Exercises in Algebraic Number Theory

Winter term 2009/2010

Universität Duisburg-Essen
Institut für Experimentelle Mathematik
Prof. Dr. Gabor Wiese, Dr. Tommaso Centeleghe

Sheet 5

To be handed in by: Friday, 20 November 2009, 2 pm.

1. (4 points) Let K be a number field and L/K and M/K finite extensions. Prove that the ring of integers of the compositum LM need not be equal to the composite of the rings of integers of L and M.
2. (4 points) Let $d \neq 0, 1$ be a squarefree integer. Show that the index of $\mathbb{Z}[\sqrt{d}]$ in the ring of integers of $\mathbb{Q}(\sqrt{d})$ is 1 or 2.
3. (4 points) Let $f \in \mathbb{Z}[X]$ and $g_1, \dots, g_r \in \mathbb{Z}[X]$ be monic distinct irreducible polynomials such that $\overline{f} = \overline{g}_1 \cdot \ldots \cdot \overline{g}_r \in \mathbb{F}_p[X]$, where the notation $\overline{f}$ means the reduction of the (coefficients of the) polynomial modulo p.

   Consider the ring $R = \mathbb{Z}[X]/(f(X)) = \mathbb{Z}[\alpha]$ for some $\alpha \in \overline{\mathbb{Q}}$ and let $\mathfrak{p}_i = (p, g_i(\alpha)) \lhd R$ for $i = 1, \dots, r$ be the prime ideal already considered in the lecture.

   Prove that $pR = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r$.
4. (4 points)

   (a) Let $f \in \mathbb{Z}[X]$ be any nonconstant polynomial. Prove that f has a zero mod p for infinitely many primes p.

   Hint: If $f(0) = 1$, then consider $f(n!)$. Next consider $g(x) = f(xf(0))/f(0)$.

   (b) Let K be any number field. Prove that there are infinitely many primes $\mathfrak{P}$ of K of residue degree 1, i.e. $f(\mathfrak{p}/(p)) = 1$, where $(p) = \mathfrak{P} \cap \mathbb{Z}$.