This piece contains the solutions for Serg Lang's Graduate Algebra Chapter II exercises on Dedekind rings.

(13) Since the ideals of $\mathfrak{o}$ are fractional ideals by definition, for a given ideal $\mathfrak{a}$ of $\mathfrak{o}$, there is a fractional ideal $\mathfrak{b} \subset K$ with $c\mathfrak{b} \subset \mathfrak{o}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$. Since, the unit 1_K is a quotient of $\mathfrak{o}$, $1_K \in \mathfrak{o}$. Therefore, let $1_K = \sum_{i \leqslant n} a_i b_i$ where $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. For any element $a \in \mathfrak{a}$, then we have $a = \sum_i a a_i b_i$. But $ca = \sum_i a_i b_i'$ where $b_i' = acb_i \in \mathfrak{o}$. If $a \neq b$ then $ca \neq cb$, thus $\mathfrak{a}$ is generated by $\{a_1, \dots, a_n\}$.

(14) *Existence*: Let S be the set of all ideals of $\mathfrak{o}$ that don't have prime factorization. Suppose S is not empty and let $\mathfrak{a}_1 \in S$. Then consider the asending chain of ideals in S

$$\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \dots$$

Since, the union ideal $\mathfrak{a} = \cup_i \mathfrak{a}_i$ is an ideal in $\mathfrak{o}$, it is fintely generated and $\mathfrak{a} = \mathfrak{a}_n$ for some n. It follows the the chain is finite and any $\mathfrak{b} \supset \mathfrak{a}$ admits prime factorization. For all $xy \in \mathfrak{a}$ and if either x or y is an element of $\mathfrak{a}$, then $\mathfrak{a}$ is a prime and there is nothing left to prove. Otherwise, let $\mathfrak{a} = \langle a_1, \dots, a_m \rangle$. Then $\mathfrak{s} = \langle a_1, \dots, a_m, x \rangle \supset \mathfrak{a}$, $\mathfrak{t} = \langle a_1, \dots, a_m, y \rangle \supset \mathfrak{a}$, and we have $\mathfrak{s}\mathfrak{t} \subseteq \mathfrak{a}$ (hence $\mathfrak{a} = \mathfrak{s}\mathfrak{t}$). Thus $\mathfrak{a} \notin S$ and by induction, S shall be empty.

Uniqueness: Let $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_s = \mathfrak{q}_1 \cdots \mathfrak{q}_r$. We induct on s. Let $s = 1$. Then we have $\mathfrak{p}_1 = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ for $r \geqslant 1$. Since all prime ideals are fintly generated, let G be a set of generators of $\mathfrak{p}_1$. Since the product on the left is a subset of each $\mathfrak{q}_i$, we have $\mathfrak{p}_1 \subseteq \mathfrak{q}_i$ for all $1 \leqslant i \leqslant r$. Take a generator $x_i \in \mathfrak{q}_i - G$ from each $\mathfrak{q}_i$. Then the product $x_1 \cdots x_r \in \mathfrak{p}_1$. By primality, one of $x_i \in \mathfrak{p}_1$, a contradiction. Thus $\mathfrak{q}_i \subseteq \mathfrak{p}_1$ (and thus $\mathfrak{q}_i = \mathfrak{p}_1$) for some i, say $i = 1$. It follows that $\mathfrak{q}_2 \cdots \mathfrak{q}_r = \mathfrak{o}$ and each $\mathfrak{q}_i = \mathfrak{o}$ since prime ideals can not be inverses of each other.

For the induction step, suppose the factorization is unique for all products up to $s - 1$ factors. By similar reasoning as above, let $x_i \in \mathfrak{q}_i - G$ where G is the generator of $\mathfrak{p}_1$. Then $x_1 \cdots x_r \in \prod \mathfrak{q}_i = \prod \mathfrak{p}_i \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s \subseteq \mathfrak{p}_1$. By primality, one of $x_1 \in \mathfrak{p}_1$ contradicting the inexistence of x_i in $G \subseteq \mathfrak{p}_1$. Thus $\mathfrak{p}_1 \supseteq \mathfrak{q}_j$ for some j. By maximality of prime ideals, $\mathfrak{p}_1 = \mathfrak{q}_j$. By cancellation and induction, the statement follows.

(15) By unique factorization, we know $(t) = \mathfrak{p}^s$. We also have $\mathfrak{p}^s \subseteq \mathfrak{p}^{s-1} \cap \mathfrak{p}$ for $s \geqslant 1$. Thus $(t) = \mathfrak{p}$.

(16) First, we show that $\mathfrak{o}_\mathfrak{p}$ is a Dedekind ring. Let $S = A - \mathfrak{p}$, and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of $\mathfrak{o}$. First, we note that if $\mathfrak{a}$ is a fractional ideal, so is $S^{-1}\mathfrak{a}$. If $xa \in \mathfrak{a}$ for all $x \in \mathfrak{o}$, $a \in \mathfrak{a}$, then $\frac{x}{s}\frac{a}{t} = \frac{xa}{st}$, which is an element of $S^{-1}\mathfrak{a}$ by multiplicativeness of S. Similarly if $c\mathfrak{a} \subseteq \mathfrak{o}$ for some $c \in \mathfrak{o}$, then $\frac{c}{1}(S^{-1}\mathfrak{a}) \subseteq \mathfrak{o}_\mathfrak{p}$.

For elements $a_i \in \mathfrak{a}$, $b \in \mathfrak{b}$ and any elements $s_i, t_i \in S$, we have the finite sum $\sum \frac{a_i}{s_i}\frac{b_i}{t_i} = \sum \frac{a_i b_i}{s_i t_i} = \frac{1}{x}\sum a_i' b_i$ where $a_i' = \prod_{j \neq i} s_j t_j a_i$ and $x = \prod_i s_i t_i$. Therefore, $S^{-1}\mathfrak{a} \cdot S^{-1}\mathfrak{b} \subseteq S^{-1}\mathfrak{a}\mathfrak{b}$. For the reverse inclustion, let

$r/s = \sum_i a_i b_i/s$, then picking $a_i' = a_i/s$ and $b_i' = bi/1$, we have $r/s = \sum_i a_i' b_i'$. This proves that localization by $\mathfrak{p}$ is multiplicative.

The group properties of the set of fractional ideals of $\mathfrak{o}_\mathfrak{p}$ then directly follows from the group properties of that of $\mathfrak{o}$. It remains to show that there is one prime ideal in $\mathfrak{o}_\mathfrak{p}$. By multiplicativeness of the homomorphism $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$, and the unique factorization proved in the previous excercise, we can express any ideal $\mathfrak{s}$ of $\mathfrak{o}_\mathfrak{p}$ as

$$\mathfrak{s} = S^{-1}\mathfrak{q}_1 \cdots S^{-1}\mathfrak{q}_m.$$

At most one of $S^{-1}\mathfrak{q}_i$ is equal to $\mathfrak{p}$ (up to uniqueness) and the rest are units. Thus the only prime ideal is $S^{-1}\mathfrak{p}$.

(17) (a) If $\mathfrak{a} \mid \mathfrak{b}$, by definition there is an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}\mathfrak{o} = \mathfrak{a}$. On the other hand, $\mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}$. From the definiton of the fractional ideals, it follows that $\mathfrak{a}^{-1}\mathfrak{b}$ is an ideal of $\mathfrak{a}$. The backward direction follows immediately.

(b) For ideals $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$, $\mathfrak{c}\mathfrak{a} + \mathfrak{c}\mathfrak{b}$ is the set of all finite sums $\sum_i c_i a_i + \sum_j c_j b_j$ where $a_i \in \mathfrak{a}$, $b_j \in \mathfrak{b}$ and $c_i, c_j \in \mathfrak{c}$. By rearranging the terms, we can write this sum as $\sum_i c_i(a_i + b_i) + \sum_j c_j(a_j + 0) + \sum_k c_k(0 + b_k)$. Hence $\mathfrak{c}(\mathfrak{a} + \mathfrak{b}) \supseteq \mathfrak{c}\mathfrak{a} + \mathfrak{c}\mathfrak{b}$. The reverse inclustion follows from the distributive property of $(+)$ over $(\cdot)$. Therefore, $\mathfrak{c}(\mathfrak{a} + \mathfrak{b}) = \mathfrak{c}\mathfrak{a} + \mathfrak{c}\mathfrak{b}$.

Now, let $\mathfrak{d} \mid \mathfrak{a}$ and $\mathfrak{d} \mid \mathfrak{b}$. Then we have $\mathfrak{a} + \mathfrak{b} = \mathfrak{d}\mathfrak{a}' + \mathfrak{d}\mathfrak{b}' = \mathfrak{d}(\mathfrak{a}' + \mathfrak{b}')$ for some ideals $\mathfrak{a}', \mathfrak{b}'$. Thus $\mathfrak{d}$ also divides $\mathfrak{a} + \mathfrak{b}$.

(18) Suppose $\mathfrak{p} \subsetneq \mathfrak{a} \subsetneq \mathfrak{o}$. Then by the above exercise, $\mathfrak{a} \mid \mathfrak{p}$, i.e. $\mathfrak{p} = \mathfrak{a}\mathfrak{c}$. But since $\mathfrak{p} \neq \mathfrak{a}$, $\mathfrak{c} \neq \mathfrak{o}$ and distinct factorizations of $\mathfrak{p}$ exist, a contradiction.

(19) By similar reasoning as question (15), for every prime ideal $\mathfrak{p}$, there is an element $t \in \mathfrak{p} - \mathfrak{p}^2$ such that $\mathfrak{p} \mid (t)$. It also directly follows that (t^n) has $\mathfrak{p}^n$ in its prime factorization.

Given distinct primes $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, and positive integers $r_1, \dots, r_n$ we can find $x_i \in \mathfrak{o}$ such that (x_i) has $\mathfrak{p}_i^{r_i}$ in its prime factorization. By the chinese remainder theorem, we then can select $x \in \mathfrak{o}$ such that $x = x_i \mod \mathfrak{p}_i^{r_i+1}$ that has the product of all the prime powers $\mathfrak{p}_i^{r_i}$ in its prime factorization.

Let $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_n^{s_n}$. Taking $r_i = s_i$ in the previous pararaph, we obtain a (x) that is a multiple of $\mathfrak{a}$ for some $y \in \mathfrak{o}$. Let $(x) = \mathfrak{a}\mathfrak{c}$ for some ideal $\mathfrak{c}$. Note that the inverse of this ideal is the fractional ideal $x^{-1}\mathfrak{o}$ which is of the form $\mathfrak{a}^{-1}\mathfrak{c}^{-1}$. Next, we construct another ideal (u) by defining r_i as follows:

$$r_i = \begin{cases} 0 & \text{if } \mathfrak{p}_i \mid \mathfrak{a} \\ m_i & \text{if } \mathfrak{p}_i^{m_i+1} + \mathfrak{c} = \mathfrak{p}_i^{m_i} \\ 0 & \text{if } \mathfrak{p}_i \mid \mathfrak{b}, \mathfrak{p}_i \nmid (x) \end{cases}$$

Now it follows that $(u) = \mathfrak{c}\mathfrak{z}$ for some ideal $\mathfrak{z}$ such that $\mathfrak{z} + \mathfrak{b} = \mathfrak{o}$. Observe that $ux^{-1}\mathfrak{a} = u\mathfrak{o}x^{-1}\mathfrak{o}\mathfrak{a} = \mathfrak{z}$. Taking $c = x/y \in K$, we conclude the proof.