IV.F. Ring extensions

In analysis, geometry, and topology, a very common situation is to have a surjective map $\pi\colon Y \twoheadrightarrow X$ spaces of some kind: Riemann surfaces, differentiable manifolds, algebraic varieties, etc. Think of Y as "lying over" X. Given a class of functions on each space closed under addition, subtraction and mutiplication, we can think of these as forming rings; and (assuming π is compatible with this class) the functions "downstairs" form a subring of the functions "upstairs" by pullback $f \mapsto f \circ \pi$.

For instance, if X and Y are Riemann surfaces, and π is holomorphic, then there is an induced map $\pi^*\colon \mathcal{M}(X) \hookrightarrow \mathcal{M}(Y)$ of fields of meromorphic functions, producing a field extension. If X and Y are noncompact, so that the holomorphic functions aren't constant,[5] we also get an induced map $\pi^*\colon \mathcal{O}(X) \hookrightarrow \mathcal{O}(Y)$ of rings of holomorphic functions. (One can do much the same with polynomial functions on algebraic varieties, which yield the *coordinate rings* defined in the next section.) This motivates the following:

IV.F.1. DEFINITION. Given a ring R, an **extension** of R is a pair $(\imath, S)$ consisting of a ring S and a ring homomorphism $\imath\colon R \hookrightarrow S$. As with fields, this is written S/R and we will usually suppress the "$\imath$".

IV.F.2. EXAMPLES. This will be a bit heuristic, as we haven't yet defined coordinate rings. But sometimes it is better to approach things "bottom-up" rather than "top-down".

(i) For any ring R, the polynomial ring $S = R[x_1, \dots, x_n]$ gives an extension. If R is the coordinate ring of a variety X over a field k, then S is that of $X \times k^n$, and $R \hookrightarrow S$ is the "pullback map" for the projection $X \times k^n \twoheadrightarrow X$. Note that S is not finitely-generated as an R module. If we pass to fraction fields, the resulting extension $\mathfrak{F}(S)/\mathfrak{F}(R)$ has

[5] Liouville's theorem, which states that a bounded entire function on the complex plane is constant, implies that holomorphic functions on a compact Riemann surface are constant. You still get a pullback map if X and Y are compact, but (assuming they are also irreducible) it's just the identity map $\mathbb{C} \to \mathbb{C}$.

transcendence degree equal to the dimension of the "fibers" of this map.

(ii) What would the ring extension look like for a surjective map between varieties of the *same dimension*? Given a polynomial $P(x) \in \mathbb{C}[x]$, the natural embedding $R := \mathbb{C}[x] \hookrightarrow \mathbb{C}[x,y]/(y^2 - P(x)) =: S$ is the pullback (on coordinate rings) associated to the 2:1 map from $Y := \{y^2 = P(x)\} \subset \mathbb{C} \times \mathbb{C}$ to $X := \mathbb{C}$ by $(x,y) \mapsto x$. The yoga here is that you get polynomial functions on Y by taking polynomials on $\mathbb{C} \times \mathbb{C}$ and going modulo the ideal of functions vanishing on Y.

One thing we would like to study is how maximal ideals in R and S are related, since these correspond to points "upstairs" and "downstairs". Notice also in this case that S has finite rank as an R-module, which makes the situation resemble a finite extension of fields. There is even an automorphism of S over R induced by sending $y \mapsto -y$.

A related example, whose relation to geometry is less clear, is that of $\mathcal{O}_K/\mathbb{Z}$ when K is a number field.

(iii) The two types of localization also produce ring extensions, assuming the multiplicative set has no zero-divisors. For instance, the embedding of $R = \mathbb{C}[x]$ in $S = R[\frac{1}{x-a}]$ represents pullback of (regular) functions from $\mathbb{C}$ to $\mathbb{C}\backslash\{a\}$. The embedding of R in its fraction field $\mathfrak{F}\{R\}$ (viz. $\mathbb{C}(x)/\mathbb{C}[x]$, or $K/\mathcal{O}_K$) also yields a ring extension. In none of these cases is S finitely generated as an R-module. However, the fraction fields are the same, so the extension isn't "transcendental" in the sense of (i).

Polynomial and power-series extensions.

We begin with a basic structural result in the "transcendental extension" case encountered in IV.F.2(i).

IV.F.3. HILBERT BASIS THEOREM. *Let R be a Noetherian ring. Then $R[x]$ is also Noetherian.*

PROOF. Let $I \subset R[x]$ be a nonzero ideal. By IV.B.10, it suffices to show that I is finitely generated. Suppose otherwise, and let $f_0(x) \in I$ be a nonconstant polynomial of lowest degree > 0.

For each $n > 0$ we choose inductively $f_n \in I \backslash (f_0, \ldots, f_{n-1})$ of minimal degree > 0, and set $d_n := \deg(f_n)$. (Clearly $d_n \geq d_{n-1}$.) Let a_n denote the coefficient of x^{d_n} in f_n, and consider the ascending chain

$$(a_0) \subsetneq (a_0, a_1) \subsetneq \cdots \subsetneq (a_0, \ldots, a_n) \subsetneq \cdots$$

in R. As R is Noetherian, this must stabilize at some m, and then $a_{m+1} = \sum_{i=0}^{m} \lambda_i a_i$ for some $\{\lambda_i\}_{i=0}^{m} \subset R$. But since $f_{m+1} \notin (f_0, \ldots, f_m)$,

$$g(x) := f_{m+1}(x) - \textstyle\sum_{i=0}^{m} \lambda_i f_i(s) x^{d_{m+1}-d_i} \notin (f_0, \ldots, f_m)$$

while having $\deg(g) < \deg(f_{m+1})$. This contradicts minimality of d_{m+1}. □

IV.F.4. COROLLARY. *If R is Noetherian, then $R[x_1, \ldots, x_n]$ is too. In particular, $k[x_1, \ldots, x_n]$ is Noetherian for any field k.*

So for instance, this means that any ideal $I \subset k[x_1, \ldots, x_n]$ has a reduced primary decomposition. We can think of this as meaning that any algebraic subset V, defined by the vanishing of all functions in I, can be written uniquely as the union of "irreducible" components corresponding to the associated primes of the RPD. (This can be as simple as separating $xy = 0$ in $\mathbb{C}^2$ into $x = 0$ and $y = 0$.)

IV.F.5. REMARK. Let R be Noetherian and P a prime ideal; then one can show that the length of a chain of primes

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d = P$$

is bounded above by the number of generators of P (which we know is finite). One calls the maximum length of such a chain the **height** of P, and the supremum of heights of its prime ideals the **(Krull) dimension** of R. While there are weird examples where this is ∞, we have $\dim(R) = 0$ for fields, 1 for PIDs, $\dim(R[x]) = \dim(R) + 1$, and $\dim(k[x_1, \ldots, x_n]) = n$. More generally, if R is the coordinate

ring of an algebraic variety over $\mathbb{C}$, then $\dim(R)$ is the same as the (complex) dimension of the associated complex analytic space.

Consider for example $R = k[x]$, and suppose $\{0\} = P_0 \subsetneq P_1 \subsetneq P_2$ is a chain of prime ideals. Then $P_1 = (f_1(x))$ and $P_2 = (f_2(x))$, since R is a PID, and then $f_2 \mid f_1 \implies f_1 = f_2 g$. Since P_1 is prime, and $f_1 \nmid f_2$ (as $P_1 \subsetneq P_2$), we have $f_1 \mid g$ hence $f_1 = f_2 h f_1 \implies f_2 \in R^*$, a contradiction. So the longest chains have length 1, like $(0) \subsetneq (x)$, and $\dim(R) = 1$.

When you study complex analytic curves $C = \{f(x,y) = 0\} \subset \mathbb{C} \times \mathbb{C}$ defined by $f \in \mathbb{C}[x,y]$, one of the basic steps is to establish something called *Weierstrass factorization*. That is, you fix an x-coordinate (say, 0) and study the restriction of the curve to the cylindrical neighborhood $\{|x| < \epsilon\} \times \mathbb{C}$ by passing to $\mathbb{C}[y][[x]]$, and split it into irreducibles there. For example, although $f(x,y) = y^2 - x^3 - x^2$ is irreducible in $\mathbb{C}[x,y]$, in $\mathbb{C}[[x]]$ we have $\sqrt{1+x}$ and so $f = (y - x\sqrt{1+x})(y + x\sqrt{1+x})$ in $\mathbb{C}[y][[x]]$. The fact that such a factorization always exists is a consequence (via taking RPD of (f)) of the Noetherianity of $\mathbb{C}[y][[x]]$, guaranteed by

IV.F.6. THEOREM. *If R is Noetherian, then so is $R[[x]]$.*

SKETCH. Given $I \subset R[[x]]$, define an ascending chain of ideals in R by $J_n := \{r \in R \mid \exists \sum_{j \geq n} c_j x^j \in I \text{ s.t. } r = c_n\}$, which stabilizes at (say) $n = m$. Pick $f_1, \ldots, f_M$ [resp. $g_1, \ldots, g_N$] in $R[[x]]$ so that their first nonzero coefficients generate the respective $\{J_n\}_{n<m}$ [resp. J_m] (which are f.g. by Noetherianity of R). For any $f \in I$, there are $r_i \in R$ such that $g := f - \sum_{i=1}^{M} r_i f_i \in I$ has order of vanishing at least m at $x = 0$. Now subtract an R-linear combination of the $\{g_j\}$ to clear the m^{th} coefficient, then a combination of the $\{xg_j\}$ to clear the $(m+1)^{\text{st}}$ coefficient, etc. (This is possible because $J_m = J_{m+1} = \cdots$.) The upshot is that f is the sum of an R-linear combination of the $\{f_i\}$ and an $R[[x]]$-linear combiantion of the $\{g_j\}$, which proves that I is finitely generated, hence (by IV.B.10) that $R[[x]]$ is Noetherian. $\square$

Integral extensions.

We turn next to the ring-extension analogue of algebraic extensions of fields, in line with Example IV.F.2(ii).

IV.F.7. DEFINITION. Let S/R be a ring extension.

(i) $s \in S$ is **integral** over R if there exists a monic polynomial $f \in R[z]$ with $f(s) = 0$.

(ii) S/R is **integral** if all elements of S are integral over R.

The examples of IV.F.2(i) (like $\mathbb{Z}[x]/\mathbb{Z}$) and IV.F.2(iii) (like $\mathbb{Q}/\mathbb{Z}$) are not integral; those of IV.F.2(ii) are. Indeed, $\mathcal{O}_K/\mathbb{Z}$ is integral by the very definition of algebraic integers. As for the 2:1 curve-cover scenario $Y \twoheadrightarrow X$: taking $s = F(x,y) \in S$, we have that $f(z) := (z - F(x,y))(z - F(x,-y)) \in \mathbb{C}[x][z] = R[z]$ is monic, with $f(s) = 0$. (Here $F(x,y) + F(x,-y)$ and $F(x,y)F(x,-y)$ are both in $\mathbb{C}[x]$ because they are "Galois-invariant".)

Moreover, in the curve-cover case there is at least one point y "upstairs" over every point x "downstairs". This translates to having a prime ideal Q of S "over" each prime ideal P of R, in the sense that $Q \cap R = P$, since functions vanishing at x pull back to ones vanishing at y. Alternatively, for $\mathcal{O}_K/\mathbb{Z}$, for each prime $(p) \subset \mathbb{Z}$, we can factor $p\mathcal{O}_K = P_1 \dots P_r$ into primes of $\mathcal{O}_K$; and then each $P_j \cap \mathbb{Z} = (p)$ (why?). We will make this sort of "primes over primes" business more rigorous later and show that it is always true for integral extensions.

The next result generalizes [**Algebra I**, III.L.1] (the $R = \mathbb{Z}$ case):

IV.F.8. PROPOSITION. *For a ring extension S/R and element $s \in S$, the following are equivalent:*

(i) *s is integral over R;*

(ii) *$R[s]$ is a finitely-generated R-module;*

(iii) *there is a subring $T \subset S$ which contains $R[s]$ and is finitely-generated as an R-module; and*

(iv) *there is an $R[s]$-submodule $M \subset S$ which is finitely-generated as R-module and has trivial annihilator in $R[s]$.*

PROOF. (i) $\Longrightarrow$ (ii): Suppose $f(x) \in R[x]$ is monic, with $f(s) = 0$; and let $g(s) \in R[s]$ be arbitrary. By the division algorithm, we have $g(x) = f(x)q(x) + r(x)$, with $\deg(r) < \deg(f) =: m$. Substitution gives $g(s) = r(s)$, and so $R[s] = R\langle 1, s, \ldots, s^{m-1}\rangle$.

(ii) $\Longrightarrow$ (iii): Take $T = R[s]$.

(iii) $\Longrightarrow$ (iv): Put $M := T$; then $R \subset R[s] \subset T \implies M$ is a f.g. R-module containing $R[s]$. Since $M \ni 1$, $\operatorname{ann}_{R[s]}(M) = \{0\}$.

(iv) $\Longrightarrow$ (i): We are given that $M = R\langle \mu_1, \ldots, \mu_n\rangle$ is closed under multiplication by $R[s]$; accordingly, write $s\mu_i = \sum_j r_{ij}\mu_j$. Letting A denote the matrix with entries $a_{ij} := -r_{ij} + s\delta_{ij}$, this becomes $\sum_j a_{ij}\mu_j = 0$. If B is the identity matrix with k^{th} column replaced by $\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$, then AB has a column of zeroes hence $0 = \det(AB) = \det(A)\det(B) = \det(A)\mu_k$. As this holds for each k, and by assumption $\operatorname{ann}_{R[s]}(M) = \{0\}$, we have $\det(A) = 0$, which says that s satisfies the characteristic polynomial of $(r_{ij}) \in M_n(R)$. □

As a consequence, we get that "finite" extensions are integral, as the examples suggest:

IV.F.9. COROLLARY. (a) *If S/R is finitely generated as an R-module, then S/R is integral.*

(b) *If S/R is an extension and $s_1, \ldots, s_n \in S$ are integral over R, then $R[s_1, \ldots, s_n]$ is a f.g. R-module which is* (*as a ring*) *integral over R.*

(c) *If S/R and T/S are integral extensions, then T/R is integral.*

PROOF. (a) Let $s \in S$, and $T := S$ in IV.F.8(iii). Done by (i).

(b) For each j, s_j is integral over $R[s_1, \ldots, s_{j-1}]$, and so $R[s_1, \ldots, s_j]$ is f.g. as a module over $R[s_1, \ldots, s_{j-1}]$ by IV.F.8[(i) $\Longrightarrow$ (ii)]. By taking all products of generators up the tower, we get a (finite) set of generators for $R[s_1, \ldots, s_n]$ as R-module. Apply part (a).

(c) Given $t \in T$, there is a monic $f = \sum_i s_i x^i \in S[x]$ with $f(t) = 0$. So t is integral over $R[s_0, \ldots, s_{n-1}]$, whence (by IV.F.8[(i) $\Longrightarrow$ (ii)]) $R[s_0, \ldots, s_{n-1}][t]$ is a f.g. $R[s_0, \ldots, s_{n-1}]$-module. By part (b),

$R[s_0 \ldots, s_{n-1}]$ is f.g. as R-module, and thus (by multiplying generators) $R[s_0, \ldots, s_{n-1}][t]$ is f.g. as R-module. Applying IV.F.8[(iii) $\Longrightarrow$ (i)] (to the subring $R[s_0, \ldots, s_{n-1}][t]$ containing $R[t]$), we get that t is integral over R. □

IV.F.10. DEFINITION. Given a ring extension S/R, the **integral closure** $\hat{R}$ (of R in S) is the subset of S comprising all elements integral over R.

The basic example to have in mind here is where $S = K$ is a number field and $R = \mathbb{Z}$; then by definition of the ring of integers, $\hat{R} = \mathcal{O}_K$.

IV.F.11. COROLLARY. *$\hat{R}/R$ is an integral extension containing all subrings of S integral over R.*

PROOF. The main thing to check is that $\hat{R}$ is a ring. Given $s, t \in \hat{R}$, $R[s, t]$ is integral over R by IV.F.9(b). So its elements st and $s \pm t$ are integral over R, i.e. belong to $\hat{R}$. □

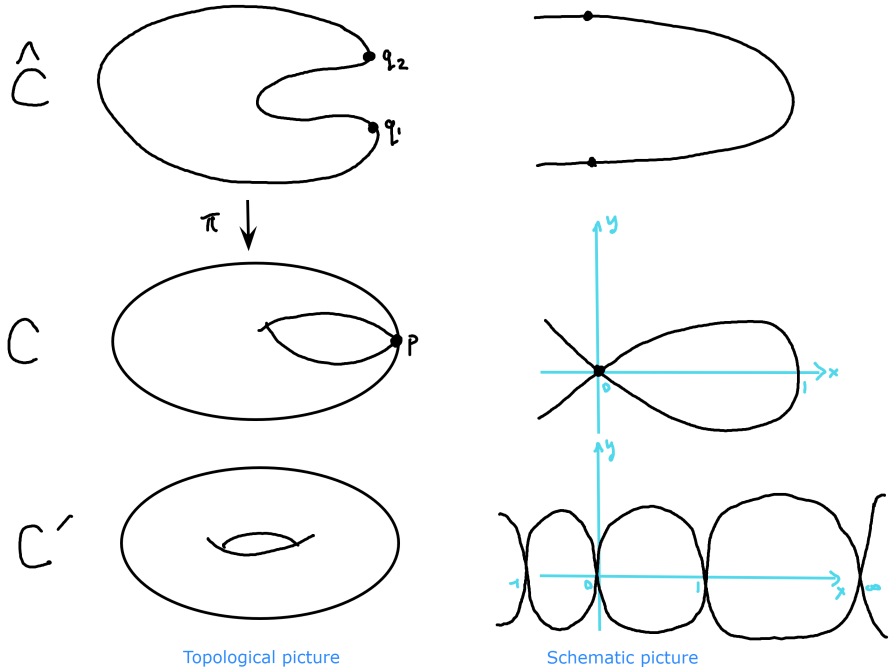
IV.F.12. DEFINITION. (i) Given a ring extension S/R, we say that R is **integrally closed** in S if $R = \hat{R}$.

(ii) Given a domain R, R is **integrally closed** or **normal** if it is integrally closed in its fraction field.

For a number field K, $\mathcal{O}_K$ is integrally closed in K (though not in $\mathbb{C}$). But here is a considerably deeper

IV.F.13. EXAMPLE. Consider the rings $R = \frac{\mathbb{C}[x,y]}{(y^2-x^3+x^2)}$ and $R' = \frac{\mathbb{C}[x,y]}{(y^2-x^3+x)}$. It turns out that R' is normal (which we won't prove), while R is not: the monic polynomial $z^2 - (x-1) \in R[z]$ has solution $\frac{y}{x}$ in $\mathfrak{F}(R)$, since $\frac{y^2}{x^2} - (x-1) = \frac{x^3-x^2}{x^2} - (x-1) = 0$. So one might ask whether $T := \frac{\mathbb{C}[x,y,z]}{(y^2-x^3+x^2, z^2-x+1)}$ gives the integral closure $\hat{R} \subset \mathfrak{F}(R)$. This isn't quite correct; as you'll see in the HW, T isn't even a domain, and one needs to add a generator to the ideal in the denominator. Once one does that, one has indeed constructed $\hat{R} = R[\frac{x}{y}] \subset \mathfrak{F}(R)$.

Geometrically, we can think of R and R' as the rings of polynomial functions on the curves $C = \{(x,y) \mid y^2 = x^2(x-1)\}$ and $C' = \{(x,y) \mid y^2 = x^3 - x\}$ in $\mathbb{C}^2$:



Topological picture Schematic picture

The key difference between these curves is that C' is nonsingular, whereas C has a "nodal" singularity at $(0,0)$ with two tangent lines, $x = \mathbf{i}y$ and $x = -\mathbf{i}y$. For hypersurfaces, a singularity is just a point where all the partials of the defining equation vanish; the corresponding coordinate ring is non-normal essentially when a hypersurface is singular in *codimension* 1. So for curves, singular means non-normal.

Replacing R by $\hat{R}$ amounts to *resolving the singularity* by disconnecting these two local branches of C, to get $\hat{C}$. (The full ideal you'll find in HW provides equations for $\hat{C}$ in $\mathbb{C}^3$, and the map π is simply the one that forgets the z-coordinate.) This makes sense because the new function $\frac{y}{x}$ distinguishes between q_1 and q_2 (by taking the distinct values $+\mathbf{i}$ and $-\mathbf{i}$), whereas the restriction of a polynomial in $\mathbb{C}[x,y]$ is well-defined at $p = (0,0)$ and so cannot.

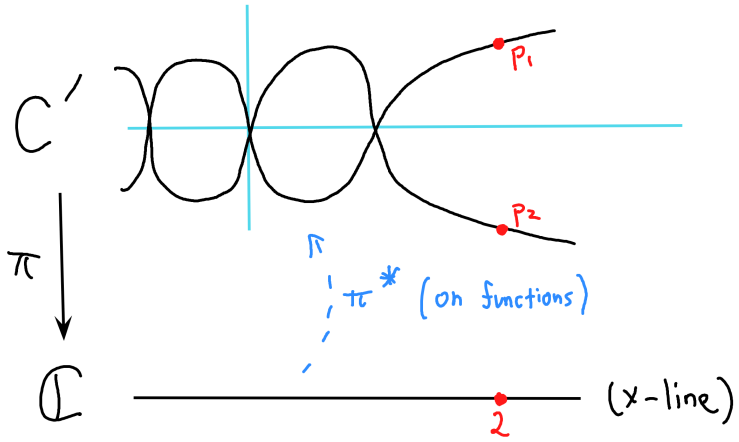
The map $\pi\colon \hat{C} \to C$ is called the *normalization* of C. This is totally different from the "Noether normalization" that we will encounter in the next section.

"Lying over" and "going up".

Let S/R be a ring extension. We are now ready to take a look at the relationship between prime ideals in R and S.

IV.F.14. PROPOSITION-DEFINITION. *Given a proper ideal I of S, $J := I \cap R$ is a proper ideal of R. We call J the* ***contraction*** *of I to R, and say that I* ***lies over*** *J. In particular, if I is prime then so is J.*

PROOF. J is an ideal because given $\jmath \in J$ and $r \in R$, $\jmath r \in (I \cap R)R \subset IS \cap R \subset I \cap R = J$; it is proper because $1 \notin I \implies 1 \notin J$. Finally, if $r_1 r_2 \in J\,(\subset I)$ for $r_1, r_2 \in R\,(\subset S)$, and I is prime, then r_1 or r_2 belongs to I, hence J. □



IV.F.15. EXAMPLES. (a) Consider $R = \mathbb{C}[x]$ inside $S' = \frac{\mathbb{C}[x,y]}{(y^2-x^3+x)}$ from IV.F.13, an inclusion given by pullback of (polynomial) functions from the x-line to $C' = \{(x,y) \mid y^2 = x^3 - x\}$. The ideals $I_1 = (x-2, y-\sqrt{6})$ and $I_2 = (x-2, y+\sqrt{6})$ in S' are prime, comprising functions on C' vanishing at $p_1 = (2,\sqrt{6})$ resp. $p_2 = (2,-\sqrt{6})$. (A product of functions FG vanishing at p_i certainly means that F or G does.)

Their contractions to R are both $J = (x-2)$, since $f(x) \in R$ vanishes on p_i iff $f(2) = 0$. So we see the reason for the terminology: the $\{I_i\}$ lie over $(x-2)$, just as the points $\{p_i\}$ lie over $x = 2$. Moreover, since

$$(y-\sqrt{6})(y+\sqrt{6}) = y^2 - 6 = x^3 - x - 6 = (x-2)(x^2+2x+3) \\ \in (x-2)S,$$

we have $I_1 \cap I_2 = I_1 I_2 = (x-2)S$.

(b) In $S = \mathbb{Z}[\sqrt{-5}]$, $I = (3, 1+\sqrt{-5})$ and $\tilde{I} = (3, 1-\sqrt{-5})$ are distinct primes whose contraction to $R = \mathbb{Z}$ is (3). (That is, I and $\tilde{I}$ lie over (3).) Moreover, their product is the ideal $(3)\mathbb{Z}[\sqrt{-5}]$.

The fact that a prime in S always contracts to a prime in R matches the geometric idea that irreducible objects "upstairs" have irreducible images "downstairs". Conversely, we might ask whether, given a prime $P \subset R$ "downstairs", there is a prime lying over it. Certainly the preimage of an irreducible (like the point $x = 2$) under the maps we've seen are not irreducible, but they do *break into* irreducibles. On the other hand, it's clear we need another hypothesis: what if, in the last picture, we replaced C' by $C' \backslash \{p_1, p_2\}$? (Or worse, how about them primes of $\mathbb{Q}$ lying over $(2) \subset \mathbb{Z}$?) I claim that integrality will suffice to rule such a situation out:

IV.F.16. THEOREM (Lying-over). *Let S/R be an integral extension, and $P \subset R$ a prime ideal. Then there exists a prime $Q \subset S$ lying over P.*

PROOF. If P is prime, then $R \backslash P$ is a multiplicative subset *of* S (in the sense of IV.A.1). Let $Q \subset S$ be maximal amongst ideals of S avoiding $R \backslash P$; then by IV.C.1, Q is prime! Clearly also $Q \cap R \subset P$. I claim that this inclusion is an equality.

Suppose otherwise, and consider $u \in P \backslash (Q \cap R)$. Then we have $Q + S(u) \supsetneq Q$, whence maximality of Q (in the above sense) gives $(Q + S(u)) \cap (R \backslash P) \neq \emptyset$. Let $c = q + su$ be an element of this latter intersection.

Since S/R is integral, there is a monic $f(x) = x^n + \sum_{j=0}^{n-1} r_j x^j \in R[x]$ with $f(s) = 0$, so that

$$0 = u^n f(s) = (su)^n + \sum_{j=0}^{n-1} r_j u^{n-j} (su)^j.$$

Substituting $su = c - q$, we find that $\nu := c^n + \sum_{j=0}^{n-1} r_j u^{n-j} c^j \in Q$. As $c, u, r_j \in R$, in fact $\nu \in R \cap Q \subset P$; and since $u \in P$ as well, we get $c^n \in P$. By primeness of P, this gives $c \in P$, a contradiction. □

We can also refine the lying-over question. For instance, say we have a map $\pi\colon Y \to X$ between surfaces. If $C \subset Y$ is an irreducible curve, and $p \in \pi(C) \subset X$ a point, is there a point of C lying over p?

IV.F.17. THEOREM (Going-up). *Let S/R be an integral extension, $P_1 \subset P \subset R$ primes, and $Q_1 \subset S$ a prime lying over P_1. Then there exists a prime Q lying over P, with $Q_1 \subset Q \subset S$.*

PROOF. We have $Q_1 \cap R = P_1 \subset P \implies Q_1 \cap (R \backslash P) = \emptyset$. Let Q be maximal among ideals of S avoiding $R\backslash P$ *and containing* Q_1. Again by IV.C.1, Q is prime, and $Q \cap R \subset P$. The remainder of the proof is as in IV.F.16. □

The reason for the name "going up" has to do with ascending chains:[6] given $P_0 \subset P_1 \subset \cdots \subset P_n$ primes of R, $Q_0 \subset Q_1 \subset \cdots \subset Q_k$ ($k < n$) primes of S, and Q_i lying over P_i for each $i \leq k$; then inductively applying IV.F.17, we can extend the latter chain by primes $Q_{k+1}, \ldots, Q_n$ lying over the corresponding $\{P_i\}$.

Now one obtains an integral extension S of R by adjoining solutions to polynomial equations, which suggests finite covers; and our main geometric example has involved a pair of curves. It doesn't seem to bold to guess that S and R should have the same (Krull) dimension. The going-up story suggests the following argument: say R has a finite dimension d, and $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d$ is a maximal chain of primes. Then (by IV.F.16-IV.F.17) there is a chain of primes

[6]There is also a "going-down" result for desceinding chains of primes, provided that (in addition to S/R being integral) R is normal. We won't prove this. All of these results — lying-over, going-up, and going-down — are due to Cohen and Seidenberg (1945).

$Q_0 \subsetneq \cdots \subsetneq Q_d$ in S lying over it, where $Q_{i-1} \subsetneq Q_i$ because their intersections with R satisfy $P_{i-1} \subsetneq P_i$. This shows $\dim(S) \geq \dim(R)$.

For the opposite inequality, begin with a chain of primes Q_i in S and intersect them with R. For this to yield a chain in R of the same length, we need to know that $Q_{i-1} \subsetneq Q_i$ contracting to the *same* prime of R cannot happen:

IV.F.18. PROPOSITION. *If S/R is integral, $P \subset R$ is prime, and $Q \subseteq Q' \subset S$ are primes both lying over P, then $Q = Q'$.*

PROOF. Suppose otherwise, and pick $u \in Q' \backslash Q$. Since u is integral over R, we may choose $f = \sum_{i=0}^{n} r_i x^i \in R[x]$ monic of least (positive) degree satisfying $f(u) \in Q$. (Certainly, if we can get $f(u) = 0$, we can get $f(u) \in Q$.) But then $r_0 = f(u) - \sum_{i=1}^{n} r_i u^i \in Q' \cap R = P = Q \cap R \subset Q \implies u(\sum_{i=1}^{n} r_i u^{i-1}) \in Q$. Since $\sum_{i=1}^{n} r_i u^{i-1} \notin Q$ by minimality, primeness of Q implies $u \in Q$, a contradiction. □

The Proposition completes the line of thought above, yielding:

IV.F.19. COROLLARY. *If S/R is integral, then* $\dim(S) = \dim(R)$.

The following restatement of IV.F.18 is also useful:

IV.F.20. COROLLARY (Incomparability). *If Q and Q' are distinct primes in an integral extension S/R lying over the same prime P, then $Q' \not\subset Q$ and $Q \not\subset Q'$.*

Finally, we get the algebraic version of "points upstairs correspond to points downstairs":

IV.F.21. COROLLARY. *Suppose S/R is integral, and $Q \subset S$ is a prime lying over $P \subset R$. Then Q is maximal in $S \iff P$ is maximal in R.*

PROOF. ($\underline{\implies}$): Let $\mathfrak{m} \supset P$ be maximal in R, and $Q' \supset Q$ be a prime lying over it (by IV.F.17). Since Q is maximal, $Q' = Q$; hence $P = Q \cap R = Q' \cap R = \mathfrak{m}$.

($\underline{\impliedby}$): Let $\mathfrak{m} \supset Q$ be maximal in S; then $P = R \cap Q \subset R \cap \mathfrak{m} \subsetneq R$. Since P is maximal, $P = R \cap \mathfrak{m}$. But then Q and $\mathfrak{m}$ both lie over P, with $Q \subset \mathfrak{m}$; and so by IV.F.18 we conclude that $Q = \mathfrak{m}$. □

Examples of integrally closed domains.

You may recall the big diagram [**Algebra I**, (III.B.1)] from when we first introduced rings last term: we have only now, with IV.F.12(ii), "filled in" the class between UFDs and commutative domains:

$$\text{(IV.F.22)} \qquad \boxed{\text{PIDs}} \subset \boxed{\text{UFDs}} \subset \boxed{\begin{array}{c}\text{integrally closed}\\ \text{domains}\end{array}} \subset \boxed{\begin{array}{c}\text{commutative}\\ \text{domains}\end{array}}$$

in which it remains to check the second inclusion:

IV.F.23. PROPOSITION. *UFDs are integrally closed.*

PROOF. Let R be a UFD, with fraction field $F := \mathfrak{F}\{R\}$. Because GCDs are defined in R, we can write any element of F as $\frac{r}{r_0}$ with $\gcd(r, r_0) = 1$. Suppose that $\frac{r}{r_0} \in \hat{R}$: that is, it satisfies a monic integral equation $(\frac{r}{r_0})^m + \sum_{j=1}^m r_j(\frac{r}{r_0})^{m-j} = 0$. Then multiplying by r_0^m, we get $r^m + \sum_{j=1}^m r_j r_0^j r^{m-j} = 0$, so that $r_0 \mid r^m$. But $\gcd(r^m, r_0) = 1$, and so $r_0 \sim 1$ is a unit, and $\frac{r}{r_0} \in R$. □

In fact, there is a key example of integrally closed domain which could replace UFDs in (IV.F.22):

IV.F.24. DEFINITION. A **Dedekind domain** is a commutative domain which is Noetherian, integrally closed, and in which every nonzero prime ideal is maximal.[7]

To see that indeed

$$\text{(IV.F.25)} \qquad \boxed{\text{PIDs}} \subset \boxed{\text{Dedekind domains}} \subset \boxed{\begin{array}{c}\text{integrally closed}\\ \text{domains}\end{array}}$$

note that:

- every prime in a PID is maximal by the argument in IV.F.5;
- PIDs are integrally closed by IV.F.23; and
- PIDs are Noetherian e.g. by IV.B.10.

[7] Some authors insist on the additional proviso "not a field" in this definition. We prefer not to do this as it ruins (IV.F.25). You can think of the difference as a Dedekind domain having Krull dimension ≤ 1 (for us) vs. $= 1$ (if fields are out).

IV.F.26. EXAMPLES. (a) Of course, $\mathbb{Z}$ is a PID hence both UFD and Dedekind domain. By the results at the end of §I.M, we also know that any ring of integers $\mathcal{O}_K$ in a number field has all ideals f.g. (hence is Noetherian by IV.B.10), and all prime ideals maximal. Since $\mathcal{O}_K$ is integrally closed by definition, it is a Dedekind domain. Notice that $\mathcal{O}_K$ is *not* a UFD unless the class number is 1 (in which case it is also a PID).

(b) Another classic PID is $k[x]$, for k any field. More generally, $k[x_1, \ldots, x_n]$ is a UFD for any field k. By the Hilbert basis theorem, it is Noetherian; and it is also integrally closed. But for $n > 1$ there are plenty of non-maximal primes, like (x_1)! (As we'll see in the next section, primes correspond to irreducible k-varieties in $\bar{k}^n$; and one can think of the height of a prime as the codimension of said variety. Maximal ideals are the primes of height n, and correspond to points[8] in k^n.) So polynomial rings in more than one variable are *not* Dedekind domains.

(c) A different generalization of $k[x]$ is the ring of polynomial functions on a *smooth* algebraic curve, e.g. $k[x,y]/(f)$ with $f = y^2 - x^3 + x$. It turns out that these are all Dedekind domains, but *not* UFDs unless the curve is *rational*, which is to say, isomorphic to (an open subset of) the k-line. (Moreover, no coordinate rings of higher-dimensional varieties will be Dedekind, as they have Krull dimension ≥ 1.)

Our goal in the remainder of this section is to prove that we have "unique ideal factorization" in Dedekind domains, just as we did in the special case $\mathcal{O}_K$. To do this, we need to introduce the objects, important in their own right, which will be the localizations of Dedekind domains at primes.

IV.F.27. DEFINITION. A **discrete valuation ring (DVR)** is a local ring, not a field, which is also a PID.

[8] if $k = \bar{k}$, to individual points; if not, then to finite collections of points on which $\mathrm{Aut}(\bar{k}/k)$ acts transitively.

Since prime ideals are maximal in a PID, and local rings have a unique maximal ideal, any DVR R has a unique prime ideal (π). Indeed, up to units π is the unique prime of R up to multiplication by a unit (why?); π is called a *uniformizer*. So every element of R is of the form $\pi^m u$, so there a well-defined *order* or *valuation*

$$\operatorname{ord}(r) := \max\{n \in \mathbb{N} \big| \ \pi^n \mid r\}$$

which, in particular, makes R into a Euclidean domain.

IV.F.28. EXAMPLES. $k[x]_{(x)}$ and $k[[x]]$ for any field k (with $\pi = x$); $\mathbb{Z}_{(p)}$ and $\hat{\mathbb{Z}}_{(p)}$ for any prime number $(\pi =)\ p$.

IV.F.29. PROPOSITION. *A domain R is a DVR $\iff$ R is Noetherian, integrally closed, and has one nonzero prime ideal.*

PROOF. ($\underline{\implies}$): follows from the definition (since a PID is Noetherian and integrally closed).

($\underline{\impliedby}$): clearly R is local and not a field; we must show that it is a PID. First, let $a \in R\backslash(R^* \cup \{0\})$, and put $M := R/(a)$. Taking a maximal element P of the set of (proper) ideals $\{\operatorname{ann}(m) \mid m \in M\backslash\{0\}\}$, we can write $P = \operatorname{ann}(b + (a)) = \{r \in R \big| \ a \mid rb\}$. Since $b \notin (a)$, we have $\frac{b}{a} \notin R$. I claim that $\frac{a}{b} \in R$, and $P = (\frac{a}{b})$.

By construction, $Pb \subset (a)$ hence $\frac{b}{a}P \subset R$. If $\frac{b}{a}P \subset P$, then P is an $R[\frac{b}{a}]$-submodule of $\mathfrak{F}\{R\}$ which is f.g. as R-module and has trivial annihilator in $R[\frac{b}{a}]$. By IV.F.8[(iv) $\implies$ (i)], we get $\frac{b}{a} \in \hat{R}$. But $\hat{R} = R$ by assumption, so $\frac{b}{a} \in R$, a contradiction. Conclude that (since P is maximal) $\frac{b}{a}P = R$ hence $P = \frac{a}{b}R = (\frac{a}{b})$. Claim is proved.

Writing $\pi := \frac{a}{b}$, for an arbitrary ideal $I \subsetneq R$ consider the ascending chain of R-modules $I \subset I\pi^{-1} \subset I\pi^{-2} \subset \cdots$ inside $\mathfrak{F}\{R\}$. If $I\pi^{-j} = I\pi^{-j-1}$ for some j, then $\pi^{-1}(I\pi^{-j}) = I\pi^{-j} \implies \pi^{-1} \in \hat{R} = R$ (again by IV.F.8[(iv) $\implies$ (i)]), a contradiction. So the chain is strictly ascending, and thus cannot be contained in R by Noetherianity. Let ℓ be the maximum integer for which $I\pi^{-\ell} \subset R$. Then $I\pi^{-\ell}$ is an ideal of R not contained in P (as $P\pi^{-1} \subset R$). Thus, $I\pi^{-\ell} = R$ and $I = (\pi^\ell)$. $\square$

IV.F.30. PROPOSITION. *The localization of a Dedekind domain R at any nonzero prime is a DVR.*

PROOF. We know that the localization R_P at a prime P preserves Noetherianity by IV.A.8(i), and produces a local ring with unique prime ideal by IV.A.13(i).

To see that localization also preserves integral closedness, write $\mathcal{S} = R\backslash P$ (so that $\mathcal{S}^{-1}R = R_P$) and suppose $a \in \mathfrak{F}\{R\} = \mathfrak{F}\{\mathcal{S}^{-1}R\}$ is integral over $\mathcal{S}^{-1}R$. Then a satisfies an equation of the form $a^m + \sum_{j=1}^{m} \frac{r_j}{s_j} a^{m-j} = 0$, and multiplying this m times by $s := s_1 \cdots s_m$ shows that sa is integral over R. Since $R = \hat{R}$ by assumption, $sa \in R$ hence $a = \frac{sa}{s} \in \mathcal{S}^{-1}R$; conclude that $\widehat{\mathcal{S}^{-1}R} = \mathcal{S}^{-1}R$.

So the localization of R satisfies the 3 properties on RHS(IV.F.29), hence is a DVR. □

IV.F.31. THEOREM. *Every proper nonzero ideal in a Dedekind domain R has a unique factorization as a product of prime ideals of R.*

PROOF. Let $\{0\} \subsetneq I \subsetneq R$ be given, and $I = \cap_{i=1}^{m} Q_i$ be a RPD. The $P_i := \mathrm{Rad}(Q_i)$ are distinct, and *maximal* (R being Dedekind). So P_i is the *only* prime containing Q_i, and does *not* contain any other Q_j; hence $Q_i + Q_j = R$ for $i \neq j$, and the $\{Q_i\}$ are coprime, whence $I = Q_1 \cdots Q_m$.

As a subset of P_i, Q_i avoids $\mathcal{S} := R\backslash P_i$. One easily checks that primary ideals avoiding $\mathcal{S}$ are in bijection with primary ideals of $\mathcal{S}^{-1}R = R_{P_i}$. Since R_{P_i} is a DVR by IV.F.30, the latter are powers of $\mathcal{S}^{-1}P_i$; hence Q_i is a power of P_i. Conclude that $I = P_1^{a_1} \cdots P_m^{a_m}$ for some $a_i \in \mathbb{Z}_{>0}$. □

Though we won't prove this, it is perhaps not surprising (in view of the examples in IV.F.26) that the intersection of the class of UFDs and the class of Dedekind domains is precisely that of PIDs. (So, for a UFD, one has Dedekind $\iff$ PID; and for a Dedekind domain, one has UFD $\iff$ PID.) That said, it's also a little weird: for non-PIDs, you have to choose between having "unique ideal factorization" (into prime ideals) and unique factorization of elements!