A *Dedekind ring* is defined to be a subring $\mathfrak{o}$ of a field K such that every element of K is a quotient of elements of $\mathfrak{o}$, and the fractional ideals form a multiplicative group. Since a Dedekind ring is defined as a subring of a field, we know $\mathfrak{o}$ is an integral domain. Let $\mathfrak{o}$ be a Dedekind ring and K its quotient field. Unless otherwise specified, all ideals are nonzero.

13. Every ideal is finitely generated.

Proof. Let $\mathfrak{a} \subseteq \mathfrak{o}$ be an ideal. If $\mathfrak{a} = 0$ then clearly $\mathfrak{a}$ is finitely generated, so assume otherwise. $\mathfrak{o}$ is a Dedekind domain, so there is a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$, so $\sum a_i b_i = 1$ for some $a_i \in \mathfrak{a}, b_i \in \mathfrak{b}$, $i = 1, \ldots, n$. For any $a \in \mathfrak{a}$, we know $ab_i \in \mathfrak{a}\mathfrak{b} = \mathfrak{o}$. Thus,

$$a = a \sum a_i b_i = \sum (ab_i) a_i \in (a_1, \ldots, a_n)$$

since each $ab_i \in \mathfrak{o}$. So $\mathfrak{a} \subseteq (a_1, \ldots, a_n)$. The reverse inclusion is obvious, since each a_i is in $\mathfrak{a}$. □

14. Every ideal has a factorization as a product of prime ideals, uniquely determined up to permutation.

Proof. First, note that $\mathfrak{o}$ is Noetherian. For, let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ be a properly increasing chain of ideals in $\mathfrak{o}$. Then the union $\mathfrak{a} = \bigcup_1^\infty \mathfrak{a}_i$ is an ideal of $\mathfrak{o}$ (we have shown this for increasing unions) and is thus generated by a finite set $(a_1, \ldots, a_n)$. For each $i = 1, \ldots, n$ there is some k_i such that $a_i \in \mathfrak{a}_{k_i}$. Let $N = \max\{k_1, \ldots, k_n\}$. Then for all $m \geq N$, $a_i \in \mathfrak{a}_m$ for all i, hence $\mathfrak{a} \subseteq \mathfrak{a}_m$. But clearly $\mathfrak{a}_m \subseteq \mathfrak{a}$, hence we have equality. Thus every properly increasing chain of ideals terminates, so $\mathfrak{o}$ is Noetherian.

First consider the case of the zero ideal. The proposition is technically false in this case: since $\mathfrak{o}$ is an integral domain, (0) is prime, thus we have factorizations $(0) = (0)\mathfrak{p}_1 \cdots \mathfrak{p}_n$ for any prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. However, if $(0) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ were another factorization where none of the factors were (0), then taking a nonzero element p_i from each factor, we would have $p_1 \cdots p_n = 0$, contradicting that $\mathfrak{o}$ is entire. Therefore, any factorization of (0) must contain (0) as a factor.

Let $\mathfrak{a}$ be a nonzero proper ideal of $\mathfrak{o}$. $\mathfrak{a}$ is contained in a maximal (hence prime) nonzero ideal $\mathfrak{p}_1$. Let $\mathfrak{a}_1 = \mathfrak{a}\mathfrak{p}_1^{-1}$. Since $\mathfrak{a} \subseteq \mathfrak{p}_1$, we know $\mathfrak{a}_1 = \mathfrak{a}\mathfrak{p}_1^{-1} \subseteq \mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathfrak{o}$, so $\mathfrak{a}_1$ is an ideal of $\mathfrak{o}$. Now, if $\mathfrak{a}_1$ is proper, then letting $\mathfrak{a}_1$ take the place of $\mathfrak{a}$, we find maximal ideal $\mathfrak{p}_2$ containing $\mathfrak{a}_1$, and again $\mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{p}_2^{-1}$ is an ideal of $\mathfrak{o}$. Continuing in this fashion, we have at the nth step produced a chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n$. If we were able to continue this process forever, it would create an infinite chain which never stabilizes, a contradiction. So there is some n such that $\mathfrak{a}_n = \mathfrak{a}_{n-1}\mathfrak{p}_n^{-1}$ is not proper, i.e. $\mathfrak{a}_{n-1}\mathfrak{p}_n^{-1} = \mathfrak{o}$. But multiplication of ideals is associative, thus $\mathfrak{a}_{n-1} = \mathfrak{p}_n$ is prime. This gives us a factorization

$$\mathfrak{a} = \mathfrak{a}_1\mathfrak{p}_1 = \mathfrak{a}_2\mathfrak{p}_2\mathfrak{p}_1 = \cdots = \mathfrak{a}_{n-1}\mathfrak{p}_{n-1} \cdots \mathfrak{p}_1 = \mathfrak{p}_n \cdots \mathfrak{p}_1$$

of $\mathfrak{a}$ into prime ideals.

One direction of the proof of exercise 17(a) is immediate: if $\mathfrak{a} \mid \mathfrak{b}$, then $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}$. Also, if $\mathfrak{p}$ contains a product $\mathfrak{a}\mathfrak{b}$, then it must contain one of $\mathfrak{a}$ or $\mathfrak{b}$. If this were not the case, then there would be some $a \in \mathfrak{a}, b \in \mathfrak{b}$ such that $a, b \notin \mathfrak{p}$. This is a contradiction, since $\mathfrak{p}$ is prime and $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. Obviously, this extends inductively to a product of any number of ideals.

Now, suppose we have two factorizations $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ into prime ideals (say with $n \leq m$). Assume without loss of generality that $\mathfrak{p}_1$ is a minimal element of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, meaning that it is not properly contained in any of the others. $\mathfrak{p}_1$ divides the product $\mathfrak{q}_1 \cdots \mathfrak{q}_m$, hence it contains one of the factors; assume without loss of generality it is $\mathfrak{q}_1$. $\mathfrak{q}_1$ divides the product $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, thus it contains some $\mathfrak{p}_k$. This gives $\mathfrak{p}_k \subseteq \mathfrak{q}_1 \subseteq \mathfrak{p}_1$. By the minimality of $\mathfrak{p}_i$, we must have equalities throughout, thus $\mathfrak{q}_1 = \mathfrak{p}_1$. Since $\mathfrak{a}$ is nonzero, $\mathfrak{p}_1$ and $\mathfrak{q}_1$ are nonzero, hence invertible. Using the associativity of multiplication of fractional ideals, we can cancel them from the product, leaving us with $\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_2 \cdots \mathfrak{q}_m$.

After repeating this process n times, we will have shown the first n factors to be equal (up to reordering). If $n \neq m$, we will have $(1) = \mathfrak{q}_{n+1} \cdots \mathfrak{q}_m$. This would imply that $\mathfrak{q}_m$ divides, and thus contains, (1) - contradicting that $\mathfrak{q}_m$ is prime. So we must have $n = m$, and the factors are equal up to permutation. □

15. Suppose $\mathfrak{o}$ has only one prime ideal $\mathfrak{p}$. Let $t \in \mathfrak{p}$ and $t \notin \mathfrak{p}^2$. Then $\mathfrak{p} = (t)$ is principal.

Proof. We cannot have $t = 0$ or else $t \in \mathfrak{p}^2$. Also, $(t) \neq \mathfrak{o}$ or else $\mathfrak{o} \subseteq \mathfrak{p}$, contradicting that $\mathfrak{p}$ is prime. Thus, (t) is a nonzero proper ideal, hence it has a unique factorization into prime ideals. This must be of the form $\mathfrak{p}^k$ for some $k \geq 1$, since $\mathfrak{p}$ is the only prime ideal. If $k \geq 2$, then $\mathfrak{p}^2 \mid (t)$ and hence $(t) \subseteq \mathfrak{p}^2$, a contradiction. So $k = 1$, thus $(t) = \mathfrak{p}$ is principal.

□

16. Let $\mathfrak{o}$ be any Dedekind ring. Let $\mathfrak{p}$ be a prime ideal. Let $\mathfrak{o}_\mathfrak{p}$ be the local ring at $\mathfrak{p}$. Then $\mathfrak{o}_\mathfrak{p}$ is Dedekind and has only one prime ideal.

Proof. First, we will develop some facts about the localization of an arbitrary integral domain R, with field of fractions K, at a multiplicative subset S. Given an R-module $\mathfrak{a} \subseteq K$, we define the *extension* of $\mathfrak{a}$ to be $S^{-1}\mathfrak{a} = \{a/s \mid a \in \mathfrak{a}, s \in S\}$, identifying the localization of R at S as a subring of K. Note $S^{-1}\mathfrak{a}$ is an $S^{-1}R$-module: if $a/s, b/t \in S^{-1}\mathfrak{a}$ for some $a, b \in \mathfrak{a}, s, t \in S$ then $\frac{a}{s} + \frac{b}{t} = \frac{as+bt}{st} \in S^{-1}\mathfrak{a}$ since $as, bt \in \mathfrak{a}$ and $st \in S$; also, if $c/r \in S^{-1}R$ then $\frac{c}{r}\frac{a}{s} = \frac{ca}{rs} \in S^{-1}\mathfrak{a}$ since $ca \in \mathfrak{a}$ and $rs \in S$. So clearly if $\mathfrak{a}$ is an ideal then $S^{-1}\mathfrak{a}$ is as well. Also, if $c\mathfrak{a} \subseteq R$ for some $c \in R$, then $c\mathfrak{a}^e \subseteq S^{-1}R$. So extension preserves both ideals and fractional ideals.

Extension also distributes over multiplication of R-modules. If $I, J \subseteq K$ are R-submodules, then

$$S^{-1}(IJ) = \left\{ \frac{\sum_i a_i b_i}{s} : a_i \in I, b_i \in J, s \in S \right\}$$

$$(S^{-1}I)(S^{-1}J) = \left\{ \sum_i \frac{a_i}{s_i}\frac{b_i}{t_i} \mid a_i \in I, b_i \in J, s_i, t_i \in S \right\} = \left\{ \sum_i \frac{a_i b_i \prod\limits_{i \neq j} s_j t_j}{\prod\limits_i s_i t_i} \mid a_i \in I, b_i \in J, s_i, t_i \in S \right\}.$$

Given an element in $S^{-1}(IJ)$, we can express it in the form $\sum\limits_i \frac{a_i}{s_i}\frac{b_i}{t_i}$ by taking $s_1 = s, s_i = 1$ for $i > 1$, and $t_i = 1$ for all i. Given an element of the form $\sum\limits_i \frac{a_i b_i \prod_{i \neq j} s_j t_j}{\prod_i s_i t_i}$, we know $a_i \prod\limits_{j \neq i} s_j \in I$ and $b_i \prod\limits_{j \neq i} t_j \in J$ since I and J are R-modules, and $\prod\limits_i s_i t_i \in S$, giving the reverse inclusion. So $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$.

Note also that, if $\mathfrak{a}$ is an ideal of $S^{-1}R$, then $\mathfrak{a} \cap R = \{a \mid a/s \in \mathfrak{a} \text{ for some } s \in S\}$ is an ideal of R: the intersection of submodules is a submodule, and the $S^{-1}R$-action on $\mathfrak{a}$ restricts to an action of R on $\mathfrak{a}$; hence both $\mathfrak{a}$ and R are R-modules. Also, the extension $S^{-1}(\mathfrak{a} \cap R)$ of $\mathfrak{a} \cap R$ is $\mathfrak{a}$, since if $a/s \in \mathfrak{a}$ for some $s \in S$, then $a/s \in \mathfrak{a}$ for all $s \in S$ because $\mathfrak{a}$ is closed under multiplication by $S^{-1}R$.

Consider an ideal $\mathfrak{a}$ of $\mathfrak{o}_\mathfrak{p}$. Here, we will denote the extension of an ideal $\mathfrak{b}$ by $\mathfrak{b}_\mathfrak{p}$. $\mathfrak{a} \cap \mathfrak{o}$ has an inverse $(\mathfrak{a} \cap \mathfrak{o})^{-1}$, which is a fractional ideal of $\mathfrak{o}$. So

$$\mathfrak{a}((\mathfrak{a} \cap \mathfrak{o})^{-1})_\mathfrak{p} = ((\mathfrak{a} \cap \mathfrak{o})(\mathfrak{a} \cap \mathfrak{o})^{-1})_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}$$

thus $((\mathfrak{a} \cap \mathfrak{o})^{-1})_\mathfrak{p}$ is the inverse of $\mathfrak{a}$. Now, if $\mathfrak{b}$ is a fractional ideal of $\mathfrak{o}_\mathfrak{p}$, then there is some $c/s \in \mathfrak{o}_\mathfrak{p}$ such that $\frac{c}{s}\mathfrak{b}$ is an ideal of $\mathfrak{o}_\mathfrak{p}$. It has an inverse $\mathfrak{a}$, which is a fractional ideal. But then $\mathfrak{o}_\mathfrak{p} = (\frac{c}{s}\mathfrak{b})\mathfrak{a} = \mathfrak{b}(\frac{c}{s}\mathfrak{a})$, hence $\frac{c}{s}\mathfrak{a}$ is the inverse of $\mathfrak{b}$. So all fractional ideals of $\mathfrak{o}_\mathfrak{p}$ are invertible, thus $\mathfrak{o}_\mathfrak{p}$ is Dedekind.

In exercise 18, we show (without using this result) that prime ideals of a Dedekind domain are maximal. Thus, $\mathfrak{o}_\mathfrak{p}$ has a unique prime ideal. □

17. As for the integers, we say $\mathfrak{a} \mid \mathfrak{b}$ if there exists and ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Prove:

(a) $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$.

Proof. If $\mathfrak{a} \mid \mathfrak{b}$, then there is some ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{ac} \subseteq \mathfrak{a}$. Suppose now that $\mathfrak{b} \subseteq \mathfrak{a}$. Then $\mathfrak{ba}^{-1} \subseteq \mathfrak{aa}^{-1} = \mathfrak{o}$. There is some nonzero $k \in \mathfrak{o}$ such that $k\mathfrak{a}^{-1} \subseteq \mathfrak{o}$, so $\mathfrak{b}(k\mathfrak{a}^{-1}) \subseteq k\mathfrak{aa}^{-1} = (k)$. Thus, every element of $\mathfrak{b}(k\mathfrak{a}^{-1})$ is divisible by k, hence (k) divides $\mathfrak{b}(k\mathfrak{a}^{-1})$. So there is some ideal $\mathfrak{c}$ such that $(k)\mathfrak{c} = \mathfrak{b}(k\mathfrak{a}^{-1})$. So $(k)\mathfrak{ca} = \mathfrak{b}(k\mathfrak{a}^{-1})\mathfrak{a} = \mathfrak{b}(k)$. Since $(k) \neq 0$, it is invertible, thus $\mathfrak{ca} = \mathfrak{b}$. So $\mathfrak{a} \mid \mathfrak{b}$. □

(b) Let $\mathfrak{a}, \mathfrak{b}$ be ideals. Then $\mathfrak{a} + \mathfrak{b}$ is their greatest common divisor. In particular, $\mathfrak{a}, \mathfrak{b}$ are relatively prime if and only if $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$.

Proof. Suppose $\mathfrak{c} \mid \mathfrak{a}$ and $\mathfrak{c} \mid \mathfrak{b}$. Then $\mathfrak{c} \supseteq \mathfrak{a}$ and $\mathfrak{c} \supseteq \mathfrak{b}$, thus $\mathfrak{c} \supseteq \mathfrak{a} + \mathfrak{b}$ and so $\mathfrak{c} \mid \mathfrak{a} + \mathfrak{b}$. By definition, $\mathfrak{a} + \mathfrak{b}$ is the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$.

If $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$, then every common divisor of $\mathfrak{a}$ and $\mathfrak{b}$ contains $\mathfrak{o}$, hence the only one is $\mathfrak{o}$. So $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. Conversely, if the only common divisor of $\mathfrak{a}$ and $\mathfrak{b}$ is $\mathfrak{o}$, then the only divisor of $\mathfrak{a} + \mathfrak{b}$ is $\mathfrak{o}$. So the only ideal containing $\mathfrak{a} + \mathfrak{b}$ is $\mathfrak{o}$. So $\mathfrak{a} + \mathfrak{b}$ is not contained in a maximal ideal, hence it must be $\mathfrak{o}$. □

18. Every prime ideal $\mathfrak{p}$ is maximal. In particular, if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct primes, then the Chinese remainder theorem applies to their powers $\mathfrak{p}_1^{r_1}, \ldots, \mathfrak{p}_n^{r_n}$.

Proof. Let $\mathfrak{p}$ be a prime ideal. $\mathfrak{p}$ is contained in a maximal ideal $\mathfrak{m}$, so $\mathfrak{m} \mid \mathfrak{p}$. Due to unique factorization, $\mathfrak{m} = \mathfrak{p}$. So $\mathfrak{p}$ is maximal. By uniqueness of prime factorizations, the only divisors of $\mathfrak{p}_i^{r_i}$ are of the form $\mathfrak{p}_i^{s_i}$ for $s_i \leq r_i$, and the only factors of $\mathfrak{p}_j^{r_j}$ are of the form $\mathfrak{p}_j^{s_j}$ where $s_j \leq r_j$. The only ideal that is of both these forms has $s_i = s_j = 0$, which means it is $\mathfrak{o}$. Since $\mathfrak{p}_i^{r_i} + \mathfrak{p}_j^{r_j}$ divides $\mathfrak{p}_i^{r_i}$ and $\mathfrak{p}_j^{r_j}$, it must be $\mathfrak{o}$. So the Chinese Remainder Theorem applies. □

19. Let $\mathfrak{a}, \mathfrak{b}$ be ideals. Show that there exists an element $c \in K$ such that $c\mathfrak{a}$ is an ideal relatively prime to $\mathfrak{b}$. In particular, every ideal class in $\mathrm{Pic}(\mathfrak{o})$ contains representative ideals prime to a given ideal.

Proof. Let the prime factors of $\mathfrak{b}$ be $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, and represent $\mathfrak{a}$ as $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} \mathfrak{p}_{n+1}^{r_{n+1}} \cdots \mathfrak{p}_{n+m}^{r_{n+m}}$, where the $\mathfrak{p}_i$ are distinct primes and each $r_i \geq 0$. There exists some $a \in \mathfrak{o}$ such that $a \equiv x_i \pmod{\mathfrak{p}_i^{r_i+1}}$ for each i, where $x_i \in \mathfrak{p}_i^{r_i} \setminus \mathfrak{p}_i^{r_i+1}$. This guarantees that (a) factors as

$$(a) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} \mathfrak{a}_1^{s_1} \cdots \mathfrak{a}_k^{s_k}$$

where the $\mathfrak{a}_i$ are primes distinct from each other and from the $\mathfrak{p}_i$. Next, find $b \in \mathfrak{o}$ for which $b \equiv 0 \pmod{\mathfrak{a}_i^{s_i}}$ for all $i \leq k$, but $b \equiv 1 \pmod{\mathfrak{p}_i}$ for all $i \leq n$. Thus,

$$(b) = \mathfrak{c}\mathfrak{a}_1^{s_1} \cdots \mathfrak{a}_k^{s_k}$$

where $\mathfrak{c}$ is relatively prime to $\mathfrak{b}$ (it is possible that $\mathfrak{c}$ has some factors of $\mathfrak{a}_i$, but we have guaranteed it has no factors of any $\mathfrak{p}_i$). Letting $c = \frac{b}{a}$, we now have

$$\begin{aligned} c\mathfrak{a} &= (b)(a)^{-1}\mathfrak{a} \\ &= (\mathfrak{c}\mathfrak{a}_1^{s_1} \cdots \mathfrak{a}_k^{s_k})(\mathfrak{p}_1^{-r_1} \cdots \mathfrak{p}_n^{-r_n} \mathfrak{a}_1^{-s_1} \cdots \mathfrak{a}_k^{-s_k})(\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} \mathfrak{p}_{n+1}^{r_{n+1}} \cdots \mathfrak{p}_{n+m}^{r_{n+m}}) \\ &= \mathfrak{c}\mathfrak{p}_{n+1}^{r_{n+1}} \cdots \mathfrak{p}_{n+m}^{r_{n+m}} \end{aligned}$$

which is an ideal of $\mathfrak{o}$ relatively prime to $\mathfrak{b}$.

For a given ideal $\mathfrak{b}$ and a given ideal class $C \in \mathrm{Pic}(\mathfrak{o})$, choose any ideal $\mathfrak{a} \in C$ and let $c\mathfrak{a}$ be relatively prime to $\mathfrak{b}$. $c\mathfrak{a} \in C$ because (c) is principal, therefore C contains a representative relatively prime to any fixed ideal. □