7. Localization

To prove Theorem 6.1 it becomes necessary to be able to add denominators to rings (and to modules), even when the rings have zero-divisors. It is a tool used all the time in commutative algebra, so we shall give some more results than strictly necessary for proving the Cohen-Seidenberg theorems. In the beginning there are a lot of straightforward verification to make, but they are all easy.

Let R be a ring and M an R-module. A multilpicatively closed subset D of R is a subset of R containing $\mathbf{1}$ and such that if $d_1, d_2 \in D$ then also $d_1 d_2 \in D$. The most important example is the complement of a prime ideal $D = R\backslash\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal, since if two elements are not in $\mathfrak{p}$ then the product is not in $\mathfrak{p}$ either.

We modify the way we constructed the field $\mathbb{Q}$ starting from the integers $\mathbb{Z}$. We first define an equivalence relation on the cartesian product set $D \times M$ (and in particular on $D \times R$).

Lemma 7.1. *Let M be a R-module and $D \subset R$ a multiplicatively closed subset.*

(i) The following defines an equivalence relation on the cartesian product $D \times M$:

$$(d_1, m_1) \sim (d_2, m_2) \iff \exists\, d_3 \in D : d_3 d_1 m_2 = d_3 d_2 m_1.$$

(ii) If $(d_1, m_1) \sim (d_1', m_1')$ and $(d_2, m_2) \sim (d_2', m_2')$ then

$$(d_1 d_2, d_1 m_2 + d_2 m_1) \sim (d_1' d_2', d_1' m_2' + d_2' m_1').$$

(iii) If $(d_1, r_1) \sim (d_1', r_1')$ in $D \times R$ and $(d_2, m_2) \sim (d_2', m_2')$ in $D \times M$, then

$$(d_1 d_2, r_1 m_2) \sim (d_1' d_2', r_1' m_2')$$

in $D \times M$.

Proof. (i) Since $1 \in D$ we have $1dm = 1dm$ it follows that $(d, m) \sim (d, m)$.

If $(d_1, m_1) \sim (d_2, m_2)$ there exists a $d_3 \in D$ such that $d_3 d_1 m_2 = d_3 d_2 m_1$ so also $(d_2, m_2) \sim (d_1, m_1)$.

If $(d_1, m_1) \sim (d_2, m_2) \sim (d_3, m_3)$ there exist $d_4, d_5 \in D$ such that $d_4 d_1 m_2 = d_4 d_2 m_1$ and $d_5 d_2 m_3 = d_5 d_3 m_2$. So

$$d_2 d_4 d_5 d_1 m_3 = d_1 d_4 d_5 d_2 m_3 = d_1 d_4 d_5 d_3 m_2 = d_3 d_5 d_4 d_1 m_2 = d_3 d_5 d_4 d_2 m_1 = d_2 d_4 d_5 d_3 m_1,$$

and $(d_1, m_1) \sim (d_3, m_3)$ since $d_2 d_4 d_5 \in D$. So $\sim$ is indeed an equivalence relation.

(ii) There exist $d_1'', d_2'' \in D$ such that $d_1'' d_1 m_1' = d_1'' d_1' m_1$ and $d_2'' d_2 m_2' = d_2'' d_2' m_2$. So

$$\begin{aligned} d_1'' d_2'' d_1' d_2' (d_1 m_2 + d_2 m_1) &= d_1 d_1' d_1'' d_2'' d_2' m_2 + d_2 d_2' d_2'' d_1'' d_1' m_1 \\ &= d_1 d_1' d_1'' d_2'' d_2 m_2' + d_2 d_2' d_2'' d_1'' d_1 m_1' \\ &= d_1'' d_2'' d_1 d_2 (d_1' m_2' + d_2' m_1') \end{aligned}$$

(iii) There exist $d_1'', d_2'' \in D$ such that $d_1'' d_1 r_1' = d_1'' d_1' r_1$, $d_2'' d_2 m_2' = d_2'' d_2' m_2$. So

$$\begin{aligned} d_1'' d_2'' d_1 d_2 r_1' m_2' &= (d_1'' d_1 r_1')(d_2'' d_2 m_2') \\ &= (d_1'' d_1' r_1)(d_2'' d_2 m_2') \\ &= d_1'' d_2'' d_1' d_2' r_1 m_2. \end{aligned}$$

□

We write $\frac{m}{d}$ for the equivalence class of (d, m), and $D^{-1}M$ for the set of equivalence classes on $D \times M$. The lemma shows that the addition

$$\frac{m_1}{d_1} + \frac{m_2}{d_2} := \frac{d_1 m_2 + d_2 m_1}{d_1 d_2}$$

is well defined on $S^{-1}M$, and that the multiplication

$$\frac{r_1}{d_1} \cdot \frac{m_2}{d_2} := \frac{r_1 m_2}{d_1 d_2}$$

of an $\frac{r_1}{d_1} \in D^{-1}R$ and an $\frac{m_2}{d_2} \in D^{-1}M$ is also well defined.

Lemma 7.2. *Let M be a R-module and $D \subset R$ a multiplicatively closed subset.*

(i) $D^{-1}R$ with the addition and internal multiplication just defined is a ring with unit $1 = \frac{1}{1}$ and $0 = \frac{0}{1}$. It is the zero ring if and only if $0 \in D$.

(ii) $D^{-1}M$ with the addition and external multiplication just defined is a $D^{-1}R$-module. $D^{-1}M = 0$ if and only if for all $m \in M$ there exists a $d \in D$ such that $dm = 0$.

(iii) Suppose $f : M \to N$ is an R-module homomorphism. Then $D^{-1}f : D^{-1}M \to D^{-1}N$ defined by $(D^{-1}f)(\frac{m}{d}) := \frac{f(m)}{d}$ is a $D^{-1}R$-module homomorphism.

(iv) Suppose $f : R \to S$ is a ring homomorphism. Then $f(D) \subset S$ is a multiplicatively closed subset and $D^{-1}f : D^{-1}R \to f(D)^{-1}S$ defined by $(D^{-1}f)(\frac{r}{d}) := \frac{f(r)}{f(d)}$ is a ring homomorphism.

(v) The map $\nu : R \to D^{-1}R : r \to \frac{r}{1}$ is a ring homomorphism. The kernel of ν is

$$\{r \in R; \exists\ d \in D : dr = 0\}.$$

In particular, the map is injective when R is an integral domain.

(vi) We can consider $D^{-1}M$ as an R-module by $r \cdot \frac{m}{d} := \frac{rm}{d}$. Then the map $\nu : M \to D^{-1}M : m \to \frac{m}{1}$ is an R-module homomorphism.

Proof. (i) and (ii) We shall constantly use that R is a ring and M an R-module. The verifications are a bit long but straightforward.

Associativity of addition:

$$\begin{aligned}(\frac{m_1}{d_1} + \frac{m_2}{d_2}) + \frac{m_3}{d_3} &= \frac{d_1 m_2 + d_2 m_1}{d_1 d_2} + \frac{m_3}{d_3} = \frac{d_1 d_2 m_3 + d_3(d_1 m_2 + d_2 m_1)}{(d_1 d_2) d_3} = \\ &= \frac{d_1 d_2 m_3 + d_1 d_3 m_2 + d_2 d_3 m_1}{d_1 d_2 d_3} = \frac{d_1(d_3 m_2 + d_2 m_3) + d_2 d_3 m_1}{d_1(d_2 d_3)} = \\ &= \frac{m_1}{d_1} + \frac{d_3 m_2 + d_2 m_3}{d_2 d_3} = \frac{m_1}{d_1} + (\frac{m_2}{d_2} + \frac{m_3}{d_3}).\end{aligned}$$

Commutativity of addition:

$$\begin{aligned}\frac{m_1}{d_1} + \frac{m_2}{d_2} &= \frac{d_1 m_2 + d_2 m_1}{d_1 d_2} = \frac{d_2 m_1 + d_1 m_2}{d_2 d_1} = \\ &= \frac{m_2}{d_2} + \frac{m_1}{d_1}.\end{aligned}$$

We have

$$\frac{m}{d} + \frac{-m}{d} = \frac{-dm + dm}{dd} = \frac{0}{dd} = \frac{0}{1} = 0$$

since $(dd, 0) \sim (1, 0)$. So $(D^{-1}M, +)$ is a commutative group.

The associativity:

$$\begin{aligned}(\frac{r_1}{d_1}\frac{r_2}{d_2})\frac{m_3}{d_3} &= \frac{r_1r_2}{d_1d_2}\cdot\frac{m_3}{d_3} = \frac{(r_1r_2)m_3}{(d_1d_2)d_3} = \frac{r_1(r_2m_3)}{d_1(d_2d_3)} = \\ &= \frac{r_1}{d_1}(\frac{r_2}{d_2}\frac{m_3}{d_3}).\end{aligned}$$

The distributivity laws:

$$\begin{aligned}\frac{r_1}{d_1}(\frac{m_2}{d_2}+\frac{m_3}{d_3}) &= \frac{r_1}{d_1}\cdot\frac{d_3m_2+d_2m_3}{d_2d_3} = \frac{r_1(d_3m_2+d_2m_3)}{d_1d_2d_3} = \\ &= \frac{d_2r_1m_3+d_3r_1m_2}{d_1d_2d_3} = \frac{d_1d_2r_1m_3+d_1d_3r_1m_2}{d_1d_2d_1d_3} = \\ &= \frac{r_1m_2}{d_1d_2}+\frac{r_1m_3}{d_1d_3} = \frac{r_1}{d_1}\frac{m_2}{d_2}+\frac{r_1}{d_1}\frac{m_3}{d_3}.\end{aligned}$$

$$\begin{aligned}(\frac{r_1}{d_1}+\frac{r_2}{d_2})\frac{m_3}{d_3} &= \frac{d_1r_2+d_2r_1}{d_1d_2}\frac{m_3}{d_3} = \frac{(d_1r_2+d_2r_1)m_3}{d_1d_2d_3} = \\ &= \frac{d_1r_2m_3+d_2r_1m_3}{d_1d_2d_3} = \frac{d_1d_3r_2m_3+d_2d_3r_1m_3}{d_1d_3d_2d_3} = \\ &= \frac{r_1m_3}{d_1d_3}+\frac{r_2m_3}{d_2d_3} = \frac{r_1}{d_1}\frac{m_3}{d_3}+\frac{r_2}{d_2}\frac{m_3}{d_3}.\end{aligned}$$

Commutativity of multiplication in $D^{-1}R$:

$$\frac{r_1}{d_1}\frac{r_2}{d_2} = \frac{r_1r_2}{d_1d_2} = \frac{r_2r_1}{d_2d_1} = \frac{r_2}{d_2}\frac{r_1}{d_1}.$$

The unit is $1 = \frac{1}{1}$:

$$\frac{1}{1}\frac{m}{d} = \frac{1m}{1d} = \frac{m}{d}.$$

We have $0 = 1$ in $D^{-1}R$ if and only if there exists a $d \in D$ such that $d = d\cdot 1 = d\cdot 0 = 0$, i.e., if $0 \in D$. By definition $\frac{m}{d} = 0$ if and only if there exists a $d' \in D$ such that $d'm = d'd0 = 0$.

(iii) Let $\frac{m_1}{d_1}, \frac{m_2}{d_2} \in D^{-1}M$ and $\frac{r}{d_3} \in D^{-1}R$. Then

$$\begin{aligned}(D^{-1}f)(\frac{r}{d_3}\frac{m_1}{d_1}+\frac{m_2}{d_2}) &= (D^{-1}f)(\frac{d_2rm_1+d_3d_1m_2}{d_3d_1d_2}) = \frac{f(d_2rm_1+d_3d_1m_2)}{d_3d_1d_2}) = \\ &= \frac{d_2rf(m_1)+d_3d_1f(m_2)}{d_3d_1d_2}) = \frac{r}{d_3}\frac{f(m_1)}{d_1}+\frac{f(m_2)}{d_2} = \\ &= \frac{r}{d_3}(D^{-1}f)(\frac{m_1}{d_1})+(D^{-1}f)(\frac{m_2}{d_2}).\end{aligned}$$

So $D^{-1}f$ is indeed a $D^{-1}R$-module homomorphism.

(iv) We skip the proof.

(v) and (vi) This follows from $\frac{m}{1}+\frac{m'}{1} = \frac{1m'+1m}{1\cdot 1} = \frac{m+m'}{1}$ and $r\cdot\frac{m}{1} = \frac{r}{1}\cdot\frac{rm}{1} = \frac{rm}{1\cdot 1} = \frac{rm}{1}$. If $r \in R$ is in the kernel, then $\frac{r}{1} = 0$, i.e., there exist a $d \in D$ such that $dr = 0$. □

Proposition 7.1. *Let R be a ring with a multiplicatively closed subset D. Let $f : R \to S$ be a ring homomorphism such that for all $d \in D$ the image $f(d) \in S$ is a unit. Then f factors uniquely through $\nu : R \to D^{-1}R$: there is a unique ring homomorphism $g : D^{-1}R \to S$ such that $f = g \circ \nu$.*

Proof. Existence: Let $\frac{r_1}{d_1} = \frac{r_2}{d_2}$, i.e, there exists a $d_3 \in D$ such that $d_3d_2r_1 = d_3d_1r_2$. So $f(d_3)f(d_2)f(r_1) = f(d_3)f(d_1)f(r_2)$, and since $f(d)$ is a unit in S for every $d \in D$, we get $f(d_1)^{-1}f(r_1) = f(d_2)^{-1}f(r_2)$. This shows that the map $g(\frac{r}{d}) := f(d)^{-1}f(r)$ is well defined. We check that g is a ring homomorphism. Let $\frac{r_1}{d_1}, \frac{r_2}{d_2}$ then

$$g(\frac{r_1}{d_1}) + g(\frac{r_2}{d_2}) = f(d_1)^{-1}f(r_1) + f(d_2)^{-1}f(r_2) = f(d_1d_2)^{-1}(f(d_2)f(r_1) + f(d_1)f(r_2)) = g(\frac{r_1}{d_1} + \frac{r_2}{d_2});$$

$$g(\frac{r_1}{d_1}) \cdot g(\frac{r_2}{d_2}) = f(d_1)^{-1}f(r_1) \cdot f(d_2)^{-1}f(r_2) = f(d_1d_2)^{-1}f(r_1r_2) = g(\frac{r_1}{d_1} \cdot \frac{r_2}{d_2})$$

and $g(1) = g(\frac{1}{1}) = f(1)^{-1}f(1) = 1$.

Unicity: Suppose $\tilde{g} : g : D^{-1}R \to S$ exists such that $f = \tilde{g} \circ \nu$. Then

$$\tilde{g}(\frac{1}{d}) = \tilde{g}((\frac{d}{1})^{-1}) = (\tilde{g}(\frac{d}{1}))^{-1} = (\tilde{g} \circ \nu(d))^{-1} = f(d)^{-1}.$$

So

$$\tilde{g}(\frac{r}{d}) = \tilde{g}(\frac{r}{1})\tilde{g}(\frac{1}{d}) = f(r)f(d)^{-1} = g(\frac{r}{d}),$$

i.e. $\tilde{g} = g$. □

Example 7.1. For any prime ideal $\mathfrak{p}$ of R its complement $D := R\backslash\mathfrak{p}$ is a multiplicatively closed subset We write $M_\mathfrak{p} := D^{-1}M$ in this case.

For any $f \in R$ the set $D = \{1, f, f^2, \ldots, f^i, \ldots\}$ is a multiplicatively closed subset of R. In this case we write $M_f := D^{-1}M$. The ring R_f is isomorphic to the ring $R[X]/(Xf - 1)$ used in the proof of the last version of the Nullstellensatz.

The subset $D \subset R$ of non zero-divisors is also a multiplicative subset. In that case we write $D^{-1}R = Q(R)$, the maximal fraction ring of R. If R is a domain, $Q(R)$ is the quotient field of R.

7.1. **Exactness of localization.** A sequence of R-module homomorphisms

$$\ldots \xrightarrow{\delta_{i+2}} M_{i+1} \xrightarrow{\delta_{i+1}} M_i \xrightarrow{\delta_i} M_{i-1} \xrightarrow{\delta_{i-1}} \ldots$$

is called *exact* if for all i we have $\mathrm{Im}(\delta_{i+1}) = \mathrm{Ker}\,\delta_i$. Localizing keeps this property intact, we say that *localizing is an exact operation.* This is a very important property of localizing.

A *short exact sequence* is an exact sequence of the form

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0;$$

i.e., f is injecive, g is surjective and the image of f equals the kernel of g.

Proposition 7.2. *The localized sequence of an exact sequence of R-modules*

$$\ldots \overset{D^{-1}\delta_{i+2}}{\longrightarrow} D^{-1}M_{i+1} \overset{D^{-1}\delta_{i+1}}{\longrightarrow} D^{-1}M_i \overset{D^{-1}\delta_i}{\longrightarrow} D^{-1}M_{i-1} \overset{D^{-1}\delta_{i-1}}{\longrightarrow} \ldots$$

is an exact sequence of $D^{-1}R$-modules.

In particular, localization preserves injectivity and surjectivity.

Proof. Fix i. Let $\frac{m_{i+1}}{d_{i+1}} \in D^{-1}M_{i+1}$, then

$$(D^{-1}\delta_i \circ D^{-1}\delta_{i+1})(\frac{m_{i+1}}{d_{i+1}}) = \frac{\delta_i \circ \delta_{i+1}(m_{i+1})}{d_{i+1}} = 0$$

since $\delta_{i+1}(m_{i+1}) \in \operatorname{Im}\delta_{i+1} = \operatorname{Ker}\delta_i$. So $\operatorname{Im} D^{-1}\delta_{i+1} \subseteq \operatorname{Ker} D^{-1}\delta_i$. Conversely, let $\frac{m_i}{d_i} \in \operatorname{Ker} D^{-1}\delta_i$, i.e. $\frac{\delta_i(m_i)}{d_i} = 0$, i.e. there is a $d \in D$ such that $d\delta_i(m_i) = 0 = \delta_i(dm_i)$. So $dm_i \in \operatorname{Ker}\delta_i = \operatorname{Im}\delta_{i+1}$, say $dm_i = \delta_{i+1}(m_{i+1})$ and $(D^{-1}\delta_{i+1})(\frac{m_{i+1}}{dd_i}) = \frac{dm_i}{dd_i} = \frac{m_i}{d_i} \in \operatorname{Im}(D^{-1}\delta_{i+1})$. □

Corollary 7.1. *(i) If N is a submodule of M, then $D^{-1}N$ is a submodule of $D^{-1}M$ and $D^{-1}(M/N)$ is isomorphic to $D^{-1}M/D^{-1}N$.*

(ii) If M_1 and M_2 are two R-modules, then $D^{-1}(M_1 \oplus M_2) \simeq D^{-1}M_1 \oplus D^{-1}M_2$. If N_1, N_2 are two submodules of M then $D^{-1}(N_1 \cap N_2) = D^{-1}N_1 \cap D^{-1}N_2$ and $D^{-1}(N_1 + N_2) = D^{-1}N_1 + D^{-1}N_2$.

(iii) Every $D^{-1}R$-submodule of $D^{-1}M$ is of the form $D^{-1}N$. It follows that if M is a Noetherian R-module, then $D^{-1}M$ is a Noetherian $D^{-1}R$.

Proof. (i) Localizing the short exact sequence

$$0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} M/N \longrightarrow 0,$$

we get the short exact sequence

$$0 \longrightarrow D^{-1}N \xrightarrow{f} D^{-1}M \xrightarrow{g} D^{-1}M/N \longrightarrow 0,$$

from which follows that $D^{-1}N$ is a submodule of $D^{-1}M$ and $D^{-1}(M/N)$ is isomorphic to $D^{-1}M/D^{-1}N$.

(ii) The map

$$D^{-1}(M_1 \oplus M_2) \to D^{-1}M_1 \oplus D^{-1}M_2 : \frac{(m_1, m_2)}{d} \mapsto (\frac{m_1}{d}, \frac{m_2}{d})$$

is an $D^{-1}R$-module homomorphism, as is straightforwardly checked, with inverse

$$(\frac{m_1}{d_1}, \frac{m_2}{d_2}) \mapsto \frac{(d_2m_1, d_1m_2)}{d_1d_2}.$$

Similarly it is shown that

$$D^{-1}(N_1 + N_2) \to D^{-1}N_1 + D^{-1}N_2 : \frac{(n_1 + n_2)}{d} \mapsto (\frac{n_1}{d} + \frac{n_2}{d})$$

is an $D^{-1}R$-module isomorphism

The exactness of the sequence

$$0 \longrightarrow N_1 \cap N_2 \longrightarrow M \longrightarrow M/N_1 \oplus M/N_2,$$

gives the exactness of

$$0 \longrightarrow D^{-1}(N_1 \cap N_2) \longrightarrow D^{-1}M \xrightarrow{f} D^{-1}M/D^{-1}N_1 \oplus D^{-1}M/D^{-1}N_2,$$

where we used the isomorphism $D^{-1}(M/N_1 \oplus M/N_2) \simeq D^{-1}M/D^{-1}N_1 \oplus D^{-1}M/D^{-1}N_2$. Since the kernel of f is $D^{-1}N_1 \cap D^{-1}N_2$, we get the isomorphism $D^{-1}(N_1 \cap N_2) = D^{-1}N_1 \cap D^{-1}N_2$.

We could also have started from the short exact sequence

$$0 \longrightarrow N_1 \cap N_2 \longrightarrow N_1 \oplus N_2 \longrightarrow N_1 + N_2 \longrightarrow 0.$$

(iii) We use the map $\nu : M \to D^{-1}M$. Let U be a $D^{-1}R$-submodule of M. Put $N := \nu^{-1}(U)$ for its preimage in M. It is an R-submodule of M. Then $\nu(N) = D^{-1}N$ is a $D^{-1}R$-submodule of U. Let $\frac{m}{d} \in U$, then $\frac{m}{1}$ is also in U, hence $m \in N$ and $\frac{m}{d} \in D^{-1}N$. So $D^{-1}N = U$.

If N is finitely generated by $n_1, \ldots, n_r$, then U is finitely generated by $\frac{n_1}{1}, \ldots, \frac{n_r}{1}$. So if M is Noetherian, then also $D^{-1}M$ is Noetherian. □

In particular, if $I \lhd R$ is an ideal then $D^{-1}I \lhd D^{-1}R$ is also an ideal, it is the ideal generated by the image $\nu(I)$. Every ideal J of $D^{-1}R$ is of the form $D^{-1}I$ for some ideal $I \lhd R$ (we can take $I = \nu^{-1}(J)$). If $I = (r_1, \dots, r_m)$ then $D^{-1}I = (\frac{r_1}{1}, \dots, \frac{r_m}{1})$. So if R is noetherian then also $D^{-1}R$ is Noetherian.

7.2. **Correspondence theorems.** Fix a ring homomorphism $f : R \to S$. For any ideal $I \lhd R$ write $I^e \lhd S$, the *extension* of I, for the ideal generated by the image $f(I)$. For any ideal $J \lhd S$ write $J^c \lhd R$, the *contraction*, for the preimage ideal $f^{-1}(J)$. Clearly, if $I_1 \subseteq I_i$ then also $I_1^e \subseteq I_2^e$, and if $J_1 \subseteq J_2$ then $J_1^c \subseteq J_2^c$. Write $\mathcal{C}$ for the collection of all contracted ideals in R, and $\mathcal{E}$ for the collection of all extended ideals in S. These to sets are in natural bijection and induce a correspondence theorem.

Proposition 7.3 (Correspondence theorem for $f : R \to S$)**.** *(i) For any ideal $I \subseteq R$ we have $I \subseteq I^{ec}$ and $I^{ece} = I^e$. For any ideal $J \subseteq S$ we have $J^{ce} \subseteq J$ and $J = J^{cec}$.*

(ii) The operations $()^e$ and $()^c$ give bijections between $\mathcal{C}$ and $\mathcal{E}$, preserving the inclusion relation $\subseteq$.

(iii) If $J_1, J_2 \in \mathcal{E}$, then $J_1 \cdot J_2 \in \mathcal{E}$ and $J_1 + J_2 \in \mathcal{E}$. If $I_1, I_2 \in \mathcal{C}$, then $I_1 \cap I_2 \in \mathcal{C}$ and $\sqrt{I_1} \in \mathcal{C}$.

Proof. (i) Let $r \in I$, then $f(r) \in I^e$, so $r \in I^{ec}$. The ideal J^{ce} is the ideal generated by $f(J^c)$. If $r \in J^c$ then $f(r) \in J$, so the ideal generated by $f(J^c)$ is contained in the ideal J. Since $I \subseteq I^{ec}$ we get $I^e \subseteq I^{ece}$, and since $(I^e)^{ce} \subseteq I^e$ we conclude $I^{ece} = I^e$. That $J^c = J^{cec}$ is proved similarly.

(ii) Every ideal in $\mathcal{C}$ is of the form J^c for some ideal $J \subseteq S$, and every ideal in $\mathcal{E}$ is of the form I^e, for some ideal $I \subset R$. Since $I^{ece} = I^e$ and $J^c = J^{cec}$ we see that contraction and extension are inverse operations.

(iii) Exercise. □

For a given ring homomorphism we have to determine what the sets $\mathcal{E}$ and $\mathcal{C}$ are to be able to profit from the correspondence theorem. If $J \subset S$ is a prime ideal, then J^c is a prime ideal of R, but if $I \subset R$ is a prime ideal of R then I^e is not a prime ideal in general. A *primary ideal* $\mathfrak{q}$ is an ideal with the property that if $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$ then there is an $n \geq 1$ such that $y^n \in \mathfrak{q}$. For example, the primary ideals in $\mathbb{Z}$ are the ideals generated by the power of a prime number. Again, if $J \subset S$ is a primary ideal, then J^c is a primary ideal of R.

Proposition 7.4. *Let $\mathfrak{a} \lhd R$ be an ideal and $\nu_{\mathfrak{a}} : R \to R/\mathfrak{a}$ the quotient map. Every ideal of $R/\mathfrak{a}$ is an extended ideal and an ideal I of R is a contracted ideal if and only if $I \supseteq \mathfrak{a}$.*

By restriction we also get a one-to-one correspondence between the set of prime ideals (resp. primary ideals, maximal ideals) in R containing $\mathfrak{a}$, and the prime ideals (resp. primary ideals, maximal ideals) in $R/\mathfrak{a}$.

For localization we get the following version.

Proposition 7.5. *Let D be a multiplicatively closed subset of R. Consider the ring homomorphism $\nu : R \to D^{-1}R$.*

(i) Every ideal of $D^{-1}R$ is an extended ideal. An ideal $I \subset R$ is a contracted ideal if and only if it has the property that if $dr \in I$ with $d \in D$ and $r \in R$ then $r \in I$. In case $\mathfrak{q} \lhd R$ is a primary ideal

with radical $\sqrt{\mathfrak{q}} = \mathfrak{p}$, then $\mathfrak{q}$ is a contracted ideal if and only if $D \cap \mathfrak{p} = \emptyset$. If $I \subset R$ is a primary ideal that is not a contracted ideal, then $I^e = D^{-1}R$.

(ii) The operation $()^e$ induces an inclusions preserving bijection between the set of prime ideals (resp. primary ideals) in $\mathcal{C}$ and the set of prime ideals (respectively primary ideals) of $D^{-1}R$. The inverse is given by the operation $()^c$.

(iii) Suppose $I = \cap_{i=1}^r \mathfrak{q}_i$, where $\mathfrak{q}_i$ are primary ideals ordered in such a way that $\sqrt{\mathfrak{q}_i} \cap D = \emptyset$ if and only if $i \leq s$. Then $I^{ec} = \cap_{i=1}^s \mathfrak{q}_i$.

Proof. (i) By Corollary 7.1(iii) every ideal of $D^{-1}R$ is an extended ideal. We always have $I^{ec} \supseteq I$. Suppose $I = I^{ec}$ and $dr \in I$ for some $d \in D$ and $r \in R$. So $\frac{r}{1} = \frac{dr}{d} \in D^{-1}I = I^e$ and so $d \in I^{ec} = I$. Conversely, suppose I has the formulated property, and $r \in I^{ec}$. Then for some $a \in I$ and $d \in D$ we have $\frac{r}{1} = \frac{a}{d}$. This means there exists a $d' \in D$ such that $d'dr = d'a \in I$. So by the assumed property, $r \in I$. So $I^{ec} = I$.

Suppose $\mathfrak{q}$ is a primary ideal such that $\sqrt{\mathfrak{q}} \cap D = \emptyset$. If $dr \in \mathfrak{q}$ for some $d \in D$ and $r \in R$, then $d \notin \sqrt{\mathfrak{q}}$ so $r \in \mathfrak{q}$, by the property of being primary. So $\mathfrak{q}$ is contracted.

Suppose there exists a $d \in D \cap \sqrt{\mathfrak{q}}$. Then there exists an n such that $d^n \in \mathfrak{q} \cap D$, so $1 = \frac{d^n}{d^n} \in \mathfrak{q}^e$ and $\mathfrak{q}^{ec} = R \neq \mathfrak{q}$ so $\mathfrak{q}$ is not a contracted ideal.

(ii) Suppose $\mathfrak{q}$ is a primary ideal such that $\sqrt{\mathfrak{q}} \cap D = \emptyset$ and $\frac{r_1}{d_1}\frac{r_2}{d_2} \in \mathfrak{q}^e$. So there exist $a \in \mathfrak{q}$, $d_3, d \in D$ such that $dd_1d_2a = dd_3r_1r_2$. So $r_1r_2 \in \mathfrak{q}$. Suppose $(\frac{r_1}{d_1})^n \notin \mathfrak{q}^e$ for all $n \geq 0$. Then at least $r_1^n \notin \mathfrak{q}$ for akk n. We conclude that $r_2 \in \mathfrak{q}$, so $\frac{r_2}{d_2} \in \mathfrak{q}^e$. So $\mathfrak{q}^e$ is a primary ideal.

(iii) Exercise. □

Corollary 7.2. *Suppose R is a ring, I and ideal and $D \subset R$ a multiplicative subset such that if $da \notin D$, for all $d \in D$ and $a \in I$. There exists a prime ideal $\mathfrak{p}$ of R containing I and with empty intersection with D.*

Proof. The proof uses the two correspondence theorems. The condition implies that $D^{-1}I \neq D^{-1}R$, or $D^{-1}R/D^{-1}I$ is not the zero ring. So by Krull's theorem, $D^{-1}R/D^{-1}I$ contains a maximal ideal, that corresponds to a prime ideal $\mathfrak{P}$ of $D^{-1}R$ containing $D^{-1}I$. It is of the form $D^{-1}\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ with empty intersection with D. Since $D^{-1}I \subseteq D^{-1}\mathfrak{p}$ we also get $I \subseteq \mathfrak{p}$. □

Corollary 7.3. *(i) Suppose R is a ring and $D \subset R$ is a multiplicative subset. If R is catenary then $D^{-1}R$ is catenary. If R is noetherian then $D^{-1}R$ is noetherian. In particular, any localization of an affine ring is Noetherian and catenary.*

(ii) A ring is catenary if for every pair of prime ideals $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$, all maximal chains of prime ideals in $R_{\mathfrak{p}_2}/\mathfrak{p}_{1\mathfrak{p}_2} \simeq (R/\mathfrak{p}_1)_{\mathfrak{p}_2}$ have the same length.

The following will be used in the proof of Going-down in the next section.

Lemma 7.3 (Lying-over)**.** *Let $f : R \to S$ be any ring homomorphism. A prime ideal $\mathfrak{p} \in R$ is a contracted ideal, i.e. $\mathfrak{p} = \mathfrak{p}^{ec}$ if and only if it is the contraction of a prime ideal in S. It is not necessarily true that $\mathfrak{p}^e$ is a prime ideal.*

Proof. Let $\mathfrak{p}$ be a contracted prime ideal, we want to show that it is also the contraction of some prime ideal of S. By assumption $\mathfrak{p} = \mathfrak{p}^{ec}$. Let $D := f(R\backslash\mathfrak{p})$. It is a multiplicatively closed subset of S disjoint from $\mathfrak{p}^e$, since otherwise there would be an $r \notin \mathfrak{p}$ such that $f(r) \in \mathfrak{p}^e$ or $r \in \mathfrak{p}^{ec} = \mathfrak{p}$,

contradiction. Let $\mathfrak{P}$ be maximal such that $\mathfrak{P} \supset \mathfrak{p}^e$ and $\mathfrak{P} \cap D = \emptyset$. By the correspondence theorem for localization, $D^{-1}\mathfrak{P}$ is a maximal ideal of $D^{-1}R$ and so $\mathfrak{P}$ is a prime ideal of S. Now $\mathfrak{p} = \mathfrak{p}^{ec} \subseteq \mathfrak{M}^c$. On the other hand, if $r \in \mathfrak{P}^c$ but $r \notin \mathfrak{p}$, then $f(r) \in \mathfrak{P}$ and $f(r) \in D$. Which is a contradiction. So $\mathfrak{p} = \mathfrak{P}^c$ is the contraction of a prime ideal. □

In other words, Lying-over holds for a prime ideal if and only if it is a contracted ideal.

Example 7.2. Consider $\mathbb{Z} \subset \mathbb{Z}[i]$. The extended ideals in $\mathbb{Z}[i]$ are those principal ideals that are generated by a non-negative integer. All ideals of $\mathbb{Z}$ are contracted ideals. $2\mathbb{Z}[i]$ (or $5\mathbb{Z}[i]$) is an extended ideal that is not a prime ideal (since $(1+i)(1-i) \in 2\mathbb{Z}[i]$ but $1+i$ and $1-i$ are not in $2\mathbb{Z}[i]$), whereas $(1+i)\mathbb{Z}[i]$ (resp, $(1+2i)\mathbb{Z}[i]$) is not an extended ideal, but it is a prime ideal having $2\mathbb{Z}$ (resp $5\mathbb{Z}$) as contraction The ideal $3\mathbb{Z}[i]$ is prime.

8. Proof of the Cohen-Seidenberg theorem

8.1. **Proof of Lying-over, Going-up and Incompatibility.** Starting from an integral extension, we get other integral extension with useful correspondence theorems.

Lemma 8.1. *Let $R \subset S$ be an integral extension of rings, $I \subseteq S$ an ideal with contraction $I^e \lhd R$. Then $R/I^c \subset S/I$ is also an integral extension of rings.*

Lemma 8.2. *Let $R \subset S$ be an integral extension of rings and $D \subset R$ a multiplicative subset. Then $D^{-1}R \to D^{-1}S$ is also an integral extension of rings.*

Proof. Let $\frac{s}{d} \in D^{-1}S$. There is an integrality relation $s^n + r_1 s^{n-1} + \ldots + r_n$, where $r_i \in R$. We obtain an integrality relation of $\frac{s}{d}$ over $D^{-1}R$: $\frac{s}{d}^n + \frac{r_1}{d}\frac{s}{d}^{n-1} + \ldots + \frac{r_n}{d^n}$. □

Proof of Cohen-Seidenberg theorem 6.1(i-iv). (i) The extension $R/\mathfrak{p} \subset S/\mathfrak{P}$ is also integral, and one of the the two domains is a field if and only if the other is a field.

(ii)[Incompatibility] We suppose $\mathfrak{Q} \supseteq \mathfrak{P}$ are two prime ideals of S with the same contraction $\mathfrak{p}$ in R. Put $D := \{r \in R; r \notin \mathfrak{p}\}$. We get an integral extension $R_\mathfrak{p} = D^{-1}R \subseteq D^{-1}S$ with unique maximal ideal $D^{-1}\mathfrak{p} \lhd R_\mathfrak{p}$. Since $\mathfrak{Q} \cap D = \mathfrak{P} \cap D = \mathfrak{p} \cap D\emptyset$ the ideals $D^{-1}\mathfrak{P} \subseteq D^{-1}\mathfrak{Q}$ of $D^{-1}S$ are prime ideals, by the correspondence theorem of localisation. We have $D^{-1}\mathfrak{P} \cap D^{-1}R = D^{-1}\mathfrak{Q} \cap D^{-1}R = D^{-1}\mathfrak{p}$, a mximal ideal, so $D^{-1}\mathfrak{P}$ and $D^{-1}\mathfrak{Q}$ are both maximal ideals, by i. So from $D^{-1}\mathfrak{Q} \supseteq D^{-1}\mathfrak{P}$ we conclude $D^{-1}\mathfrak{Q} \supseteq \mathfrak{P}$ i.e. $\mathfrak{P}^e = \mathfrak{Q}^e$. Hence by the correspondence theorem, $\mathfrak{P} = \mathfrak{Q}$.

(iii)[Lying-over] Let $\mathfrak{p}$ be a prime ideal of R, and put $D = \{r \in R; r \notin \mathfrak{p}\}$. Then we have an integral extension $R_\mathfrak{p} = D^{-1}R \subset D^{-1}S$ and $D^{-1}\mathfrak{p}$ is the unique maximal ideal of $R_\mathfrak{p}$. Let $\mathfrak{P}$ be a prime ideal of S such that $D^{-1}\mathfrak{P}$ is a maximal ideal of $D^{-1}R$. Then by (i) the intersection $D^{-1}\mathfrak{P} \cap D^{-1}R$ is a maximal ideal, hence $D^{-1}\mathfrak{p}$. So

$$\mathfrak{P} \cap R = (D^{-1}\mathfrak{P} \cap D^{-1}S) \cap R = (D^{-1}\mathfrak{P} \cap D^{-1}R) \cap R = D^{-1}\mathfrak{p} \cap R = \mathfrak{p},$$

which shows that there is a prime ideal in S lying over $\mathfrak{p}$.

(iv) We get an integral extension $R/\mathfrak{p}_m \subseteq S/\mathfrak{P}_m$. By the correspondence theorem we can assume R and S are domains, $m = 0$ and $\mathfrak{P}_0 = (0)$. By Lying-over there is a prime ideal $\mathfrak{P}_1$ in S lying over $\mathfrak{p}_1$. Of course, $\mathfrak{P}_0 = (0) \subset \mathfrak{P}_1$. We repeat this process to go up all the way. □

8.2. **Proof of Going-down theorem.** The Going-down theorem is the trickiest to prove of the Cohen-Seidenberg theorems. We need the extra assumption that R and S are domains, and that R is integrally closed in its field of fractions $K := Q(R)$. We say that s is *integral over an ideal* $I \subset R$ if there exists an integrality relation $s^d + r_1 s^{d-1} + \ldots + r_d = 0$ where all coefficients lie in I, i.e., $r_i \in I$ for $1 \leq i \leq d$. The collection of all elements integral over a given ideal I can be described.

Lemma 8.3. *Let $R \subset S$ be an integral extension of domains and suppose that R is integrally closed in its fraction field $K = Q(R)$. Let $I \subseteq R$ be an ideal.*

(i) The collection of all elements in S that are integral over I equals the ideal $\sqrt{I}^e$, the radical of the extension to I in S.

(ii) Let $s \in S$ be integral over I. Then it is algebraic over K and the coefficients of its minimal polynomial lie in $\sqrt{I}$, the radical of I.

Proof. (i) Let $s^d + r_1 s^{d-1} + \ldots + r_d = 0$ where all coefficients lie in I be an integrality relation for $s \in S$, where all coefficients lie in I. So $s^d = -r_1 s^{d-1} - r_2 s^{d-2} - \ldots - r_d \in I^e$ and $s \in \sqrt{I^e}$.

In the other direction, let $s \in \sqrt{I^e}$, so there exists an equation $s^d = \sum_{i=0}^n a_i s_i$, where $a_i \in I$ and $s_i \in S$. Since S is integral over R, the subring $M := R[s_1, \ldots, s_n]$ of S is finitely generated over R and $s^d M \subseteq IM$. Let $m_1, \ldots, m_r$ be a generating set for M as R-module. Then there are $b_{ij} \in I$ such that $s^d m_i = \sum_j b_{ij} m_j$. Let F be the characteristic polynomial of the $r \times r$-matrix (a_{ij}). By Cayley-Hamilton's theorem, see the proof of Proposition 4.1 and the remark following it, $F(s^d)$ acts trivially on M, and since $1 \in M$ we get $F(s^d) = F(s^d)1 = 0$. Since every a_{ij} is in I, the coefficients (except the principal) of F lie in I. So s^d satisfies an integrality relation over I; the same equation can serve as integrality relation of s over I.

(ii) Let $s \in S$ be integral over I then it is algebraic over K. Let $F \in K[X]$ be the minimal polynomial of s over K, and $f(X) \in R[X]$ be a monic polynomial with non-principal coefficients in I such that $f(s) = 0$. We shall work with another integral extension. Let L be an algebraic closure of the quotient field of S, and let $\tilde{S}$ be the integral closure of R in L. In particular it contains S. Since L is algebraically closed there are $\tilde{s_1}, \ldots, \tilde{s_n}$ such that $F = \prod_{i=1}^n (X - \tilde{s_i}) \in L[X]$. Since F divides f in $K[X]$, for every i we have $f(\tilde{s_i}) = 0$, so each $\tilde{s_i}$ is integral over I. Since the non-principal coefficients of F are homogeneous polynomials in the $\tilde{s_i}$'s it follows that the non-principal coefficients of F are elements of K that are integral over I. Since R is integrally closed in K, it follows that all these coefficients lie in R and are integral over I. By (i), it follows that these elements lie in the radical of I. □

Proof of Going-down theorem 6.1(v). We start with a special case, the general case will follow iteratively. Let $R \subset S$ be an integral extension of domains, where R is integrally closed in it's field of fractions K. Let $\mathfrak{p}_1 \subset \mathfrak{p}_2$ be two prime ideal of R and $\mathfrak{P}_2$ a prime ideal of S such that $\mathfrak{P}_2 \cap R = \mathfrak{p}_2$. We want to show there exists a prime ideal $\mathfrak{P}_1$, contained in $\mathfrak{P}_2$ such that $\mathfrak{P}_1 \cap R = \mathfrak{p}_1$. By the correspondence theorem for localization the prime ideals contained in $\mathfrak{P}_2$ are in one-to-one correspondence with the prime ideals in $S_{\mathfrak{P}_2}$. So what we are looking for is a prime ideal, say $\mathfrak{Q}$, in $S_{\mathfrak{P}_2}$ such that $\mathfrak{Q} \cap R = \mathfrak{p}_1$. By Proposition 7.3, such a prime ideal exists if and only if $\mathfrak{p}_1$ is a contracted ideal in R for the extension $R \subset S_{\mathfrak{P}_2}$, i.e. $\mathfrak{p}_1 S_{\mathfrak{P}_2} \cap R \subseteq \mathfrak{p}_1$.

Let $r = \frac{s}{d} \in \mathfrak{p}_1 S_{\mathfrak{P}_2} \cap R$ with $s \in \mathfrak{p}_1 S$ and $d \in S \backslash \mathfrak{P}_2$ and suppose $r \notin \mathfrak{p}_1$. We intend do derive a contradiction. By the previous lemma s is integral over $\mathfrak{p}_1$ and its minimal polynomial over the field of fractions of R is of the form $X^n + r_1 X^{n-1} + \ldots + r_n$, where each $r_i \in \mathfrak{p}_1$. Now $X^n + \frac{r_1}{r} X^{n-1} + \frac{r_2}{r^2} X^{n-2} + \ldots + \frac{r_n}{r^n}$ has as root $d = r^{-1} s \in S \backslash \mathfrak{P}_2$ and the coefficients lie in K. It is the minimal polynomial of d over K. By the previous lemma it follows that $\frac{r_i}{r^i} \in R$ and $r_i \in \mathfrak{p}_1$. We supposed that $r \notin \mathfrak{p}_1$, it follows from the primeness of $\mathfrak{p}_1$ and $r^i \cdot \frac{r_i}{r^i} = r_i \in \mathfrak{p}_1$ that $\frac{r_i}{r^i} \in \mathfrak{p}_1$ for all i. It follows that

$$d^n = -(\frac{r_1}{r} d^{n-1} + \frac{r_2}{r^2} d^{n-2} + \ldots + \frac{r_n}{r^n}) \in \mathfrak{p}_1 S \subseteq \mathfrak{p}_2 S \subseteq \mathfrak{P}_2,$$

hence $d \in \mathfrak{P}_2$. Which is the desired contradiction. This finishes the proof of the Going-down theorem. □

8.3. **Invariant theory and going down.** The Going-down theorem was proved under the hypothesis of integral closedness of the small ring. There are other situations where Going-down holds, even when this hypothesis does not hold. This is the case in invariant theory of finite groups.

Proposition 8.1. *Let S be a ring and G a finite group of ring automorphisms. Put $R := S^G$ for the ring of invariants.*

(i) The extension $R \subset S$ is integral, so Lying-over, Incompatibility and Going-up hold.

(ii) If $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are prime ideal of S both lying over the same prime ideal of R, then there exists a $\sigma \in G$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$. Or in other words, the prime ideals of R are in correspondence with the G-orbits of prime ideals in R.

(iii) Going-down also holds (without any extra assumptions on S and R).

(iv) If S is a domain integrally closed in its field of fractions L, then R is also domain integrally closed in its field of fractions K, and $K = L^G$.

Proof. (i) Let $s \in S$, then $F = \prod_{\sigma \in G}(X - \sigma(s))$ is a polynomial such that $\sigma(F) = F$, when we extend the action to $S[X]$ by trivial action on X. So $F \in S[X]^G = S^G[X] = R[X]$ and $F(s) = 0$, so s is integral over R.

(ii) Let $x \in \mathfrak{P}_1$, then $y = \prod_{\sigma \in G} \sigma(y)$ is an invariant contained in $\mathfrak{P}_1$. Since $\mathfrak{P}_1 \cap R = \mathfrak{P}_2 \cap R$, it follows that $y \in \mathfrak{P}_2$. Since $\mathfrak{P}_2$ is prime one of the factors $\sigma(x)$ is in $\mathfrak{P}_2$, or $x \in \sigma^{-1}(\mathfrak{P}_2)$. So $\mathfrak{P}_1$ is contained in the union $\cup_{\sigma \in G}\sigma(\mathfrak{P}_2)$. By prime avoidance, see Lemma 8.4, we get that there exists a $\sigma \in G$ such that $\mathfrak{P}_1 \subseteq \sigma(\mathfrak{P}_2)$. Since

$$\sigma(\mathfrak{P}_2) \cap R = \sigma(\mathfrak{P}_2 \cap R) = \mathfrak{P}_2 \cap R = \mathfrak{P}_1 \cap R,$$

it follows from the incompatibility theorem that $\mathfrak{P}_1 = \sigma(\mathfrak{P}_2)$.

(iii) Suppose $\mathfrak{p}_1 \subset \mathfrak{p}_2$ are prime ideals in R and $\mathfrak{P}_2$ a prime ideal of S such that $\mathfrak{P}_2 \cap R = \mathfrak{p}_2$. By Lying-over and Going-up there are prime ideals $\mathfrak{Q}_1 \subset \mathfrak{Q}_2$ such that $\mathfrak{Q}_i \cap R = \mathfrak{p}_i$. By (ii) there exists a $\sigma \in G$ such that $\sigma(\mathfrak{Q}_2) = \mathfrak{P}_2$. Then $\mathfrak{P}_1 = \sigma(\mathfrak{Q}_1) \subset \sigma(\mathfrak{Q}_2) = \mathfrak{P}_2$ and $\mathfrak{P}_1 \cap R = \sigma(\mathfrak{Q}_1) \cap R = \mathfrak{p}_1$. So we proved Going-down in this special case. The general case follows iteratively.

(iv) Write L for the fraction field of S and K for the fraction field of R. Then G also acts on L by field automorphisms $\sigma\left(\frac{a}{b}\right) := \frac{\sigma(a)}{\sigma(b)}$ (check that the action is well defined at least). We certainly have $K \subseteq L^G$, the invariant field of the action. But we even have equality: suppose $z = \frac{a}{b} \in L^G$. Write $b_1 = \prod_{\sigma \in G} \sigma(b)$ and $a_1 = a \prod_{\sigma \neq \mathbf{1}_G} \sigma(b)$. Then $z = \frac{a_1}{b_1}$, $b_1 \in S^G = R$ and therefore $a_1 = zb_1 \in L^G \cap S = S^G = R$. Or $z = \frac{a_1}{b_1} \in K$.

Let now $z \in K$ be integral over R, then it is also integral over S, hence $z \in S \cap K = S \cap L^G = S^G = R$. □

Remark. Consider the correspondence theorem for the integral extension $R = S^G \subset S$. By Lying-over all the prime ideals of R are contracted ideals. If we have projection operator $F : S \to R$ as in Proposition 3.1, then every ideal in R is a contracted ideal. This does not need the case without the presence of such a projection operator.

8.4. **Prime avoidance.** By definition, if a product of two elements lies in a prime ideal, then at least one of the two elements lies in the prime ideal. The analogous property hold for ideals: if a product of ideals is contained in a prime ideal, then at least one of those ideals is contained in the

prime ideal . Another property is: if an ideal is contained in the union of two prime ideals, then it necessarily lies in at least one of the two.

Lemma 8.4 (Prime avoidance lemma)**.** *Let R be a ring.*

(i) Let $I_1, \dots, I_n$ be ideals and $\mathfrak{p}$ a prime ideal containing the intersection $\cap_i I_i$ (or containing only the prodiuct ideal $I_1 \cdot I_2 \cdots I_n$). Then $I_i \subseteq \mathfrak{p}$ for some i. If even $\mathfrak{p} = \cap_i I_i$ then $\mathfrak{p} = I_i$ for some i.

(ii) Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals and I an ideal contained in the union $\cup_i \mathfrak{p}_i$. Then $I \subseteq \mathfrak{p}_i$ for some i.

Proof. (i) Suppose non of the I_i's is contained in $\mathfrak{p}$. Then for every i we can pick an $x_{\in} I_i$ such that $x_i \notin \mathfrak{p}$. The product $x := x_1 x_2 \dots x_n \in \prod_i I_i \subseteq \cap_i I_i \subset \mathfrak{p}$ is then in the prime ideal $\mathfrak{p}$ hence one of the x_i is in $\mathfrak{p}_i$. Contradiction. So there eixsts an i such that $I_i \subseteq \mathfrak{p}$. If even $\mathfrak{p} = \cap_i I_i$, then $I_i \subseteq \mathfrak{p}$ also.

(ii) We prove this result by induction on n. If $n = 1$ it is obviously true. Assume the result is true for $n - 1$. If I is contained in the union of the prime ideals except one, we can use induction to conclude. Suppose that for every i the ideal I is not contained in $\cup_{j \neq i} \mathfrak{p}_j$. So for every i we can pick an $x_i \in I$ such that $x_i \notin \mathfrak{p}_j$, if $j \neq i$. Since I is nevertheless in the union of all prime ideals, it follows that $x_i \in \mathfrak{p}_i$. Consider now the following element contained in I;

$$x = \sum_{j=1}^{n} x_1 x_2 \dots x_{j-1} x_{j+1} x_{j+2} \cdots x_n.$$

If $i \neq j$ the summand $x_1 x_2 \dots x_{j-1} x_{j+1} x_{j+2} \cdots x_n$ is contained in $\mathfrak{p}_i$, since x_i appears as a factor. So $x \in \mathfrak{p}_i$ if and only if $x_1 x_2 \dots x_{i-1} x_{i+1} x_{i+2} \cdots x_n \in \mathfrak{p}_i$. If so, then at least one factor x_j $(j \neq i)$ is contained in $\mathfrak{p}_i$ (since $\mathfrak{p}_i$ is a prime ideal). Contradiction. So x is not contained in the union of the $\mathfrak{p}_i$'s, hence not contained in I. Contradiction. So there is an i such that I is contained in $\mathfrak{p}_i$. $\square$

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA