Problem Set 5.

1. Another application of Chebotarev density! Let $L/K$ be a Galois extension of number fields. Let $Q \subset O_L$ be a nonzero prime ideal, and let $P = Q \cap O_K$. Recall that we showed that the natural map of $G_Q$ to the Galois group of the finite fields $O_L/Q$ over its subfield $O_K/P$ is a surjection, with kernel $I_Q$. This led to the definition of the Frobenius element $\sigma_Q$ which is a particular generator of the cyclic group $G_Q/I_Q$. Further, if we write $L$ as the splitting field of a monic polynomial with coefficients in $O_K$ we see that $I_Q$ is trivial when $Q$ is not one of the finite number of primes containing the discriminant of the polynomial.

a) We say that $P$ splits completely in $L$ if there are $[L:K]$ different prime ideals in $O_L$ which contain $P$. Show that $P$ splits completely if and only if some (and hence all) decomposition group $G_Q$ is trivial.

b) Show that if $M/L/K$ are all Galois extensions, then any prime $P$ in $O_K$ which splits completely in $M$ will also split completely in $L$.

c) Show that the Chebotarev density theorem implies that the density of primes splitting completely in $L/K$ is $1/[L:K]$.

d) Show that if $L_1, L_2$ are Galois extensions of a number field $K$ such that almost all primes of $K$ which split completely in $L_1$ also split completely in $L_2$ then $L_2 \subset L_1$. Hint: Consider the Galois extension $M = L_1L_2$ and show that a Frobenius element for $M/K$ associated to a prime is trivial if and only if the corresponding Frobenius elements for $L_1/K, L_2/K$ are trivial. Then use c).

e) Show that if Galois extensions $L_1, L_2$ of $K$ are such that the set of primes splitting completely in $L_1$ agrees with the set of primes splitting completely in $L_2$ up to a finite set then $L_1 = L_2$.

2. Let $K$ be a pure cubic number field: $K = \mathbb{Q}(\alpha)$ and $\alpha^3$ is rational.

a) Show that there exist unique square free relatively prime integers $a > b \geq 1$ such that $K = \mathbb{Q}((ab^2)^{1/3})$.

b) Suppose $\alpha^3 = ab^2$. Let $\beta = \alpha^2/b$ so that $\beta^2 = \alpha a, \beta^3 = a^2b, \alpha^2 = b\beta, \alpha\beta = ab$. Show that the set $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta$ is an order in $K$. Show that $d(\mathbb{Z}[\alpha]) = -27a^2b^4$, $d(\mathbb{Z}[\beta]) = -27a^4b^2$, and $d(\mathcal{O}) = -27a^2b^2$.

c) Show that $\mathcal{O}$ is the maximal order in $K$ if $ab^2 \not\equiv \pm 1 \pmod{9}$ and is of index 3 in the maximal order if $ab^2 \equiv \pm 1 \pmod{9}$.

3. Discriminants of cubic fields do not determine the field.

a) Show that if $p > q$ are primes the pure cubic fields $\mathbb{Q}((pq)^{1/3})$ and $\mathbb{Q}((pq^2)^{1/3})$ have the same discriminant $-27p^2q^2$ when neither of $pq, pq^2$ are $\pm 1$ modulo 9.
b) Show that if the two number fields in part a) with discriminant $-27p^2q^2$ are isomorphic then they are isomorphic to $\mathbb{Q}(p^{1/3})$ and to $\mathbb{Q}(q^{1/3})$. Show that the discriminants of these latter fields have greatest common divisor dividing 27. Use this to show that under the assumptions of part a), the two fields given with the same discriminant $-27p^2q^2$ are not isomorphic.

c) Show that there are infinitely many discriminants of cubic fields for which there exist non-isomorphic cubic fields with that discriminant, so that contrary to the quadratic case the discriminant of a cubic number field does not determine the number field up to isomorphism.