Dr. Marques Sophie
Office 519

Number theory

Spring Semester 2014
marques@cims.nyu.edu

Problem Set #12

Exercise 1 p 84

Show that $\mathbb{C}[X,Y]/(XY-X)$, $\mathbb{C}[X,Y]/(XY-1).$, $\mathbb{C}[X,Y]/(X^2-Y^3)$, $\mathbb{C}[X,Y]/(Y^2-X^2-X^3)$ are one-dimensional noetherian rings. Which ones are integral domains? Describe their normalizations.

Hint: For instance, in the last example, put $t = X/Y$ and show that the homomorphism $\mathbb{C}[X,Y] \to \mathbb{C}[t]$, $X \mapsto t^2-1$, $Y \mapsto t(t^2-1)$, has kernel $(Y^2-X^2-X^3)$ has kernel $(Y^2-X^2-X^3)$.

Solution: *The quotient ring $\frac{\mathbb{C}[X,Y]}{I}$ is Noetherian as quotient of the Noetherian domain $\mathbb{C}[X,Y]$, for any ideal I. When I is a prime ideal, $\frac{\mathbb{C}[X,Y]}{I}$ is of dimension 1.*

1. *$\frac{\mathbb{C}[X,Y]}{(XY-X)}$ is not a domain. Indeed, $X(Y-1) \subseteq (XY-Y)$ but $X \not\subset (XY-X)$ and $(Y-1) \not\subset (XY-X)$. Thus $(XY-Y)$ is not a prime ideal, and so the quotient ring is not a domain. Thus we cannot consider the normalization. The quotient ring $\frac{\mathbb{C}[X,Y]}{(XY-X)}$ is Noetherian as quotient of the Noetherian domain $\mathbb{C}[X,Y]$. Finally, $\frac{\mathbb{C}[X,Y]}{(XY-X)}$ has Krull dimension 1. Since we get that the maximal ideal are of the $(x-a, y-b)$ $a \neq 0$ and $b \neq 1$, and $(x-a) \subseteq (x-a, y-b)$.*

2. *We will construct a bijective ring homomorphism from this quotient ring to $\mathbb{C}[u, \frac{1}{u}]$. Since $\mathbb{C}[u, u^{-1}] = \mathbb{C}[u]$ localized at the prime ideal (u), this is a DVR (since $\mathbb{C}[u]$ is a PID). We construct our map:*

$$\phi : \mathbb{C}[X,Y] \to \mathbb{C}[u, \frac{1}{u}]$$

$$\phi(X) = u; \phi(Y) = \frac{1}{u}$$

This homomorphism is surjective, so if we quotient the base space by the kernel of this map, we will get an isomorphism. The kernel of this map is precisely the ideal $XY-1$. Thus:

$$\frac{\mathbb{C}[X,Y]}{XY-1} \cong \mathbb{C}[u, \frac{1}{u}]$$

This is a DVR, so we are done.

3. *We prove that we have an isomorphism*

$$\mathbb{Q}[X,Y]/(X^2-Y^3) \simeq \mathbb{Q}[t^2, t^3]$$

and conclude, since $\mathbb{Q}[T^2, T^3]$ being a integral domain implies $(X^2 - Y^3)$ will be a prime ideal.
For this, consider the morphism:

$$\begin{array}{rcll} \phi: & \mathbb{Q}[X,Y] & \to & \mathbb{Q}[T^2,T^3] \\ & X & \mapsto & T^3 \\ & Y & \mapsto & T^2 \end{array}$$

It is clearly a surjective morphism and $(X^2 - Y^3) \subseteq ker(\phi)$.
Take an element $f(X,Y) \in Ker(\phi)$, i.e. as a polynomial in variable X and coefficients coming from $k[Y]$. If you divide $f(X,Y)$ by $(X^2 - Y^3)$, we will get

$$f(X,Y) = g(X,Y)(X^3 - Y^2) + r(X,Y)$$

where $r(X,Y) \in k[Y][X]$ and degree of $r(X,Y)$ is less than two. But then $f(T^3,T^2) = 0$ implies $r(T^3,T^2) = 0$. But if $r(X,Y)$ is not zero, $r(T^3,T^2)$ cannot be zero because $r(X,Y)$ is a polynomial of degree less two in variable X with coefficients in $K[Y]$. So that $r(T^3,T^2) = 0$ and $f(X,Y) \in ker(\phi)$.
As a consequence it is an integral domain but not integrally closed $t = \bar{x}y$ is in the fraction field and integral (satisfies $z^2 - t^2 = 0$ in $\mathbb{C}[t^2,t^3]$) but not in $\mathbb{C}[t]$. So the normalization in $\mathbb{C}[t]$ obtained by adjoining $t = \bar{x}/\bar{y}$ (being a UFD we know it is integrally closed.)

4. *We define our map:*

$$\phi : \mathbb{C}[X,Y] \to \mathbb{C}[u^2 - 1, u(u^2 - 1)]$$

$$\phi(X) = u^2 - 1; \phi(Y) = u(u^2 - 1)$$

This homomorphism is surjective and the kernel is precisely generated by the ideal $(Y^2 - X^2 - X^3)$. Now, $t = \bar{x}/\bar{y}$ is integral over $\mathbb{C}[t^2-1, t(t^2-1)]$, $z^2 - (t^2-1) - 1 = 0$ in $\mathbb{C}[t^2-1, t(t^2-1)][z]$) but not it in not in $\mathbb{C}[t^2-1, t(t^2-1)]$. The normalization is obtained adkoining t since we obtain a UFD $\mathbb{C}[t]$.

Exercise 2 p 84
Let a and b be positive integers that are not perfect squares. Show that the fundamental unit of the order $A = \mathbb{Z} + \mathbb{Z}\sqrt{a}$ of the field $\mathbb{Q}(\sqrt{a})$ is also the fundamental unit of the order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{a} + \mathbb{Z}\sqrt{-b} + \mathbb{Z}\sqrt{a}\sqrt{-b}$ in the field $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$.
Solution:
By Theorem 12.12 we know that $\mathcal{O}_K^*/\mathcal{O}$ is finite, and $rank(\mathcal{O}^*) = rank(\mathcal{O}_K^*) = r + s - 1 = 4/2 - 1 = 1$ since K has 4 complex embeddings. Clearly $A^* \subseteq \mathcal{O}^*$ and $1 = rank(A^*) = rank(\mathcal{O}^*)$. Using the notation of p39, we denote $\Gamma_1 = \lambda(A^*)$ and $\Gamma_2 = \lambda(\mathcal{O}^*)$, they are free module of same rank 1. Sso that Γ_2/Γ_1 is of finite rank r and $r\Gamma_2 \subseteq \Gamma_1 \subseteq \Gamma_2$. As a consequence $r \in \mathbb{N}$ is a unit, that implies that $r = 1$ and then $\Gamma_1 = \Gamma_2$.

Exercise 3 p 84
Let K be a number field of degree $n = [K : \mathbb{Q}]$. A complete module of K is a subgroup

of the form $M = \mathbb{Z}\alpha_1 + ...\mathbb{Z}\alpha_n$, where $\alpha_1, ..., \alpha_n$ are linearly independent elements of K. Show that the ring of multipliers

$$\mathcal{O} = \{\alpha \in K | \alpha M \subseteq M\}$$

is an order in K, but in general not the maximal order.

Solution:
Easily, we can check that $\mathcal{O}$ is a ring. Moreover, for any $0 \neq m \in M$, we have that $\mathcal{O} \subseteq m^{-1}M$, let $a \in \mathcal{O}$, $a = am^{-1}m \subseteq m^{-1}aM \subseteq m^{-1}M$. Then, $M \subseteq \mathcal{O} \subseteq m^{-1}M$. So, the $\mathcal{O}$ is a free module of $rank(\mathcal{O}) = rank(M) = n$. Moreover, for any $\alpha \in M$, $\mathbb{Z}[\alpha]$ is a finitely generated module as a consequence α is integral over $\mathbb{Z}$. That proves that $\mathcal{O}$ is an order.
For any $b \in \mathcal{O}$, se have the relations

$$b\theta_j = \sum_{i=1} c_{i,j}\theta_i$$

$c_{i,j} \in A$ so we have $\sum_{i=1}^{m}(\delta_{i,j}b - c_{i,j})_{i,j \in [1,m]}$; it is a matrix in $M_m(A)$ let $Adj(T)$ be its adjoint and $\Theta := (\theta_1, ..., \theta_m)^t$ then $det(T)\Theta = Adj(T)T\Theta = 0$. This implies $det(T)M = 0$.
Since $det(T) = f(b)$ for some monic $f \in A[x]$. It follows that $f(b) = 0$, so b is integral over R. So that $\mathcal{O} \subseteq \mathcal{O}_K$.
Now, consider $K = \mathbb{Q}(\sqrt{5})$, then $\mathcal{O}_K = \mathbb{Z} + \frac{1+\sqrt{5}}{2}\mathbb{Z}$, now if $M = \mathbb{Z} + \sqrt{5}\mathbb{Z}$, $\frac{1}{2} \notin \mathcal{O}$ so that $\mathcal{O} \neq \mathcal{O}_K$.
Exercise 4 p 84
Determine the ring of multiplier $\mathcal{O}$ of the complete module $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$. Show $\epsilon = 1 + \sqrt{2}$ is a fundamental unit of $\mathcal{O}$. Determine all integer solutions of "Pell's equation"

$$x^2 - 2y^2 = 7$$

Hint: $N(x + y\sqrt{2}) = x^2 - 2y^2$, $N(3 + \sqrt{2}) = N(5 + 3\sqrt{2}) = 7$.
Solution:
$\mathbb{Z} + \mathbb{Z}\sqrt{2}$ is the maximal order of $\mathbb{Q}(\sqrt{2})$ so that $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ and we have seen that $\epsilon = 1 + \sqrt{2}$ is a fundamental unit of $\mathcal{O}$. Moreover $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ is a UFD and $7 = (3 + \sqrt{2})(3 - \sqrt{2}) = (5 + 3\sqrt{2})(5 - 3\sqrt{2})$. We notice that $\frac{3+\sqrt{2}}{3-\sqrt{2}} = \frac{11+6\sqrt{2}}{7} \notin \mathbb{Z}[\sqrt{2}]$ and then $3 + \sqrt{2}$ and $3 - \sqrt{2}$ are not associated one to the other. we see that $\frac{5+3\sqrt{2}}{3-\sqrt{2}} = \frac{21+14\sqrt{2}}{7} = 3 + 2\sqrt{2} = (1 + \sqrt{2})^2 \in \mathbb{Z}[\sqrt{2}]^*$. So that $5 + 3\sqrt{2}$ and $3 - \sqrt{2}$ are associated and $5 - 3\sqrt{2}$ and $3 + \sqrt{2}$ are associated. Now, let (x, y) an arbitrary solution of the Pell equation then $N(x + y\sqrt{2}) = 7 = (x + y\sqrt{2})(x - y\sqrt{2})$ so the $(x + y\sqrt{2})$ is associated to $3 + \sqrt{2}$ or to $5 + 3\sqrt{2}$.

Exercise 5 p 84:
In a one-dimensional noetherian integral domain the regular prime ideals $\neq 0$ are precisely the invertible prime ideals.
Solution:

Suppose first that $\mathfrak{p}$ is regular then $A_\mathfrak{p}$ is a dvr (principal domain with one only prime ideal) and $\mathfrak{p}A_\mathfrak{p}$ is principal and then $\mathfrak{p}$ is invertible by the proposition 12.4.
Now, suppose that $\mathfrak{p}$ is invertible, again by the proposition 12.4, $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is a principal ideal so the ring $\mathcal{O}_\mathfrak{p}$ is a dvr so in particler a PID and UFD so that $\mathcal{O}_\mathfrak{p}$ is integrally closed and $\mathfrak{p}$ is regular.

[1]

[1] $(\star)$ = easy , $(\star\star)$= medium, $(\star\star\star)$= challenge