Math 80220 Algebraic Number Theory
Problem Set 8

Andrei Jorza

due Friday, April 6

1. Show that $\mathbb{Q}(\sqrt{3},\sqrt{5})$ is everywhere unramified over $\mathbb{Q}(\sqrt{15})$. (Remark: $\mathbb{Q}(\sqrt{3},\sqrt{5})$ is the largest extension of $\mathbb{Q}(\sqrt{15})$ which is everywhere unramified.) [Hint: Compute the different. You may use that that $\mathcal{O}_{\mathbb{Q}(\sqrt{3}.\sqrt{5})}$ has as integral basis $1, \sqrt{3}, \frac{1+\sqrt{5}}{2}, \frac{\sqrt{3}+\sqrt{15}}{2}$].]

2. Consider the extension $K = \mathbb{Q}(\sqrt{2+\sqrt{3}})/\mathbb{Q}$.
   (a) Write $\alpha = \sqrt{2+\sqrt{3}}$. Show that the roots of the minimal polynomial of α are $\pm\alpha, \pm\alpha^{-1}$ and deduce that $\alpha \in \mathcal{O}_K^\times$.
   (b) Show that $K/\mathbb{Q}$ is Galois with Galois group $G_{K/\mathbb{Q}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ having generators $\sigma(\alpha) = \alpha^{-1}$ and $\tau(\alpha) = -\alpha$.
   (c) Show that $(3)\mathcal{O}_K = (\sqrt{3})^2$ is the prime factorization in $\mathcal{O}_K$. Conclude that $I_{\sqrt{3}/3} = \{1, \sigma\tau\}$ but $P_{\sqrt{3}/3} = \{1\}$. (You may assume that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2+\sqrt{3}}]$.)
   (d) Show that $(2)\mathcal{O}_K = \mathfrak{q}^4$ where $\mathfrak{q} = (\alpha + 1)$ is the prime factorization in $\mathcal{O}_K$. Show that $I_{\mathfrak{q}/2} = P_{\mathfrak{q}/2} = G_{K/\mathbb{Q}}$, $D_{\mathfrak{q}/2,3} = D_{\mathfrak{q}/2,4} = \{1, \tau\}$ and $D_{\mathfrak{q}/2,m} = \{1\}$ for $m \geq 5$. [Hint: Check that $\alpha + 1 \mid \alpha - 1$.]

3. In this problem you will construct number fields whose rings of integers cannot be generated (as an algebra) by few elements. Let $n \geq 2$ be an integer and let $K = \mathbb{Q}(\sqrt[n]{2})$ with ring of integers $\mathcal{O}_K$.
   (a) Suppose $p \nmid 2[\mathcal{O}_K : \mathbb{Z}[\sqrt[n]{2}]]$ be a prime which splits completely in K. Show that $n \mid p-1$ and that $2^{(p-1)/n} \equiv 1 \pmod{p}$.
   (b) Show that there exists a unique subfield $F \subset \mathbb{Q}(\zeta_p)$ with $[F : \mathbb{Q}] = n$.
   (c) Let $\mathfrak{q} \mid 2$ be an ideal of $\mathbb{Z}[\zeta_p]$ and $\mathfrak{p} = \mathfrak{q} \cap F$. Show that the image of $\mathrm{Frob}_{\mathfrak{q}/2}$ in $G_{F/\mathbb{Q}}$ is $\mathrm{Frob}_{\mathfrak{p}/2}$ and deduce that $\mathrm{Frob}_{\mathfrak{p}/2} = 1$. [Hint: What is $\mathrm{Frob}_{\mathfrak{q}/2} \in G_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} \cong (\mathbb{Z}/p\mathbb{Z})^\times$?]
   (d) Deduce that 2 splits completely in F.
   (e) Assume that $\mathcal{O}_F = \mathbb{Z}[\alpha_1, \ldots, \alpha_m]$. Show that we have induced ring homomorphisms
   $$\mathbb{Z}[X_1, \ldots, X_m] \twoheadrightarrow \mathcal{O}_F \twoheadrightarrow \oplus_{\mathfrak{p}|2} k_{\mathfrak{p}/2}$$
   where the n quotients $\mathbb{Z}[X_1, \ldots, X_m] \twoheadrightarrow k_{\mathfrak{p}/2} \cong \mathbb{F}_2$ are distinct.
   (f) Show that there are at most 2^m distinct ring homomorphisms $\mathbb{Z}[X_1, \ldots, X_m] \twoheadrightarrow \mathbb{F}_2$ and deduce that $\mathcal{O}_F$ cannot be generated as an algebra over $\mathbb{Z}$ by fewer than $\lceil \log_2(n) \rceil$ elements. [Hint: where can X_i go under such a ring homomorphism?]

   For example, $p = 151$ splits completely in $\mathbb{Q}(\sqrt[5]{2})$ and so 2 splits completely in $\mathbb{Q}(\zeta_{151})$. The subfield $F \subset \mathbb{Q}(\zeta_{151})$ of order 5 over $\mathbb{Q}$ is the splitting field of the polynomial $X^5+X^4-60X^3-12X^2+784X+128$ and has ring of integers that cannot be generated by two elements. Can it be generated by 3 elements? Moreover, for any n there exist infinitely many p which split completely in $\mathbb{Q}(\sqrt[n]{2})$ and so we have an infinite family of examples. I got this example from `http://wstein.org/129-05/challenges.html`