ÉNS Lyon
2017-2018

Number Theory
M1

Exercise sheet 3
Decomposition into product of prime ideals

Exercise 1. [The quadratic case]

Let $d \neq 0, 1$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$. As the case $d \neq 1 \mod 4$ has been done in class, we assume here that $d = 1 \mod 4$.

(a) Give an element $\alpha \in K$ such that $\mathbb{Z}[\alpha] = \mathcal{O}_K$. What is its minimal polynomial P over $\mathbb{Q}$?

(b) For every prime number p, determine the factorisation of P modulo p. Deduce the factorisation of $p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$.

(c) What are the prime numbers who ramify in $\mathcal{O}_K$? Split in $\mathcal{O}_K$? Are inert in $\mathcal{O}_K$?

Exercise 2. [Sum and product of ideals]

Let A be a Dedekind ring and I, J two (nonzero) ideals of A.

(a) Prove that for every nonzero prime ideal $\mathfrak{p}$ of A, the power of $\mathfrak{p}$ appearing in the decomposition of I is exactly the maximal integer n such that $I \subset \mathfrak{p}^n$.

(b) Give the decompositions of $IJ, I \cap J$ and $I + J$ in terms of the decompositions of I and J.

(c) Deduce that $IJ = (I + J)I \cap J$.

Exercise 3. [Resultant and discriminant]

Let A be a commutative ring and

$$P = \sum_{k=0}^{m} a_k X^k, \quad Q = \sum_{\ell=0}^{n} b_\ell X^\ell \in A[X]$$

of respective degrees m and n. The resultant of P, Q, denoted by $\mathrm{Res}(P, Q)$, is the determinant of the $(m + n)$-matrix

$$\begin{pmatrix}
a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & 0 \\
a_{m-1} & a_m & \ddots & \vdots & \vdots & b_n & \ddots & \vdots \\
\vdots & a_{m-1} & \ddots & 0 & \vdots & & \ddots & 0 \\
\vdots & \vdots & \ddots & a_m & b_1 & & & b_n \\
a_0 & & & a_{m-1} & b_0 & \ddots & \vdots & \vdots \\
0 & \ddots & & \vdots & 0 & \ddots & b_1 & \vdots \\
\vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 & b_1 \\
0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0
\end{pmatrix}$$

Prove that this is the determinant of $(S,T) \mapsto PS+QT$ from $A_{n-1}[X] \times A_{m-1}[X]$ to $A_{m+n-1}[X]$ for well-chosen bases of these spaces.

(a) Prove that if $\varphi : A \to B$ is a ring morphism,

$$\mathrm{Res}(\varphi(P), \varphi(Q)) = \varphi(\mathrm{Res}(P,Q))$$

for the induced morphism $\varphi : A[X] \to B[X]$ (acting term by term), if $\deg \varphi(P) = m$ and $\deg \varphi(Q) = n$. What happens if $\deg \varphi(P) = m$ but $\deg \varphi(Q) < n$?

(b) We assume here that A is an integral domain and fix $K = \mathrm{Frac}\, A$. Prove that $\mathrm{Res}(P;Q)$ is the determinant of the multiplication by $\overline{Q}$ in the K-vector space $K[X]/(P)$. Deduce that for every nonconstant $P, Q, R \in A[X]$,

$$\mathrm{Res}(P, QR) = \mathrm{Res}(P,Q)\,\mathrm{Res}(P,R),$$

and that if

$$P = a\prod_{i=1}^{m}(X-\alpha_i), \quad Q = b\prod_{j=1}^{n}(X-\beta_j),$$

then

$$\mathrm{Res}(P,Q) = a^n b^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j).$$

When is it zero ?

(c) For a number field $K = \mathbb{Q}(\alpha)$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, if $P \in \mathbb{Z}[X]$ is the minimal polynomial of α over $\mathbb{Q}$, prove that

$$\mathrm{disc}\, K = \pm \mathrm{Res}(P, P').$$

(d) Deduce that a prime number p is ramified in $\mathcal{O}_K$ if and only if p divides $\mathrm{disc}\, K$ (it is actually true even if $\mathcal{O}_K$ is not monogenous).

Exercise 4. [Valuations on Dedekind rings]

Let A be a Dedeking ring and $K = \mathrm{Frac}\, A$.

For every nonzero prime $\mathfrak{p}$ ideal of A and every nonzero $a \in A$, define $v_{\mathfrak{p}}(a)$ as the power of $\mathfrak{p}$ appearing in the decomposition of aA.

(a) Prove that for every nonzero $a, b \in A$ with $a+b \neq 0$, $v_{\mathfrak{p}}(a+b) \geq \min(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b))$ and $v_{\mathfrak{p}}(ab) = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b)$.

(b) Deduce that $v_{\mathfrak{p}}$ extends to a group morphism from K^* to $\mathbb{Z}$. One also define by convention $v_{\mathfrak{p}}(0) = +\infty$.

(c) For the prime number p below $\mathfrak{p}$ (i.e. $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$), what is $v_{\mathfrak{p}}(p)$?

(d) Prove the approximation lemma: for every distincts nonzero prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ of A, every $x_1, \cdots, x_r \in A$ and every $n_1, \ldots, n_r \in \mathbb{N}$ there exists $x \in A$ such that $v_{\mathfrak{p}_i}(x - x_i) \geq n_i$ for all $i \in \{1, \cdots, r\}$.

(e) Prove that for every $x \in K$, x belongs to A if and only if $v_{\mathfrak{p}}(x) \geq 0$ for every nonzero prime ideal $\mathfrak{p}$ of A.

Exercise 5. [Dedekind rings and factorization]

Let A be an integral domain.

(a) Assume that every nonzero ideal of A has a unique decomposition into a product of maximal ideals of A. Prove that every nonzero prime ideal of A is maximal, and that A is noetherian.

(b) Using the previous exercise on valuations (which only needs the decomposition exhibited as before), prove that A is integrally closed by arguing on the $\mathfrak{p}$-adic valuations of an element of $\operatorname{Frac} A$ integral over A. We have thus proved that A is a Dedekind domain.

(c) Assume here that A is both a Dedekind domain and a unique factorization domain. Prove that every nonzero prime ideal $\mathfrak{p}$ of A contains some irreducible element $x_{\mathfrak{p}}$ of A, and prove that necessarily $(x_{\mathfrak{p}}) = \mathfrak{p}$. Deduce that A is a principal ideal domain.