Answers to the problem set 2 [1]

Exercise 2.1: 1) First note that K is still the fraction field of $S^{-1}A$, since $A \subseteq S^{-1}A \subseteq K$, so $K = \mathrm{Frac}(A) \subseteq \mathrm{Frac}(S^{-1}A) \subseteq \mathrm{Frac}(K) = K$. Besides, since $\mathfrak{a}$ is a fractional ideal there exists $d \in A$ such that $d\mathfrak{a} \subseteq A$, hence $dS^{-1}\mathfrak{a} = S^{-1}d\mathfrak{a} \subseteq S^{-1}A$.

2) Every element of $\mathfrak{a}\mathfrak{b}$ can be written like $\sum_{1\leq i\leq n} a_i b_i$ where $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. So, for every $s \in S$, we have $s^{-1}(\sum_{1\leq i\leq n} a_i b_i) = \sum_{1\leq i\leq n} (s^{-1}a_i)b_i \in S^{-1}\mathfrak{a}.S^{-1}\mathfrak{b}$. On the other hand, for any $x = \sum_{1\leq i\leq n} a_i/t_i.b_i/s_i$ in $S^{-1}\mathfrak{a}.S^{-1}\mathfrak{b}$, if we put $a'_i = (a_i.t_1\cdots t_n)/t_i, b'_i = (b_i.s_1\cdots s_n)/s_i, r = \Pi s_i t_i$ then $a'_i \in \mathfrak{a}, b'_i \in \mathfrak{b}$ and $r \in S$. But, $x = r^{-1}\sum_{1\leq i\leq n} a'_i b'_i \in S^{-1}(\mathfrak{a}\mathfrak{b})$.

So, $S^{-1}(\mathfrak{a}\mathfrak{b}) = S^{-1}\mathfrak{a}.S^{-1}\mathfrak{b}$.

3) First, note that $\mathfrak{a}'$ is an A-submodule of K. In fact, if $a, b \in \mathfrak{a}'$ then $(a+b)\mathfrak{a} = a\mathfrak{a} + b\mathfrak{a} \subseteq A$, also for any $r \in A$, $ra\mathfrak{a} \subseteq rA \subseteq A$, so $ra \in \mathfrak{a}'$. So, $\mathfrak{a}'$ is an A-submodule of K. Now, since $\mathfrak{a}$ is a fractional ideal, there is a $d \in A$ such that $d\mathfrak{a} \subseteq A$, so for any $0 \neq b \in A$ we have $db\mathfrak{a}' \subseteq A$ and $ab \in A$.

Obviously, $S^{-1}\mathfrak{a}' \subseteq \{a \in K | a\mathfrak{a} \subseteq S^{-1}A\} = \{a \in K | aS^{-1}\mathfrak{a} \subseteq S^{-1}A\} = (S^{-1}\mathfrak{a})'$. Now, if $a\mathfrak{a} \subseteq S^{-1}A$ and $l_1, \cdots, l_k \in \mathfrak{a}$ is a set of generators as an A-module then $a.l_i = a_i/t_i$ for some $a_i \in A$ and $t_i \in S$. Since S is multiplicative closed subset of A we can assume that all t_i's are the same. So, $at.l_i \in A$ and hence $at \in \mathfrak{a}'$. Therefore $a \in S^{-1}\mathfrak{a}'$.

4) If A is a DVR then any fractional ideal is of the form (π^k) where k is an integer. In fact, any (π^k) would be obviously a fractional ideal. Conversely, if J is a fractional ideal then for some $x = \pi^l u \in A$, $xJ \subseteq A$. So, $xJ = (\pi^r)$ for some r. Therefore, $J = u^{-1}(\pi^{r-l}) = (\pi^{r-l})$. Now if $\mathfrak{a} = (\pi^k)$ is any fractional ideal then $\mathfrak{a}'$ would be obviously (π^{-k}). So, $\mathfrak{a}\mathfrak{a}' = A$. Now if A is a Dedekind domain and $\mathfrak{a}\mathfrak{a}' \subsetneq A$, then there exists a prime ideal $\mathfrak{p} \subseteq A$ such that $\mathfrak{a}\mathfrak{a}' \subseteq \mathfrak{p}$. Then since A is Noetherian then using 3) we conclude that:

$$(\mathfrak{a}\mathfrak{a}')_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}\mathfrak{a}'_{\mathfrak{p}} \subseteq \mathfrak{p}_{\mathfrak{p}} \ (*)$$

But, since A is a Dedekind domain then $A_{\mathfrak{p}}$ would be a DVR and since $\mathfrak{a}_{\mathfrak{p}}$ is a fractional ideal of $A_{\mathfrak{p}}$ we see $\mathfrak{a}_{\mathfrak{p}}\mathfrak{a}'_{\mathfrak{p}} = A_{\mathfrak{p}}$ which is a contradiction to $(*)$. Hence, $\mathfrak{a}\mathfrak{a}' = A$ and we are done. □

Exercise 2.2: 1) This is just true by the definition, since the image of $K^* \to \mathrm{Id}(A)$ is exactly $\mathrm{P}(A)$. So, the sequence is exact at $\mathrm{Id}(A)$. On the other hand, $(\alpha) = A$ for $\alpha \in K^*$ iff $\alpha \in A^*$. So, we are done.

2) (a) ⇔ (b) is just by definition. For (b) ⇔ (c), if $I \subseteq A$ is an ideal of A, then it would be also a fractional ideal and since $\mathrm{Id}(A) = \mathrm{P}(A)$, there exists $\alpha \in K$ such that I is the principal fractional ideal generated by α. Then obviously $\alpha \in A$ and the ideal I is principal. So, I is a PID. Conversely, if A is a PID and J is a fractional ideal then $aJ \subseteq A$ would be an ideal of A and so there exists $b \in A$ such that $aJ = (b)$. Hence, $J = (\frac{b}{a})$.
(c) ⇔ (d) is always true, in fact every PID is a UFD in general. Conversely, if A is a UFD and I is a non-zero prime ideal of A then take $0 \neq x \in I$ and factorize x as $p_1^{n_1}\cdots p_k^{n_k}$

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

where p_i are prime elements of A then since I is prime one of the p_i's must lie inside I. But since A is a Dedekind domain each non-zero prime is maximal, so I must be (p_i) for some i. If I is not prime and $I = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$ is a factorization of I into prime ideals then each $\mathfrak{p}_i$ is principal as we discussed above. If $\mathfrak{p} = (a_i)$ then we have $I = (a_1^{n_1} \cdots a_k^{n_k})$. □

Exercise 2.3: 1) Define $\alpha : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{m}]$ as $\alpha(P) := P(\sqrt{m})$. We first check that α is a $\mathbb{Z}$-algebra homomorphism. Note that: $\alpha(P+Q) = P(\sqrt{m}) + Q(\sqrt{m}) = \alpha(P) + \alpha(Q)$, also $\alpha(P.Q) = (PQ)(\sqrt{m}) = P(\sqrt{m}).Q(\sqrt{m}) = \alpha(P).\alpha(Q)$. α is obviously surjective, since $\alpha(a + bX) = a + b\sqrt{m}$. On the other hand, $X^2 - m$ lies in the kernel of α, so we would have the induced map $\phi : \mathbb{Z}[X]/(X^2 - m) \to \mathbb{Z}[\sqrt{m}]$. Now, any element in $\mathbb{Z}[X]/(X^2 - m)$ would be like $a + bX + (X^2 - m)$. Also, $\phi(\overline{a + bX}) = a + b\sqrt{m}$, but since m is square free and also not equal to 1, $a + b\sqrt{m}$ cannot be zero for any $a, b \in \mathbb{Z}$, so ϕ is injective.

Obviously, $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}$, since if $ab \in \mathfrak{p} \subseteq P$ for $a, b \in \mathbb{Z}$, then since P is prime a or b must lie inside P and consequently, a or b would lie inside $\mathfrak{p}$. Now, notice that $\mathbb{Z}[\sqrt{m}]$ is integral over $\mathbb{Z}$. Hence, for any $0 \neq x \in P$, there exist a minimal natural number n and $a_1, a_2, \cdots, a_n \in \mathbb{Z}$ such that $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$. a_n cannot be zero, since, $\mathbb{Z}[\sqrt{m}]$ is a domain and n is the least natural number which the non-zero element x is a root of a monic ploynomial with cofficients in $\mathbb{Z}$. But this way, $a_n = -(x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x)$ would lie inside both $\mathbb{Z}$ and P. So, $\mathfrak{p}$ would be non-zero.

2,3) A is a finite over $\mathbb{Z}$, so A/P is finite over $\mathbb{F}_\mathfrak{p}$. Now, if $0 \neq x \in A/P$ then since A/P is a finite vector space over $\mathbb{F}_\mathfrak{p}$, there exists a minimal natural number n and $a_1, \cdots, a_n \in \mathbb{F}_\mathfrak{p}$, such that $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$. a_n is not zero because of the way we chose n and also A/P is a domain, so:

$$x[(x^{n-1} + a_1 x^{n-2} + a_2 x^{n-3} + \cdots + a_{n-1})(-a_n)^{-1}] = 1$$

Hence A/P is a field and therefore P is maximal. In fact, we proved that every non-zero prime ideal of A is maximal. Now, A is a Noetherian domain which every non-zero prime ideal is maximal, so by the definition of a Dedekind domain, A is a Dedekind domain iff it is integrally closed. □

Exercise 2.4: 1) $\text{Frac}(A) = \mathbb{Q}(\sqrt{-5})$, so because of the exercise 2.3 we just need to prove that the integral closure of A in $\mathbb{Q}(\sqrt{-5})$ is just A. So, take $\alpha = r + s\sqrt{-5}$ with $r, s \in \mathbb{Q}$ integral over A. Then we have:

$$\alpha = r + s\sqrt{-5} \Rightarrow (\alpha - r)^2 = -5s^2 \Rightarrow \alpha^2 - 2r\alpha + r^2 + 5s^2 = 0$$

So, α is a root of $f(x) = x^2 - 2rx + r^2 + 5s^2 \in \mathbb{Q}[X]$. Notice that s cannot be zero when α is not in A, so α does not belong to $\mathbb{Q}$, and 2 is the smallest degree of a polynomial with cofficients in $\mathbb{Q}$ such that α could be a root of. Now, if $\overline{\alpha} = r - s\sqrt{-5}$, then $\overline{\alpha}$ would be also a root of f. So, α and $\overline{\alpha}$ are both integral over $\mathbb{Z}[\sqrt{-5}]$ and hence over $\mathbb{Z}$. But, as we already know if $A \subseteq B$ is an extension of rings, then the integral elemenets of A in B would form a ring. So, $2r = \alpha + \overline{\alpha}$ and $\alpha.\overline{\alpha} = r^2 + 5s^2$ are both integral over $\mathbb{Z}$. But, they are rational numbers and $\mathbb{Z}$ is integrally closed, so they must belong to $\mathbb{Z}$. So, $r = \frac{a}{2}$ with $a \in \mathbb{Z}$ and also we can write s as $\frac{p}{2q}$ where $p, q \in \mathbb{Z}$ and $(p, q) = 1$. Then we have

$$4q^2 | a^2 q^2 + 5p^2 \Rightarrow q^2 | 5p^2 \Rightarrow q^2 | 5 \Rightarrow q = 1$$

Therefore, $4|a^2+p^2$, but as we know this is possible iff both a and p are even, since $0,1$ are the only quadratic residue mod 4. Hence, both r and s are natural.

2) $N(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha} = a - b\sqrt{-5}$. So, if $N(\alpha) = 1$ then $\overline{\alpha} = \alpha^{-1}$. But if $\alpha\beta = 1$ then $N(\alpha)N(\beta) = 1$ since N is multiplicative. Now, as N is a natural-valued function we have $N(\alpha) = 1$

3) We have already done something very similar in Exercise 1.1. Note that $N(\alpha)$ cannot be 3 for any $\alpha \in \mathbb{Z}[\sqrt{-5}]$, since $a^2+5b^2 = 3$ does not have any solution in the natural numbers. In fact, b cannot be zero and it is at least one. So, $a^2 + 5b^2$ must be at least 5 which is a contradiction. Therefore if $\alpha = \beta\gamma$ where $N(\alpha) = 9$ then since $9 = N(\alpha) = N(\beta)N(\gamma)$, one of the $N(\beta)$ and $N(\gamma)$ must be 1. So, either β or γ is a unit. Hence, α is irreducible.

4) If $9 = (3)^2$ then as $(2+\sqrt{-5})(2-\sqrt{-5}) = 9$ we must have $2+\sqrt{-5} \in (3)$ or $2-\sqrt{-5} \in (3)$. So, $3-(2+\sqrt{-5})$ or $3-(2-\sqrt{-5})$ must be inside (3). But, in any case, $N(3) = 9$ must divide $N(1-\sqrt{-5}) = N(1+\sqrt{-5}) = 6$ which is a contradiction. $\square$