{Q}(\zeta_{11}) \hookrightarrow \mathbb{C}$, show that complex conjugation induces an automorphism $\sigma(\tau) : \mathbb{Q}(\zeta_{11}) \overset{\cong}{\to} \mathbb{Q}(\zeta_{11})$. Does this automorphism depend on the choice of τ?

(5) Let L/K be a finite extension of degree d, $\tau_1, ..., \tau_d : L \to \bar{K}$ the embeddings of L in $\bar{K}$ and $\alpha_1, ..., \alpha_d$ d elements of L. Prove that the discriminant can be computed as

$$\Delta(\alpha_1, ..., \alpha_d) = \det(\tau_i(\alpha_j))^2.$$

(6) Compute the rings of integers in $\mathbb{Q}(\sqrt{d})$. You should notice a difference depending on whether or not $d \equiv 1 \mod 4$. What do you conclude about the discriminants of these fields?

(7) * Let A be a finite abelian group. Does there exist an abelian extension K of $\mathbb{Q}$ with Galois group A? How small can you arrange for the discriminant to be?

[1]Hint: Use infinite descent. Assume you have a solution (x_0, y_0, z_0) and assume it is that for which $x_0 + y_0 + z_0$ is as small as possible. Then argue that one of x_0 and y_0 must be even, wlog x_0, factorise $x_0^4 = (z_0 - y_0^2)(z_0 + y_0^2)$ and proceed to look for a smaller solution and obtain a contradiction.