Localization

Let \( D \) be an integral domain.

**Definition.** A subset \( S \subset D \) is multiplicative if:

\[
0 \not\in S, 1 \in S \text{ and } s, t \in S \text{ implies } st \in S
\]

**Examples.**

(a) The abelian group \( D^* \) of units in \( D \) is multiplicative.

(b) The set \( \{1, f, f^2, ..., \} \) of powers of \( f \neq 0 \) is multiplicative.

(c) The complement of an ideal \( I \subset D \) is multiplicative if and only if \( I \) is prime.

**Proposition 1.** Given a multiplicative subset \( S \subset D \), let:

\[
S^{-1}D = \left\{ \frac{r}{s} \mid r \in D, s \in S \right\} / \sim
\]

where

\[
\frac{r_1}{s_1} \sim \frac{r_2}{s_2} \text{ if and only if } r_1s_2 - r_2s_1 = 0
\]

and equip \( S^{-1}D \) with fraction addition and multiplication:

\[
\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2 + r_2s_1}{s_1s_2} \quad \text{and} \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}
\]

Then \( S^{-1}D \) is an integral domain with \( 0 = \frac{0}{1}, 1 = \frac{1}{1} \) and injective homomorphism:

\[
f : D \to S^{-1}D \text{ given by } f(r) = \frac{r}{1}
\]

**Proof.** This mainly amounts to proving well-definedness.

(i) \( \sim \) is an equivalence relation. Transitivity is the only non-obvious property:

\[
r_1s_2 - r_2s_1 = 0, r_2s_3 - r_3s_2 = 0 \Rightarrow
s_2(r_1s_3 - r_3s_1) = s_3(r_1s_2 - r_2s_1) + s_1(r_2s_3 - r_3s_2) = 0
\]

\[
\Rightarrow r_1s_3 - r_3s_1 = 0
\]

(ii) Addition is determined by passing to common denominators:

\[
\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2 + r_2s_1}{s_1s_2}
\]

as well as the distributive law and requirement that:

\[
\frac{r}{1} \cdot \frac{1}{s} = \frac{r}{s}
\]

which also determines multiplication. But you should check this is well-defined.

(iii) \( S^{-1}D \) is an integral domain, since:

\[
\frac{r_1r_2}{s_1s_2} = 0 \text{ if and only if } r_1r_2 = 0 \text{ if and only if either } r_1 = 0 \text{ or } r_2 = 0
\]

since \( D \) has no zero divisors.

**Remarks.**

(a) If \( S \subset D^* \), then \( f : D \to S^{-1}D \) is an isomorphism with

\[
\frac{r}{s} = \frac{s^{-1}r}{1}
\]
(b) If \( S = D - \{0\} \), then \( S^{-1}D \) is a field. This is the field of fractions \( k(D) \) of the domain \( D \). All other domains \( S^{-1}D \) sit in between \( D \) and the field of fractions:

\[
D \subset S^{-1}D \subset k(D)
\]

(c) If \( S = \{1, f, \ldots\} \), then \( S^{-1}D \) is denoted by \( D_f \), and:

\[
q : D[x] \to D_f; \ q(x) = 1/f \text{ is surjective with kernel } I = (1 - fx)
\]

so \( D_f \) is a quotient ring of the polynomial ring.

(d) If \( S = P^c \) for \( P \subset D \), then \( S^{-1}D \) is denoted by \( D_P \). This is usually not a quotient ring of a polynomial ring \( D[x_1, \ldots, x_n] \) with any (finite) number of variables. We’ll see this when we prove the Hilbert Nullstellensatz.

Concrete Example. Let \( D = \mathbb{Z} \). Then:

(a) \( k(\mathbb{Z}) = \mathbb{Q} \), the field of rational numbers.

(b) \( \mathbb{Z}_n = \mathbb{Z}[\frac{1}{n}] \) are the rational numbers whose denominators (in lowest terms) divide some power of \( n \). Note that:

\[
\mathbb{Z}_n = \mathbb{Z}_{p_1, \ldots, p_r} = \mathbb{Z}[\frac{1}{p_1}, \ldots, \frac{1}{p_r}]
\]

where \( p_1, \ldots, p_r \) are the distinct prime factors of \( n \).

(c) \( \mathbb{Z}_{(p)} \) are the rational numbers whose denominators (in lowest terms) are not divisible by \( p \). Sometimes this is written \( \mathbb{Z}_p \), which is confusing given (b). In fact, there are a whole lot of rings that might be written as \( \mathbb{Z}_p \), so context is everything!

Let \( D \) be a UFD. Then an element:

\[
\frac{r}{s} \in k(D)
\]

is in lowest terms if the prime factorizations of \( r \) and \( s \) contain no associated common primes. This ratio is, moreover, unique up to multiplying numerator and denominator by the same unit in \( D \). A polynomial \( f(x) \in D[x] \) is in lowest terms if the factorizations of the coefficients of \( f(x) \) contain no associated common primes.

Gauss’ Lemma relies on:

**Proposition 2.** If \( f(x), g(x) \in D[x] \) are in lowest terms, then so is \( f(x)g(x) \).

**Proof.** Let \( f(x) = a_dx^d + \ldots + a_0 \), \( g(x) = b_ex^e + \ldots + b_0 \) and let \( p \in D \) be prime. Then \( p \) does not divide all the \( a \)'s and it does not divide all the \( b \)'s, so:

\[
p \text{ divides } a_0, \ldots, a_{k-1} \text{ but not } a_k \text{ and } p \text{ divides } b_0, \ldots, b_{l-1} \text{ but not } b_l
\]

for some \( k \leq d \) and \( l \leq e \). Then \( p \) does not divide the coefficient:

\[
\cdot a_{k+1}b_{l-1} + a_kb_l + a_{k-1}b_{l+1} + \cdots
\]

of \( x^{k+l} \) in the product \( f(x)g(x) \). So the product is in lowest terms! \( \square \)

Now we can prove:

**Gauss’ Lemma.** If \( D \) is a UFD, then \( D[x] \) is a UFD.

**Proof.** First of all, \( k(D)[x] \) is a Euclidean domain, so it is also a PID and UFD. Now suppose \( f(x) \in D[x] \). Since a prime in \( D \) is also a prime in \( D[x] \), we may remove all the common prime factors of the coefficients of \( f(x) \) and write it as

\[
p_1 \cdots p_r \cdot g(x) \text{ where } g(x) \in D[x] \text{ is lowest terms}
\]
We may factor the polynomial \( g(x) \) in the Euclidean domain \( k(D)[x] \) to get:
\[
g(x) = h_1(x) \cdots h_s(x)
\]
where each \( h_i(x) \in k(D)[x] \) is prime.

There are now unique fractions (in lowest terms) so that the polynomials:
\[
q_i(x) = \left( \frac{r_i}{s_i} \right) h_i(x) \in D[x]
\]
are in lowest terms and then it follows from the Proposition that both:
\[
g(x) \quad \text{and} \quad q_1(x) \cdots q_s(x) = \left( \prod \frac{r_i}{s_i} \right) g(x) = \left( \frac{r}{s} \right) g(x) \in D[x]
\]
are in lowest terms.

It follows that \( r \) and \( s \) (chosen to have no common prime factors) have no prime factors at all! So \( u = r/s \in D^* \) and:
\[
f(x) = u^{-1} p_1 \cdots p_r \cdot q_1(x) \cdots q_s(x)
\]
is the desired factorization into primes. \( \square \)

Example. In \( \mathbb{Q}[x] \), we have:
\[
x^2 - 1 = \left( \frac{2}{3} x - \frac{2}{3} \right) \left( \frac{3}{2} x + \frac{3}{2} \right)
\]
which we can put into (slightly inefficient, to play devil’s advocate) lowest terms:
\[
- \frac{3}{2} \left( \frac{2}{3} x - \frac{2}{3} \right) = -x + 1 \quad \text{and} \quad \frac{2}{3} \left( \frac{3}{2} x + \frac{3}{2} \right) = x + 1
\]
and then
\[
x^2 - 1 = (-1)(-x + 1)(x - 1) \quad \text{with the unit } u = -1
\]

**Eisenstein’s Criterion.** If \( D \) is a UFD, \( f(x) \in D[x], p \in D \) is a prime and:

(a) \( p \) divides all the coefficients of \( f(x) \) except the leading coefficient.

(b) \( p^2 \) does not divide the constant term of \( f(x) \).

Then \( f(x) \) is irreducible as a polynomial in \( k(D)[x] \).

**Proof.** By Gauss’ lemma, if \( f(x) \) is reducible in \( k(D)[x] \), then it factors:
\[
f(x) = g(h(x))h(x)
\]
by polynomials of smaller degree in \( D[x] \).

Let \( pD \subset D \) be the ideal generated by \( p \) and note that \( pD[x] \subset D[x] \) is also a prime ideal, since:
\[
D[x]/pD[x] = (D/p)[x]
\]
By (a) above, if we let \( \overline{f}(x) = f(x) + pD[x] \), then we have:
\[
a_d x^d = \overline{f}(x) = \overline{g}(x) \cdot \overline{h}(x) \in (D/p)[x]
\]
from which it follows that:
\[
\overline{g}(x) = bx^d \quad \text{and} \quad \overline{h}(x) = cx^{d-e} \quad \text{for some } e < d \quad \text{and} \quad b, c \in D/pD
\]
But then \( p \) divides the constant terms of \( g(x) \) and \( h(x) \), which violates (b). \( \square \)

Example. The polynomials:
\[
x^{a-1} + x^{a-2} + \cdots + 1 = \frac{x^a - 1}{x - 1} \in \mathbb{Q}[x]
\]
are irreducible if and only if \( a \) is a prime number. If \( a = bc \), then \( x^b - 1 \mid x^a - 1 \).
If \( a = p \) is prime, apply Eisenstein to \((x + 1)^p - 1\) using the binomial theorem.
Next, let \( P \subset D \) be a prime ideal in an integral domain and let:
\[
D \subset D_P = S^{-1}D
\]
be the inclusion of domains in Proposition 1

**Proposition 3.**

(a) There is a unique maximal ideal \( \mathfrak{m}_P \subset D_P \).

(b) There are maps between the set of ideals in \( D_P \) and the set of ideals in \( P \):
\[
\{ \text{ideals } J_P \subset D_P \} \leftrightarrow \{ \text{ideals } J \subset P \subset D \}
\]
\[
J_P \mapsto D \cap J_P = \{ a \in D \mid \frac{a}{1} \in J_P \}; \quad J \mapsto J_P := \{ \frac{a}{s} \mid a \in J, s \notin P \} / \sim
\]
that satisfy:
\[
J \subset (J_P \cap D) \text{ and } (J_P \cap D)_P = J_P
\]
Moreover, if \( Q \subset D \) is a prime ideal, then \( Q_P \subset D_P \) is also prime and \( Q = (Q_P \cap D) \).

Thus there is a bijection:
\[
\{ \text{prime ideals } Q_P \subset D_P \} \leftrightarrow \{ \text{prime ideals } Q \subset P \subset D \}
\]
and in particular, \( \mathfrak{m}_P \) maps to \( P \) under the bijection.

*Example.* Consider the prime ideal \( P = 2\mathbb{Z} \). Then \( \mathbb{Z}_P \) has only the ideals:
\[
\{0\} \text{ and } \mathfrak{m}^k = \left\{ \frac{a}{s} \mid 2^k \text{ divides } a \text{ and } s \text{ is odd} \right\}
\]
but there are lots more ideals contained in \( 2\mathbb{Z} \) than the ideals \( 2^k\mathbb{Z} \).

**Definition.** In general, the ideal \( \text{sat}(J) = J_P \cap D \) is called the saturation of \( J \subset P \) with respect to \( P \) and an ideal \( J \subset P \) is saturated if \( J = \text{sat}(J) \).

The Proposition says that prime ideals are saturated.

*Exercise.* Check that \( \text{sat}(J) = \text{sat}(\text{sat}(J)) \), so saturations of ideals are saturated!

**Proof of Prop 3.** We already know that \( I \cap D \subset D \) is an ideal when \( I \subset D_P \) is an ideal and it is prime when \( I \) is prime. Likewise, if \( J \subset D \) is an ideal, then:
\[
J_P = \left\{ \frac{a}{s} \mid a \in J, s \in S \right\} \subset D_P
\]
is closed under sums as well as products with elements \( r/s \), so \( J_P \subset D_P \) is an ideal.

It is a little problematic to think of the ideal in this way, though, because of the equivalence of fractions, since it is possible to have \( r/s \in J_P \) without having \( r \in J \).

Instead, we will use the alternative formulation:
\[
J_P = \{ x \in D_P \mid x s \in J \text{ for some } s \in S \}
\]
Now suppose \( Q \subset P \subset D \) is prime, and \( xy \in Q_P \) for some \( x, y \in D_P \). Then:
\[
x s_1, y s_2 \in D \text{ and } x y s \in Q \text{ for some } s_1, s_2, s \notin P \text{ so } (x s_1)(y s_2)s \in Q \text{ and } x s_1 \text{ or } y s_2 \in Q
\]
so \( Q_P \) is prime. Moreover, primeness of \( Q \) implies that:
\[
x \in D \text{ and } x s \in Q \Rightarrow x \in Q
\]
from which it follows that \( Q_P \cap D = Q \). The equality \( Q_P = (Q_P \cap D)_P \) is easy. \( \square \)

*Example.* The localizations of polynomial rings:
\[
k[x_1, \ldots, x_n]_{\mathfrak{m}_P} = \left\{ \frac{f}{g} \mid f, g \in k[x_1, \ldots, x_n] \text{ and } g(p) \neq 0 \right\}
\]
at the maximal ideal kernels of \( \text{ev}_p : k[x_1, \ldots, x_n] \to k; \text{ev}_p(f) = f(p) \) are the rings of rational functions that are defined in a neighborhood of \( p \).
Definition. A commutative ring $R$ with 1 is a local ring if $R$ has a unique maximal ideal $m$ which (Zorn’s Lemma) necessarily contains all other ideals $I \subset R$.

Remark. In a local ring $R$, every element of the complement $m^c$ is a unit.

Aside from the fields, we’ve seen one local ring persistently in our examples: $R = k[[x]]$ with maximal ideal $m = \langle x \rangle$

but now we have a machine for producing local rings $(D, P, m)$ from any pair $(D, P)$ consisting of a domain and a prime ideal.

We finish with an important class of rings (the next simplest after the fields).

Definition. A Noetherian domain $D$ satisfying:

(i) $D$ is a local ring with (non-zero) maximal ideal $m$.

(ii) $m = \langle \pi \rangle$ is principal

is called a discrete valuation ring (DVR).

Proposition 3. Every element $a \in D$ in a DVR is a product:

$$u\pi^r$$

for a unique $r$ and $u \in D^*$

Thus the only ideals in a DVR are the principal ideals $m^r = \langle \pi^r \rangle$ for $r \geq 1$.

Proof. Every irreducible element $a \in D$ is of the form:

$$a = u\pi$$

since $a \in \langle \pi \rangle$ is divisible by $\pi$, which is not a unit (hence it is an associate of $a$).

Thus the factorization of an arbitrary: $b = a_1 \cdots a_r$ as a product of irreducibles is

$$b = (u_1\pi) \cdots (u_r\pi) = u\pi^r$$

and the uniqueness is clear by cancellation. For the rest of the proof, note that:

$$\langle u_1\pi^{r_1}, \ldots, u_n\pi^{r_n} \rangle = \langle u_1\pi^{r_1} \rangle$$

if $r_1 \leq \cdots \leq r_n$ □

Thus in particular, a DVR is a local PID (and conversely).

Let $D$ be a DVR and let $k(D)$ be the field of fractions. Then:

$$k(D) = \{ u\pi^r \mid u \in D^* \text{ and } r \in \mathbb{Z} \}$$

and the mapping:

$$\nu : k(D)^* \to \mathbb{Z}; \nu(u\pi^r) = r$$

has the following properties:

(i) $\nu(ab) = \nu(a) + \nu(b)$

(ii) $\nu(a + b) \leq \min(a, b)$ with equality when $\nu(a) \neq \nu(b)$.

(iii) $D = \{ a \in k(D) \mid \nu(a) \geq 0 \}$ and $m = \{ a \in k(D) \mid \nu(a) \geq 1 \}$.

A mapping from a field to an ordered abelian group satisfying (i) and (ii) is a valuation, and when the ordered abelian group is $\mathbb{Z}$, then the mapping is a discrete valuation. Hence the name.

Definition. A domain $D$ with the property that localization $D_P$ at each non-zero prime ideal is a DVR is called a Dedekind domain.

Remark. In number theory, these are the rings of integers in a number field and in algebraic geometry, these are the (coordinate rings of) smooth affine curves.