May 15th, 2013

Zahlentheorie II

Exercise sheet 5[1]

Exercise 1 (8 Points)**.** Let $m \in \mathbb{Z}$ be a square-free integer $\neq 0, 1$, i.e. $m = \pm \prod_{i=1}^{n} p_i$, where the p_i's are distinct prime numbers and $n \geq 1$. Show that the integral closure A of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{m})$ equals

$$A = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2 \text{ or } 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & \text{if } m \equiv 1 \bmod 4. \end{cases}$$

(Here $\mathbb{Z}[a]$ denotes the smallest subring of $\mathbb{C}$ which is generated by $\mathbb{Z}$ and a.) Proceed as follows: Take $\alpha = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ with $x, y \in \mathbb{Q}$. We set $\alpha' = x - y\sqrt{m}$.

(i) (2 Points) Show that $\alpha \in A \iff \alpha + \alpha' \in \mathbb{Z}$ and $\alpha\alpha' \in \mathbb{Z}$.
(ii) (2 Points) Show that $2x \in \mathbb{Z}$ and $x^2 - my^2 \in \mathbb{Z}$ implies $2y \in \mathbb{Z}$.
(iii) (1 Point) Deduce that $\alpha \in A \iff 2x, 2y, x^2 - my^2 \in \mathbb{Z}$.
(iv) (2 Points) Show for $a, b \in \mathbb{Z}$ we have

$$a^2 - mb^2 \equiv 0 \bmod 4 \iff \begin{cases} a \equiv b \equiv 0 \bmod 2 & \text{if } m \equiv 2 \text{ or } 3 \bmod 4 \\ a \equiv b \bmod 2 & \text{if } m \equiv 1 \bmod 4. \end{cases}$$

(v) (1 Point) Deduce the description of A above. (*Hint:* In (iii) set $a := 2x$ and $b := 2y$.)

Remark 1. It follows that any Dedekind domain A which is finite over $\mathbb{Z}$ such that its field of fraction has degree 2 over $\mathbb{Q}$ has the above shape.

Exercise 2 (4 Points)**.** Let A be a Dedekind domain and $f \in A[X]$ a monic polynomial and suppose that $B := A[X]/(f)$ is again a Dedekind domain. Denote by x the image of X in B (in particular $B = A[x]$). Let $\mathfrak{p}$ be a maximal ideal in A and denote by $\bar{f} \in A/\mathfrak{p}[X]$ the reduction modulo $\mathfrak{p}$ of f. Let

$$\bar{f}(X) = \bar{f}_1(X)^{e_1} \cdots \bar{f}_r(X)^{e_r} \text{ in } A/\mathfrak{p}[X], \text{ with } e_i \geq 1,$$

be the factorization of $\bar{f}$ into distinct irreducible monic polynomials $\bar{f}_i \in A/\mathfrak{p}[X]$.

Give a proof of the following result which is already known from the lecture: The distinct prime ideals in B lying over $\mathfrak{p}$ are exactly given by

$$\mathfrak{q}_i := \mathfrak{p}B + f_i(x)B, \quad i = 1, \ldots r,$$

[1]Questions or comments to kay.ruelling@fu-berlin.de or come to A3, Room 108.

where $f_i \in A[X]$ is some lift of $\bar{f}_i$. Further, the inertia degree of $\mathfrak{q}_i$ over $\mathfrak{p}$ is given by the degree of $\bar{f}_i$ and the ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$ is given by e_i, i.e.

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} \quad \text{and} \quad [B/\mathfrak{q}_i : A/\mathfrak{p}] = \deg(\bar{f}_i).$$

Exercise 3. (8 Points) Let m and A be as in Excercise 1. Let p be a prime number. Denote by r the number of prime ideals in A over p, by $e_1, \ldots, e_r$ their ramification indices and by $f_1, \ldots, f_r$ their inertia degrees. Show:

(i) $r = 1$, $e_1 = 1$, $f_1 = 2 \iff (p \not| 2m$ and m is not a square mod $p)$ or $(p = 2$ and $m \equiv 5 \bmod 8)$.

(ii) $r = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1 \iff (p \not| 2m$ and m is a square mod $p)$ or $(p = 2$ and $m \equiv 1 \bmod 8)$.

(iii) $r = 1$, $e_1 = 2$, $f_1 = 1 \iff p|m$ or $(p = 2$ and $m \equiv 3 \bmod 4)$.

(*Hint:* Notice that on the right hand side all primes are occurring, thus it suffices to show these $\Longleftarrow$ directions. Use Exercise 2 for this.)

Further for p a prime number and $\mathfrak{q} \subset A$ a prime above p give a local parameter of $A_{\mathfrak{q}}$ in all cases.

Exercise 4 (5 Points)**.** Let $p \neq 2$ be a prime number. We want to show the following theorem:

$$\exists\, a, b \in \mathbb{Z} \text{ with } p = a^2 + b^2 \Longleftrightarrow p \equiv 1 \bmod 4.$$

To show this proceed as follows:

(i) (2 Points) Show that $\mathbb{Z}[i]$ is an euclidean domain with respect to the function $\mathbb{Z}[i] \to \mathbb{N}_0$, $\alpha \mapsto |\alpha|^2 = \alpha\bar{\alpha}$, where $\bar{\alpha}$ denotes the complex conjugate of α, i.e. you have to show that for all $\alpha, \beta \in \mathbb{Z}[i]$, there exist $\gamma, \rho \in \mathbb{Z}[i]$ with

$$\alpha = \gamma\beta + \rho \text{ and } |\rho|^2 < |\beta|^2.$$

(*Hint:* Reduce to find a γ with $|\frac{\alpha}{\beta} - \gamma| < 1$.)

(ii) (1 Point) Show that -1 is a square modulo p iff $p \equiv 1 \bmod 4$. (*Hint:* $\mathbb{F}_p^\times$ is a cyclic group of order $p - 1$.)

(iii) (1 Point) Now assume that $p \equiv 1 \bmod 4$. Show that there exists a $\alpha \in \mathbb{Z}[i]$ such that $p = \alpha\bar{\alpha}$ and conclude this $\Longleftarrow$ direction. (*Hint:* By (i) $\mathbb{Z}[i]$ is a PID, use Exercise 3 to conclude that $p = \alpha\beta$ for prime elements $\alpha, \beta \in \mathbb{Z}[i]$ and show that $\beta = \bar{\alpha}$.)

(iv) (1 Point) Show if $p = a^2 + b^2$, then p is not a prime in $\mathbb{Z}[i]$ and conclude that $p \equiv 1 \bmod 4$. (*Hint:* Use Exercise 3 for the second part.)