Answers to the problem set 1 [1]

Exercise 1.1: Let define $N : \mathbb{Z}[\sqrt{-6}] \to \mathbb{N} \cup \{0\}$ as $N(z) := |z|^2$ where $|.|$ is the usual norm on the complex numbers. Then set $S := \{n | \exists\, z \in \mathbb{Z}[\sqrt{-6}]$ such that $N(z) = n\} \subseteq \mathbb{N} \cup \{0\}$. Then we prove:

Lemma 1: $2, 3 \notin S$.

Proof: If $N(x + y\sqrt{-6}) = 2$ then $x^2 + 6y^2 = 2$, so x must be even and hence $x^2 + 6y^2$ is at least 4 if $x > 0$, which is not possible. So, $x = 0$ and $6y^2 = 2$ which is absurd. Hence $2 \notin S$.

If $N(x + y\sqrt{-6}) = 3$, then $x^2 + 6y^2 = 3$, hence $3|x$. If $x \neq 0$, then $3 = x^2 + 6y^2 \geq 9$, so $x = 0$ and $6y^2 = 3$, which cannot happen.

Lemma 2: $z \in \mathbb{Z}[\sqrt{-6}]$ is a unit iff $N(z) = 1$.

Proof: If $N(z) = z\bar{z} = 1$ then since $\bar{z} \in \mathbb{Z}[\sqrt{-6}]$, we conclude that z is a unit in $\mathbb{Z}[\sqrt{-6}]$, but if $zz' = 1$ for some $z' \in \mathbb{Z}[\sqrt{-6}]$, then $N(z)N(z') = 1$ and since $N(z), N(z') \in \mathbb{N} \cup \{0\}$, we have $N(z) = 1$.

Now we have $N(2) = 4$, so if $2 = ab$ then $4 = N(a)N(b)$, but because of the above two lemmas we see one of a or b must be unit in $\mathbb{Z}[\sqrt{-6}]$. So, 2 is irreducible in $\mathbb{Z}[\sqrt{-6}]$. We can do the same to prove 3 and $\sqrt{-6}$ are irreducible elements. Note that $-2 = (-1)(2)$, obviously -1 is unit so -2 is irreducible. Note that neither 2 nor 3 are accosiated to $\sqrt{-6}$, since they have different norms. $\square$

Exercise 1.2: a) If $x = \frac{a}{b}$, $a = u_1\pi^n$ and $b = u_2\pi^m$, then we have $x = u_1{u_2}^{-1}\pi^{n-m}$, note that $u_1{u_2}^{-1} \in A$. On the other hand if, $x = u_1\pi^n = u_1'\pi'^{n'}$ be two different representations of $x \in K^\times$ then $n = n'$, since if for example $n > n'$ then $\pi^{n-n'} = {u'_1}^{-1}u_1$, so π is a unit in A . Hence since $\mathfrak{m}$ is generated by π we see $\mathfrak{m} = A$, which is a contradiction. So, $n = n'$. Also, obviously, $\nu(\pi^n) = n$ for $n \in \mathbb{Z}$. So, ν is surjective. Now if $x = a\pi^n$ and $y = b\pi^m$ with $n \geq m$, then $x + y = \pi^m(a\pi^{n-m} + b)$. But, $a\pi^{n-m} + b \in A$, so $\nu(a\pi^{n-m} + b) \geq 0$. Therefore $\nu(x + y) \geq m = \nu(y)$. Note that ν is homomorphism since $\nu(\pi^n u_1.\pi^m u_2) = \nu(\pi^{n+m}u_1u_2) = n + m.$, since u_1u_2 is a unit.

b) First note that $0 \in A$ and A is actually a subring of K. We need to show it is closed under multiplication and also addition. Because of (ii) we see it is closed under addition and since ν is a homomorphism we see if $x, y \in A$ then $\nu(xy) = \nu(x) + \nu(y) \geq 0$.
Also, $\mathfrak{m}$ is an ideal since if $\nu(x) > 0$ and $\nu(y) \geq 0$ then $\nu(xy) = \nu(x) + \nu(y) > 0$. In addition, if $\nu(x) = 0$ then $\nu(x^{-1}) = 0$ and therefore $x^{-1} \in A$. So, A is local and $\mathfrak{m}$ is the only maximal ideal. Note that $\mathfrak{m}$ is principal since if there exists $\pi \in A$ such that $\nu(\pi) = 1$ then $\pi \in \mathfrak{m}$ and if for $x \in \mathfrak{m}$ we have $\nu(x) = n$ then $\nu(x\pi^{-n}) = 0$, and as above $u = x\pi^{-n}$ is a unit in A.Hence $x = u\pi^n$ and $\mathfrak{m}$ is generated as an A-module by π.

c) If $x \in K$ is integral over A, then there exist $a_i \in A$ such that $\sum_{i=0}^{n} a_i x^i = 0$ with $a_n = 1$.

Now if $\nu(x) < 0$ then $\nu(x^n) < \nu(a_i x^i)$ for $i < n$ and we reach a contradiction by the following simple remark.

Remark: $\nu(x) > \nu(y)$ implies $\nu(x + y) = \nu(y)$.

[1] Questions and comments to siinarezazadeh@gmail.com or come to office A3, 111.

Proof: $\nu(x+y) = \nu(y) + \nu(1+\frac{x}{y})$, but $1+\frac{x}{y}$ does not belong to $\mathfrak{m}$ since $\nu(\frac{x}{y}) > 0$ and therefore $\frac{x}{y} \in \mathfrak{m}$ and $1+\frac{x}{y} \notin \mathfrak{m}$, so $\nu(1+\frac{x}{y}) = 0$. Hence, since $\nu(x) < 0$ we have $\nu(\sum_{i=0}^{n} a_i x^i) = v(x^n) < 0$, but $\nu(\sum_{i=0}^{n} a_i x^i) = \nu(0) = +\infty$. □

Exercise 1.3: a) The addition and multiplication can be defined formally as follow: if $A = \sum_{i\in\mathbb{Z}} a_i T^i, B = \sum_{i\in\mathbb{Z}} b_i T^i$ then $A + B = \sum_{i\in\mathbb{Z}} (a_i + b_i)T^i$. Also $AB := \sum_{i\in\mathbb{Z}} c_i T^i$, where $c_k = \sum_{i\in\mathbb{Z}} a_i b_{k-i}$. Note that if $a_i = b_i = 0$ for $i < N$, then $a_i + b_i = 0$ for $i < N$ and also $c_k = 0$ for $k < 2N$. Now we try to prove $k((T))$ is a field. We just need to prove any non-zero element in $k((T))$ has an inverse. Every element of $k((T))$ can be written like $T^n f$ such that $f = \sum_{i\geq 0} a_i T^i$, $a_0 \neq 0$ and $n \in \mathbb{Z}$. But obviously T^n is invertible for any $n \in \mathbb{Z}$, since $T^n T^{-n} = 1$ and $T^{-n} \in k((T))$, so we just need to prove if $f = \sum_{i\geq 0} a_i T^i$ is invertible. Set $g = \sum_{i\geq 0} b_i T^i$, we want to find b_i's such that $fg = 1$. But this exactly means,

$$
\begin{aligned}
a_0 b_0 &= 1 \\
a_0 b_1 + a_1 b_0 &= 0 \\
a_0 b_2 + a_1 b_1 + a_2 b_0 &= 0 \\
&\vdots \\
a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_n b_0 &= 0 \\
&\vdots
\end{aligned}
$$

Now, since $a_0 \neq 0$ from the first equation we have $b_0 = {a_0}^{-1}$, from the second equation we find $b_1 = {a_0}^{-1}(-a_1 b_0)$, and so inductively we would find b_n for every n.
Alternatively, one can write $f = \sum_{i\geq 0} a_i T^i = 1 - g$ where $g \in (T)$. In this case, $\sum_{i\geq 0} g^i$ would be the inverse of $1 - g$. Note that if $g \notin (T)$ then $f = \sum_{i\geq 0} g^i$ would not belong to $k((T))$.

b) Define the valuation $\nu : k((T))^\times \to \mathbb{Z}$ as $\nu(f) = k$ where $f = \sum_{i\geq k} a_i T^i$ where $a_k \neq 0$. And also set $\nu(0) = +\infty$. Then obviously $\nu : k((T))^\times \to \mathbb{Z}$ is a homomorphism and it satisfies the conditions (i) and (ii) of the Exercise 1.2.
Note that $\nu(f) \geq 0$ iff $f \in k[[T]]$, so because of 1.2 b) $k[[T]]$ is a valuation ring, and also $\mathfrak{m} = (T)$. So, the residue field would be $k[[T]]/(T)$ which is obviously k . □

Exercise 1.4: a) We know that since $A \subseteq B$ is an integral extension, there exists a prime ideal $\mathfrak{q}$ of Spec(B) such that $\mathfrak{q} \cap A = \mathfrak{p}$, so $\mathfrak{p} \subseteq \mathfrak{q}$, and hence $\mathfrak{p}B \subseteq \mathfrak{q}$.

b) Set $S = A - \mathfrak{p}$ and consider it as a multiplicative closed subset of K, then we have:

$$S^{-1}(\mathfrak{a}B \cap A) = S^{-1}(\mathfrak{a}B) \cap S^{-1}(A) = S^{-1}(\mathfrak{a})S^{-1}(B) \cap S^{-1}(A)$$

Note that $S^{-1}(B)$ is the integral closure of $S^{-1}(A)$ in K, now because of $\mathfrak{a} \subseteq \mathfrak{a}B \cap A$ and the following lemma we just need to prove when A is a DVR.

Lemma: If $I \subseteq J$ are two ideals in the ring A and $I_{\mathfrak{p}} = J_{\mathfrak{p}}$ for every $\mathfrak{p} \in \mathrm{Spec}(A)$, then $I = J$.
Proof: Since $(J/I)_{\mathfrak{p}} = 0$ for every prime implies $J/I = 0$ we conclude.

Now for a DVR A, the ideal $\mathfrak{a}$ would be principal and hence it is generated by element $x \in A$, so if $bx \in \mathfrak{a}B \cap A$, then $bx \in A \subseteq K$, and therefore $b \in K$. But we know from Exercise 1.2 that A is integrally closed and so $B \cap K = A$ and $b \in A$ hence $bx \in \mathfrak{a}$ and we are done.

c) If $\mathfrak{a} \subseteq \mathfrak{a}'$ then obviously $\mathfrak{a}B \subseteq \mathfrak{a}'B$, now if $\mathfrak{a}B \subseteq \mathfrak{a}'B$, then we have $\mathfrak{a}B \cap A \subseteq \mathfrak{a}'B \cap A$, so by b) $\mathfrak{a} \subseteq \mathfrak{a}'$. $\square$