Exercises in Algebraic Number Theory

Winter term 2009/2010

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

Sheet 1

To be handed in by: Wednesday, 21 October 2009 (before the lecture).

---

1. (a) (2 points) Show that there exist infinitely many prime numbers $p \equiv -1 \mod 3$.

   (b) (2 points) Let $a, n \in \mathbb{N}$ with $n \geq 2$ such that $a^n - 1$ is a prime number. Show that $a = 2$ and n is a prime number. Such primes are called *Mersenne primes*.

2. Let ζ be a root of the polynomial $X^2 + X + 1 \in \mathbb{Z}[X]$ and consider the ring $A := \mathbb{Z}[\zeta]$. Complex conjugation σ is the only nontrivial Galois autormorphism of $\mathbb{Q}(\zeta)/\mathbb{Q}$ and induces a ring automorphism of A. One disposes of the norm

$$N : A \to \mathbb{Z}, \quad a \mapsto a \cdot \sigma(a),$$

   which is (obviously) a multiplicative function. Prove the following assertions (1 point each).

   (a) The ring A is Euclidean with respect to the norm N and is, hence, by a well-known theorem factorial, i.e. a unique factorisation domain.

   (b) The unit group $A^\times$ is equal to $\{\pm 1, \pm\zeta, \pm\zeta^2\}$ and is cyclic of order 6.

   (c) The element $\lambda = 1 - \zeta$ is a prime element in A and $3 = -\zeta^2\lambda^2$.

   (d) The quotient $A/(\lambda)$ is equal to $\mathbb{F}_3$.

3. Let B be a commutative integral domain and $A \subseteq B$ a subring. An element $b \in B$ is called *integral over* A if there exists a monic polynomial $f \in A[X]$ such that $f(b) = 0$.

   Suppose that $b, c \in B$ are integral over A with polynomials $f, g \in A[X]$ such that $f(b) = g(c) = 0$.

   (a) (2 points) Use the resultant to exhibit a monic polynomial $F \in A[X]$ such that $F(b + c) = 0$.
   Hint: Recall that the resultant of two polynomials can be expressed in terms of the differences of the roots of the polynomials. Introduce an extra polynomial variable Y and consider the polynomials $f(X)$ and $g(Y - X)$.

   (b) (2 points) Use the resultant to exhibit a monic polynomial $F \in A[X]$ such that $F(bc) = 0$.
   Hint: Adapt the construction from (a).

4. (4 points) Let $d \neq 0, 1$ be a squarefree integer and consider the field $\mathbb{Q}(\sqrt{d})$.

   (a) Compute the minimal polynomial of $a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$.

   (b) Assume $d \equiv 2, 3 \mod 4$ and let $a + b\sqrt{d}$ be an integral element over $\mathbb{Z}$ (see previous exercise for the definition). Show that a and b are integers.

   (c) Assume $d \equiv 1 \mod 4$ and let $a + b\sqrt{d}$ be an integral element over $\mathbb{Z}$. Show that the maximum denominator of a and b (represented in lowest terms) is 2.