Problem Set 4.

1. Let K be a pure cubic number field: $K = \mathbf{Q}(\alpha)$ has degree 3 over $\mathbf{Q}$ and α^3 is rational.
   a) Show that there exist unique square free relatively prime integers $a > b \geq 1$ such that K is isomorphic to $\mathbf{Q}((ab^2)^{1/3})$.
   b) Suppose $\alpha^3 = ab^2$. Let $\beta = \alpha^2/b$ so that $\beta^2 = \alpha a, \beta^3 = a^2 b, \alpha^2 = b\beta, \alpha\beta = ab$. Show that the set $\mathcal{O} = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta$ is an order in K. Show that $d(\mathbf{Z}[\alpha]) = -27a^2b^4, d(\mathbf{Z}[\beta]) = -27a^4b^2,$ 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 $ab^2 \equiv \pm 1 \pmod 9$.
2. Discriminants of cubic fields do not determine the field.
   a) Show that if $p > q$ are primes the pure cubic fields $\mathbf{Q}((pq)^{1/3})$ and $\mathbf{Q}((pq^2)^{1/3})$ have the same discriminant $-27p^2q^2$ when neither of pq, pq^2 are ± 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 $\mathbf{Q}(p^{1/3})$ and to $\mathbf{Q}(q^{1/3})$. 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.
3. Let p be a prime number, let ρ be a primitive p^{th} root of unity, and let K be the number field $\mathbf{Q}(\rho)$.
   a) Show that $\mathbf{Z}[\rho]$ is an order in K with discriminant $(-1)^{(p-1)(p-2)/2}p^{p-2}$.
   b) Show that the map $\phi : K \to Q$ given by $\phi(z) = Tr_{K/Q}(1-\rho)z$ is a rational vector space map with $\rho, \rho^2, \ldots, \rho^{p-1}$ spanning the kernel and $\phi(1)$ an integer prime to p. Use this together with (a) to show that if $\mathbf{Z}[\rho]$ was not the maximal order in K there would be an algebraic integer $\alpha = m/p + \sum_{i=1}^{p-2} a_i\rho^i$ with $a_i \in \mathbf{Q}$ and $1 \leq m \leq p-1$. Show by applying ϕ that this is impossible.
   c) Show using a) that any quadratic number field K is contained in the field generated by roots of unity of order $|d_K|$. Hint: Show this first for $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})$ for odd primes p and take compositums of fields.

   Remark: It is a theorem of Kronecker and Weber that any number field K which is a Galois extension of $\mathbf{Q}$ with abelian Galois group is a subfield of the field generated by the roots of unity of order $|d_K|$.