Solutions to Problem Set 10

1) The ring $R_{\mathfrak{p}}$ is Noetherian (because R is Noetherian), an integral domain (because f is irreducible), local (because $\mathfrak{p}$ is prime), and has dimension 1 (because $\mathbb{C}[x,y]$ has dimension 2 and any prime ideal in $R_{\mathfrak{p}}$ would correspond to a prime ideal of $\mathbb{C}[x,y]$ containing $\mathfrak{p}$). Therefore, Proposition 9.2 gives a number of criteria that would show that $R_{\mathfrak{p}}$ is a DVR. The easiest to work with is the fact that:

$$R_{\mathfrak{p}} \text{ is a DVR} \quad \Leftrightarrow \quad \dim_{\mathbb{C}} \mathfrak{m}/\mathfrak{m}^2 = 1 \tag{1}$$

where $\mathfrak{m} \subset R_{\mathfrak{p}}$ is the maximal ideal (corresponding to the image of (x,y) modulo f inside the localization $R_{\mathfrak{p}}$). Indeed, the quotient $\mathfrak{m}/\mathfrak{m}^2$ is generated as a vector space by the images of x and y. These are linearly dependent over $\mathbb{C}$ (which is equivalent to the condition in the right hand side of (1)) if and only if there exists some linear combination $\alpha x + \beta y \in (f) + (x,y)^2$. This is true if and only if the linear part of the polynomial f is non-zero.

2) Let K be the fraction field of R, and $v : K \to \Gamma$ denote the valuation such that $R = \{x \in K \text{ such that } v(x) \geq 0\}$. The maximal ideal $\mathfrak{m}$ consists of those elements x such that $v(x) > 0$ and the group of units consists of those elements x such that $v(x) = 0$. Consider the subset:

$$\Gamma_0 = \{\gamma \in \Gamma \text{ such that } -v(x) < \gamma < v(x) \ \forall x \in \mathfrak{p}\}$$

Because $\mathfrak{p}$ is prime, one sees that $\gamma, \gamma' \in \Gamma_0 \Rightarrow \gamma + \gamma' \in \Gamma_0$ (to be precise, one would need to assume v is surjective, and therefore replace Γ by the image of v in the definition of the valuation). Therefore, Γ_0 is a subgroup of Γ and the quotient group Γ/Γ_0 inherits a total ordering. This allows us to define the valuation:

$$v' : K \xrightarrow{v} \Gamma \twoheadrightarrow \Gamma/\Gamma_0$$

and let R' be the valuation ring of v'. By definition, $R' \supset R$ and the maximal ideal of R' is $\mathfrak{p}$. Moreover, the homomorphism v descends to a valuation:

$$v_0 : (R'/\mathfrak{p})^* \to \Gamma_0$$

whose ring of integers is precisely $R/\mathfrak{p}$ (it may seem counter-intuitive that v_0 is well-defined on the quotient, but all you need to do is observe that if $a \in R' \backslash \mathfrak{p}$ and $b \in \mathfrak{p}$ then $v(a+b) = \min(v(a), v(b)) = v(a)$).

3) For any non-zero element $a \in R$, define its valuation $v(a) = n \geq 0$ as the natural number such that $a = \mathfrak{m}^n \backslash \mathfrak{m}^{n+1}$, where $\mathfrak{m} = (x) \subset R$ is the maximal ideal. The reason this is well-defined is the fact that $\cap_{n=0}^{\infty} \mathfrak{m}^n = \{0\}$, because this intersection definitely holds in the bigger ring $\mathbb{C}[[x]]$ (see Exercise 9.4).

Let's check the fact that v defines a correct valuation. Since R is local, any element $a \in R \backslash \mathfrak{m}$ is a unit, and therefore any element $a \in \mathfrak{m}^n \backslash \mathfrak{m}^{n+1}$ can be written uniquely as $a = x^n u$ where u is a unit. Therefore, the fact that $a = x^n u$ and $a' = x^{n'} u'$ implies that $aa' = x^{n+n'} uu'$, and therefore $v(aa') = v(a) + v(a')$. One similarly proves the inequality $v(a + a') \geq \min(v(a), v(a'))$.

4) The ring of integers is $R = \mathbb{Z}[\sqrt{-5}]$. Note that in this ring, the principal ideal (2) is not prime, because there exist situations such as:

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

However, because R is a Dedekind domain, the principal ideal (2) factors as a product of prime ideals. An example of such a factorization is:

$$(2) = \mathfrak{m}^2 \qquad \text{where} \qquad \mathfrak{m} = (2, 1 + \sqrt{-5})$$

is actually maximal. The above equality implies that $2[\mathfrak{m}] = 0$ in the ideal class group, and indeed we will show that the ideal class group is $\mathbb{Z}/2\mathbb{Z}$. To do so, it is enough to show that any non-principal maximal ideal $\mathfrak{m}' \subset R$ is equivalent to $\mathfrak{m}$ in the ideal class group.

Claim 1: $\mathfrak{m}'$ contains some prime number $p \in \mathbb{Z}$, namely the characteristic of the residue field $\mathbb{Z}[\sqrt{-5}]/\mathfrak{m}'$. Assume p odd, otherwise $\mathfrak{m}' = \mathfrak{m}$.

Claim 2: since $\mathfrak{m}'$ is not principal, it contains some element $a + b\sqrt{-5}$ with $0 \leq b < p$. By multiplying this number with some integer and reducing modulo p, we may assume $b = 1$.

Claim 3: we have

$$\mathfrak{m}' = \{0, a + \sqrt{-5}, 2a + 2\sqrt{-5}, ..., (p-1)a + (p-1)\sqrt{-5}\} + (p) \qquad (2)$$

since if there existed any element $l + k\sqrt{-5} \in \mathfrak{m}'$ with $l \neq ak$ modulo p, then we would have $1 \in \mathfrak{m}'$. We conclude that:

$$\mathfrak{m}' = (p, a + \sqrt{-5})$$

Claim 4: in particular we have $\sqrt{-5}(a + \sqrt{-5}) \in \mathfrak{m}'$, so this element is of the form in (2). Concretely, this means that there exists $k \in \mathbb{N}$ such that:

$$-5 + a\sqrt{-5} = ka + k\sqrt{-5} \text{ mod } p \qquad \Longrightarrow -5 = ka \text{ and } a = k \text{ mod } p$$

i.e. $p | a^2 + 5$. Use these formulas to produce some $\lambda \in \mathbb{Q}(\sqrt{-5})$ such that:

$$(2, 1 + \sqrt{-5}) \cdot \lambda = (p, a + \sqrt{-5})$$