Algebraic Number Theory 88-798
Question Sheet 4
Due Jan. 13, 2009

Please feel free to e-mail me at `mschein@math.biu.ac.il` with any questions.

(1) Let $d \in \mathbb{Z}$ be a square-free integer, and let $p \in \mathbb{Z}$ be a prime number such that $p \nmid 2d$. Show that p splits completely (מתפרק לגמרי) in $\mathbb{Q}(\sqrt{d})$ if the equation $x^2 \equiv d \mod p$ has a solution and that p is inert otherwise.

(2) Let L/K be a Galois extension with non-cyclic Galois group $\mathrm{Gal}(L/K)$. Prove that no prime ideal of $\mathcal{O}_K$ is inert in L.

(3) Let L/K be an extension of number fields, and let N/K be its normal closure. In other words, $N \supset L \supset K$ is the smallest extension such that N/K is Galois. Show by means of the following steps that a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ splits completely in L if and only if it splits completely in N.
   (a) Show that if $\mathfrak{p}$ splits completely in N, then it splits completely in L.
   (b) Let G be a group and let $U, V \subset G$ be two subgroups. If $g, h \in G$, we say that $g \sim h$ if there exist $u \in U$ and $v \in V$ such that $h = ugv$. Then $\sim$ is an equivalence relation, and the equivalence classes UgH are called double cosets. The set of double cosets is written $U\backslash G/V$. (Note that if U is trivial, then the double cosets are just the usual left cosets of V.)
   Set $G = \mathrm{Gal}(N/K)$ and $H = \mathrm{Gal}(N/L) \subset G$. Choose a prime ideal $\mathcal{P}_N$ of N dividing $\mathfrak{p}$, and let $G_{\mathcal{P}_N} \subset G$ be its decomposition subgroup (תת-חבורת פירוק). Let $A_{\mathfrak{p}}$ be the set of prime ideals of $\mathcal{O}_L$ dividing $\mathfrak{p}$. Show that the following map is a bijection:
$$\begin{aligned} H\backslash G/G_{\mathcal{P}_N} &\rightarrow A_{\mathfrak{p}} \\ \sigma(\in G) &\mapsto \sigma(\mathcal{P}_N) \cap \mathcal{O}_L \end{aligned}$$
   (c) Suppose now that $\mathfrak{p}$ splits completely in L. For any $\sigma \in G$, show that $H\sigma G_{\mathcal{P}_N} = H\sigma$. Conclude that $\sigma G_{\mathcal{P}_N} \subseteq H\sigma$ for all $\sigma \in G$.
   (d) Let $\tilde{H} = \bigcap_{\sigma \in G} \sigma^{-1} H \sigma$. Show that $G_{\mathcal{P}_N} \subset \tilde{H}$ and that $\tilde{H} \subset H$ is a normal subgroup. Conclude that either $\tilde{H} = H$ or $\tilde{H}$ is trivial, and in both cases show that $\mathfrak{p}$ splits completely in N.

(4) Let $p \in \mathbb{Z}$ be an odd prime number such that $p \equiv 2 \mod 3$. If $L = \mathbb{Q}(\sqrt[3]{2})$, prove that $p\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_2$, where $f(\mathcal{P}_1|p) = 1$ and $f(\mathcal{P}_2|p) = 2$.
   Hint: Use the previous exercises. You may also use the following facts without proof:
   (a) If m is a cube-free integer, then $\mathbb{Q}(\sqrt[3]{m})$ has discriminant $-27m^2$.
   (b) Let n be an integer, and let ζ_n be a primitive n-th root of unity ($(\zeta_n)^n = 1$ and $(\zeta_n)^m \neq 1$ for $1 \leq m < n$). An odd prime number p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \mod n$.