Exercises in Commutative Algebra

Winter Term 2011/2012

Université du Luxembourg
Prof. Dr. Gabor Wiese

Sheet 5
17/10/2011

1. Let $d \neq 0, 1$ be a squarefree integer (meaning that no prime factor divides d twice). Show that the ring of integers of $\mathbb{Q}(\sqrt{d})$ is equal to:
$$\begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \mod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{if } d \equiv 1 \mod 4. \end{cases}$$

2. Show that the ring of integers of $\mathbb{Q}(\sqrt{-13})$ is not a factorial ring.

   Hint: Factor $14 = 2 \cdot 7$ in one more way: $14 = \alpha \cdot \beta$. Do not forget to show that α, β are not associated with 2 or 7.

3. In this exercise all primitive Pythagorean triples are determined by computating in the factorial ring $\mathbb{Z}[i]$ (recall: it is Euclidean!).

   A triple (a, b, c) of positive integers is called a *Pythagorean Triple* if $a^2 + b^2 = c^2$. It is called *primitive* if the greatest common divisor of a, b, c equals 1 and if a is odd (and thus b even).

   (a) Show how to associate with any Pythagorean Triple a primitive one.

   (b) Let (a, b, c) be a primitive Pythagorean Triple. Show that $a + ib$ and $a - ib$ are coprime in $\mathbb{Z}[i]$.

   (c) Conclude from (b) that $a + ib$ and $a - ib$ are squares in $\mathbb{Z}[i]$ if (a, b, c) is a primitive Pythagorean Triple.

   (d) Conclude from (c) that there are $u, v \in \mathbb{N}$ such that
   $$a = u^2 - v^2 \quad \text{and} \quad b = 2uv.$$

   (e) Finally, check quickly that – conversely – equations as in (d) always give a Pythagorean Triple.

4. Let R be a factorial ring with field of fractions K.

   (a) Let $f \in K[X]$ be a non-constant polynomial. We know from Sheet 4, Exercise 4(b), that there is $c \in K^\times$ such that $\tilde{f} := \frac{1}{c} f$ is a primitive polynomial in $R[X]$. Derive the following statement from Sheet 4, Exercise 4:
   $$f \text{ is irreducible in } K[X] \quad \Leftrightarrow \quad \tilde{f} \text{ is irreducible in } R[X].$$

   [Remark: In Exercise 4(h) of Sheet 4 the assumption should have been that $f \in R[X] \setminus R$ is <u>primitive</u>. The ‘primitive’ was missing. Sorry.]

   (b) (*Reduction of polynomials modulo primes.*) Let p be a prime element of R. Consider the natural surjective ring homomorphism $R \to R/(p)$ given by sending $r \in R$ to its residue class $\overline{r} := r + (p)$. Convince yourself that the map
   $$R[X] \to R/(p)[X], \quad f = \sum_{i=0}^{d} a_i X^i \mapsto \sum_{i=0}^{d} \overline{a_i} X^i =: \overline{f}$$
   is a surjective ring homomorphism. If you find this obvious, skip it!

(c) (*Reduction criterion for irreducible polynomials.*) Let p be a prime element of R. Let $f \in R[X]$ be a primitive polynomial such that p does not divide the highest coefficient of f (i.e. $f = \sum_{i=0}^{d} a_i X^i$ and $p \nmid a_d$).

Show: If $\overline{f}$ is irreducible in $R/(p)[X]$, then f is irreducible as an element of $R[X]$ and f is irreducible as an element of $K[X]$.

(d) (*Eisenstein criterion.*) Let p be a prime element of R. Let $f = \sum_{i=0}^{d} a_i X^i \in R[X]$ be a non-constant primitive polynomial. Assume

$$p \nmid a_d, \quad p \mid a_i \text{ for } i = 0, \dots, d-1 \text{ and } p^2 \nmid a_0.$$

Then f is irreducible as an element of $R[X]$ and as an element of $K[X]$.

(e) Show that the following polynomials are irreducible in the indicated polynomial ring:

(1) $5X^3 + 63X^2 + 168 \in \mathbb{Q}[X]$,

(2) $X^6 + X^3 + 1 \in \mathbb{Q}[X]$,

(3) $X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$,

(4) $X^4 - 3X^3 + 3X^2 - X + 1 \in \mathbb{Q}[X]$,

(5) $X^9 + XY^7 + Y \in \mathbb{Q}[X, Y]$,

(6) $X^2 - Y^3 \in \mathbb{C}[X, Y]$.

Hint: The two criteria (reduction and Eisenstein) help you, but, they alone do not suffice.