IV. Commutative rings

If noncommutative rings are at the heart of the theory of linear representations of finite groups, then commutative rings underpin that of algebraic varieties and schemes. In this final stretch of the course, we will cover just enough commutative algebra to reach the Hilbert Nullstellensatz, which will give a bijective correspondence between (i) varieties (solution sets of polynomial equations in n variables) over an algebraically closed field k and (ii) radical ideals (which contain f if they contain a power of f) in the polynomial ring $k[x_1, \ldots, x_n]$. This is, in some sense, the foundational result of algebraic geometry.

It is helpful to have a running example in mind while reading through the definitions and proofs, starting with localization. For some purposes $R = \mathbb{Z}$ will do, but $R = \mathbb{C}[x]$ (or $\mathbb{C}[x, y]$) gives a more geometric feel to the material, as it comprises the *regular* (think "algebraic holomorphic") functions on the "complex line" $\mathbb{C}$. So when *localization* ***away from*** *an element* $r \in R$ tells us to consider the ring of fractions $R[\frac{1}{r}]$, one can take $r = x - a \in \mathbb{C}[x]$ and think of the functions of the form $\frac{Q(x)}{(x-a)^k}$ (Q polynomial), which are the regular functions on $\mathbb{C}\backslash\{a\}$ (hence the "away from").

Similarly, when *localization* ***at*** *a prime ideal* P of R defines R_P to consist of fractions $\frac{r}{s}$ ($r \in R$, $s \in R\backslash P$), one can take $P = (x - a)$ and think of rational functions $\frac{Q(x)}{R(x)}$ with $x - a \nmid R(x)$. These are regular functions on "$\mathbb{C}$ minus everything but a" (by which one means the complement of *some* finite point set not including a, or an "inverse limit" of such complements). The upshot is that this leaves one with only one maximal ideal, namely $(x - a)$, in $\mathbb{C}[x]_{(x-a)}$, and quotienting by it evaluates these rational functions at a (hence the "at").

IV.A. Localization

Let R be a commutative ring. The aim of this section is to construct rings of fractions which are "intermediate" between R and its fraction field, in the sense that there are restrictions on the denominators which are allowed, and the result is (in general) not a field.

IV.A.1. DEFINITION. A subset $\mathcal{S} \subset R$ is said to be **multiplicative** if $\mathcal{S}$ contains 1, does not contain 0, and

$$a, b \in \mathcal{S} \quad \implies \quad ab \in \mathcal{S}.$$

IV.A.2. EXAMPLE. Given a prime ideal $P \subset R$, $R \backslash P$ is multiplicative (why?). Given an element $r \in R$, so is $\{r^k\}_{k \geq 0}$. These are the most important examples.

Given a multiplicative subset $\mathcal{S}$, define an equivalence relation "$\sim$" on $R \times \mathcal{S}$ by

$$\text{(IV.A.3)} \quad (r, s) \sim (r', s') \iff \exists\, s_1 \in \mathcal{S} \text{ such that } s_1(s'r - sr') = 0.$$

The RHS is equivalent to $rs' = r's$ provided R has no zero-divisors.[1] Taking the quotient by (IV.A.3), put

$$\text{(IV.A.4)} \qquad \mathcal{S}^{-1}R := \frac{R \times \mathcal{S}}{\sim}.$$

By "0" and "1" in $\mathcal{S}^{-1}R$ we'll mean the equivalence classes of $(0, 1)$ and $(1, 1)$, respectively. These are distinct, since $s_1(1 \cdot 1 - 0 \cdot 1) = 0$ is impossible. More generally, denote the equivalence-class of (r, s) by $\frac{r}{s} \in \mathcal{S}^{-1}R$, and write $\frac{r}{s} = \frac{r'}{s'}$ to mean that $(r, s) \sim (r', s')$. We notice right away that $\frac{tr}{ts} = \frac{r}{s}$ for any $t \in \mathcal{S}$, since $1(trs - rts) = 0$. Clearly, it's consistent with all of this to write $r = \frac{r}{1}$.

IV.A.5. PROPOSITION. *$\mathcal{S}^{-1}R$ is a commutative ring, which is a domain if R is.* (*In the special case where R is a domain and $\mathcal{S} = R \backslash \{0\}$, it is the fraction field of R.*)

---

[1] Clearly, it would have been a *terrible* idea to allow $0 \in \mathcal{S}$, because then everything would be equivalent (and the quotient (IV.A.4) would be zero)!

SKETCH. There are a lot of little checks here, beginning with the well-definedness of multiplication $\frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$ and addition $\frac{r}{s} + \frac{r'}{s'} := \frac{rs'+r's}{ss'}$. For instance, suppose $\frac{r}{s} = \frac{r_0}{s_0}$; then for some $s_1 \in \mathcal{S}$, we have $s_1(rs_0 - sr_0) = 0 \implies s_1\{rs_0(s')^2 - sr_0(s')^2 + ss_0s'r' - ss_0r's'\} = 0 \implies \frac{r_0s'+r's_0}{s_0s'} = \frac{rs'+r's}{ss'} \implies \frac{r_0}{s_0} + \frac{r'}{s'} = \frac{r}{s} + \frac{r'}{s'}$. So addition is well-defined. I leave the distributivity and associativity to you.

Clearly, a product $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$ is zero iff $s_1rr' = 0$ for some $s_1(\neq 0)$. If R is a domain, this only happens if $r = 0$ or $r' = 0$, in which case $\frac{r}{s}$ or $\frac{r'}{s'}$ is zero. For the parenthetical on the fraction field, see [**Algebra I**, III.F.10]. □

The natural ring homomorphism

$$\begin{aligned} \phi_{\mathcal{S}} \colon R &\to \mathcal{S}^{-1}R \\ r &\mapsto r\,(:= \tfrac{r}{1}) \end{aligned} \tag{IV.A.6}$$

is evidently injective iff $\frac{r}{1} = \frac{0}{1} \implies r = 0$, which is equivalent to $\mathcal{S}$ containing no zero divisors. If $\mathcal{S} \subset R^*$ then (IV.A.6) is also surjective (hence an isomorphism) because every $\frac{r}{s}$ already exists on the LHS. Indeed, the whole point of these *fraction rings* is to turn the elements of $\mathcal{S}$ into units: we have $\phi_{\mathcal{S}}(\mathcal{S}) \subset (\mathcal{S}^{-1}R)^*$ since $s \cdot \frac{1}{s} = 1$. (This does no good if they already were units!) In fact, (IV.A.6) has the *universal property* of factoring *any* map sending $\mathcal{S}$ to units:

IV.A.7. THEOREM. *Let $f\colon R \to T$ be a homomorphism satisfying $f(\mathcal{S}) \subset T^*$. Then there exists a unique homomorphism $\bar{f}\colon \mathcal{S}^{-1}R \to T$ such that $\bar{f} \circ \phi_{\mathcal{S}} = f$.*

PROOF. Set $\bar{f}(\frac{r}{s}) := f(s)^{-1}f(r)$, which we can do since $f(s) \in T^*$. This is well-defined, since $\frac{r}{s} = \frac{r'}{s'} \implies s_1(rs' - sr') = 0 \implies f(s_1)f(rs' - sr') = 0 \implies f(rs' - sr') = 0$ (since $f(s_1) \in T^*$) $\implies f(s)^{-1}f(r) = f(s')^{-1}f(r')$. Clearly $\bar{f}(\phi_{\mathcal{S}}(r)) = f(r)$, and checking $\phi_{\mathcal{S}}$ a homomorphism is easy.

For the uniqueness, suppose $g\colon \mathcal{S}^{-1}R \to T$ has $g \circ \phi_{\mathcal{S}} = f$. Then $1 = g(s \cdot \frac{1}{s}) = g(s) \cdot g(\frac{1}{s}) \implies g(\frac{r}{s}) = g(\frac{1}{s})g(r) = g(s)^{-1}g(r) = f(s)^{-1}f(r) \implies g = \bar{f}$. □

Next we want to consider ideals in the fraction rings. Given an ideal $I \subset R$, we can define one in $\mathcal{S}^{-1}R$ by $\mathcal{S}^{-1}I := (I \times \mathcal{S})/\sim$, and this is compatible with sums, products, and intersections (of ideals). But it is only interesting if I avoids the multiplicative subset:

IV.A.8. PROPOSITION. (i) $\mathcal{S}^{-1}I = \mathcal{S}^{-1}R \iff \mathcal{S} \cap I \neq \emptyset$.
(ii) *Every ideal in* $\mathcal{S}^{-1}R$ *is of the form* $\mathcal{S}^{-1}I$.

PROOF. (i) ($\impliedby$): $s \in \mathcal{S} \cap I \implies 1_{\mathcal{S}^{-1}R} = \frac{s}{s} \in \mathcal{S}^{-1}I$.
($\implies$): $\phi_{\mathcal{S}}^{-1}(\mathcal{S}^{-1}I) = \phi_{\mathcal{S}}^{-1}(\mathcal{S}^{-1}R) = R \implies 1 = \phi_{\mathcal{S}}(1_R) = \frac{\imath}{s}$ for some $\imath \in I \implies s_1(\imath - s) = 0$ for some $s_1 \in \mathcal{S} \implies s_1 s = s_1 \imath \in \mathcal{S} \cap I$.

(ii) Let $J \subset \mathcal{S}^{-1}R$ be an ideal. Then $\phi_{\mathcal{S}}^{-1}(J) =: I$ is an ideal in R, and $\mathcal{S}^{-1}I = \mathcal{S}^{-1}R \cdot \phi_{\mathcal{S}}(I) \subset \mathcal{S}^{-1}R \cdot J \subset J$. But if $\frac{r}{s} \in J$, then $\phi_{\mathcal{S}}(r) = \frac{r}{1} = \frac{s}{1} \cdot \frac{r}{s} \in J \implies r \in \phi_{\mathcal{S}}^{-1}(J) = I \implies \frac{r}{s} \in \mathcal{S}^{-1}I$. $\square$

Given the central role of prime ideals in the structure of commutative rings, the compatibility of this construction with primality is of particular importance:

IV.A.9. LEMMA. *If* $P \subset R$ *is a prime ideal with* $P \cap \mathcal{S} = \emptyset$, *then* $\mathcal{S}^{-1}P \subset \mathcal{S}^{-1}R$ *is prime, and*

$$\phi_{\mathcal{S}}^{-1}(\mathcal{S}^{-1}P) = P. \tag{IV.A.10}$$

PROOF. First we check (IV.A.10): clearly $\phi_{\mathcal{S}}(P)\,(= \frac{P}{1}) \subset \mathcal{S}^{-1}P$. Conversely, $r \in \phi_{\mathcal{S}}^{-1}(\mathcal{S}^{-1}P) \implies \phi_{\mathcal{S}}(r) \in \mathcal{S}^{-1}P \implies \frac{r}{1} = \frac{p}{s}$ ($p \in P$, $s \in S$) $\implies s_1(sr - p) = 0$ (for some $s_1 \in S$) $\implies (s_1 s)r = s_1 p \in P$. But $s_1 s \in \mathcal{S}$ hence $\notin P$, so we must have $r \in P$ since P is prime.

Now for primality of $\mathcal{S}^{-1}P$: suppose $\frac{r}{s} \cdot \frac{r'}{s'} \in \mathcal{S}^{-1}P$. Then $\frac{rr'}{ss'} = \frac{p}{s_0}$, whence $s_1 s_0 rr' = s_1 ss' p \in P$. Since P is prime (and $s_1 s_0 \notin P$), we must have $rr' \in P$ hence $r \in P$ or $r' \in P$, and then $\frac{r}{s}$ or $\frac{r'}{s'}$ belongs to $\mathcal{S}^{-1}P$. $\square$

IV.A.11. THEOREM. *There is a bijection*

$$\boxed{\begin{array}{c}\textit{prime ideals in } R\\ \textit{disjoint from } \mathcal{S}\end{array}} \longleftrightarrow \boxed{\textit{prime ideals in } \mathcal{S}^{-1}R}$$

induced by

$$P \longmapsto \mathcal{S}^{-1}P.$$

PROOF. The assignment $P \mapsto \mathcal{S}^{-1}P$ is injective by (IV.A.10). For the surjectivity, let $J \subset \mathcal{S}^{-1}R$ be prime; then $P := \phi_{\mathcal{S}}^{-1}(J)$ is an ideal with $\mathcal{S}^{-1}P = J$, by the proof of IV.A.8(ii). It remains to show that P is prime: so let $ab \in P$. Then $\phi_{\mathcal{S}}(ab) = \phi_{\mathcal{S}}(a)\phi_{\mathcal{S}}(b) \in J \implies \phi_{\mathcal{S}}(a)$ or $\phi_{\mathcal{S}}(b) \in J \implies a$ or $b \in \phi_{\mathcal{S}}^{-1}(J) = P$, done. □

Returning to the two key types of multiplicative sets from IV.A.2, we have the

IV.A.12. DEFINITION. (i) Let $\mathcal{S} = R\backslash P$, with $P \subset R$ a prime ideal. Then $R_P := \mathcal{S}^{-1}R$ is called the **localization of R at P**.

(ii) Let $\mathcal{S} = \{r^k\}_{k\geq 0}$, for some $r \in R\backslash\{0\}$. Then $R[\frac{1}{r}] := \mathcal{S}^{-1}R$ is called the **localization of R away from r**.

IV.A.13. COROLLARY. (i) *Sending $Q \mapsto Q_P := \mathcal{S}^{-1}Q$ induces a bijection from prime ideals of R contained in P to prime ideals of R_P; and $P_P = PR_P$ is the unique maximal ideal of R_P.*

(ii) *Similarly, prime ideals of R not containing r are in bijection with prime ideals of $R[\frac{1}{r}]$.*

PROOF. Most of this follows from IV.A.11. For the uniqueness statement in (i), observe that a maximal ideal of R_P is prime hence of the form Q_P for $Q \subset P$ prime; and then $Q_P \subset P_P$ ($\implies Q_P = P_P$.). Also note in (ii) that $r \notin Q$ (and Q prime) implies that no power of r belongs to Q. □

IV.A.14. DEFINITION. A **local ring** is a commutative ring with a unique maximal ideal $\mathfrak{m}$.

By IV.A.13(i), the localization R_P at a prime ideal P is a local ring. If $P = \mathfrak{m}$ is maximal, this has a nice relationship to the reduction mod $\mathfrak{m}$ map $\rho \colon R \twoheadrightarrow R/\mathfrak{m}$. Since $R/\mathfrak{m} =: k_{\mathfrak{m}}$ is a field, called the **residue field** of $\mathfrak{m}$, ρ sends $\mathcal{S} := R\backslash\mathfrak{m}$ to units. By the universal property IV.A.7, ρ factors through maps

$$R \to R_{\mathfrak{m}} \overset{\rho_{\mathfrak{m}}}{\twoheadrightarrow} R/\mathfrak{m}. \tag{IV.A.15}$$

Since $\rho_{\mathfrak{m}}$ maps onto a field, its kernel is a maximal ideal; this can only be $\mathfrak{m}R_{\mathfrak{m}}$. We conclude that $R/\mathfrak{m} \cong R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}$.

IV.A.16. PROPOSITION. *For a commutative ring R, the following are equivalent:*
(i) *R is local;*
(ii) *all nonunits of R belong to some proper ideal; and*
(iii) *the nonunits of R form an ideal.*

PROOF. (i) $\implies$ (ii): Let $\mathfrak{m}$ denote *the* maximal proper ideal of R. Then $a \in R$ nonunit $\implies (a) \subsetneq R \implies (a) \subset \mathfrak{m} \implies a \in \mathfrak{m}$.
(ii) $\implies$ (iii): clear, since a proper ideal can't contain units.
(iii) $\implies$ (i): it is maximal and contains all proper ideals. $\square$

We should say a few words about localization of R-modules. For any R-module M and multiplicative subset $\mathcal{S}$, we can define $\mathcal{S}^{-1}M$ just as in (IV.A.3)-(IV.A.4), only with "$r \in R$" replaced by "$\mu \in M$". This is an $\mathcal{S}^{-1}R$-module with elements written as fractions $\frac{\mu}{s}$. In particular, when $\mathcal{S} = R \backslash P$ with P prime, $M_P := \mathcal{S}^{-1}M$ is called the **localization of M at P**.

Now recall that the annihilator of an R-module (or R-submodule, or element in an R-module), written $\mathrm{ann}_R(\cdot)$, is an ideal in R.

IV.A.17. LEMMA. *If M is a f.g. R-module, then we have the equality*

$$\mathcal{S}^{-1}\mathrm{ann}_R(M) = \mathrm{ann}_{\mathcal{S}^{-1}R}(\mathcal{S}^{-1}M) \tag{IV.A.18}$$

of ideals in $\mathcal{S}^{-1}R$. (If we replace M by an element $\mu \in M$ in (IV.A.18)*, the finite generation hypothesis on M may be dropped.)*

PROOF. We know the RHS is of the form $\mathcal{S}^{-1}J$ by IV.A.8(ii). Writing $I = \mathrm{ann}_R(M)$, $\mathcal{S}^{-1}I$ annihilates $\mathcal{S}^{-1}M$ hence $\mathcal{S}^{-1}I \subset \mathcal{S}^{-1}J$. Conversely, writing $\mu_1, \ldots, \mu_k$ for generators of M, any $\jmath \in J$ kills $\frac{\mu_1}{1}, \ldots, \frac{\mu_k}{1}$. So there exist $s_1, \ldots, s_k \in \mathcal{S}$ such that $s_i \jmath \mu_i = 0$ $(\forall i)$, and hence $s_1 \cdots s_k \jmath \in I$. Writing $\jmath = \frac{s_1 \cdots s_k \jmath}{s_1 \cdots s_k} \in \mathcal{S}^{-1}I$, we see that $J \subset \mathcal{S}^{-1}I$ hence $\mathcal{S}^{-1}J \subset \mathcal{S}^{-1}I$. $\square$

IV.A.19. THEOREM. *Let M be an R-module, and suppose $M_{\mathfrak{m}} = \{0\}$ for every maximal ideal $\mathfrak{m} \subset R$. Then $M = \{0\}$.*

PROOF. Given $\mu \in M$, put $I := \mathrm{ann}_R(\mu)$. For any maximal ideal $\mathfrak{m} \subset R$, since $\frac{\mu}{1} = 0 \in M_{\mathfrak{m}}\,(= \{0\})$, IV.A.17 gives (with $\mathcal{S} = R\backslash\mathfrak{m}$) $\mathcal{S}^{-1}I = \mathrm{ann}_{R_{\mathfrak{m}}}(0) = R_{\mathfrak{m}} = \mathcal{S}^{-1}R$. By IV.A.8(i), $I \cap \mathcal{S} \neq \emptyset$ hence $I \not\subset \mathfrak{m}$. So I is contained in no maximal ideal, and thus $I = R$. But then $1 \in R$ annihilates μ, i.e. $\mu = 1\mu = 0$.

Since $\mu \in M$ was arbitrary, we get $M = \{0\}$. $\square$

IV.A.20. REMARK. Theorem IV.A.19 says that M is determined by its localizations at maximal ideals. In fact, not just M, but its submodules and quotient modules, like kernels and images of homomorphisms.

This is really important in algebraic geometry, where R is typically a ring of regular functions on a variety X, and M represents "sections" of some object, like a sheaf (or vector bundle), "over" X. The maximal ideals correspond to "closed points" x in X, and the localizations to functions resp. sections on a "limit of open neighborhoods" of x, which form the "stalk" of the sheaf (or vector bundle). For this reason we shall speak of $M_{\mathfrak{m}}$ as a **stalk** of the module (at $\mathfrak{m}$).

Similarly, since $\mathfrak{m}$ represents functions that vanish at x in this analogy, setting them to zero (i.e. going modulo $\mathfrak{m}$) should correspond to *evaluation at x*, e.g. in the *fiber* of a vector bundle over x. Recall that $\mathfrak{m}R_{\mathfrak{m}}$ is the unique maximal ideal of $R_{\mathfrak{m}}$, and $k_{\mathfrak{m}} := R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}} \cong R/\mathfrak{m}$ the *residue field* of $\mathfrak{m}$. The point is then that "evaluation at x" corresponds to the quotient map $M \twoheadrightarrow M/\mathfrak{m}M$, where $M/\mathfrak{m}M$ is a $k_{\mathfrak{m}}$-module, i.e. vector space. Moreover, this factors through the localization, viz.

$$M \to M_{\mathfrak{m}} \twoheadrightarrow M_{\mathfrak{m}}/\mathfrak{m}M_{\mathfrak{m}} \cong M/\mathfrak{m}M,$$

essentially by tensoring over R with (IV.A.15) (though I won't explain this). We call the vector space $M/\mathfrak{m}M$ the **fiber** of M at $\mathfrak{m}$.