METU, Fall 2011, Math 523.

Homework 4

1. Let K be a number field of degree n and let A be an additive subgroup of $\mathcal{O}_K$ generated by the set $\{\alpha_1, \ldots, \alpha_n\}$ freely. Prove that $|\mathcal{O}_K/A|^2$ divides $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$.

2. Let $f(x) = x^5 + ax + b$ with $a, b \in \mathbf{Z}$ and assume f is irreducible over $\mathbf{Q}$. Let α be a root of f and let $K = \mathbf{Q}(\alpha)$ be the corresponding quintic extension.

   - Show that $\mathrm{disc}(\alpha) = 4^4a^5 + 5^5b^4$.
   - *Bonus question:* Write a PARI-code which gives all pairs of integers (a, b) satisfying $1 \leq a, b \leq 50$ such that $\mathrm{disc}(\alpha)$ is squarefree. (Observe that this implies $\mathcal{O}_K = \mathbf{Z}[\alpha]$ for the resulting number fields.)

3. Let m_1, m_2 be two distinct squarefree integers and suppose that $K_i = \mathbf{Q}(\sqrt{m_i})$ be the corresponding quadratic fields. If $\{1, \alpha_1\}$ and $\{1, \alpha_2\}$ are integral bases for K_1 and K_2 respectively, then is it true that $\{1, \alpha_1, \alpha_2, \alpha_1\alpha_2\}$ is an integral basis for the composite field K_1K_2? If it is not true all the time, find a sufficient condition.

4. Let m be a squarefree and cubefree integer such that $m \not\equiv \pm 1 \pmod 9$.

   - Prove that $\{1, \sqrt[3]{m}, (\sqrt[3]{m})^2\}$ is an integral basis for the pure cubic field $\mathbf{Q}(\sqrt[3]{m})$.
   - Suppose that $K = \mathbf{Q}(\sqrt[3]{5}, \sqrt{19})$. Find an integral basis for $\mathcal{O}_K$ using the previous part.

5. Let $\mathcal{O} = \mathbf{Z}[\sqrt{-3}]$ and let $\mathfrak{p} \subset \mathcal{O}$ be the ideal generated by 2 and $1 + \sqrt{-3}$.

   - Show that $\mathfrak{p}$ is the unique prime ideal containing (2).
   - Prove that $\mathfrak{p} \neq (2)$ but $\mathfrak{p}^2 = (2)\mathfrak{p}$.
   - Is it possible to factor ideals in $\mathcal{O}$ uniquely into prime ideals?
   - Can we find a quadratic extension $K = \mathbf{Q}(\sqrt{m})$ such that $\mathcal{O}_K = \mathcal{O}$?