Dedekind Rings

Remark In principal ideal rings all non-zero prime ideals are maximal ideals.

We introduce a few properties on localizations which will be used later.

Lemma 0.1. *If the ring R is noetherian and $\mathfrak{p}$ is a non-zero prime ideal of R then also the localization $R_{\mathfrak{p}}$ is noetherian.*

Proof. Let $\tilde{\mathfrak{a}}$ be an ideal of $R_{\mathfrak{p}}$. It is of the form $\frac{\mathfrak{a}}{R\setminus\mathfrak{p}}$ with an ideal $\mathfrak{a}$ of R. The ideal $\mathfrak{a}$ is finitely generated, say with generators $a_i \in R$ $(1 \leq i \leq n)$. Clearly, the same elements generate $\tilde{\mathfrak{a}}$.

□

Lemma 0.2. *Let R be a ring with prime ideals $\mathfrak{p}, \mathfrak{q}$ subject to $\mathfrak{p} \subset \mathfrak{q}$. Then the corresponding ideals*

$$\tilde{\mathfrak{p}} = \frac{\mathfrak{p}}{R \setminus \mathfrak{q}} \ , \ \tilde{\mathfrak{q}} = \frac{\mathfrak{q}}{R \setminus \mathfrak{q}}$$

are prime ideals of $R_{\mathfrak{q}}$ satisfying $\tilde{\mathfrak{p}} \subset \tilde{\mathfrak{q}}$.

Proof. We start to show that prime ideals $\mathfrak{p}$ of R which are contained in the prime ideal $\mathfrak{q}$ satisfy $\tilde{\mathfrak{p}} \cap R = \mathfrak{p}$ from which the second statement immediately follows. Clearly, we have $\mathfrak{p} \subseteq \tilde{\mathfrak{p}} \cap R$. On the other hand, any element of $\tilde{\mathfrak{p}}$ is of the form π/s with $\pi \in \mathfrak{p},\ s \in R \setminus \mathfrak{q}$. If it is contained in R as well we obtain $\pi = rs$ for some element $r \in R$. Since s is not contained in $\mathfrak{p}$ we must have $r = \pi/s \in \mathfrak{p}$, hence, $\tilde{\mathfrak{p}} \cap R \subseteq \mathfrak{p}$.

Next we show that $\tilde{\mathfrak{p}}$ is a prime ideal of $R_{\mathfrak{q}}$. If the product of two elements r/s and u/v of $R_{\mathfrak{q}}$ is contained in $\tilde{\mathfrak{p}}$ we get $ru \in \mathfrak{p}$, hence either $r \in \mathfrak{p}$ (with the consequence $r/s \in \tilde{\mathfrak{p}}$) or $u \in \mathfrak{p}$ (with the consequence $u/v \in \tilde{\mathfrak{p}}$).

Finally, $x \in \mathfrak{q} \setminus \mathfrak{p}$ also belongs to $\tilde{\mathfrak{q}}$ but not to $\tilde{\mathfrak{p}}$.

□

Lemma 0.3. *Let R be a noetherian ring. For every non-zero ideal $\mathfrak{a} \subset R$ of R there exist prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_r$ subject to*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a} \subseteq \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r \ . \tag{1}$$

Proof Let us assume that the set $\mathcal{M}$ of non-zero ideals of $\mathfrak{a} \subset R$ which do not satisfy (1) is not empty. Since R is noetherian $\mathcal{M}$ contains a maximal element, say $\mathfrak{a}$. Since $\mathfrak{a}$ itself cannot be a prime ideal there

exist elements $b, c \in R \setminus \mathfrak{a}$ with $ab \in \mathfrak{a}$. We put $\mathfrak{b} := \mathfrak{a} + Rb$, $\mathfrak{c} := \mathfrak{a} + Rc$ and obtain:

$$\mathfrak{a} \subset \mathfrak{b},\ \mathfrak{a} \subset \mathfrak{c},\ \mathfrak{bc} \subseteq \mathfrak{a}, \mathfrak{b} \subset R, \mathfrak{c} \subset R\ .$$

(We note that in case $\mathfrak{b} = R$ we had $\mathfrak{c} = \mathfrak{c}R = \mathfrak{cb} \subseteq \mathfrak{a}$, and, analogously, we conclude for $\mathfrak{c} = R$.) From this

$$\mathfrak{bc} \subseteq \mathfrak{a} \subseteq \mathfrak{b} \cap \mathfrak{c}$$

is immediate. Since $\mathfrak{b}$ and $\mathfrak{c}$ do not belong to $\mathcal{M}$ they both satisfy (1). But then also $\mathfrak{a}$ satisfies 1 in contradiction to $\mathfrak{a} \in \mathcal{M}$. □

Definition 0.4. *A unital entire ring R is called a* **Dedekind ring** *if it has the properties*

(1) *R is noetherian,*
(2) *R is integrally closed,*
(3) *in R every non-zero prime ideal is maximal.*

In what follows we assume that R is a unital entire ring with quotient field F. Clearly, the non-zero ideals of R form a multiplicative monoid with unit element R. In order to obtain a group structure (if R has additional properties) we need to introduce so-called fractional ideals since proper ideals $0 \neq \mathfrak{a} \subset R$ cannot have an inverse belonging to R but only to the full quotient ring F of R which is a field.

Definition 0.5. *Any non-zero R-module $\mathfrak{A}$ in F for which a non-zero element $a \in R$ exists such that $a\mathfrak{A}$ is an ideal $\mathfrak{a}$ of R is called a* **fractional ideal** *of R. We denote the set of all fractional ideals of R by I_R or just I.*

The usual non-zero ideals of R are also fractional ideals (with denominator 1). They are sometimes called **integral ideals**. We list several useful properties of fractional ideals.

- the product, the sum, and the intersection of fractional ideals belong to I.

  To see this we assume that the ideals are given in the form $\mathfrak{A} = \frac{1}{a}\mathfrak{a}$, $\mathfrak{B} = \frac{1}{b}\mathfrak{b}$ with ideals $\mathfrak{a}$, $\mathfrak{b}$ and elements a, b of R. We then get

$$\mathfrak{AB} = \frac{1}{ab}(\mathfrak{ab})\ \ , \mathfrak{A} + \mathfrak{B} = \frac{1}{ab}(b\mathfrak{a} + a\mathfrak{b})\ \ , \mathfrak{A} \cap \mathfrak{B} = \frac{1}{ab}(b\mathfrak{a} \cap a\mathfrak{b})\ \ .$$

- Much more important is the so-called **ring of multipliers** for an ideal $\mathfrak{A} \in I$:

$$[R/\mathfrak{A}] := \{x \in F \mid x\mathfrak{A} \subseteq R\}\ \ ,$$

respectively the **quotient of two ideals**:

$$[\mathfrak{A}/\mathfrak{B}] := \{x \in F \mid x\mathfrak{B} \subseteq \mathfrak{A}\} \ .$$

Those elements x satisfy

$$(ax)\mathfrak{b} \subseteq b\mathfrak{a}$$

so that ax fulfills Kronecker's condition and is integral. Hence, one easily sees that $[\mathfrak{A}/\mathfrak{B}]$ is indeed a fractional ideal. We remark that $[R/\mathfrak{A}]$ equals $\mathfrak{A}^{-1}$ in case $\mathfrak{A}$ is invertible. Because of $\mathfrak{A}^{-1}\mathfrak{A} = R$ we see that $\mathfrak{A}^{-1} \subseteq [R/\mathfrak{A}]$. On the other hand, if $x \in [R/\mathfrak{A}]$ satisfies $x\mathfrak{A} \subseteq R$ and therefore $xR = x\mathfrak{A}\mathfrak{A}^{-1} \subseteq R\mathfrak{A}^{-1} = \mathfrak{A}^{-1}$.

We note hat the inverse of an ideal is uniquely determined if it exists. Similarly, for invertible ideals $\mathfrak{A}$ we have $[\mathfrak{A}/\mathfrak{A}] = R$. Namely, by definition R is contained in the left-hand side; but $x \in F$ satisfying $x\mathfrak{A} \subseteq \mathfrak{A}$ upon multiplication with $\mathfrak{A}^{-1}$ also fulfills $xR \subseteq R$, hence, $x \in R$.

Lemma 0.6. *If an ideal $\mathfrak{a}$ of R is contained in an integral invertible ideal $\mathfrak{m}$ then $\mathfrak{a}$ is a multiple of $\mathfrak{m}$ with an ideal of R, namely*

$$\mathfrak{a} \ = \ (\mathfrak{a}\mathfrak{m}^{-1})\mathfrak{m} \ .$$

Conversely, if the ideal $\mathfrak{a}$ is a multiple of an ideal $\mathfrak{m}$ of R, i.e. $\mathfrak{a} = \mathfrak{m}\mathfrak{b}$ for an integral ideal $\mathfrak{b}$, then $\mathfrak{a}$ is contained in $\mathfrak{m}$.

Proof For $\mathfrak{a} \subseteq \mathfrak{m} \subseteq R$ we get $\mathfrak{a}\mathfrak{m}^{-1} \subseteq \mathfrak{m}\mathfrak{m}^{-1} = R \subseteq \mathfrak{m}^{-1}$. (The same applies to proper containment.)
For the second statement, we conclude via $\mathfrak{a} = \mathfrak{m}\mathfrak{b} \subseteq \mathfrak{m}R = \mathfrak{m}$.
□

Corollary 0.7. *If an integral ideal $\mathfrak{a}$ of R is properly contained in a maximal ideal $\mathfrak{m}$ which is invertible then*

$$\mathfrak{a} \ = \ (\mathfrak{a}\mathfrak{m}^{-1})\mathfrak{m} \ .$$

and $\mathfrak{a}\mathfrak{m}^{-1}$ is an ideal of R properly containing $\mathfrak{a}$.

Proof We only need to show that

$$\mathfrak{a}\mathfrak{m}^{-1} = \mathfrak{a}\,, \quad \text{respectively} \quad \mathfrak{a} = \mathfrak{a}\mathfrak{m} \tag{2}$$

is impossible. If the ring R is local then $\mathfrak{m}$ coincides with the Jacobson radical of R and Nakayama's Lemma tells us that (2) implies $\mathfrak{a} = 0$ contrary to our assumption.

If R is not local we apply localisation with respect to $\mathfrak{m}$. We let

$$\tilde{R} = \frac{R}{R \setminus \mathfrak{m}}\tilde{\mathfrak{m}} = \frac{\mathfrak{m}}{R \setminus \mathfrak{m}} \ , \ \tilde{\mathfrak{a}} = \frac{\mathfrak{a}}{R \setminus \mathfrak{m}} \ .$$

Again, $\tilde{\mathfrak{m}}$ is the Jacobson radical of $\tilde{R}$ and we get

$$\tilde{\mathfrak{a}} = \tilde{R}\mathfrak{a} = \tilde{R}\mathfrak{a}\mathfrak{m} = \tilde{R}\mathfrak{a}\tilde{R}\mathfrak{m} = \tilde{\mathfrak{a}}\tilde{\mathfrak{m}} \ .$$

According to Nakayama's Lemma the ideal $\tilde{\mathfrak{a}}$, and therefore also the ideal $\mathfrak{a}$, is zero.

□

As a consequence of the proof we see that a non-zero prime ideal $\mathfrak{p}$ which is contained in an invertible maximal ideal $\mathfrak{m}$ necessarily coincides with $\mathfrak{m}$. If every non-zero ideal of R is invertible then every non-zero prime ideal of R is maximal.

We show that R is also noetherian and integrally closed in that case. If the ideal $\mathfrak{a}$ satisfies $\mathfrak{a}\mathfrak{a}^{-1} = R$ we have an equation

$$\sum_{i=1}^{n} a_i b_i = 1$$

with elements $a_i \in \mathfrak{a},\ b_i \in \mathfrak{a}^{-1}$ and get

$$1 \in \left(\sum_{i=1}^{n} a_i R \right) \mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} = R \ ,$$

hence

$$\sum_{i=1}^{n} a_i R \ = \ \mathfrak{a} \ .$$

Is an element $x \in F \setminus R$ is integral over R then it satisfies an equation

$$x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n \ = \ 0 \ \ (a_i \in R) \ .$$

The fractional ideal

$$\mathfrak{a} \ := \ \sum_{i=0}^{n-1} x^i R$$

then satisfies the Kronecker condition $x\mathfrak{a} \subseteq \mathfrak{a}$ which implies $xR = x\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} = R$, hence $x \in R$ follows.

Subsequently we derive several criteria for rings to be of Dedekind type.

Theorem 0.8. *For unital entire rings R the following conditions are equivalent:*

(1) *R is a Dedekind ring.*
(2) *The fractional ideals of R form a group.*
(3) *Every non-zero ideal $\mathfrak{a}$ of R is a product of non-zero prime ideals.*

Proof The proof of this important theorem is rather lengthy. We have already seen that (2) implies (1).

(1) $\Rightarrow$ (2) and (3)

Let $\mathfrak{a}$ be a non-zero ideal of the Dedekind ring R. If $\mathfrak{a}$ has a multiplicative inverse it is necessarily $[R/\mathfrak{a}]$. Obviously, $[R/\mathfrak{a}]\mathfrak{a} \subseteq R$ and we need to show equality. We assume that the set of non-zero non-invertible ideals of R is non-empty. Since R is noetherian that set contains a maximal element, say $\mathfrak{a}$. We will show below that $\mathfrak{a}$ is a product of prime ideals. We therefore only need to show the invertibility of prime ideals (respectively, maximal ideals).

Let $\mathfrak{a}$ be a maximal ideal of R. Because of

$$\mathfrak{a} = \mathfrak{a}R \subseteq \mathfrak{a}[R/\mathfrak{a}] \subseteq R$$

we either have $\mathfrak{a} = \mathfrak{a}[R/\mathfrak{a}]$ or $\mathfrak{a}[R/\mathfrak{a}] = R$. We just need to exclude the first possibility.

Let us therefore assume $\mathfrak{a} = \mathfrak{a}[R/\mathfrak{a}]$.
Since R is noetherian the ideal $\mathfrak{a}$ is finitely generated, say $\mathfrak{a} = Ra_1 + ... + Ra_n$. For any element $x \in [R/\mathfrak{a}]$ we get

$$x(a_1, ..., a_n) \;=\; (a_1, ..., a_n)M_x$$

with a matrix $\mathcal{M}_x \in R^{n\times n}$. This is a Kronecker condition for x, hence the element x is integral over R and therefore belongs to R. It remains to show the existence of an element $x \in [R/\mathfrak{a}] \setminus R$.

For this we let $0 \neq \pi \in \mathfrak{a}$. According to 0.3 the ideal πR contains a product of non-zero prime ideals. Among all those products contained in πR we choose one with a minimal number of factors, say $\mathfrak{p}_1 \cdots \mathfrak{p}_s$. Then we have

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \;\subseteq\; \pi R \;\subseteq\; \mathfrak{a}$$

and

$$\prod_{\substack{i=1\\ i\neq j}}^{s} \mathfrak{p}_i \;\not\subseteq\; \pi R \;\; (1 \leq j \leq s) \;\; .$$

Since $\mathfrak{a}$ is a maximal ideal one of the factors $\mathfrak{p}_j$ must be contained in $\mathfrak{a}$. Reordering the $\mathfrak{p}_i$ suitably we can assume that $\mathfrak{p}_1 \subseteq \mathfrak{a}$, hence $\mathfrak{p}_1 = \mathfrak{a}$. This implies

$$\frac{1}{\pi}\prod_{i=2}^{s} \mathfrak{p}_i \;\not\subseteq\; R$$

but

$$\frac{1}{\pi}\prod_{i=s}^{s} \mathfrak{p}_i \;\subseteq\; R \;\; ,$$

and therefore

$$\frac{1}{\pi}\prod_{i=2}^{s}\mathfrak{p}_i \;\subseteq\; [R/\mathfrak{p}_1] \;=\; [R/\mathfrak{a}] \;\;.$$

This shows the existence of an element $x \in \frac{1}{\pi}\prod_{i=2}^{s}\mathfrak{p}_i \setminus R$ which belongs to $[R/\mathfrak{a}]$.

Now, we can prove that every ideal $0 \neq \mathfrak{a}$ of R is a product of prime ideals. Let us assume that there exists an ideal which is not a product of prime ideals. According to 0.3 there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ subject to

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \subset \mathfrak{a} \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k \;\;.$$

Moreover, we assume that $\mathfrak{a}$ is chosen such that k is minimal. For $k = 1$ we get $\mathfrak{p}_1 \subset \mathfrak{a}$, hence $\mathfrak{a} = R$, a contradiction. For $k > 1$ we already know that $\mathfrak{p}_1$ is invertible and obtain

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \subset \mathfrak{p}_1^{-1}\mathfrak{a} \subset \mathfrak{p}_1^{-1}\mathfrak{p}_1 = R \;\;.$$

(In case $\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_1^{-1}\mathfrak{p}_1$ we had $\mathfrak{a} = \mathfrak{p}_1$.) This implies that $\mathfrak{p}^{-1}\mathfrak{a}$ is an ideal of R which contains a product of prime ideals with a smaller number of factors than $\mathfrak{a}$. Hence, $\mathfrak{p}_1^{-1}\mathfrak{a}$ is a product of prime ideals and therefore also $\mathfrak{a} = \mathfrak{p}_1(\mathfrak{p}_1^{-1}\mathfrak{a})$.

Remark We also show that such a representation is unique up to the order of the factors. This will be needed later.

Let us assume that the ideal $\mathfrak{a}$ of R has two representations

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \;=\; \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

with ideals of $\mathbb{P}_R$. Since $\mathfrak{p}_1$ divides the right-hand side it must be contained in one of the factors $\mathfrak{q}_j$. Reordering the factors suitably we can assume that $\mathfrak{p}_1 \subseteq \mathfrak{q}_1$. Since we showed that non-zero prime ideals in rings with property (ii) are maximal we get $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying the equation by $\mathfrak{p}_1^{-1}$ we get

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \;=\; \mathfrak{q}_2 \cdots \mathfrak{q}_s \;\;.$$

A repeated application of this procedure eventually yields $r = s$ and $\mathfrak{p}_i = \mathfrak{q}_i$ for $1 \leq i \leq r$.

To finish the proof of the theorem we will also show (3) $\Rightarrow$ (2). We remark, however, that this is merely of theoretical interest and will not be needed furthermore.

(3) $\Rightarrow$ (2)

We prove the statement via several reduction steps.

(i) Since every non-zero ideal of R is a product of prime ideals it suffices to prove that all non-zero prime ideals of R are invertible.

(ii) Let $\mathfrak{p}$ be a non-zero prime ideal of R. It contains an element $0 \neq \pi \in \mathfrak{p}$. Then $R\pi$ is a product of prime ideals, say $\mathfrak{p}_1, ..., \mathfrak{p}_r$, each of which is invertible according to

$$\mathfrak{p}_i^{-1} \;=\; \frac{1}{\pi} \prod_{\substack{j=1 \\ j \neq i}}^{r} \mathfrak{p}_j \;\; .$$

On the other hand, πR and therefore $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ is contained in $\mathfrak{p}$. Hence, one of the factors of that product must be contained in $\mathfrak{p}$. By reordering the $\mathfrak{p}_i$ if necessary we can assume that $\mathfrak{p}_1 \subseteq \mathfrak{p}$. If we can show that $\mathfrak{p}_1$ is maximal we are done.

(iii) We want to show that $\mathfrak{p}_1 + Rx = R$ for all elements $x \in R \setminus \mathfrak{p}_1$. For this we choose $\pi \in \mathfrak{p}_1$ arbitrarily. We assume that

$$(\mathfrak{p}_1 + Rx)^2 \;=\; \mathfrak{p}_1 + rx^2 \tag{3}$$

which we shall prove in the next paragraph. Then we obtain

$$\pi \in \mathfrak{p}_1 + Rx^2 = (\mathfrak{p}_1 + Rx)^2 = \mathfrak{p}_1^2 + x\mathfrak{p}_1 + Rx^2 \subseteq \mathfrak{p}_1^2 + Rx \;\; . \tag{4}$$

Hence, there exist elements $q \in \mathfrak{p}_1^2$, $r \in R$ satisfying $\pi = q + rx$. Then $rx = \pi - q$ is in $\mathfrak{p}_1$ and since $\mathfrak{p}_1$ is a prime ideal we must have $r \in \mathfrak{p}_1$ implying $\mathfrak{p}_1 \subseteq \mathfrak{p}_1^2 + x\mathfrak{p}_1$. We recall that the prime ideal $\mathfrak{p}_1$ was shown to be invertible. Therefore we get

$$R \;=\; \mathfrak{p}_1\mathfrak{p}_1^{-1} \;\subseteq\; (\mathfrak{p}_1^2 + x\mathfrak{p}_1)\mathfrak{p}_1^{-1} \;\subseteq\; \mathfrak{p}_1 + xR \;\subseteq\; R \;\; .$$

Hence, the ideal $\mathfrak{p}_1$ is maximal. It must coincide with $\mathfrak{p}$ which is therefore invertible what we wanted to show.

(iv) Let $\mathfrak{p}_1$ be a prime ideal and $x \in R \setminus \mathfrak{p}_1$. We still need to show that

$$(\mathfrak{p}_1 + Rx)^2 \;=\; \mathfrak{p}_1 + rx^2 \;\; .$$

The ideals $\mathfrak{p}_1 + Rx^i \;\; (i = 1, 2)$ can be presented as products of prime ideals in the form

$$\mathfrak{p}_1 + Rx^i \;=\; \prod_{j=1}^{m} \mathfrak{q}_j^{m_{ij}} \;\; (m_{ij} \in \mathbb{Z}^{\geq 0} \,,\; m_{1j} + m_{2j} > 0) \;\; .$$

We apply the residue class map $\; : R \to R/\mathfrak{p}_1 =: \overline{R}$ to these presentations and obtain

$$\overline{x}^i \overline{R} \;=\; \prod_{j=1}^{m} \overline{\mathfrak{q}}_j^{m_{ij}} \;\; .$$

As above we conclude that all ideals $\overline{\mathfrak{q}}_j$ are invertible. We already know that a presentation of an ideal by a product of invertible prime ideals is unique up to the order of the factors. This has the consequence $2m_{1j} = m_{2j}$ and concludes the proof.

□

We list two consequences of that theorem which will be needed in a valuation theoretic characterisation of Dedekind rings in the next theorem.

Lemma 0.9. *A local Dedekind ring R is a principal ideal domain and a discrete valuation ring.*

Proof. Let $\mathfrak{p}$ be the maximal ideal of R. We choose $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then $\pi R = \mathfrak{p}\mathfrak{a}$ for some ideal $\mathfrak{a}$ of R. If $\mathfrak{a}$ is a proper ideal of R it is contained in the only maximal ideal $\mathfrak{p}$. But this would imply $\pi \in \mathfrak{p}^2$, a contradiction. Hence, $\mathfrak{a}$ equals R and the maximal ideal $\mathfrak{p}$ is a principal ideal. The corresponding exponential valuation η is a discrete valuation with valuation ring R. If $\mathfrak{a}$ is a non-zero ideal of R it contains an element a subject to $\eta(a) = \min\{\eta(x) \mid 0 \neq x \in \mathfrak{a}\}$. As above we conclude that $\mathfrak{a} = (R\pi)^{\eta(a)}$.

□

Lemma 0.10. *Let R be a unital commutative ring and $\mathfrak{p}$ be a non-zero prime ideal of R. If $\mathfrak{p}$ is contained in a maximal ideal $\mathfrak{m}$ of R for which the localisation $R_\mathfrak{m}$ is a discrete valuation ring then $\mathfrak{p}$ equals $\mathfrak{m}$.*

Proof. In the localisation $R_\mathfrak{m}$ the ideal $R_\mathfrak{m}\mathfrak{p}$ is a prime ideal which is contained in the maximal ideal $R_\mathfrak{m}\mathfrak{m}$. Because of the preceding lemma both ideals coincide. We obtain

$$\mathfrak{m} = R_\mathfrak{m}\mathfrak{m} \cap R = R_\mathfrak{m}\mathfrak{p} \cap R \subseteq \frac{\mathfrak{p}}{R \setminus \mathfrak{p}} \cap R = \mathfrak{p} \ ,$$

so that $\mathfrak{p}$ and $\mathfrak{m}$ indeed coincide.

□

Theorem 0.11. *For unital entire rings R the following conditions are equivalent:*

(1) *R is a Dedekind ring.*
(2) *For every maximal ideal $\mathfrak{m}$ of R the localization $R_\mathfrak{m}$ is a discrete valuation ring and every non-zero element $a \in R$ is contained in at most finitely many maximal ideals of R.*

(1) $\Rightarrow$ (2)

At first we show that every $a \in R \setminus 0$ is contained in at most finitely many maximal ideals. Again we use that prime ideals are maximal.

Because of the previous theorem the principal ideal aR is a product of finitely many prime ideals of R and we also showed that such a representation is unique. If a is contained in a maximal ideal $\mathfrak{m}$ then we get $aR = \mathfrak{m}(aR\mathfrak{m}^{-1})$, hence $\mathfrak{m}$ occurs in the prime ideal product representation of aR. This restricts $\mathfrak{m}$ to a finite set.

For a proof of the first statement we again note that all prime ideals are maximal.

Since R is noetherian every localisation $R_\mathfrak{p}$ of R is noetherian, too, as we saw in 0.1.

Next we prove that for every non-zero prime ideal $\mathfrak{p}$ of R the localisation $R_\mathfrak{p}$ is integrally closed. If $x \in \mathcal{Q}(R)$ is integral over $R_\mathfrak{p}$ then it satisfies an equation

$$x^n \ + \ \sum_{i=1}^{n} a_i x^{n-i} \ = \ 0 \ \ (a_i = \frac{r_i}{s_i} \text{ with } r_i \in R\,, s_i \in R \setminus \mathfrak{p}) \ .$$

Setting $s = s_1 \cdots s_n$ we see that sx is integral over R. Hence, we get $sx \in R$ and $x \in R_\mathfrak{p}$.

If $\tilde{\mathfrak{q}} = \frac{\mathfrak{q}}{R\setminus\mathfrak{p}}$ is a non-zero prime ideal of $R_\mathfrak{p}$ then we must have $\tilde{\mathfrak{q}} \subseteq \mathfrak{p}R_\mathfrak{p}$ and $\tilde{\mathfrak{q}} \cap R \subseteq \mathfrak{p}$. Since $\mathfrak{q} = \tilde{\mathfrak{q}} \cap R$ is a prime ideal of (the Dedekind ring) R we obtain $\mathfrak{q} = \mathfrak{p}$, hence $\tilde{\mathfrak{q}} = \mathfrak{q}R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$. Therefore every prime ideal of $R_\mathfrak{p}$ is maximal.

Thus we have shown that $R_\mathfrak{p}$ is a (local) Dedekind ring. By 0.9 it is therefore a discrete valuation ring. We fix a maximal ideal $\mathfrak{m}$ of R. Then we get the map

$$\nu_\mathfrak{m} \ : \ R \to \mathbb{Z} \cup \{\infty\} \ : \ \left\{ \begin{matrix} 0 \\ 0 \neq x \end{matrix} \right\} \mapsto \left\{ \begin{matrix} \infty \\ \nu_\mathfrak{m} \end{matrix} \right\}$$

if $(0) \neq xR = \mathfrak{m}^{\nu_\mathfrak{m}(xR)}\mathfrak{q}$ and $\mathfrak{m}$ does not divide $\mathfrak{q}$. Since the representation of ideals from I as products of prime ideals is unique this is indeed a map and it is easily seen that $\nu_\mathfrak{m}$ is even an exponential valuation on R. Extending it to the quotient field F we get a discrete valuation on F. Clearly, the corresponding valuation ring R_ν contains $R_\mathfrak{p}$. But any $x \notin R_\mathfrak{p}$ has a $\nu_\mathfrak{m}$- value larger than one and can therefore not belong to $R_\mathfrak{m}$.

(2) $\Rightarrow$ (1)

We start to show that R is noetherian. Let $\mathfrak{a}$ be a non-zero ideal of R and $0 \neq a \in \mathfrak{a}$. Let $\mathfrak{m}_1, ..., \mathfrak{m}_r$ be all maximal ideals of R which contain a. In the corresponding discrete valuation rings $R_{\mathfrak{m}_i}$ $(1 \leq i \leq r)$ the ideal $\mathfrak{a}R_{\mathfrak{m}_i}$ is principal according to 0.9. We can choose an element $a_i \in \mathfrak{a}$ as generator (compare 0.1). Then the ideal $\mathfrak{b} := Ra + Ra_1 + ... + Ra_r$

is contained in $\mathfrak{a}$. We will show that both ideals coincide. For this let $\mathfrak{m}$ be an arbitrary maximal ideal of R.

It satisfies $\mathfrak{a}R_\mathfrak{m} = \mathfrak{b}R_\mathfrak{m}$. For $\mathfrak{m} \in \{\mathfrak{m}_1, ..., \mathfrak{m}_r\}$ this follows from $\mathfrak{a}R_{\mathfrak{m}_i} = a_i R_{\mathfrak{m}_i} \subseteq \mathfrak{b}R_{\mathfrak{m}_i} \subseteq \mathfrak{a}R_{\mathfrak{m}_i}$. If $\mathfrak{m}$ does not contain a, however, we get $a^{-1} \in R_\mathfrak{m}$, hence $\mathfrak{b}R_\mathfrak{m} \ni 1$ and therefore $R_\mathfrak{m} \supseteq \mathfrak{a}R_\mathfrak{m} \supseteq \mathfrak{b}R_\mathfrak{m} \supseteq R_\mathfrak{m}$.

For $x \in \mathfrak{a}$ we obtain $xR_\mathfrak{m} \subseteq \mathfrak{b}R_\mathfrak{m}$, hence $x = \frac{u}{v}$ with elements $u \in \mathfrak{b}$ and $v \in R \setminus \mathfrak{m}$. The set $\mathcal{B} := \{y \in R \mid yx \in \mathfrak{b}\}$ is an ideal of R which contains v and is therefore not contained in $\mathfrak{m}$. Since $\mathfrak{m}$ was chosen arbitrarily the non-zero ideal $\mathcal{B}$ is not contained in any maximal ideal of R, it must therefore coincide with R. This implies $1 \in \mathcal{B}$ and $x \in \mathfrak{b}$.

Because of 0.10 every non-zero prime ideal $\mathfrak{p}$ of R is maximal.

We still need to show that R is integrally closed. Clearly, we have

$$R \subseteq \bigcap_{\mathfrak{m}\,\mathrm{max}} R_\mathfrak{m} \ .$$

We want to prove equality. Let x be in the intersection of the discrete valuation rings $R_\mathfrak{m}$. For each maximal ideal $\mathfrak{m}$ we can write $x = \frac{u_\mathfrak{m}}{v_\mathfrak{m}}$ with elements $u_\mathfrak{m} \in R$, $v_\mathfrak{m} \in R \setminus \mathfrak{m}$. We put $\mathcal{B} := \{y \in R \mid yx \in R\}$. Clearly, $\mathcal{B}$ is an ideal of R which contains $v_\mathfrak{m}$. It is therefore not contained in $\mathfrak{m}$. Consequently, $\mathcal{B}$ is not contained in any maximal ideal of R, it must therefore coincide with R. This implies $1 \in \mathcal{B}$ and $x \in R$.

Finally, Lemma 1.3 of the section "Integral Bases" tells us that valuation rings are integrally closed. An element $x \in R$ which is integral over R is a priori integral over any valuation ring containing R. It therefore belongs to all those valuation rings and consequently to their intersection R.

□

In the remainder of this section we consider the consequences which the concept of a Dedekind ring yields for global fields. We therefore assume that F_0 is either the rational number field $\mathbb{Q}$ (**number field case**) or a rational function field in one variable T over a finite field $\mathbb{F}_q$ (**function field case**)with Euclidean subrings $o_{F_0} = \mathbb{Z}, \mathbb{F}_q[T]$, respectively. Let E be a finite extension of F_0 of degree n. We always assume that E/F_0 is separately generated, i.e. $E = F_0(\rho)$ for a suitable o_{F_0}–integral element $\rho \in \bar{F}_0$. This is guaranteed in the number field case and it can also be achieved in the function field case by an appropriate choice of the rational function field. Then the integral closure $o_E = Cl(o_{F_0}, E)$ is a Dedekind ring. By definition it is integrally closed. Every non-zero prime ideal $\mathfrak{p}$ of o_E is maximal since the residue class ring $o_E/\mathfrak{p}$ is a finite entire ring, hence a field. To see hat the ring o_E is also noetherian is a little more complicated. Clearly, we have

$o_{F_0}[\rho] \subseteq o_E \subseteq o_{F_0}^{\#}[\rho]$ where $o_{F_0}^{\#}[\rho]$ is the dual of the free o_{F_0}–module $o_{F_0}[\rho]$ with respect to the trace bilinear form

$$Tr \ : \ E \times E \to F_0 \ : \ (x,y) \mapsto Tr_{E/F_0}(xy)$$

which is non–degenerate according to our separability assumption. Since $o_{F_0}^{\#}[\rho]$ has an o_{F_0}–basis (the dual basis to $1, \rho, ..., \rho^{n-1}$ with respect to Tr) and o_{F_0} is a principal entire ring it follows that o_E and every non-zero ideal of that ring have o_{F_0}–bases of n elements. We note that these considerations do not remain valid if we consider relative extensions E/F whence o_F is not a principal ideal ring.

We denote the set of all non-zero prime ideals of o_E by $\mathbb{P}_E$. Since o_E is a Dedekind ring every fractional ideal $\mathfrak{a}$ is a (unique) product of prime ideals. Every such ideal has an o_{F_0}–basis of n elements. On the other hand, over o_E we can generate it by just two elements.

Lemma 0.12. *Let $\mathfrak{a}$ be an integral ideal of o_E and $0 \neq a \in \mathfrak{a}$ arbitrary. Then there exists $\alpha \in \mathfrak{a}$ such that $\mathfrak{a}$ is the greatest common divisor of two principal ideals:*

$$\mathfrak{a} \ = \ ao_E + \alpha o_E \ .$$

Proof. Let $\mathfrak{a} = \prod_{\mathfrak{p} \in \mathbb{P}_E}^{k} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}$ be the prime ideal decomposition of $\mathfrak{a}$. We note that almost all exponents are zero. Likewise, we have $ao_E = \prod_{\mathfrak{p} \in \mathbb{P}_E}^{k} \mathfrak{p}^{\nu_{\mathfrak{p}}(a)}$ with $\nu_{\mathfrak{p}}(a) \geq \nu_{\mathfrak{p}}(\mathfrak{a})$. By S we denote the finite subset of $\mathbb{P}_E$ of those prime ideals $\mathfrak{p}$ with $\nu_{\mathfrak{p}}(\mathfrak{a}) > 0$ and by T the finite subset of $\mathbb{P}_E$ with $0 = \nu_{\mathfrak{p}}(\mathfrak{a}) < \nu_{\mathfrak{p}}(a)$. We choose elements $\alpha_{\mathfrak{p}} \in \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})} \setminus \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})+1}$ for all $\mathfrak{p} \in S$. By the Chinese Remainder Theorem there exists $\alpha \in o_E$ subject to $\alpha \equiv \alpha_{\mathfrak{p}} \bmod \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})+1}$ for all $\mathfrak{p} \in S$ and $\alpha \equiv 1 \bmod \mathfrak{p}$ for all $\mathfrak{p} \in T$. It is easy to see that the greatest common divisor of ao_E and of αo_E equals $\mathfrak{a}$.

□

Definition 0.13. *For integral ideals $\mathfrak{a}$ of o_E we define their* **index** *as the o_{F_0}–module index $(o_E : \mathfrak{a})$. In the number field case this is a positive integer which is also said to be the* **norm** *$N(\mathfrak{a})$ of $\mathfrak{a}$. In the function field case the index is a monic polynomial of $o_{F_0}[T]$ and we put $N(\mathfrak{a}) := q^{\deg(o_E:\mathfrak{a})}$.*

We remark that the norm of an ideal $\mathfrak{a}$ is just the determinant of a transformation matrix of a basis of o_E to a basis of $\mathfrak{a}$ in Hermite normal form.

We will show that the norm is a multiplicative function.

Lemma 0.14. *We have $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ for any two integral ideals $\mathfrak{a}, \mathfrak{b}$ of o_E.*

Proof. Since the considered ideals are power products of prime ideals it suffices to show that

$$N\left(\prod_{i=1}^{k}\mathfrak{p}_i^{m_i}\right) \;=\; \prod_{i=1}^{k} N(\mathfrak{p})^{m_i}$$

for pairwise different prime ideals $\mathfrak{p}_i \in \mathbb{P}_E$ and positive exponents m_i. We will do this in two steps. The first one is elementary. Namely,

$$N\left(\prod_{i=1}^{k}\mathfrak{p}_i^{m_i}\right) \;=\; \prod_{i=1}^{k} N(\mathfrak{p}^{m_i})$$

is just a consequence of the Chinese Remainder Theorem stating that

$$o_E/\prod_{i=1}^{k}\mathfrak{p}_i^{m_i}$$

is isomorphic to the direct product

$$\prod_{i=1}^{k} o_E/\mathfrak{p}_i^{m_i} \quad .$$

The Dedekind property of o_E is only reqired for the second step. In order to prove that $N(\mathfrak{p}^m) = N(\mathfrak{p})^m$ holds for prime ideals it suffices to show that the o_{F_0}–modules $o_E/\mathfrak{p}$ and $\mathfrak{p}^{m-1}/\mathfrak{p}^m$ are isomorphic for $m \geq 2$. We choose an element $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ and introduce the o_{F_0}–module homomorphism

$$\varphi \;:\; o_E \to \mathfrak{p}^{m-1}/\mathfrak{p}^m \;:\; x \mapsto x\pi^{m-1} + \mathfrak{p}^m \quad .$$

The kernel of φ equals $\mathfrak{p}$. It remains to show that φ is also surjective. For this we let $y \in \mathfrak{p}^{m-1}$. Because of $\pi^{m-1}o_E + \mathfrak{p}^m = \mathfrak{p}^{m-1}$ there exists an element $z \in o_E$ such that the residue classes $\pi^{m-1}z + \mathfrak{p}^m$ and $y + \mathfrak{p}^m$ coincide, hence $y = \varphi(z)$.

□

Examples

(1) Let $R = R_0[\sqrt{d}]$ be a quadratic order, i.e. $d \in R_0$ is not a square. We will discuss the form of R_0–bases of non-zero ideals $\mathfrak{a}$ of R. In general, they are given by a transformation matrix A in column reduced Hermite normal form:

$$(\alpha_1, \alpha_2) \;=\; (1, \sqrt{d})\, A \text{ with } A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\in\; R_0^{2\times 2} \text{ and } ac > 0 \quad .$$

Clearly, $\mathfrak{a} = R_0\alpha_1 + R_0\alpha_2$ is a free R_0-module of rank 2. The ideal property of $\mathfrak{a}$ additionally requires $R\mathfrak{a} \subseteq \mathfrak{a}$ which is tantamount to $\sqrt{d}\alpha_1, \sqrt{d}\alpha_2 \in \mathfrak{a}$. We obtain as necessary and sufficient conditions:

$$c \mid a\,, c \mid b\,, a \mid (cd - b^2/c) \quad . \tag{5}$$

(2) We consider the subring $R = \mathbb{Z}[\sqrt{5}]$ of the maximal order $o_E = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ of $E = \mathbb{Q}(\sqrt{5})$. The $\mathbb{Z}$-module $\mathfrak{p} := \mathbb{Z}1 + (1+\sqrt{5})\mathbb{Z}$ has index 2 in R. Because of (5) $\mathfrak{p}$ is an ideal of R, and therefore it is a maximal ideal of R. However, some easy computations show that $N(\mathfrak{p})^2 = 2^2 \neq 8 = N(\mathfrak{p}^2)$.

This shows the predominant role of the maximal order of a global field. On the other hand, we must usually start with the suborder $R = \mathbb{Z}[\rho]$ of the maximal order o_E of $E = \mathbb{Q}(\rho)$ in which arithmetic is easier in general. We would therefore like to have a transfer from the maximal ideals of R to those of o_E for as many maximal ideals as possible. Fortunately, the set of those is easy to characterize.

Definition 0.15. *Let $R \subseteq S$ be orders of E. The subset*

$$\mathfrak{F}_{S,R} := \{x \in R \mid xS \subseteq R\}$$

is called the **conductor** *of R in S. If R, S are fixed we just write $\mathfrak{F}$ for the conductor.*

Remarks It is easily seen that $\mathfrak{F}$ is an ideal of R as well as of S. Namely, for $x, y \in \mathfrak{F}$ and $r \in R\,,\ s \in S$ we get xS, $yS \subseteq R$ and therefore $(x-y)S$, rxS, $sxS = x(sS)$ are all subsets of R. Hence, the elements $x - y$, rx, sx belong to $\mathfrak{F}$. If D denotes the determinant of a transformation matrix of an R_0–basis of S to an R_0–basis of R then DS is an ideal contained in $\mathfrak{F}$. The same holds for the largest elementary divisor of such a matrix.

We want to study the relations between the non-zero ideals of S and those of R in greater detail.

Lemma 0.16. *Let R be a suborder of S of conductor $\mathfrak{F}$. Then*

$$D_S := \{\mathfrak{A} \mid 0 \neq \mathfrak{A} \text{ ideal of } S \text{ with } \mathfrak{A} + \mathfrak{F} = S\}$$

and

$$D_R := \{\mathfrak{a} \mid 0 \neq \mathfrak{a} \text{ ideal of } R \text{ with } \mathfrak{a} + \mathfrak{F} = R\}$$

satisfy:

(1) *D_S and D_R are multiplicative monoids.*

(2) $\kappa \ : \ D_R \to D_S \ : \ \mathfrak{a} \mapsto \mathfrak{a}S$ *is an isomorphism. Its inverse is* $\kappa^{-1} \ : \ D_S \to D_R \ : \ \mathfrak{A} \mapsto \mathfrak{A} \cap R$.

(3) *For any* $\mathfrak{A} \in D_S$ *the residue class rings* $S/\mathfrak{A}$ *and* $R/\mathfrak{A} \cap R$ *are isomorphic.*

Proof. (1) Clearly, the multiplication of ideals of a ring is associative. For $\mathfrak{A} + \mathfrak{F} = \mathfrak{B} + \mathfrak{F} = S$ we also obtain $S = (\mathfrak{A} + \mathfrak{F})(\mathfrak{B} + \mathfrak{F}) \subseteq \mathfrak{AB} + \mathfrak{F} \subseteq S$. Hence, we get $\mathfrak{AB} \in D_S$. (For D_R the proof is analogous.) The units of D_S, D_R are S, R, respectively.
(2) From algebra we recall that ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ of a unital ring satisfy $\mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c} \subseteq \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c})$. Equality holds in case $\mathfrak{b} \subseteq \mathfrak{a}$ or $\mathfrak{c} \subseteq \mathfrak{a}$. We will also use $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$ in case $\mathfrak{a} + \mathfrak{b} = R$.
For establishing an isomorphism between D_R and D_S we introduce the mapping

$$\kappa \ : \ D_R \to D_S \ : \ \mathfrak{a} \mapsto S\mathfrak{a} \ .$$

For any $\mathfrak{a} \in D_R$ the image $\kappa(\mathfrak{a})$ is an ideal of S. Because of $S\mathfrak{a} + \mathfrak{F} = S(\mathfrak{a}+\mathfrak{F}) = SR = S$ it belongs to D_S. Clearly, we have $\kappa(\mathfrak{ab}) = \kappa(\mathfrak{a})\kappa(\mathfrak{b})$ so that κ is a homomorphism.
Next we prove that κ is injective. For this it suffices to show that the intersection of $\kappa(\mathfrak{a})$ with R is $\mathfrak{a}$. We conclude as follows:

$$\begin{aligned} \mathfrak{a} &\subseteq S\mathfrak{a} \cap R \\ &= S\mathfrak{a} \cap (\mathfrak{a} + \mathfrak{F}) \\ &= S\mathfrak{a} \cap \mathfrak{a} + S\mathfrak{a} \cap \mathfrak{F} \\ &= \mathfrak{a} + S\mathfrak{a}\mathfrak{F} \\ &= \mathfrak{a} + \mathfrak{a}\mathfrak{F} \\ &= \mathfrak{a} \ . \end{aligned}$$

For proving the surjectivity of κ we choose an arbitrary ideal $\mathfrak{A} \in D_S$. Intersecting $S = \mathfrak{A}+\mathfrak{F}$ with R we get $R = R\cap(\mathfrak{A}+\mathfrak{F}) = R\cap\mathfrak{A}+R\cap\mathfrak{F} = R\cap\mathfrak{A}+\mathfrak{F}$ and the ideal $R\cap\mathfrak{A}$ is in D_R. All we need to show is therefore $S(R \cap \mathfrak{A}) = \mathfrak{A}$:

$$\begin{aligned} \mathfrak{A} &= \mathfrak{A}R \\ &= \mathfrak{A}(R \cap \mathfrak{A} + \mathfrak{F}) \\ &= \mathfrak{A}(R \cap \mathfrak{A}) + \mathfrak{A}\mathfrak{F} \\ &= \mathfrak{A}(R \cap \mathfrak{A}) + \mathfrak{A} \cap \mathfrak{F} \\ &= \mathfrak{A}(R \cap \mathfrak{A}) + R \cap \mathfrak{A} \cap \mathfrak{F} \\ &= \mathfrak{A}(R \cap \mathfrak{A}) + (R \cap \mathfrak{A})\mathfrak{F} \\ &= (\mathfrak{A} + \mathfrak{F})(R \cap \mathfrak{A}) \\ &= S(R \cap \mathfrak{A}) \ . \end{aligned}$$

(3) For an ideal $\mathfrak{A} \in D_S$ we consider the map

$$\varphi \ : \ R \to S/\mathfrak{A} \ : \ r \mapsto r + \mathfrak{A} \ .$$

φ is clearly a ring homomorphism with kernel $R \cap \mathfrak{A}$. We show that φ is also surjective. For this let s be an arbitrary element of $S = \mathfrak{A} + \mathfrak{F}$. Hence, there are elements $a \in \mathfrak{A}$ and $f \in \mathfrak{F} \subseteq R$ with $s = a + f$. This yields $s + \mathfrak{A} = f + \mathfrak{A} = \varphi(f)$. Then the homomorphism theorem for rings states

$$S/\mathfrak{A} \cong R/\ker(\varphi) \ .$$

□

If the superorder S of R is maximal then all ideals of D_S are invertible. In that case we get the following corollary.

Corollary 0.17. *If R is a suborder of the maximal order o_E of E of conductor $\mathfrak{F}$ the semigroups $D_E := D_{o_E}$, D_R of the previous lemma satisfy:*

(1) *Every ideal $\mathfrak{a} \in D_R$ is a product of maximal ideals of R and the multiplicity of each maximal ideal in that product is uniquely determined.*
(2) *D_L, D_R are monoids with cancellation law: $\mathfrak{ac} = \mathfrak{bc}$ yields $\mathfrak{a} = \mathfrak{b}$ in D_R, and similarly in D_E.*

Proof

(1) Any ideal $\mathfrak{A}$ of D_E has a unique presentation as a product of prime ideals of o_E, say

$$\mathfrak{A} \ = \ \prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \ . \tag{6}$$

Applying κ^{-1} to this equation yields

$$\mathfrak{a} := \mathfrak{A} \cap R = \kappa^{-1}(\mathfrak{A}) = \prod_{i=1}^{r} (\kappa^{-1}(\mathfrak{P}_i))^{e_i} \ . \tag{7}$$

Since every prime ideal $\mathfrak{P}_i$ is a maximal ideal of o_E we conclude from part (3) of the preceding lemma that all ideals $\kappa^{-1}(\mathfrak{P}_i) = \mathfrak{P}_i \cap R$ are maximal ideals of R. Eventually the presentation in (7) is unique since that in (6) is unique and κ is an isomorphism.
(2) The cancellation law in D_E holds since o_E is a Dedekind ring, every non-zero ideal has a multiplicative inverse. The cancellation law for D_R then is a consequence of the first part of this corollary.

□

The relation between ideals of a suborder R and the maximal order o_E will now be used to exhibit the decomposition of primes in a finite separable extension. Let us assume that E/F is a finite separable extension of degree n. As a generator of E over F we choose a zero ρ of a monic polynomial of degree n, say $f(t) = t^n + a_1 t^{n-1} + ... + a_{n-1} + a_n \in o_F[t]$. Then the ideal decomposition of the ideal $\mathfrak{p}R$ of a prime ideal $\mathfrak{p}$ of o_F in $R = o_F[\rho]$ can be obtained from a modulo $\mathfrak{p}$ factorisation of $f(t)$. By the preceding corollary that can be lifted to a decomposition of $\mathfrak{p}o_E$ for those ideals $\mathfrak{p}R$ which are comaximal to the conductor $\mathfrak{F} = \mathfrak{F}_{o_E,R}$.

For this we consider the ring epimorphism

$$: \ o_F[t] \to o_F/\mathfrak{p}o_F[t] \ : \ \sum_{i=0}^{m} g_i t^i \mapsto \sum_{i=o}^{m} (g_i + \mathfrak{p})t^i$$

which is used for the introduction of the map

$$\Phi \ : \ R \to \overline{o_F}[t]/\overline{f}(t)\overline{o_F}[t] \ : \ g(\rho) = \sum_{i=0}^{m} g_i \rho^i \mapsto (\overline{g}(t) + \overline{f}(t)\overline{o_F}[t]) \ .$$

We note that the representation of an element of R as a polynomial in ρ with coefficients in o_F is not unique (if we do not demand that the degree of that polynomial is less than n). Hnece, we need to show that Φ is well defined. Since $f(t)$ is the minimal polynomial of ρ over o_F two representations of an element $x \in R$ in the form $g(\rho) = h(\rho)$ with polynomials $g, h \in o_F[t]$ imply that $f(t)$ divides the difference $g(t) - h(t)$. But then also $\overline{f}(t)$ divides $\overline{g}(t) - \overline{h}(t)$ and we obtain $\Phi(g(\rho)) = \Phi(h(\rho))$. It is easy to see that Φ is a surjective ring homomorphism. Its kernel is

$$\ker(\Phi) \quad = \quad \{g(\rho) \in R \mid \overline{f}(t) \mid \overline{g}(t)\} \ .$$

We have already noted that each $x \in R$ can be presented in the form $x = g(\rho)$ with a polynomial $g(t) \in o_F[t]$ of degree $\deg(g) < n$. Because of $\deg(\overline{f}) = n$ we obtain

$$\ker(\Phi) \quad = \quad \{g(\rho) \in R \mid \overline{g}(t) = 0\} = \quad \mathfrak{p}R \ .$$

The isomorphism theorem for rings yields that $R/\mathfrak{p}R$ and $\overline{o_F}[t]/\overline{f}(t)\overline{o_F}[t]$ are isomorphic.

If we assume that the ideal $\mathfrak{p}R$ is comaximal to the conductor $\mathfrak{F}$ of R in o_E then $\mathfrak{p}R$ is a product of maximal ideals of R containing $\mathfrak{p}R$. Those maximal ideals are in $1-1-$correspondence with the maximal ideals of $R/\mathfrak{p}R$ and the latter with those of $\overline{o_F}[t]/\overline{f}(t)\overline{o_F}[t]$ by the isomorphism we just established.

The maximal ideals of $\overline{o_F}[t]/\overline{f}(t)\overline{o_F}[t]$ are principal ideals whose generators are therefore monic irreducible polynomials. Let us assume that that the image $\overline{f}(t)$ of the monic polynomial $f(t) \in o_F[t]$ in $\overline{o_F}[t]$ decomposes into

$$\overline{f}(t) \quad = \quad \prod_{i=1}^{g} \overline{f}_i(t)^{e_i}$$

with monic polynomials $f_i(t) \in o_F[t]$ for which the $\overline{f}_i(t)$ remain irreducible in $\overline{o_F}[t]$. Then the maximal ideals of $\overline{o_F}[t]/\overline{f}(t)\overline{o_F}[t]$ are the g principal ideals with generators

$$\overline{f}_i(t) + \overline{f}(t)\overline{o_F}[t] \ \ (1 \leq i \leq g) \ \ .$$

From this we conclude that there exist exactly g maximal ideals in $R/\mathfrak{p}R$ which are principal with generators

$$f_i(\rho) + \mathfrak{p}R \ \ .$$

Finally, the maximal ideals of R containing $\mathfrak{p}$ are

$$f_i(\rho)R + \mathfrak{p}R$$

and the maximal ideals of o_E containing $\mathfrak{p}$ are

$$f_i(\rho)o_E + \mathfrak{p}o_E \ \ (1 \leq i \leq g) \ \ .$$

Thus we proved the first part of the following theorem.