The Facets of Geometry

Algebraic, Arithmetical, Topological, Analytic & Categorical

(Under heavy construction!!)

March 20, 2024

I follow here the footing of thy feet,
That with thy meaning, so I may the rather meet.
-Edmund Spenser

Todo list

Contents

Part I

The Algebraic Viewpoint

Part II

The Arithmetic Viewpoint

Part III

The Topological Viewpoint

Goals:

1. Define real and complex manifolds from locally ringed spaces, examples (Wedhorn).
2. Basic constructions like linearization, product, fiber products, submanifolds, quotients (Wedhorn for theory and Bredon for applications).
3. $\mathcal{O}_X$-modules and global algebra.
4. Lie groups (Wedhorn and Taubes).
5. Torsors and 1^{st}-Cech cohomology group (Wedhorn and Mumford's chapter on cohomology of sheaves).
6. Bundles and applications (Taubes Ch.3,4,5,6,7,10, Wedhorn and Bredon both for theory and their exercises for applications).
7. Singular homology and cohomology as ES-axioms. Properties, applications and results (Bredon and May). Singular cohomology as sheaf cohomology (Wedhorn Chapter 11).
8. Fundamental group and covering maps (classification) as etale spaces of certain sheaves (Bredon Chapter 3 and my algebraic topology notes).
9. Differential forms and de-Rham cohomology (Wedhorn's Section 8.6 and Bredon's Chapter 5, with examples and exercises).
10. ($\star$ **Geometric milestone**) *Covariant derivative, connections, classes and curvature* (Taubes Ch. 11,12,13,14,15,16).
11. ($\star$ **Algebraic milestone**) *Cohomological methods in geometry* (Bredon's Chapter 6 full).
12. ($\star$ **Homotopical milestone**) *Homotopical methods* (Bredon's Chapter 7 and May).

I have to rearrange the following chapters to suit the above outline.

These chapters need not be filled with unwarranted details. They should provide the point of the construction clearly and all minute details can be safely skipped over after understanding them.

Part IV

The Analytic Viewpoint

Part V

The Categorical Viewpoint

Out of the four, this is the most foundational and the deepest one of them all. It has to be, as the main motive here is to understand some of the foundational notions of geometry, like *intersection* and *deformation*, and to act as their natural mathematical residential address. However, we would need to cover a lot of ground before we start doing geometry in this new world, most of it is due to a fundamental different way of thinking than what is done classically (more categorical than set theoretic, the latter is abound in some of the previous chapters of this book). But the rewards are high, for it will provide us a deeper understanding of fundamental questions raised throughout this book, one of them being the question of *a concrete, robust and complete theory of intersections of manifolds and schemes.*

Part VI

Special Topics

Chapter 22

Commutative Algebra

Contents

In this chapter, we collect topics from contemporary commutative algebra. The most need of all this material comes from algebraic goemetry. In particular, in the following, we list out the topics that we would need for our treatment of basic algebraic geometry.

1. Dimension theory : For dimension of schemes, Hauptidealsatz, local complete intersection, etc.
2. Integral dependence : For proper maps between affine varieties, normalization, finiteness of integral closure, certain DVRs of dimension 1, etc.
3. Field theory : For birational classification of varieties, primitive element theorem, basic algebra in general, etc.
4. Completions : Local analysis of singularities, formal schemes, complete local rings, Cohen structure theorem, Krull's theorem, etc.
5. Valuation rings : For curves and their non-singular points (DVRs) and various equivalences, Dedekind domains, etc.
6. Multiplicities : For intersections in projective spaces, intersection multiplicity, Hilbert polynomials, flat families, etc.
7. Kähler differentials : For differential forms on schemes, this will be used consistently in further topics.

8. Depth and Cohen-Macaulay : For local complete intersections, blowing up, etc.
9. Tor and Ext functors : They are tools for other algebraic notions, generizable to global algebra, tor dimension, etc.
10. Projective modules : For vector bundles, projective dimension and Ext, pd + depth = dim for regular local rings, etc.
11. Flatness : Family of schemes varying continuously, smooth and étalé maps, etc.
12. Lifting properties - Étale, unramified and smooth morphisms : These are used heavily for the corresponding scheme maps, and beyond.

Notation 22.0.0.1. Let R be a ring and $f(x) \in R[x]$ be a polynomial. We will denote $c_n(f) \in R$ to be the coefficient of x^n in $f(x)$. If $f(x,y) \in R[x,y]$, then we will denote $c_{n,m}(f) \in R$ to be the coefficient of $x^n y^m$ in $f(x,y)$. We may also write $c_{x^n}(f)$ for $c_n(f)$ and $c_{x^n y^m}(f)$ for $c_{n,m}(f)$ if it makes statements more clear.

Remark 22.0.0.2. We will consistently keep using the geometric viewpoint given by the theory of schemes (see Chapter 1) in discussing the topics below, as a viewpoint to complement the algebraic viewpoint. This will also showcase the usefulness of scheme language.

22.1 General algebra

We discus here general results about prime ideals, modules and algebras.

22.1.1 Jacobson radical and Nakayama lemma

Let R be a ring. Denote the set of all units of R as $R^\times$. The *Jacobson radical* is an ideal $\mathfrak{r}$ of R formed by the intersection of all maximal ideals of R. A *finitely generated R-module* M is a module which has a finite collection of elements $\{x_1, \dots, x_n\} \subset M$ such that for any $z \in M$, there are $r_1, \dots, r_n \in R$ so that $z = r_1x_1 + \cdots + r_nx_n$. More concisely, if there is a surjection R-module homomorphism $R^n \twoheadrightarrow M$. We then have the following results about $\mathfrak{r}$.

Proposition 22.1.1.1. *Let R be a ring and let $\mathfrak{r}$ denotes it Jacobson radical. Then,*

1. *$x \in \mathfrak{r}$ if and only if $1 - xy \in R^\times$ for any $y \in R$.*
2. *(Nakayama lemma) Let M be a finitely generated R-module. If $\mathfrak{q} \subseteq \mathfrak{r}$ is an ideal of R such that $\mathfrak{q}M = M$, then $M = 0$.*
3. *Let M be a finitely generated module and $\mathfrak{q} \subseteq \mathfrak{r}$. Let $N \leq M$ be a submodule of M such that $M = N + \mathfrak{q}M$, then $M = N$.*
4. *If R is a local ring and M, N are two finitely generated modules, then*

$$M \otimes_R N = 0 \iff M = 0 \text{ or } N = 0.$$

Proof. 1. (L ⇒ R) Suppose there is $y \in R$ such that $1 - xy \notin R^\times$. Since each non-unit element is contained in a maximal ideal by Zorn's lemma, therefore $1 - xy \in \mathfrak{m}$ for some maximal ideal. Since $x \in \mathfrak{r}$, therefore $x \in \mathfrak{m}$. Hence $xy, 1 - xy \in \mathfrak{m}$, which means that $1 \in \mathfrak{m}$, a contradiction.
(R ⇒ L) Suppose $1 - xy \in R^\times$ for all $y \in R$ and $x \notin \mathfrak{r}$. Then, again by Zorn's lemma we have $x \in R^\times$. Hence let $y = x^{-1}$ to get that $1 - xy = 1 - 1 = 0 \in R^\times$, a contradiction.

2. Suppose $M \neq 0$. Since M is finitely generated, therefore there is a submodule $N \subset M$ such that M/N is simple (has no proper non-trivial submodule). Simple R-modules are isomorphic to $R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of R via the map $M' \mapsto R/\mathrm{Ann}(x)$ where $x \neq 0$ in M. Therefore $M/N \cong R/\mathfrak{m}$. Then, $\mathfrak{m}R \neq R$ which is same as $\mathfrak{m}M \neq M$. Since $\mathfrak{q} \subseteq \mathfrak{r} \subseteq \mathfrak{m}$, hence $\mathfrak{q}M \neq M$, a contradiction.

3. Apply 2. on M/N.

4. The only non-trivial part is L $\Rightarrow$ R. Since $(M \otimes_R N)/\mathfrak{m}(M \otimes_R N) = M/\mathfrak{m}M \otimes_{R/\mathfrak{m}} N/\mathfrak{m}N$, therefore we have $M/\mathfrak{m}M \otimes_{R/\mathfrak{m}} N/\mathfrak{m}N = 0$. Since $R/\mathfrak{m}$ is a field therefore $M/\mathfrak{m}M = 0$ WLOG. Hence, $M = \mathfrak{m}M$ and since R is local, therefore $\mathfrak{r} = \mathfrak{m}$. We conclude by Nakayama. □

22.1.2 Localization

We next consider localization of rings and R-modules. Take any multiplicative set $S \subset R$ which contains 1. Then, localizing an R-module M on S is defined as

$$S^{-1}M := \{m/s \mid m \in M, s \in S\}.$$

where $m/s = n/t$ if and only if $\exists u \in S$ such that $u(mt - ns) = 0$. We have that $S^{-1}M$ is an R-module where addition $m/s + n/t = (mt + ns)/st$. In the case when $M = R$, we get a ring structure on $S^{-1}R$ as well where multiplication is given by $m/s \cdot n/t := mn/st$. There is a natural map $M \to S^{-1}M$ which maps $m \mapsto m/1$ and it may not be an injection if $\exists m \in M$ and $s \in S$ such that $s \cdot M = 0$.

Lemma 22.1.2.1. *Let $S \subset R$ be a multiplicative set in a ring R and M be an R-module. Then,*

$$S^{-1}M \cong S^{-1}R \otimes_R M.$$

Proof. One can do this by directly checking the universal property of tensor product of $S^{-1}R$ and M over R for $S^{-1}M$. We have the map $\varphi : S^{-1}R \times M \to S^{-1}M$ given by $(r/s, m) \mapsto rm/s$. Now for any bilinear map $f : S^{-1}R \times M \to N$, we can define the map $\tilde{f} : S^{-1}M \to N$ given by $\tilde{f}(m/s) := f(1/s, m)$. Clearly, $\tilde{f}$ is well-defined and $\tilde{f}\varphi = f$. Moreover, if $g : S^{-1}M \to N$ is such that $g\varphi = f$, then $g(m/s) = f(1/s, m) = \tilde{f}(m/s)$. Hence $\tilde{f}$ is unique with this property. □

Lemma 22.1.2.2. *Localization w.r.t a multiplicative set $S \subset R$ is an exact functor on* **Mod**(R).

Proof. Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of R-modules. Then we have the localized sequence $S^{-1}M' \to S^{-1}M \to S^{-1}M''$. Since $S^{-1}0 = 0$, therefore this is left exact. Exactness at middle follows from exactness at middle of the first sequence. The right exactness can be seen by right exactness of tensor product functor $S^{-1}R \otimes_R -$ and by Lemma 22.1.2.1. □

Lemma 22.1.2.3. *Let R be a ring and $S \subset R$ be a multiplicative set. Then*

$$\begin{aligned}\{\textit{prime ideals of } R \textit{ not intersecting } S\} &\xrightarrow{\cong} \{\textit{prime ideals of } S^{-1}R\}\\ \mathfrak{p} &\longmapsto S^{-1}\mathfrak{p}\end{aligned}$$

Proof. Trivial. □

Next we see an important property of modules, that is their ”local characteristic”. This means that one can check whether an element of a module is in a submodule by checking it locally at each prime, as the following lemma suggests. This has geometric significance in algebraic geometry (M induces and is induced by a quasi-coherent sheaf over $\operatorname{Spec}(R)$, see **??**).

Lemma 22.1.2.4. *Let M be an R-module. Then,*

1. *$M \neq 0$ if and only if there exists a point $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $M_\mathfrak{p} \neq 0$.*
2. *If $N \subset M$ is a submodule and $0 \neq x \in M$, then $x \in N$ if and only if $x \in N_\mathfrak{p} \subseteq M_\mathfrak{p}$ for each point $\mathfrak{p} \in \operatorname{Spec}(R)$.*

Proof. 1. (L $\Rightarrow$ R) Since $\exists x \in M$ which is non-zero, therefore consider the annihilator ideal $\operatorname{Ann}(x) = \{r \in R \mid rx = 0\}$ of R. Then, this ideal is contained in a maximal ideal $\mathfrak{m}$ of R by Zorn's lemma. Hence consider $M_\mathfrak{m}$, which contains $x/1$. Now if there exists $r \in R \setminus \mathfrak{m}$ such that $rx = 0$, then $r \in \operatorname{Ann}(x)$, but since $\mathfrak{m} \supseteq \operatorname{Ann}(x)$, hence we have a contradiction.
(R $\Rightarrow$ L) Let $\mathfrak{p} \in \operatorname{Spec}(R)$ be such that $x/r \in M_\mathfrak{p}$ and $x/r \neq 0$. Since $M_\mathfrak{p}$ is an R-module, therefore $r \cdot (x/r)$ is well-defined in $M_\mathfrak{p}$. Hence $(rx)/r = x/1 \in M_\mathfrak{p}$. If $x/1 = 0$ in $M_\mathfrak{p}$, therefore $\varphi_\mathfrak{p}(x) = 0$ and hence $x = 0$ as $\varphi_\mathfrak{p}$ is injective. Thus, $x/r = 0$ in $M_\mathfrak{p}$, a contradiction. Therefore $x/1 \neq 0$ and hence $x \neq 0$ in M.

2. This follows from using 1. on the module $(N + Rx)/N$. We do this by observing the following chain of equivalences, whose key steps are explained below:

$$x \in N \iff N + Rx = N \iff (N + Rx)/N = 0 \iff ((N + Rx)/N)_\mathfrak{p}\, \forall \mathfrak{p} \in \operatorname{Spec}(R) \iff$$
$$(N + Rx)_\mathfrak{p}/N_\mathfrak{p} = 0 \forall \mathfrak{p} \in \operatorname{Spec}(R) \iff (N + Rx)_\mathfrak{p} = N_\mathfrak{p} \forall \mathfrak{p} \in \operatorname{Spec}(R) \iff$$
$$N_\mathfrak{p} + (Rx)_\mathfrak{p} = N_\mathfrak{p} \forall \mathfrak{p} \in \operatorname{Spec}(R) \iff (Rx)_\mathfrak{p} \subseteq N_\mathfrak{p} \forall \mathfrak{p} \in \operatorname{Spec}(R) \iff \varphi_\mathfrak{p}(x) = x/1 \in N_\mathfrak{p} \forall \mathfrak{p} \in \operatorname{Spec}(R).$$

For two submodules $N, K, L \subset M$ where $L \subseteq N$ and $\mathfrak{p} \in \operatorname{Spec}(R)$, we get $(N/L)_\mathfrak{p} = N_\mathfrak{p}/L_\mathfrak{p}$ by exactness of localization (Lemma 22.1.2.2) on the exact sequence

$$0 \to L \to N \to N/L \to 0.$$

Finally $(N + K)_\mathfrak{p} = N_\mathfrak{p} + K_\mathfrak{p}$ in $M_\mathfrak{p}$ is true by direct checking and where we use the primality of $\mathfrak{p}$. □

Remark 22.1.2.5. (*Few life hacks*) The above proof tells us few ways how one can approach the problems in ring theory. Note especially that $x \in N$ if and only if $N + Rx = N$, which quickly turns a set-theoretic relation into an algebraic one, where we can now use various constructions as we did, like localization.

The following is the universal property for localization.

Proposition 22.1.2.6. *Let R be a ring and S be a multiplicative set. If $\varphi : R \to T$ is a ring homomorphism such that $\varphi(S) \subseteq T^\times$ where $T^\times$ is the unit group of T, then there exists a unique map $\tilde{\varphi} : S^{-1}R \to T$ such that the following commutes*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "i"'] & T \\ S^{-1}R \arrow[ur, dashed, "\tilde{\varphi}"'] & \end{tikzcd}.$$

Proof. Pick any ring map $\varphi : R \to T$. Take any map $f : S^{-1}R \to T$ which makes the above commute. We claim that $f(r/s) = \varphi(r)\varphi(s)^{-1}$. Indeed, we have that $f(r/1) = \varphi(r)$ for all $r \in R$. Further, for any $s \in S$, we have $f(1/s) = 1/f(s/1) = 1/\varphi(s) = \varphi(s)^{-1}$. Consequently, we get for any $r/s \in S^{-1}R$ the following

$$f\left(\frac{r}{s}\right) = f\left(\frac{r}{1}\cdot\frac{1}{s}\right) = f\left(\frac{r}{1}\right)\cdot f\left(\frac{1}{s}\right) = \varphi(r)\varphi(s)^{-1}.$$

This proves uniqueness. Clearly, this is a ring homomorphism. This completes the proof. □

Remark 22.1.2.7. As Proposition 22.1.2.6 is the universal property of localization, therefore the construction $S^{-1}R$ is irrelevant; the property above completely characterizes localization upto a unique isomorphism.

Lemma 22.1.2.8. *Let R be a ring and $f \in R \setminus \{0\}$. Then,*

$$R_f \cong \frac{R[x]}{\langle fx - 1\rangle}.$$

In particular, R_f is a finite type R-algebra.

Proof. We shall use Proposition 22.1.2.6. We need only show that $R[x]/\langle fx-1\rangle$ satisfies the same universal property as stated in Proposition 22.1.2.6. Indeed, we first have the map $i : R \to R[x]/\langle fx-1\rangle$ given by $r \mapsto r + \langle fx-1\rangle$. Let $\varphi : R \to T$ be any map such that $\varphi(f) \in T^\times$. We claim that there exists a unique map $\tilde{\varphi} : R[x]/\langle fx-1\rangle \to T$ such that $\tilde{\varphi} \circ i = \varphi$. Indeed, take any map $g : R[x]/\langle fx-1\rangle \to T$ such that $g \circ i = \varphi$. Thus, for all $r \in R$, we have $g(r + \langle fx-1\rangle) = \varphi(r)$. As $fx + \langle fx-1\rangle = 1 + \langle fx-1\rangle$, therefore we obtain that $g(f + \langle fx-1\rangle)\cdot g(x + \langle fx-1\rangle) = \varphi(f)\cdot g(x+\langle fx-1\rangle) = 1$. Hence, we see that $g(x + \langle fx-1\rangle) = \varphi(f)^{-1}$. Hence for any element $p(x) + \langle fx-1\rangle$, we see that $f(p(x) + \langle fx-1\rangle) = p(\varphi(f)^{-1})$. This makes g unique well-defined ring homomiorphism. This completes the proof. □

The following is a simple but important application of technique of localization.

Lemma 22.1.2.9. *Let R be a ring. Then the nilradical of R, $\mathfrak{n}$, the ideal consisting of nilpotent elements is equal to the intersection of all prime ideals of R:*

$$\mathfrak{n} = \bigcap_{\mathfrak{p}\in\operatorname{Spec}(R)} \mathfrak{p}.$$

Proof. Take $x \in \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}$. We then have $x \in \mathfrak{p}$ for each $\mathfrak{p} \in \mathrm{Spec}\,(R)$. Hence if for each $n \in \mathbb{N}$ we have that $x^n \neq 0$, then we get that $S = \{1, x, x^2, \dots\}$ forms a multiplicative system. Considering the localization $S^{-1}R$, we see that it is non-zero. Therefore $S^{-1}R$ has a prime ideal, which corresponds to a prime ideal $\mathfrak{p}$ of R which does not intersects S, by Lemma 22.1.2.3. But this is a contradiction as x is in every prime ideal.
Conversely, take any $x \in \mathfrak{n}$ and any prime ideal $\mathfrak{p} \in \mathrm{Spec}\,(R)$. Since $x^n = 0$ for some $n \in \mathbb{N}$, therefore $x^n \in \mathfrak{p}$ for each $\mathfrak{p} \in \mathrm{Spec}\,(R)$. Hence it follows from primality of each $\mathfrak{p}$ that $x \in \mathfrak{p}$. □

We next give two results which are of prominent use in algebraic geometry. The first result says that finite generation of a module can be checked locally.

Lemma 22.1.2.10. *Let M be an R-module and suppose $f_i \in R$ are elements such that $\sum_{i=1}^n Rf_i = R$. Then, the following are equivalent:*

1. *M is a finitely generated R-module.*
2. *M_{f_i} is a finitely generated R_{f_i}-module for all $i = 1, \dots, n$.*

Proof. (1. ⇒ 2.) This is simple, as finite generation is preserved under localization.
(2. ⇒ 1.) Let M_{f_i} be generated by $m_{ij}/(f_i)^{n_{ij}}$ for $j = 1, \dots, n_i$. Let $N \leq M$ be a submodule generated by m_{ij} for each $j = 1, \dots, n_i$ and for each $i = 1, \dots, n$. Clearly, N is a finitely generated R-module. Moreover, N_{f_i} for each $i = 1, \dots, n$ is equal to M_{f_i}. Since localization at a prime ideal $\mathfrak{p} \lneq R$ is given by direct limit of all localization of elements not in $\mathfrak{p}$, therefore $(M/N)_{\mathfrak{p}} \cong \varinjlim_{i=1,\dots,n} (M/N)_{f_i}$ and since $M_{f_i} = N_{f_i}$, therefore $(M/N)_{f_i} = 0$. It follows that $(M/N)_{\mathfrak{p}} = 0$ for all primes $\mathfrak{p}$ and hence $M/N = 0$ by Lemma 22.1.2.4, 1, hence $M = N$ and M is finitely generated. □

The second result gives a partial analogous result as to Lemma 22.1.2.10 did, but for algebras. This is again an important technical tool used often in algebraic geometry.

Lemma 22.1.2.11. *Let A be a ring and B be an A-algebra. Suppose $f_1, \dots, f_n \in B$ are such that $\sum_{i=1}^n Bf_i = B$. If for all $i = 1, \dots, n$, B_{f_i} is a finitely generated A-algebra, then B is a finitely generated A-algebra.*

Proof. Let B_{f_i} be generated by

$$\left\{ \frac{b_{ij}}{f_i^{n_j}} \right\}_{j=1,\dots,M_i}$$

as an A-algebra, for each $i = 1, \dots, n$. Further, we have $c_1, \dots, c_n \in B$ such that $c_1 f_1 + \dots + c_n f_n = 1$. We claim that $S = \{b_{ij}, f_i, c_i\}_{i,j}$ is a finite generating set for B.

Let C be the sub-algebra of B generated by S. Pick any $b \in B$. We wish to show that $b \in C$. Fix an $i = 1, \dots, n$. Observe that the image of b in the localized ring B_{f_i} is generated by some polynomial with coefficients in A and indeterminates replaced by

$$\left\{ \frac{b_{ij}}{f_i^{n_j}} \right\}_{j=1,\dots,M_i}.$$

We may multiply b by $f_i^{N_i}$ for N_i large enough so that $f_i^{N_i}b$ is then represented by a polynomial with coefficients in A evaluated in f_i and b_{ij} for $j = 1, \dots, M_i$. Consequently, $f_i^{N_i}b \in C$, for each $i = 1, \dots, n$. Observe that $f_1, \dots, f_n$ in C generates the unit ideal in C. By Lemma 22.22.0.2, 2, we see that $f_1^{N_1}, \dots, f_n^{N_n}$ also generates the unit ideal in C. Hence, we have $d_1, \dots, d_n \in C$ such that $1 = d_1 f_1^{N_1} + \dots + d_n f_n^{N_n}$. Multiplying by b, we obtain $b = d_1 f_1^{N_1} b + \dots + d_n f_n^{N_n}$ where by above, we now know that each term is in C. This completes the proof. □

An observation which is of importance in the study of varieties is the following.

Lemma 22.1.2.12. *Let R be an integral domain. Then*

$$\bigcap_{\mathfrak{m} < R} R_{\mathfrak{m}} \cong R$$

where the intersection runs over all maximal ideals $\mathfrak{m}$ of R and the intersection is carried out in the fraction field $R_{\langle 0 \rangle}$.

Proof. We already have that

$$R \hookrightarrow R_{\mathfrak{m}}$$

for any maximal ideal $\mathfrak{m} < R$. Thus,

$$R \hookrightarrow \bigcap_{\mathfrak{m} < R} R_{\mathfrak{m}}.$$

Thus it would suffice to show that $\bigcap_{\mathfrak{m} < R} R_{\mathfrak{m}} \hookrightarrow R$. Indeed, consider the following map

$$\begin{aligned} \bigcap_{\mathfrak{m} < R} R_{\mathfrak{m}} &\longrightarrow R \\ [f_{\mathfrak{m}}/g_{\mathfrak{m}}] &\longmapsto f_{\mathfrak{m}} g_{\mathfrak{m}'} \end{aligned}$$

where $f_{\mathfrak{m}}/g_{\mathfrak{m}} = f_{\mathfrak{m}'}/g_{\mathfrak{m}'}$ for two maximal ideals $\mathfrak{m}, \mathfrak{m}'$ in R. Thus, $f_{\mathfrak{m}} g_{\mathfrak{m}'} = f_{\mathfrak{m}'} g_{\mathfrak{m}}$. Hence the above map is well-defined and is injective as $f_{\mathfrak{m}} g_{\mathfrak{m}'} = 0$ implies $f_{\mathfrak{m}} = 0$ as $g_{\mathfrak{m}'} \neq 0$. The result follows. □

Homogeneous localization

The following is a discussion on localization of a graded ring S at a homogeneous prime ideal $\mathfrak{p}$. Let T denote the multiplicative subset of S consisting of all homogeneous elements not contained in $\mathfrak{p}$. Then $T^{-1}S$ is a graded ring whose degree d-elements are a/f where $a \in S_{d+e}$ and $f \in T$ of degree e. These form an additive abelian group where $a/f + b/g = ag + bf/fg$ where $a \in S_{d+k}, b \in S_{d+l}$ and $f, g \in T$ are of degree k and l respectively. Indeed, then $ag + bf \in S_{d+k+l}$ and $fg \in T$ of degree $k + l$. Consequently, we define

$$S_{(\mathfrak{p})} := (T^{-1}S)_0$$

where $(T^{-1}S)_0$ is the degree 0 elements in the localization $T^{-1}S$. We call this the *homogeneous localization* of the graded ring S at the homogeneous prime ideal $\mathfrak{p}$. Thus $S_{(\mathfrak{p})} = (S_{\mathfrak{p}})_0$, i.e. homogeneous localization just picks out degree 0 elements from the usual localization. Note that the usual localization $T^{-1}S$ is a graded ring where grading is given by subtracting the degree of numerator by degree of denominator.

Lemma 22.1.2.13. *Let S be a graded ring and $\mathfrak{p}$ be a homogeneous prime ideal of S. Then, the homogeneous localization $S_{\mathfrak{p}}$ is a local ring.*

Proof. Consider the set $\mathfrak{m} := (\mathfrak{p} \cdot T^{-1}S) \cap S_{\mathfrak{p}}$. Then, $\mathfrak{m}$ is a maximal ideal of $S_{\mathfrak{p}}$ as any element not in $\mathfrak{m}$ in $S_{\mathfrak{p}}$ is a fraction f/g where $\deg f = \deg g$ and $f \notin \mathfrak{p}$ and thus it is invertible. Consequently, $S_{\mathfrak{p}}$ is local. □

Remark 22.1.2.14. Note that if S is a graded domain, then $S_{(\langle 0 \rangle)}$ yields a field whose elements are of the form f/g where $\deg f = \deg g$ and f, g g is a non-zero homogeneous element of S. This field is called the *homogeneous fraction field* of graded domain S. This is a subfield of usual fraction field $S_{\langle 0 \rangle}$.

Let S be a graded ring and $g \in S$ be a homogeneous element. The *homogeneous localization of S at g* is defined to be the following subring of S_g:

$$S_{(g)} := \{f/g^n \in S_g \mid f \text{ is homogeneous with } \deg f = n \deg g,\ n \in \mathbb{N}\} \leq S_g.$$

Let S be a graded ring. Then an S-module M is said to be *graded S-module* if $M = \bigoplus_{d \in \mathbb{Z}} M_d$ where $M_d \leq M$ is a subgroup of M such that $S_d \cdot M_e \subseteq M_{d+e}$. Then, for a homogeneous element $g \in S$, we denote by $M_{(g)}$ the following submodule of M_g:

$$M_{(g)} := \{m/g^n \mid m \text{ is homogeneous with } \deg m = n \deg g,\ n \in \mathbb{N}\} \leq M_g.$$

For each graded S-module M, one can attach a sequence of graded modules.

Definition 22.1.2.15. (**Twisted modules**) Let S be a graded ring and M a graded S-module. Then, define

$$M(l) := \bigoplus_{d \in \mathbb{Z}} M_{d+l}$$

to be the *l-twisted graded module of M*.

An important lemma with regards to localization of a graded ring at a positive degree element is as follows, it will prove its worth in showing that projective spectrum of a graded ring is a scheme (see Lemma **??**).

Lemma 22.1.2.16. *Let S be a graded ring and $f \in S_d$, $d > 0$. Then we have a bijection*

$$D_+(f) \cong \operatorname{Spec}\left(S_{(f)}\right)$$

where $D_+(f) \subseteq \operatorname{Spec}(S)$ is the set of all homogeneous prime ideals of S which does not contain f and does not contain S_+.

Proof. Consider the following map

$$\begin{aligned}\varphi : D_+(f) &\longrightarrow \mathrm{Spec}\left(S_{(f)}\right)\\ \mathfrak{p} &\longmapsto (\mathfrak{p}\cdot S_f)_0,\end{aligned}$$

that is, the degree zero elements of the prime ideal $\mathfrak{p}\cdot S_f$ of S_f. Indeed, $\varphi(\mathfrak{p})$ is a prime ideal of $S_{(f)}$. Further, if $(\mathfrak{p}\cdot S_f)_0 = (\mathfrak{q}\cdot S_f)_0$ for $\mathfrak{p},\mathfrak{q} \in D_+(f)$, then for any $g \in \mathfrak{p}$, one observes via above equality that $g \in \mathfrak{q}$. Consequently, $\mathfrak{p} = \mathfrak{q}$. Thus φ is injective. For surjectivity, pick any prime ideal $\mathfrak{p} \in \mathrm{Spec}\left(S_{(f)}\right)$. We will construct a prime ideal $\mathfrak{q} \in D_+(f)$ such that $\varphi(\mathfrak{q}) = \mathfrak{p}$. Indeed, let $K = \{g \in S \mid g \text{ is homogeneous } \& \ \exists n > 0 \text{ s.t. } g/f^n \in \mathfrak{p}\}$ and consider the ideal

$$\mathfrak{q} = \langle K\rangle.$$

We thus need to check the following statements to complete the bijection:

1. $\mathfrak{q}$ is not the unit ideal of S,
2. $\mathfrak{q}$ is homogeneous in S,
3. $\mathfrak{q}$ is prime in S,
4. $\mathfrak{q}$ doesn't contain f,
5. $(\mathfrak{q}\cdot S_f)_0 = \mathfrak{p}$.

Statement 4 tells us that $\mathfrak{q}$ doesn't contain S_+. Statement 1 follows from a degree argument; if $1 \in \mathfrak{q}$, then $1 = a_1g_1+\dots+a_mg_m$ for $g_i \in K$ and $a_i \in S$, but 1 is a degree 0 element whereas the minimum degree of the right is atleast > 0. Statement 2 is immediate as $\mathfrak{q}$ is generated by homogeneous elements. For statement 3, it is enough to check for homogeneous elements $h,k \in S$ that $hk \in \mathfrak{q} \implies h \in \mathfrak{q}$ or $k \in \mathfrak{q}$. This is immediate, after observing that any homogeneous element of $\mathfrak{q}$ is in K because K is the set of all homogeneous elements of S of positive degree which is not a power of f. Statements 4 and 5 are immediate checks. □

Local rings

A ring R is said to be *local* if there is a unique maximal ideal of R. In such a case we denote it by $(R,\mathfrak{m})$.

Definition 22.1.2.17. (**Zariski (co)tangent space**) Let $(R,\mathfrak{m})$ be a local ring. Then, we define the Zariski *cotangent space* of $(R,\mathfrak{m})$ to be $T^*R = \mathfrak{m}/\mathfrak{m}^2$ and the Zariski *tangent space* to be its dual $TR = \mathrm{Hom}_k\left(\mathfrak{m}/\mathfrak{m}^2, k\right)$.

Remark 22.1.2.18. The Zariski cotangent space T^*R is a κ-vector space where $\kappa = R/\mathfrak{m}$ is the residue field. Indeed, the scalar multiplication is given by

$$\begin{aligned}\kappa \times T^*R &\longrightarrow T^*R\\ (c+\mathfrak{m}, x+\mathfrak{m}^2) &\longmapsto cx+\mathfrak{m}^2\end{aligned}$$

where $c \in R$ and $x \in \mathfrak{m}$. Indeed, this is well-defined as can be seen by a simple check. Consequently, the tangent space $TR = \mathrm{Hom}_k\left(\mathfrak{m}/\mathfrak{m}^2, k\right)$ is also a κ-vector space.

Definition 22.1.2.19. (**Regular local ring**) Let $(A,\mathfrak{m})$ be a local ring with $k = A/\mathfrak{m}$ being the residue field. Then A is said to be regular if $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim A$.

There is an important geometric lemma that one should keep in mind about certain local rings.

Definition 22.1.2.20. (**Rational local k-algebras**) Let k be a field. A local k-algebra $(R, \mathfrak{m})$ is said to be rational if its residue field $\kappa = R/\mathfrak{m}$ is isomorphic to the field k.

Rational local k-algebras have a rather simple tangent space.

Proposition 22.1.2.21. *Let $(A, \mathfrak{m}_A)$ be a rational local k-algebra. Then,*

$$TA \cong \mathrm{Hom}_{k,\mathrm{loc}}(A, k[\epsilon])$$

where $k[\epsilon] := k[x]/x^2$ is the ring of dual numbers and $\mathrm{Hom}_{k,\mathrm{loc}}(A, k[\epsilon])$ denotes the set of all local k-algebra homomorphisms.

Proof. Pick any k-algebra homomorphism $\varphi : A \to k[\epsilon]$. Denote by $\mathfrak{m}_\epsilon = \langle \epsilon \rangle \lneq k[\epsilon]$ the unique maximal ideal of $k[\epsilon]$. Since

$$k[\epsilon]/\mathfrak{m}_\epsilon \cong k,$$

therefore $k[\epsilon]$ is a rational local k-algebra as well. By Lemma 22.22.0.7, we may write $A = k \oplus \mathfrak{m}_A$ and $k[\epsilon] = k \oplus \mathfrak{m}_\epsilon$. We now claim that the datum of a local k-algebra homomorphism $\varphi : A \to k[\epsilon]$ is equivalent to datum of a k-linear map of k-modules $\theta : \mathfrak{m}_A/\mathfrak{m}_A^2 \to k$.

Indeed, we first observe that for any $\varphi : A \to k[\epsilon]$ as above, we have $\varphi(\mathfrak{m}_A) \subseteq \mathfrak{m}_\epsilon$. Thus, $\varphi(\mathfrak{m}_A^2) \subseteq \mathfrak{m}_\epsilon^2 = 0$. Thus, we deduce that for any such φ, $\mathrm{Ker}(\varphi) \supseteq \mathfrak{m}_A^2$. It follows from universal property of quotients that any such φ is in one-to-one correspondence with k-algebra homomorphisms

$$\tilde{\varphi} : A/\mathfrak{m}_A^2 \cong k \oplus (\mathfrak{m}_A/\mathfrak{m}_A^2) \longrightarrow k[\epsilon].$$

As $\varphi(\mathfrak{m}_A) \subseteq \mathfrak{m}_\epsilon$, therefore $\tilde{\varphi}(\mathfrak{m}_A/\mathfrak{m}_A^2) \subseteq \mathfrak{m}_\epsilon$. Thus, we obtain a k-linear map of k-modules

$$\theta : \mathfrak{m}_A/\mathfrak{m}_A^2 \longrightarrow k \cong \mathfrak{m}_\epsilon$$

where $\mathfrak{m}_\epsilon \cong k$ as k-modules. It suffices to now show that from any such θ, one can obtain a unique k-algebra map $\tilde{\varphi} : k \oplus (\mathfrak{m}_A/\mathfrak{m}_A^2) \to k[\epsilon]$, which furthermore sets up a bijection between all such $\tilde{\varphi}$ and θ.

Indeed, from k-linear map θ, we may construct the following k-algebra map

$$\begin{aligned} \tilde{\varphi} : k \oplus (\mathfrak{m}_A/\mathfrak{m}_A^2) &\longrightarrow k[\epsilon] \\ (k + \bar{m}) &\longmapsto k + \theta(\bar{m})\epsilon. \end{aligned}$$

Then we observe that $\tilde{\varphi}$ is a k-algebra homomorphism as

$$\begin{aligned} \tilde{\varphi}((k_1 + \bar{m}_1)(k_2 + \bar{m}_2)) &= \tilde{\varphi}(k_1k_2 + k_1\bar{m}_2 + k_2\bar{m}_1 + \bar{m}_1\bar{m}_2) \\ &= k_1k_2 + k_1\theta(\bar{m}_2)\epsilon + k_2\theta(\bar{m}_1)\epsilon + \theta(\bar{m}_1\bar{m}_2)\epsilon \\ &= k_1k_2 + k_1\theta(\bar{m}_2)\epsilon + k_2\theta(\bar{m}_1)\epsilon \\ &= (k_1 + \theta(\bar{m}_1)\epsilon) \cdot (k_2 + \theta(\bar{m}_2)\epsilon) \\ &= \tilde{\varphi}(k_1 + \bar{m}_1) \cdot \tilde{\varphi}(k_2 + \bar{m}_2). \end{aligned}$$

Hence, from θ one obtain $\tilde{\varphi}$ back, thus setting up a bijection and completing the proof. □

22.1.3 Structure theorem

Let M be a finitely generated R-module. We can understand the structure of such modules completely in terms of the ring R, when R is a PID (so that it's UFD). This is the content of the structure theorem. We first give the following few propositions which is used in the proof of the structure theorem but is of independent interest as well, in order to derive a usable variant of structure theorem. The following theorem tells us a direct sum decomposition exists for any finitely free torsion module over a PID.

Proposition 22.1.3.1. *Let M be a finitely generated torsion module over a PID R. If* $\mathrm{Ann}(M) = \langle c\rangle$ *where $c = p_1^{k_1} \dots p_r^{k_r}$ and $p_i \in R$ are prime elements, then*

$$M \cong M_1 \oplus \cdots \oplus M_r$$

where $M_i = \{x \in M \mid p_i^{r_i} x = 0\} \leq M$ for all $i = 1, \dots, r$, that is, where $\mathrm{Ann}(M_i) = \langle p_i^{r_i}\rangle$ *for all $i = 1, \dots, r$.*

The next result tells us that we can further write each of the above M_is as a direct sum decomposition of a special kind.

Proposition 22.1.3.2. *Let M be a finitely generated torsion module over a PID R. If* $\mathrm{Ann}M = \langle p^r\rangle$ *where $p \in R$ is a prime element, then there exists $r_1 \geq r_2 \geq \cdots \geq r_k \geq 1$ such that*

$$M \cong R/\langle p^{r_1}\rangle \oplus \cdots \oplus R/\langle p^{r_k}\rangle.$$

The structure theorem is as follows.

Theorem 22.1.3.3. *(Structure theorem) Let R be a PID and M be a finitely generated R-module. Then there exists an unique $n \in \mathbb{N} \cup \{0\}$ and $q_1, \dots q_r \in R$ unique upto units such that $q_{i-1} | q_i$ for all $i = 2, \dots, r$ and*

$$M \cong R^n \oplus R/\langle q_1\rangle \oplus \cdots \oplus R/\langle q_r\rangle.$$

The most useful version of this is the following:

Corollary 22.1.3.4. *Let M be a finitely generated torsion module over a PID R. Then, there exists k-many prime elements $p_1, \dots, p_k \in R$, $n_j \in \mathbb{N}$ for each $j = 1, \dots, k$ and $1 \leq r_{1j} \leq \cdots \leq r_{n_j j} \in \mathbb{N}$ for each $j = 1, \dots, k$ such that*

$$M \cong \bigoplus_{j=1}^{k} \left(R/\langle p_j^{r_{1j}}\rangle \oplus \cdots \oplus R/\langle p_j^{n_j j}\rangle \right).$$

Proof. This is a consequence of Propositions 22.1.3.1 and 22.1.3.2. □

This is the famous structure theorem for finitely generated modules over a PID. Note that the ring $\mathbb{Z}$ is PID and any abelian group is a $\mathbb{Z}$-module. Thus, we can classify finitely generated abelian groups using the structure theorem.

Example 22.1.3.5. An example of a module which is not finitely generated is the polynomial module $R[x]$ over a ring R. Indeed, the collection $\{1, x, x^2, \dots\}$ will make it free but not finitely generated.

Example 22.1.3.6. Classification of all abelian groups of order $360 = 2^3 \cdot 3^2 \cdot 5$, for example, can be achieved via structure theorem. Indeed using Corollary 22.1.3.4, we will get that there are 6 total such abelian groups given by

- $\left(\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)$
- $\left(\frac{\mathbb{Z}}{2^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)$
- $\left(\frac{\mathbb{Z}}{2^3\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)$
- $\left(\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{3^2\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)$
- $\left(\frac{\mathbb{Z}}{2^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{3^2\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)$
- $\left(\frac{\mathbb{Z}}{2^3\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{3^2\mathbb{Z}}\right) \oplus \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)$

22.1.4 UFDs

22.1.5 Gauss' lemma

Add results surrounding primitive polynomials and Gauss' lemma here from notebook.

Spectra of polynomial rings over UFDs

We now calculate the prime spectra of polynomial rings over UFDs. For that, we need the following two lemmas.

Lemma 22.1.5.1. *Let R be a UFD and $I \leq R[x]$ be an ideal containing two elements with no common factors. Then I contains a non-zero constant from R.*

Proof. Indeed, let $f, g \in R[x]$ be two elements with no common factors. Let Q denote the fraction field of R. We first claim that $f, g \in Q[x]$ have no common factor as well. Indeed, suppose $h(x) \in Q[x]$ is a common factor of $f(x)$ and $g(x)$. It follows from the result on primitive polynomials that we can write $h(x) = ch_0(x)$ where $c \in Q$ and $h_0(x) \in R[x]$ is primitive. Hence, we see that $h_0(x) \in R[x]$ is a polynomial such that $h_0|f$ and $h_0|g$ in $Q[x]$. Again, by general results in UFD, we then conclude that $h_0|f$ and $h_0|g$ in $R[x]$. As f and g have no common factor, therefore $h_0(x) \in R[x]$ is a unit. Hence $h(x) \in Q[x]$ is a unit. Thus, there is no common factor of $f(x)$ and $g(x)$ in $Q[x]$ if there is none in $R[x]$.

Hence, $f(x), g(x)$ in $Q[x]$ have gcd 1, where $Q[x]$ is a PID. Consequently, $f(x)$ and $g(x)$ generates the unit ideal in $Q[x]$. It follows that there exists $p(x), q(x) \in Q[x]$ such that

$$1 = p(x)f(x) + q(x)g(x).$$

By theorem on primitive polynomials, we may write $p(x) = \frac{a}{b}p_0(x)$ and $q(x) = \frac{c}{d}q_0(x)$ where $a/b, c/d \in Q$ and $p_0(x), q_0(x) \in R[x]$ are primitive. The above equation hence becomes

$$\begin{aligned} 1 &= \frac{a}{b}p_0(x)f(x) + \frac{c}{d}q_0(x)g(x) \\ &= \frac{adp_0(x)f(x) + bcq_0(x)g(x)}{bd}, \end{aligned}$$

which thus yields

$$bd = adp_0(x)f(x) + bcq_0(x)g(x)$$

where RHS is in $I \leq R[x]$ because $ad, p_0, bc, q_0 \in R[x]$ and $f, g \in I$ and LHS is in R. Hence $I \cap R$ is not zero. □

Lemma 22.1.5.2. *Let R be a PID and $f, g \in R[x]$ be non-zero polynomials such that f and g have no common factors. Then,*

1. *any prime ideal $\mathfrak{p} \lneq R[x]$ containing f and g is maximal,*
2. *any maximal ideal $\mathfrak{m} \lneq R[x]$ containing f and g is of the form $\langle p, h(x)\rangle$ where $p \in R$ is prime and $h(x)$ is prime modulo p,*
3. *there are only finitely many maximal ideals of $R[x]$ containing f and g.*

Proof. 1. : Let $\mathfrak{p} \lneq R[x]$ be a prime ideal containing f and g. Observe by Lemma 22.1.5.1 that there exists $b \in R \setminus 0$ such that $b \in \mathfrak{p} \cap R$, that is, $\mathfrak{p} \cap R \neq 0$. As R is a PID and $\mathfrak{p} \cap R$ is a prime ideal of R, therefore $\mathfrak{p} \cap R = pR$ for some prime element $p \in \mathfrak{p} \cap R$. We wish to show that $R[x]/\mathfrak{p}$ is a field. Indeed, we see that (note $\langle p, \mathfrak{p}\rangle = \mathfrak{p}$ as $p \in \mathfrak{p}$)

$$\begin{aligned} \frac{R[x]}{\mathfrak{p}} &\cong \frac{\frac{R[x]}{pR[x]}}{\frac{\langle p,\mathfrak{p}\rangle}{pR[x]}} = \frac{\frac{R[x]}{pR[x]}}{\frac{\mathfrak{p}}{pR[x]}} \\ &\cong \frac{\frac{R}{pR}[x]}{\overline{\mathfrak{p}}} \end{aligned}$$

where $\overline{\mathfrak{p}} = \pi(\mathfrak{p})$ where $\pi : R[x] \twoheadrightarrow \frac{R}{pR}[x]$ is the quotient map. As R is a PID and pR is a non-zero prime ideal, therefore it is maximal. Consequently, R/pR is a field and hence $\frac{R}{pR}[x]$ is a PID. Suppose $\overline{\mathfrak{p}} = 0$, then f and g have a common factor given by $p \in R$, which is not possible. Consequently, $\overline{\mathfrak{p}}$ is a proper prime ideal of $\frac{R}{pR}[x]$ by correspondence theorem. But in PIDs, non-zero prime ideals are maximal ideals, hence we obtain that $\frac{R}{pR}[x]/\overline{\mathfrak{p}}$ is a field, as required.

2. : Let $\mathfrak{m} \lneq R[x]$ be a maximal ideal of $R[x]$ containing f and g. Hence, from Lemma 22.1.5.1 and R being a PID, there exists $p \in R$ a prime such that $\mathfrak{m} \cap R = pR$. Hence R/pR is a field as R is a PID and pR a non-zero prime ideal (so maximal). Consequently, we have a quotient map

$$\pi : R[x] \twoheadrightarrow \frac{R[x]}{pR[x]} \cong \frac{R}{pR}[x]$$

As $p \in \mathfrak{m}$, therefore by correspondence thereom $\pi(\mathfrak{m}) = \overline{\mathfrak{m}}$ is a maximal ideal of $\frac{R}{pR}[x]$. As R/pR is a field, therefore $\frac{R}{pR}[x]$ is a PID. Hence, $\overline{\mathfrak{m}} = \langle \overline{h(x)} \rangle$ for some $h(x) \in R[x]$ such that $\overline{h(x)}$ is irreducible (so it generates a maximal ideal). Again, by correspondence theorem we have $\pi^{-1}(\overline{\mathfrak{m}}) = \mathfrak{m} = h(x)R[x] + pR[x] = \langle p, h(x)\rangle$, as required.

3. : We will use notations of proof of 2. above. Take any maximal ideal $\mathfrak{m} = \langle p, h(x)\rangle \lneq R[x]$ which contains $f(x)$ and $g(x)$, $p \in R$ is prime and $h(x)$ is irreducible modulo p. As R is a PID, so it is a UFD, hence $R[x]$ is a UFD by Gauss' lemma. Hence, writing $f(x)$

and $g(x)$ as product of prime factors in $R[x]$, we observe that there exists distinct primes $p(x), q(x) \in R[x]$ such that $p(x), q(x) \in \mathfrak{m}$. Replacing f by p and g by q, we may assume f and g are irreducible (or prime) in $R[x]$.

By Lemma 22.1.5.1, there exists $b \in R \setminus 0$ such that $b \in \mathfrak{m} \cap R$. As the proof of 2. above shows, $p|b$ in R. As R is a PID, so it is a UFD, hence there are only finitely many choices for p.

Now, going modulo prime p, we see that $\overline{f(x)}, \overline{g(x)} \in \overline{\mathfrak{m}} \lneq \frac{R}{pR}[x]$ has a common factor in $\frac{R}{pR}[x]$, given by $\overline{h(x)}$ as $\overline{\mathfrak{m}} = \langle \overline{h(x)} \rangle$ (by proof of 2.). As $\overline{h(x)}$ generates a maximal ideal in $\frac{R}{pR}[x]$, therefore $\overline{h(x)}$ is a prime element of $\frac{R}{pR}[x]$, which has to divide $\overline{f(x)}$ and $\overline{g(x)}$. As $\frac{R}{pR}[x]$ is a PID, therefore there are only finitely many choices for $\overline{h(x)}$, and since $\mathfrak{m} = \pi^{-1}(\langle \overline{h(x)} \rangle)$, therefore every choice of p as above, yields finitely many choices for $\mathfrak{m}$.

Consequently, there are finitely many choices for p and once p is fixed, there are only finitely many choices for the ideal $\overline{\mathfrak{m}}$. As $\mathfrak{m} = \pi^{-1}(\overline{m})$, therefore there are finitely many maximal ideals containing f and g. □

We now classify Spec $(R[x])$ for a UFD R.

Theorem 22.1.5.3. *Let R be a PID. Any prime ideal $\mathfrak{p} \lneq R[x]$ is of one of the following forms*

1. $\mathfrak{p} = \mathfrak{o}$,
2. $\mathfrak{p} = \langle f(x) \rangle$ *for some irreducible* $f(x) \in R[x]$,
3. $\mathfrak{p} = \langle p, h(x) \rangle$ *for some prime* $p \in R$ *and* $h(x) \in R[x]$ *irreducible modulo* p *and this is also a maximal ideal.*

Proof. Indeed, pick any prime ideal $\mathfrak{p} \lneq R[x]$. If $\mathfrak{p}$ is 0, then it is prime as $R[x]$ is a domain. We now have two cases. If $\mathfrak{p}$ is principal, then $\mathfrak{p} = \langle f(x) \rangle$ for some $f(x) \in R[x]$. As $\langle f(x) \rangle$ is prime therefore $f(x)$ is a prime element. As $R[x]$ is a UFD by Gauss' lemma, therefore $f(x)$ is also irreducible. Consequently, $\mathfrak{p} = \langle f(x) \rangle$ where $f(x)$ is irreducible.

On the other hand if $\mathfrak{p}$ is not principal, there exists $f(x), g(x) \in \mathfrak{p}$ such that $f(x) \not| g(x)$ and $g(x) \not| f(x)$. As $R[x]$ is a UFD and $\mathfrak{p}$ is prime, therefore there exists prime factors of f and g which are in $\mathfrak{p}$. Replacing f and g by these prime factors, we may assume f and g are distinct irreducibles in $\mathfrak{p}$. Consequently, by Lemma 22.1.5.2, we see that $\mathfrak{p} = \langle p, h(x) \rangle$ for some prime $p \in R$ and $h(x)$ irreducible modulo p. Moreover by Lemma 22.1.5.2 we know that $\mathfrak{p}$ in this case is maximal. □

We now portray their use in the following.

Lemma 22.1.5.4. *Let F be an algebraically closed field. Then,*

1. *every non-constant polynomial* $f(x, y) \in F[x, y]$ *has at least one zero in* F^2,
2. *every maximal ideal of* $F[x, y]$ *is of the form* $\mathfrak{m} = \langle x - a, y - b \rangle$ *for some* $a, b \in F$.

Proof. 1. : Take any polynomial $f(x, y) \in F[x, y]$. Going modulo y, we see that $\overline{f(x, y)} \in F[x, y]/\langle y \rangle = F[x]$. If $\overline{f(x, y)} = 0$, then $(a, 0)$ is a root of $f(x, y)$ for any $a \in F$. if $\overline{f(x, y)} \neq 0$, then since F is algebraically closed, therefore we may write $\overline{f(x, y)} = (x - a_1) \dots (x - a_n)$. Consequently, any $(a_i, 0)$ is a zero of $f(x, y)$. Hence, in any case, $f(x, y)$ has a root in F^2.
2. : Let $R = F[x]$. We know that R is a PID. Take any maximal ideal $\mathfrak{m} \lneq R[y] = F[x, y]$.

Then by Theorem 22.1.5.3, we have that either $\mathfrak{m} = \langle f(x,y)\rangle$ where $f(x,y)$ is irreducible or $\mathfrak{m} = \langle p(x), h(x,y)\rangle$ where $p(x) \in R$ is prime and $h(x,y)$ is irreducible modulo $p(x)$.

In the former, we claim that $\langle f(x,y)\rangle$ is not maximal. Indeed, by item 1, we have that $f(x,y)$ has a zero in F^2, say (a,b). Dividing $f(x,y)$ by $y-b$ in $R[y]$, we obtain $f(x,y) = h(x,y)(y-b) + k(x)$, where $k(x) \in R$. Consequently, $k(a) = 0$. Hence, $k(x) = (x-a)l(x)$. Thus, we have $f(x,y) = h(x,y)(y-b) + (x-a)l(x)$, showing $f(x,y) \in \langle x-a, y-b\rangle$. By Theorem 22.1.5.3 above, we know that $\langle x-a, y-b\rangle \in R[y]$ is a maximal ideal and we also know that it contains $f(x,y)$. We hence need only show that $\langle f(x,y)\rangle \subsetneq \langle x-a, y-b\rangle$. Indeed, observe that $x-a \notin \langle f(x,y)\rangle$ as if it is, then $f(x,y)|x-a$. But then $f(x,y)$ is in R, hence $y-b \notin \langle f(x,y)\rangle$. So in either case, $\langle f(x,y)\rangle$ is properly contained in $\langle x-a, y-b\rangle$, showing that $\langle f(x,y)\rangle$ cannot be maximal. Thus, no maximal ideal of $R[y]$ can be of the form $\langle f(x,y)\rangle$.

In the latter, where $\mathfrak{m} = \langle p(x), h(x,y)\rangle$ where $p(x) \in R$ is prime and $h(x,y)$ is irreducible modulo $p(x)$, we first see that $p(x) = x-a$ for some $a \in F$ as $R = F[x]$ and only primes of $F[x]$ are of this type. Let $\pi : R \twoheadrightarrow \frac{R}{p(x)R}[y] \cong \frac{R}{\langle x-a\rangle}[y] \cong F[y]$ be the quotient map by the ideal $p(x)R[y]$. Then we see that by correspondence theorem, $\pi(\mathfrak{m}) = \overline{\mathfrak{m}} = \langle \overline{h(x,y)}\rangle$ is a prime ideal of $F[y]$. Hence, $\overline{\mathfrak{m}} = \langle k(y)\rangle$ for some $k(y) \in F[y]$. Further, since $\overline{\mathfrak{m}}$ is prime and F algebraically closed, therefore $k(y) = y-b$. Thus, we see that modulo $p(x)$ we have $h(x,y) = k(y) = y-b$. We then see that $\mathfrak{m} = \pi^{-1}(\overline{\mathfrak{m}}) = \pi^{-1}(\langle \overline{y-b}\rangle) = \langle p(x), y-b\rangle = \langle x-a, y-b\rangle$, as required. □

Another example gives us finiteness of intersection of two algebraic curves over an algebraically closed field.

Proposition 22.1.5.5. *Let F be an algebraically closed field and $f, g \in F[x,y]$ be two polynomials with no common factors. Then, $Z(f) \cap Z(g)$ is a finite set, that is, f and g intersects at finitely many points in $\mathbb{A}^2_F$.*

Proof. We first show that for any $h(x,y) \in F[x,y]$, $h(a,b) = 0$ for some $(a,b) \in F^2$ if and only if $h \in \langle x-a, y-b\rangle$. Clearly, $(\Leftarrow)$ is immediate. For $(\Rightarrow)$, we proceed as follows. Going modulo $y-b$ in $F[x,y]$, we obtain $\overline{h(x,y)} \in F[x,y]/\langle y-b\rangle \cong F[x]$. Observe that $\langle y-b\rangle$ is the kernel of the map $F[x,y] \to F[x]$ taking $y \mapsto b$, hence $\overline{h(x,y)} = \overline{h(x,b)}$. As F is algebraically closed, therefore we may write

$$\overline{h(x,b)} = \overline{h(x,y)} = (x-c_1)\dots(x-c_n)$$

for $c_i \in F$. As, $h(a,b) = 0$, therefore $(x-a)|\overline{h(x,b)}$. Hence, for some i, we must have $c_i = a$. This allows us to write

$$h(x,y) - (x-a)k(x) \in \langle y-b\rangle$$

for some $k(x) \in F[x]$. It follows that for some $q(x,y) \in F[x,y]$ we have

$$h(x,y) - (x-a)k(x) = (y-b)q(x,y)$$

Thus, $h(x,y) \in \langle x-a, y-b\rangle$. This completes the proof of the claim above.

Now, using above claim $f(a,b) = 0 = g(a,b)$ if and only if $f, g \in \langle x-a, y-b\rangle$. By

Lemma 22.1.5.2, as f and g have no common factors, therefore there are finitely many maximal ideals containing f and g. Further, by Lemma 22.1.5.4, we know that each such maximal ideal is of the form $\langle x-a, y-b\rangle$. Hence, there are only finitely many maximal ideals containing f and g, each of which looks like $\langle x-a, y-b\rangle$. Hence, by above claim, there are finitely many points $(a,b) \in F^2$ such that $f(a,b) = 0 = g(a,b)$. □

22.1.6 Finite type k-algebras

We discuss basic theory of finite type k-algebras, that is, algebras of form $k[x_1,\dots,x_n]/I$.

Recall that for a field k, we denote by $k[x]$ the polynomial ring in one variable and we denote the rational function field $k(x)$ to be the field obtained by localizing at prime $\mathfrak{o}$. Further if K/k is a field extension and $\alpha \in K$, then $k[\alpha]$ is a subring of K generated by $\alpha \in K$ and it contains k. Whereas, $k(\alpha)$ is a field extension $k \hookrightarrow k(\alpha) \hookrightarrow K$. The following lemma shows that if K is algebraic, then $k(\alpha) = k[\alpha]$.

Lemma 22.1.6.1. *Let k be a field and K/k be an algebraic extension. If $\alpha_1,\dots,\alpha_n \in K$, then $k[\alpha_1,\dots,\alpha_n] = k(\alpha_1,\dots,\alpha_n)$.*

Proof. The proof uses a standard observation in field theory. First, let $f_1(x) \in k[x]$ be the minimal polynomial of α_1. Consequently, by a standard result in field theory, $k[\alpha_1] = k[x]/f_1(x)$ is a field. Thus $k[\alpha_1] = k(\alpha_1)$. Now observe that $K/k(\alpha_1)$ is an algebraic extension. Consequently, the same argument will yield $k(\alpha_1)[\alpha_2]$ to be a field. By above, we thus obtain $k(\alpha_1)[\alpha_2] = k[\alpha_1][\alpha_2] = k[\alpha_1,\alpha_2]$ to be a field. Consequently, $k[\alpha_1,\alpha_2] = k(\alpha_1,\alpha_2)$. One completes the proof now by induction. □

Lemma 22.1.6.2. *Let k be a field and K/k be an algebraic extension. Then the homomorphism*

$$\begin{aligned} k[x_1,\dots,x_n] &\longrightarrow k(\alpha_1,\dots,\alpha_n) \\ x_i &\longmapsto \alpha_i \end{aligned}$$

has kernel which is a maximal ideal generated by n elements.

Proof. (*Sketch*) Use the proof of Lemma 22.1.6.1 to obtain that for each $1 \le i \le n$, we have that $k(\alpha_1,\dots,\alpha_{i-1})[\alpha_i] \cong k(\alpha_1,\dots,\alpha_{i-1})[x_i]/p_i(\alpha_1,\dots,\alpha_{i-1},x_i)$ and divide an element $p \in k[x_1,\dots,x_n]$ in the kernel inductively by p_i and replacing p_i by remainder, starting at $i = n$. □

Let us now observe a basic fact. Next, we observe that residue fields of any point in an affine n-space over k is an algebraic extension of k. **TODO : Till Jacobson rings from Matsumura.**

22.2 Noetherian modules and rings

Let R be a ring. An R-module M is said to be *noetherian* if it satisfies either of the following equivalent properties:

1. Every increasing chain of submodules of M eventually stabilizes.
2. Every non-empty family of submodules of M has a maximal element.
3. Every submodule is finitely generated.

We prove the equivalence of 1 and 3 as in Proposition 22.2.0.3. But before, let us see that noetherian hypothesis descends to submodules and to quotients:

Lemma 22.2.0.1. *Let R be a ring and M be a noetherian R-module.*

1. *If N is a submodule of M, then N is noetherian.*
2. *If M/N is a quotient of M, then M/N is noetherian.*

Proof. 1. Take any submodule of M which is in N, then it is a submodule of N which is finitely generated.
2. Take any submodule of M/N, which is of the form K/N where $K \subseteq M$ is a submodule of M containing N. Hence K is finitely generated and so is N. Thus K/N is finitely generated. □

We also have that a finitely generated module over noetherian ring necessarily has to be noetherian, so every submodule is also finitely generated, which is not usually the case. This is another hint why having noetherian hypothesis can greatly ease calculations.

Lemma 22.2.0.2. *Let R be a noetherian ring and let M be an R-module. Then M is a noetherian module if and only if M is finitely generated.*

Proof. The only non-trivial side is R $\Rightarrow$ L. Since M is finitely generated, therefore there is a surjection $f : R^n \twoheadrightarrow M$ where R^n is noetherian as R is noetherian (you may like to see it as a consequence of Corollary 22.2.0.5). Now take an increasing chain of submodules $N_0 \subseteq N_1 \subseteq \dots$ of M. This yields an increasing chain of ideals $f^{-1}(N_0) \subseteq f^{-1}(N_1) \subseteq \dots$, which stabilizes as R is noetherian. Applying f to the chain again we get that $N_0 \subseteq N_1 \subseteq \dots$ stabilizes. □

Here's the proof of equivalence as promised.

Proposition 22.2.0.3. *Let R be a ring. An R-module M is noetherian if and only if every submodule of M is finitely generated.*

Proof. (L $\implies$ R) Suppose R-module M is noetherian and let $S \subseteq M$ be a submodule of M. Note S is also noetherian. This means that any subcollection of submodules of S has a maximal element. Let such a subcollection be the collection of all finitely generated submodules of S, which clearly isn't empty as $\{0\}$ is there. This would have a maximal element, say N. If $N = S$, we are done. If not, then take $x \in S \setminus N$ and look at $N + Rx \subset S$. Clearly this is a submodule of S strictly containing N and is also finitely generated as N is too. This contradicts the maximality of N. Hence every submodule of M is finitely generated.
(R $\implies$ L) Let every submodule of M be finitely generated. We wish to show that this

makes M into a noetherian module. So take any ascending chain of submodules $S_0 \subseteq S_1 \subseteq S_2 \subseteq \dots$. Consider the union $S = \cup_{i=0}^{\infty} S_i$. S is also a submodule because for any $x, y \in S$, since $\{S_i\}$ is an ascending chain, there exists S_i such that $x, y \in S_i$, and so $x + y \in S_i \subseteq S$. By hypothesis, $S = \langle x_1, \dots, x_k \rangle$. Let S_{n_i} be the smallest submodule containing x_i. Then $S_{\max n_i}$ is a member of the chain which contains each of the x_is, which thus means that the $S_{\max n_i}$ is generated by x_is because if it didn't then S would have either a smaller or a larger generating set, contradicting the generation by $x_1, \dots, x_k$. Hence the chain stabilizes after $S_{\max n_i}$. □

The reason one dwells with the noetherian hypothesis is reflected in the following properties enjoyed by it. Given a short exact sequence of modules, it is possible to figure out whether the middle module is noetherian or not by checking the same for the other two:

Proposition 22.2.0.4. *Let $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ be a short exact sequence of R-modules. Then, the module M is noetherian if and only if M' and M'' are noetherian.*

Proof. (L $\implies$ R) Let M be noetherian. Then if we consider any ascending chain in M' or M'', then we get an ascending chain in M because of the maps f and g. Remember inverse image of an injective and direct image of a surjective module homomorphism of a submodule is also a submodule.
(R $\implies$ L) Consider an ascending chain of submodules $S_0 \subseteq S_1 \subseteq \dots$ in M. We then have two more ascending chains $\{(f)^{-1}(S_i)\}$ and $\{g(S_i)\}$ in M' and M'' respectively. Since these are noetherian, therefore for both of them $\exists k \in \mathbb{N}$ such that these two chains stabilizes after k. Now, we wish to show that $\{S_i\}$ also stabilizes after k. For this, we just need to show that $S_{k+1} \subseteq S_k$. Hence take any $m \in S_{k+1}$. We have $g(m) \in g(S_k)$, therefore $\exists s \in S_k$ such that $g(m) = g(s) \implies g(m-s) = 0$ in M''. Since the sequence is exact, therefore $\exists m' \in M'$ such that $f(m') = m - s$, or, $m - s \in \operatorname{im}(f)$. Since $m \in S_{k+1}$ and $s \in S_k \subseteq S_{k+1}$, therefore $m - s \in S_{k+1}$. Hence $m - s \in \operatorname{im}(f) \cap S_{k+1}$ and since $\operatorname{im}(f) \cap S_{k+1} = \operatorname{im}(f) \cap S_k$, therefore $m - s \in S_k$ and thus $m \in S_k$. This proves $S_{k+1} \subseteq S_k$, proving $S_k = S_{k+1} = \dots$. □

An easy consequence of the above is that direct sum of finitely many noetherian modules is again noetherian:

Corollary 22.2.0.5. *Suppose $\{M_i\}_{i=1}^n$ be a collection of noetherian R-modules. Then $\bigoplus_{i=1}^n M_i$ is also a noetherian R-module.*

Proof. Since the sum $\bigoplus_{i=1}^n M_i$ sits at the middle of the following short exact sequence:

$$0 \longrightarrow M_1 \xrightarrow{f} \bigoplus_{i=1}^{n} M_i \xrightarrow{g} \bigoplus_{i=2}^{n} M_i \longrightarrow 0$$

where f is given by $m \longmapsto (m, 0, \dots, 0)$ and g is given by $(m_1, \dots, m_n) \longmapsto (m_2, \dots, m_n)$. The fact that this is indeed exact is simple to see. One can next use induction to complete the proof. □

An important result in the theory of noetherian rings is the following, which gives us few more (but highly important) examples of noetherian rings in nature. In particular it tells us that the one of the major class of rings which are studied in algebraic geometry, polynomial rings over algebraically closed fields, are noetherian.

Theorem 22.2.0.6. *(Hilbert basis theorem) Let R be a ring. If R is noetherian, then*

1. *$R[x_1, \dots, x_n]$ is noetherian,*
2. *$R[[x_1, \dots, x_n]]$ is noetherian.*

Proof. 1. We need only show that if R is noetherian then so is $R[x]$. Pick any ideal $I \leq R[x]$. We wish to show it is finitely generated. We go by contradiction, let I not be finitely generated.

Let $f_1 \in I$ be the smallest degree non-constant polynomial[1] and denote $I_1 = \langle f_1 \rangle$. Let $f_2 \in I \setminus I_1$ be the smallest degree non-constant polynomial and denote $I_2 = \langle f_1, f_2 \rangle$. Inductively, we define $I_n = \langle f_1, \dots, f_n \rangle$ where $f_n \in I \setminus I_{n-1}$ is of least degree non-constant. As I is not finitely generated, therefore for all $n \in \mathbb{N}$, $I_n \lneq I$. Let $f_n(x) = a_n x^m +$ other terms for each $n \in \mathbb{N}$ so that $a_n \in R$ represents the coefficient of the leading term of $f_n(x)$. Consequently, we obtain a sequence $\{a_n\} \subseteq R$. Let $J = \langle a_1, \dots, a_n, \dots \rangle$. As R is noetherian, therefore there exists $n \in \mathbb{N}$ such that $J = \langle a_1, \dots, a_n \rangle$. It follows that for some $r_1, \dots, r_n \in R$ we have

$$a_{n+1} = r_1 a_1 + \cdots + r_n a_n.$$

We claim that $I = \langle f_1, \dots, f_n \rangle =: I_n$.

If not then $f_{n+1} \in I \setminus I_n$ is of least degree non-constant. We will now show that $f_{n+1} \in I_n$, thus obtaining a contradiction. Indeed, we have by the way of choice of f_{n+1} that $\deg f_{n+1} \geq \deg f_i$ for each $i = 1, \dots, n$. Consequently the polynomial

$$g = \sum_{i=1}^{n} r_i f_i \cdot x^{\deg f_{n+1} - \deg f_i}$$

has the property that its degree is equal to $\deg f_{n+1}$ and the coefficient of its leading term is equal to f_{n+1}. It follows that the polynomial $g - f_{n+1} \in I$ has degree strictly less than that of f_{n+1}. By minimality of f_{n+1}, it follows that $g - f_{n+1} \in I_n$. Note that by construction $g \in I_n$. Hence $f_{n+1} \in I_n$, as required.

2. **TODO** : *Write it from your exercise notebook.* □

Any localization of noetherian ring is again noetherian.

Proposition 22.2.0.7. *Let R be a noetherian ring and $S \subset R$ be a multiplicative set. Then $S^{-1}R$ is a noetherian ring.*

Proof. Any ideal of R is $S^{-1}I$ where $I \subseteq R$ is an ideal by exactness of localization (Lemma 22.1.2.2). As I is finitely generated as an R-module, therefore $S^{-1}I$ is finitely generated as an $S^{-1}R$-module, as needed. □

Lemma 22.2.0.8. *Let R be a ring with $\langle f_1, \dots, f_n \rangle = R$. If each R_{f_i} is noetherian, then R is noetherian.*

Proof. Pick any ideal $I \subseteq R$. We wish to show it is finitely generated. By exactness of localization (Lemma 22.1.2.2), we get $I_{f_i} \subseteq R_{f_i}$ is an ideal, thus finitely generated as R_{f_i}-module. By Lemma 22.1.2.10, I is finitely generated as an R-module. □

[1] this exists by well-ordering by degree.

Corollary 22.2.0.9. *Let R be a ring. Then, R is noetherian if and only if R_f is noetherian for all $f \in R$.* □

22.3 Supp (M), Ass (M) and primary decomposition

Let R be a ring and M be a finitely generated R-module. In the classical case when R is a field and M is then a finite dimensional R-vector space, if $x \in M$ then if even a single element of R annihilate x, then all elements of R annihilate x. This luxury is not enjoyed when R is a ring because not all elements of R may be invertible. What one does then is to study the associated annihilating ideals corresponding to each element of M. The global version of this idea is exactly the concept of *annihilator ideal of* M, i.e. $\mathfrak{a}_M := \{r \in R \mid rM = 0\}$. A module M is then called *faithful* if $\mathfrak{a}_M = 0$.

Now, if we have an R-module M, then we get an ideal of R. This gives us a closed subset of Spec (R) (see Section 1.2). A basic question that then arises is what is the relationship between the module M and the closed set $V(\mathfrak{a}_M) \hookrightarrow \operatorname{Spec}(R)$. The following answers that.

Lemma 22.3.0.1. *Let R be a ring and M be a finitely generated R-module. If $\mathfrak{p} \in \operatorname{Spec}(R)$ and $\mathfrak{a}_M = \operatorname{Ann}(M)$ be the annihilator ideal, then the following are equivalent:*

1. *$M_\mathfrak{p} \neq 0$.*
2. *$\mathfrak{p} \in V(\mathfrak{a}_M)$.*

Proof. If we can show that $\operatorname{Ann}_{R_\mathfrak{p}}(M_\mathfrak{p}) = (\mathfrak{a}_M)_\mathfrak{p}$, then we have the following equivalence

$$M_\mathfrak{p} \neq 0 \iff \operatorname{Ann}_{R_\mathfrak{p}}(M_\mathfrak{p}) \neq R_\mathfrak{p} \iff (\mathfrak{a}_M)_\mathfrak{p} \lneq R_\mathfrak{p} \iff \mathfrak{a}_M \subseteq \mathfrak{p}$$

where last equivalence follows from a modified version of Lemma 22.1.2.3. Hence we reduce to showing that $\operatorname{Ann}_{R_\mathfrak{p}}(M_\mathfrak{p}) = (\mathfrak{a}_M)_\mathfrak{p}$. It is easy to see that $\operatorname{Ann}_{R_\mathfrak{p}}(M_\mathfrak{p}) \supseteq (\mathfrak{a}_M)_\mathfrak{p}$. Let $r/s \in \operatorname{Ann}_{R_\mathfrak{p}}(M_\mathfrak{p})$. We wish to show that $r/s \in (\mathfrak{a}_M)_\mathfrak{p}$. Since M is finitely generated, therefore let $\{m_1, \dots, m_n\}$ be a generating set of M. We thus reduce to showing that $r/s \cdot m_i/1 = 0$ for each $i = 1, \dots, n$. This is exactly the data provided by the fact that $r/s \in \operatorname{Ann}_{R_\mathfrak{p}}(M_\mathfrak{p})$. □

The above lemma hence gives us a closed subset of Spec (R) attached to each finitely generated R-module M. This has a name.

Definition 22.3.0.2. (**Support of a module**) Let R be a ring and M be a finitely generated R-module. Let $\mathfrak{a}_M$ be the annihilator ideal of M. Then, the support of the module M is defined to be the closed set $\operatorname{Supp}(M) := V(\mathfrak{a}_M) \hookrightarrow \operatorname{Spec}(R)$. By Lemma 22.3.0.1, it is equivalently given by the set of all those points $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $M_\mathfrak{p} \neq 0$.

We then define prime ideals associated to an R-module.

Definition 22.3.0.3. (**Associated prime ideals**) Let R be a noetherian ring and M be an R-module. A prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ is said to be associated to M if there exits $m \in M$ such that

$$\mathfrak{p} = \{r \in R \mid rm = 0\}.$$

The subspace of Spec (R) of all prime ideals associated to M is denoted $\operatorname{Ass}(M) \hookrightarrow \operatorname{Spec}(R)$.

One can have the following alternate definition of an associated prime ideal.

Lemma 22.3.0.4. *Let R be a noetherian ring and M be an R-module. Then,*

$$\mathfrak{p} \in \operatorname{Ass}(M) \iff \exists N \leq M \text{ such that } N \cong R/\mathfrak{p}.$$

Proof. L $\Rightarrow$ R is easy, just consider the map $R \to M$ given by $r \mapsto rm$ where $m \in M$ corresponds to $\mathfrak{p}$. Conversely, take any $0 \neq n \in N$. Then $\mathfrak{p} = \{r \in R \mid rn = 0\}$ as if $r \in R$ is such that $rn = 0$ and $n = s + \mathfrak{p}$, then $rn = rs + \mathfrak{p} = \mathfrak{p}$, that is $rs \in \mathfrak{p}$ and since $s \notin \mathfrak{p}$, therefore $r \in \mathfrak{p}$. Conversely, if $r \in \mathfrak{p}$ then for all $n \in N$, $rn = 0$. □

So, for an R-module M, we get two subspaces of $\operatorname{Spec}(R)$, one is the closed subspace called support $\operatorname{Supp}(M)$ and the other is $\operatorname{Ass}(M)$. Support will be used later, but the concept of associated prime ideals of M have a deeper connection with the ring R. They are not unrelated.

Lemma 22.3.0.5. *Let M be an R-module. Then* $\operatorname{Ass}(M) \hookrightarrow \operatorname{Supp}(M) \hookrightarrow \operatorname{Spec}(R)$.

Proof. For $\mathfrak{p} \in \operatorname{Ass}(M)$ let $m \in M$ such that its annihilator is $\mathfrak{p}$. Then, for any $r \in \mathfrak{a}_M$, $rm = 0$ and hence $r \in \mathfrak{p}$. Thus $\mathfrak{p} \in V(\mathfrak{a}_M) = \operatorname{Supp}(M)$. □

We wish to show the following result from which primary decomposition follows.

Theorem 22.3.0.6. *Let R be a noetherian ring and M be a finitely generated R-module. Then there exists an injective map*

$$M \longrightarrow \prod_{\mathfrak{p} \in \operatorname{Ass}(M)} E_{\mathfrak{p}}$$

where for each $\mathfrak{p} \in \operatorname{Ass}(M)$, $E_{\mathfrak{p}}$ *is an R-module where* $\operatorname{Ass}(E_{\mathfrak{p}}) \hookrightarrow \operatorname{Spec}(R)$ *is a singleton given by* $\{\mathfrak{p}\}$.

This result clearly tells us that points of $\operatorname{Ass}(M)$ are somewhat special. Let us investigate[2].

Lemma 22.3.0.7. *Let R be a noetherian ring and M be a finite R-module*[3]*. Then,*

1. *If $N \subseteq M$ is a submodule, then* $\operatorname{Ass}(N) \subseteq \operatorname{Ass}(M)$.
2. *If $N \subseteq M$ is a submodule, then* $\operatorname{Supp}(N) \subseteq \operatorname{Supp}(M)$.
3. *If $N \subseteq M$ is a submodule, then* $\operatorname{Ass}(N) \subseteq \operatorname{Ass}(M) \subseteq \operatorname{Ass}(N) \cup \operatorname{Ass}(M/N)$.
4. *For any point* $\mathfrak{p} \in \operatorname{Spec}(R)$, *we have* $\mathfrak{a}_{R/\mathfrak{p}} := \operatorname{Ann}(R/\mathfrak{p}) = \mathfrak{p}$. *Thus,* $\operatorname{Supp}(R/\mathfrak{p}) = V(\mathfrak{p})$ *is an irreducible closed subset of* $\operatorname{Spec}(R)$.
5. *For any point* $\mathfrak{p} \in \operatorname{Spec}(R)$, *we have* $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$. *Thus,* $\operatorname{Ass}(R/\mathfrak{p})$ *is exactly the generic point of* $\operatorname{Supp}(R/\mathfrak{p})$.
6. *For all* $\mathfrak{p} \in \operatorname{Spec}(R)$, *there exists a maximal submodule $N \subseteq M$ such that* $\mathfrak{p} \notin \operatorname{Ass}(N)$.
7. *For all* $\mathfrak{p} \in \operatorname{Ass}(M)$, *there exists a maximal submodule $N \subsetneq M$ such that* $\mathfrak{p} \notin \operatorname{Ass}(N)$ *and none of these maximal submodules are isomorphic to $R/\mathfrak{p}$.*

[2] The following was a personal investigation of the author, who, in the process of overcoming his inexperience as a true researcher, would like to apologize for the mess that is the Lemma 22.3.0.7.

[3] this is just another name for finitely generated R-modules.

Proof. Note that by Lemma 22.2.0.2, M is a Noetherian module.

1. If $\mathfrak{p} \in \operatorname{Ass}(N)$, then for some $n \in N$, $\mathfrak{p} = \{r \in R \mid rn = 0\}$. Result follows as $n \in M$.
2. If $\mathfrak{p} \in \operatorname{Supp}(N)$, then $\mathfrak{p} \supseteq \mathfrak{a}_N$. Result follows as $\mathfrak{a}_N \supseteq \mathfrak{a}_M$.
3. By 1, we need only show $\operatorname{Ass}(M) \subseteq \operatorname{Ass}(N) \cup \operatorname{Ass}(M/N)$. Pick $\mathfrak{p} \in \operatorname{Ass}(M)$. By the Lemma 22.3.0.4 and it's proof, the submodule E of M containing of all elements of M who have annihilator as $\mathfrak{p}$ is isomorphic to $R/\mathfrak{p}$. If $E \cap N =$, then M/N has a submodule isomorphic to $R/\mathfrak{p}$ and hence $\mathfrak{p} \in \operatorname{Ass}(M/N)$. Otherwise if $E \cap N \neq \emptyset$, then pick $x \in E \cap N$. Since $x \in E$, so annihilator of x is $\mathfrak{p}$ and thus $\mathfrak{p} \in \operatorname{Ass}(E \cap N)$. By another use of Lemma 22.3.0.4, there is a submodule $F \subseteq E \cap N$ which is isomorphic to $R/\mathfrak{p}$. It follows that N has a submodule isomorphic to $R/\mathfrak{p}$. By a final use of Lemma 22.3.0.4, we conclude that $\mathfrak{p} \in \operatorname{Ass}(N)$.
4. $\operatorname{Ann}(R/\mathfrak{p}) = \{r \in R \mid r(R/\mathfrak{p}) = \mathfrak{p}\}$. It follows from primality of $\mathfrak{p}$ that $\operatorname{Ann}(R/\mathfrak{p}) = \mathfrak{p}$.
5. As above, this reduces to primality of $\mathfrak{p}$.
6. The set of all submodules N of M satisfying $\operatorname{Ass}(N) \notin p$ has a maximal element as M is a noetherian module.
7. If $\mathfrak{p} \in \operatorname{Ass}(M)$, then the maximal N obtained from 5 cannot be M. The other fact follows from 4.

□

With the above investigation, we are now ready to prove Theorem 22.3.0.6.

Proof of Theorem 22.3.0.6. **TODO**. □

The primary decomposition now is a corollary.

Corollary 22.3.0.8. *(Primary decomposition theorem[4])*

Complete this fr
Local Algebra, C
ter 22.

[4] for finitely generated modules over a Noetherian ring.

22.4 Tensor, symmetric & exterior algebras

22.4.1 Results on tensor products

We collect some important results on tensor products in this section which are used all over the text. The following results are immediate corollaries of definition of tensor product, but are of immense use in general.

Proposition 22.4.1.1. *Following are some basic properties of tensor products.*

1. *Tensor product is associative and commutative upto isomorphism.*
2. *If $\{M_\lambda\}$ is a family of R-modules and N is an R-module, then*
$$\left(\bigoplus_\lambda M_\lambda\right) \otimes_R N \cong \bigoplus_\lambda M_\lambda \otimes_R N.$$
3. *Let $\varphi : R \to S$ be a ring homomorphism and M, N be two R-modules. Then the scalar extended modules $M \otimes_R S$ and $N \otimes_R S$ satisfy the following*
$$(M \otimes_R S) \otimes_S (N \otimes_R S) \cong (M \otimes_R N) \otimes_R S.$$
4. *Let R be a ring and M be an R-module. If $I, J \leq R$ are two ideals, then*
$$R/I \otimes_R R/J \cong R/I + J$$
as rings.
5. *If R, S are two rings, then*
$$R \otimes_S S[x] \cong R[x]$$
as rings.

Proof. **TODO.** □

The following is a helpful lemma showing that tensor product commutes with direct limits in all positions.

Lemma 22.4.1.2. *Let M_i, N_i bet R_i-modules where I is directed set and $\{M_i\}, \{N_i\}$ and $\{R_i\}$ are directed systems of modules and rings. Let $M := \varinjlim_{i \in I} M_i$, $N := \varinjlim_{i \in I} N_i$ and $R := \varinjlim_{i \in I} R_i$. Then,*
$$\varinjlim_{i \in I} (M_i \otimes_{R_i} N_i) \cong M \otimes_R N$$
as R-modules.

Proof. We will construct R-linear maps $f : \varinjlim_{i \in I}(M_i \otimes_{R_i} N_i) \longleftrightarrow M \otimes_R N : g$ which will be inverses to each other. We first construct f as follows. For each $i \in I$, we have
$$f_i : M_i \otimes_{R_i} N_i \to M \otimes_{R_i} N \to M \otimes_R N$$

given by $(m_i \otimes n_i) \mapsto ((m_i) \otimes (n_i)) \mapsto ((m_i) \otimes (n_i))$. Note that M, N are R_i-modules canonically. By universal property of $\varinjlim_{i \in I}$, we obtain f as above. To construct g, we need only construct an R-bilinear map

$$\begin{aligned} M \times N &\longrightarrow \varinjlim_{i \in I}(M_i \otimes_{R_i} N_i) \\ ((m_i)_{i\in I}, (n_i)_{i \in I}) &\longmapsto ((m_i \otimes n_i)_{i \in I}). \end{aligned}$$

This can be said to be R-bilinear, thus yielding a map g as required. It is straightforward to see they are inverses to each other. □

The following says that localization commutes with tensor products.

Lemma 22.4.1.3. *Let M, N be two R-modules and $S \subseteq R$ be a multiplicative set. Then,*

$$S^{-1}(M \otimes_R N) \cong S^{-1}M \otimes_{S^{-1}R} S^{-1}N.$$

Proof. We may write by Lemma 22.1.2.1 the following

$$\begin{aligned} S^{-1}M \otimes_{S^{-1}R} S^{-1}N &\cong (M \otimes_R S^{-1}R) \otimes_{S^{-1}R} (S^{-1}R \otimes_R N) \\ &\cong M \otimes_R (S^{-1}R \otimes_{S^{-1}R} (S^{-1}R \otimes_R N)) \\ &\cong M \otimes_R (N \otimes_R S^{-1}R) \\ &\cong (M \otimes_R N) \otimes_R S^{-1}R \\ &\cong S^{-1}(M \otimes_R N). \end{aligned}$$

This completes the proof. □

Next, we discuss the notion of fiber of a map of rings. This is easily understood in the scheme language.

Definition 22.4.1.4 (Fiber at a prime ideal). Let $\varphi : R \to S$ be a ring homomorphism and let $\mathfrak{p} \lneq R$ be a prime ideal. Then the fiber of φ at $\mathfrak{p}$ is defined to be $S \otimes_R \kappa(\mathfrak{p})$.

One of the fundamental observation about fiber at a prime ideal is that it is indeed the fiber of the corresponding map of schemes (see Proposition 1.6.5.1), so that the notation makes sense.

22.4.2 Determinants

Fix a commutative ring R with unity for the remainder of this section. We shall show in this section that there exists a unique determinant map over $M_n(R)$. This will motivate further notions discussed in later sections.

We begin by defining a multilinear map over $M_n(R)$.

Definition 22.4.2.1. (**Multilinear map over** $M_n(R)$) Let $n \in \mathbb{N}$ and consider $M_n(R)$. An n-linear map over $M_n(R)$ is a function

$$D : M_n(R) \longrightarrow R$$

which is linear in each row. That is, if A_i denotes the i^{th}-row of matrix A and $c \in R$, then for each $i = 1, \dots, n$, we have

$$\begin{aligned} D(A_1, \dots, A_{i-1}, cA_i + B_i, A_{i+1}, \dots, A_n) &= cD(A_1, \dots, A_{i-1}, A_i, A_{i+1}, \dots, A_n) \\ &\quad + D(A_1, \dots, A_{i-1}, B_i, A_{i+1}, \dots, A_n). \end{aligned}$$

We may abbreviate the above by simply writing $D(cA_i + B_i) = cD(A_i) = D(B_i)$.

Example 22.4.2.2. The map

$$\begin{aligned} D : M_n(R) &\longrightarrow R \\ A &\longmapsto cA_{1k_1}A_{2k_2}\dots A_{nk_n} \end{aligned}$$

is an n-linear map where $c \in R$ is a constant and $1 \le k_i \le n$ are n integers.

We first see that linear combination of n-linear maps is again n-linear.

Lemma 22.4.2.3. *Let $D_1, \dots, D_r$ be n-linear maps and $c_1, \dots, c_r \in R$. Then $c_1D_1 + \dots + c_rD_r$ is an n-linear map.*

Proof. By induction, we may assume $r = 2$. Now this is a straightforward check. □

We now come more closer to determinants by defining the following type of n-linear maps.

Definition 22.4.2.4. (**Alternating & determinant maps**) An n-linear map $D : M_n(R) \to R$ is said to be alternating if

1. $D(A) = 0$ if $A_i = A_j$ for any $i \neq j$,
2. $D(\sigma_{ij}(A)) = -D(A)$ where σ_{ij} swaps rows A_i and A_j.

An alternating n-linear map $D : M_n(R) \to R$ is said to be determinant if $D(I_n) = 1$.

Proposition 22.4.2.5. *If $D : M_n(R) \to R$ is an n-linear map such that $D(A) = 0$ whenever $A_i = A_{i+1}$ for some $1 \le i \le n$, then D is alternating.*

Proof. Let $A \in M_n(R)$ and $1 \le i \neq j \le n$ be such that $A_i = A_j$. We first wish to show that $D(\sigma_{ij}(A)) = -D(A)$. We may assume $j > i$. We go by strong induction over $j - i$. We first show this for $j = i + 1$. Indeed, we then have $D(\sigma_{i,i+1}(A)) = D(A_{i+1}, A_i)$. Writing $0 = D(A_{i+1} + A_i, A_i + A_{i+1}) = D(A_{i+1}, A_i) + D(A_i, A_{i+1})$. Thus we get $D(A_{i+1}, A_i) = -D(A_i, A_{i+1})$.

In the inductive case, suppose $D(\sigma_{ij}(A)) = -D(A)$ for all $j - i \le k$. We wish to show that if $j - i = k + 1$, then the same holds. As $\sigma_{i,i+k+1}(A) = \sigma_{i+k,i+k+1} \circ \sigma_{i,i+k} \circ \sigma_{i+k,i+k+1}(A)$, therefore we are done.

To get that $D(A) = 0$ for A such that $A_i = A_j$ for some $j > i$, we may simply swap rows till they are adjacent, which will be zero by our hypothesis. □

We now define the main candidate for the determinant function over $M_n(R)$.

Definition 22.4.2.6. (E_j) Let $D : M_{n-1}(R) \to R$ be an $n-1$-linear map. For each $1 \leq j \leq n$, define the following map

$$\begin{aligned} E_j : M_n(R) &\longrightarrow R \\ A &\longmapsto \sum_{i=1}^{n} (-1)^{i+j} A_{ij} D(A[i|j]). \end{aligned}$$

Further denote $D_{ij}(A) := D(A[i|j])$.

Theorem 22.4.2.7. *Let $n \in \mathbb{N}$ and $D : M_{n-1}(R) \to R$ be an alternating $n-1$-linear map. For each $1 \leq j \leq n$, the map $E_j : M_n(R) \to R$ defined as above is an alternating n-linear map. If moreover D is a determinant map, then so is each E_j.*

Proof. Fix $1 \leq j \leq n$. We first wish to show that E_j is n-linear. As $D_{ij} : M_n(R) \to R$ is linear in every row except i. Thus $A \mapsto A_{ij} D_i j(A)$ is n-linear. It follows from Lemma 22.4.2.3 that E_j is n-linear.

To show that E_j is alternating, it would suffice from Proposition 22.4.2.5 to show that $E_j(A) = 0$ if A has any two adjacent rows equal, say $A_k = A_{k+1}$. This one checks directly by the definition of E_j.

To see that E_j is determinant if D is determinant is also easy to see. □

We now show the uniqueness of determinants and alternating n-linear maps (upto the value on I_n).

Theorem 22.4.2.8. *Let $D : M_n(R) \to R$ be an alternating n-linear map over $M_n(R)$. Then,*

1. *D is given explicitly on $A \in M_n(R)$ by*

$$D(A) = \left(\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) A_{1\sigma(1)} \dots A_{n\sigma(n)} \right) D(I),$$

hence D is unique upto its value over I,

2. *if D is determinant map, then it is uniquely given by*

$$D(A) = \det A := \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) A_{1\sigma(1)} \dots A_{n\sigma(n)},$$

3. *any alternating map D on $M_n(R)$ is thus uniquely determined by its value on I as*

$$D(A) = (\det A) \cdot D(I).$$

Proof. The proof is straightforward but tedious. **TODO**. □

Corollary 22.4.2.9. *Let $n \in \mathbb{N}$.*

1. *If $A, B \in M_n(R)$, then $\det(AB) = \det(A) \cdot \det(B)$.*
2. *If $B \in M_n(R)$ is obtained by $B_j = A_j + cA_i$ for some fixed $1 \leq i, j \leq n$ and rest of the rows of B are identical to A, then $\det(B) = \det(A)$.*

3. If $M \in M_{r+s}(R)$ is given by

$$M = \begin{bmatrix} A_{r\times r} & B_{r\times s} \\ 0 & C_{s\times s} \end{bmatrix}$$

then $\det(M) = \det(A)\cdot\det(C)$.

4. For each $1 \le j \le n$, we have

$$\det(A) = E_j(A) = \sum_{i=1}^{n} (-1)^{i+j} A_{ij} \det(A[i|j]).$$

Proof. (*Sketch*) For 1. we can contemplate

$$\begin{aligned} D : M_n(R) &\longrightarrow R \\ A &\mapsto \det(AB). \end{aligned}$$

One claims that D is an n-linear alternating map. Then apply Theorem 22.4.2.8, 3.

2. Follows by multilinearity of det.

3. As elementary row operations only change determinant upto sign and restricting an $r+s$-linear alternating map to first r or last s entries keeps it r-linear and s-linear alternating respectively, therefore the result follows.

4. Follows from Theorem 22.4.2.7 and Theorem 22.4.2.8. □

Construction 22.4.2.10. (*Adjoint of a matrix*) Let $A \in M_n(R)$ be a square matrix. By Corollary 22.4.2.9, the sum $E_j(A) = \det(A)$ for each $1 \le j \le n$

$$\det(A) = \sum_{i=1}^{n} A_{ij} (-1)^{i+j} \det(A[i|j]).$$

Hence, let us define $C_{ij} := (-1)^{i+j}\det(A[i|j])$ as the ij^{th}-*cofactor of A*. Consequently, we get a matrix $(\text{Adj}A)_{ij} = C_{ji}$, called the *adjoint matrix*. Hence, we may rewrite the determinant as

$$\begin{aligned} \det(A) &= \sum_{i=1}^{n} A_{ij} C_{ij} \\ &= \sum_{i=1}^{n} (\text{Adj}A)_{ji} A_{ij}. \end{aligned}$$

Thus,

$$\det(A) I = \text{Adj}(A) \cdot A.$$

This also allows us to write that in the case when A is invertible, we have

$$A^{-1} = \frac{1}{\det A}\text{Adj}(A).$$

As similar matrices have same determinant, therefore each linear operator on a finite dimensional vector space has a unique determinant. Thus determinants are invariants of linear operators upto similarity.

22.4.3 Multilinear maps

We now put the previous discussion in a more abstract framework where we work with modules over a commutative ring with 1. We first recall that the rank of a finitely generated module is the size of the smallest generating set. Further recall that a finitely generated free R-module V has a well-defined rank and the smallest generating set is moreover a basis of V (i.e. linearly independent set of generators).

For this section, we would hence fix a commutative ring R with 1.

Definition 22.4.3.1. (**r-linear forms over a module**) Let V be an R-module. An r-linear form L over V is a function

$$L : V^r = V \times \cdots \times V \longrightarrow R$$

such that for any $c \in R$, $\beta_i \in V$ and $(\alpha_1, \ldots, \alpha_r) \in V^r$, we have

$$L(\alpha_1, \ldots, c\alpha_i + \beta_i, \ldots, \alpha_n) = cL(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n) + L(\alpha_1, \ldots, \beta_i, \ldots, \alpha_n)$$

for any $1 \leq i \leq r$. An r-linear form is usually also called an r-tensor. A 2-linear form/tensor is also usually called a bilinear form. Note that an r-linear form may not be linear. Denote the R-module of all r-linear forms by $M^r(V)$.

Remark 22.4.3.2. Let $f_1, \ldots, f_r \in V^* = \operatorname{Hom}_R(V, R) = M^1(V)$ be a collection of linear functionals. We then obtain $L \in M^r(V)$ given by

$$L(\alpha_1, \ldots, \alpha_r) = f_1(\alpha_1) \cdot \cdots \cdot f_r(\alpha_r).$$

Example 22.4.3.3. We give some examples.

1. Let $V = R^n$ be a free R-module of rank n. Then for a fixed matrix $A \in M_n(R)$, the map

$$\begin{aligned} V \times V &\longrightarrow R \\ (x, y) &\longmapsto x^t A y \end{aligned}$$

is a bilinear form over V.

2. Let $V = R^n$ be a free R-module of rank n. Then we obtain the following n-linear form

$$\begin{aligned} \det : V^n &\longrightarrow R \\ (\alpha_1, \ldots, \alpha_n) &\longmapsto \det(A) \end{aligned}$$

where $A \in M_n(R)$ whose i^{th}-row is α_i. Hence, determinant is an n-tensor/n-linear form over V.

Remark 22.4.3.4. (General expression of an r-linear form) Let $L \in M^r(V)$ be an r-form over an R-module V where V is a free module of rank n. Further denote $e_1, \ldots, e_n$ be a basis of V. For any $(\alpha_1, \dots, \alpha_r) \in V^r$, we may write $\alpha_i = \sum_{j=1}^n A_{ij} e_j$. Hence we have $A \in M_{r\times n}(R)$. This yields by n-linearity of L that

$$\begin{aligned} L(\alpha_1, \dots, \alpha_r) &= \sum_{j_r=1}^n \cdots \sum_{j_1=1}^n A_{1j_1} \dots A_{rj_r} L(e_{j_1}, \dots, e_{j_r}) \\ &= \sum_{J=\{j_1,\dots,j_r\}} A_J L(e_J) \end{aligned}$$

where $J \in X$ where X is the set of all r-tuples with entries in $\{1, \dots, n\}$. There are therefore n^r terms in the above sum.

Definition 22.4.3.5. (**Tensor product of linear forms**) Let M be an R-module. We then define

$$\begin{aligned} -\otimes - : M^r(V) \times M^s(V) &\longrightarrow M^{r+s}(V) \\ (L, M) &\longmapsto L \otimes M \end{aligned}$$

where $L \otimes M : V^{r+s} \to R$ is given by $(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s) \mapsto L(\alpha_1, \dots, \alpha_r) M(\beta_1, \dots, \beta_s)$.

Remark 22.4.3.6. We have following observations about tensor of forms:
1. $L \otimes (T + S) = L \otimes T + L \otimes S$,
2. $(L \otimes T) \otimes N = L \otimes (T \otimes N)$,
3. $c(L + T) \otimes S = cL \otimes S + cT \otimes S$,
4. $L \otimes T \neq T \otimes L$.

We now come to an important theorem about $M^r(V)$

Theorem 22.4.3.7. *Let V be a free R-module of rank n and $B = \{e_1, \dots, e_n\} \subseteq V$ be a basis of V. Let X denote the set of all r-tuples with entries in $\{1, \dots, n\}$. Then,*
1. *the R-module $M^r(V)$ is free of rank n^r,*
2. *a basis of $M^r(V)$ is given by $f_J = f_{j_1} \otimes \dots \otimes f_{j_r}$ where $B^* = \{f_1, \dots, f_n\} \subseteq V^* = M^1(V)$ is the dual basis of B, where $J = \{j_1, \dots, j_r\}$ varies over all elements of X.*

Proof. (*Sketch*) We claim that $\{f_J\}_{J\subseteq X}$ forms a basis of $M^r(V)$. Pick any $(\alpha_1, \dots, \alpha_r) \in V^r$, then by Remark 22.4.3.4, we first have $\alpha_i = \sum_{j=1}^n f_j(\alpha_i) e_j$. Consequently,

$$\begin{aligned} L(\alpha_1, \dots, \alpha_r) &= \sum_{J=\{j_1,\dots,j_r\}} L(e_{j_1}, \dots, e_{j_r}) \cdot f_{j_1} \otimes \dots \otimes f_{j_r}(\alpha_1, \dots, \alpha_r) \\ &= \sum_{J=\{j_1,\dots,j_r\}} L(e_J) f_{j_1} \otimes \dots \otimes f_{j_r}(\alpha_1, \dots, \alpha_r). \end{aligned}$$

Thus, $\{f_J\}_{J\subseteq X}$ spans $M^r(V)$. For linear independence, take any combination

$$\sum_{J\subseteq X} c_J f_J = 0.$$

On the LHS, apply e_I to get $c_I = 0$ for each $I \subseteq X$. □

Definition 22.4.3.8. (**Alternating r-linear forms**) Let V be an R-module. An r-linear form $L \in M^r(V)$ is said to be alternating if

1. $L(\alpha_1, \dots, \alpha_r) = 0$ if $\alpha_i = \alpha_j$ for $i \neq j$,
2. $L(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(r)}) = \operatorname{sgn}(\sigma) L(\alpha_1, \dots, \alpha_r)$ for all $\sigma \in S_r$.

The collection of all alternating r-linear forms is denoted by $\Lambda^r(V)$ and its a submodule of $M^r(V)$. Note that the second axiom follows from 1, but is important to keep it in mind.

Observe that $\Lambda^1(V) = M^1(V) = V^*$.

Remark 22.4.3.9. Consider $V = R^n$, a free R-module of rank n. We saw earlier that $\det \in M^n(V)$ is an n-linear form.. Theorem 22.4.2.8 shows that det is moreover an unique alternating form with $\det(e_1, \dots, e_n) = 1$. Thus, $\det \in \Lambda^n(V) \subseteq M^n(V)$ is the unique alternating n-linear form over V such that $\det(e_1, \dots, e_n) = 1$, i.e. $\Lambda^n(V)$ is a free R-module of rank 1.

Construction 22.4.3.10. Let V be an R-module. We now construct an R-linear map $\pi_r : M^r(V) \to \Lambda^r(V)$. For each $L \in M^r(V)$, define $L_\sigma \in M^r(V)$ given by $L_\sigma(\alpha_1, \dots, \alpha_r) = L(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(r)})$ for $(\alpha_1, \dots, \alpha_r) \in V^r$. Consequently, we claim that the following map is well-defined:

$$\begin{aligned}\pi_r : M^r(V) &\longrightarrow \Lambda^r(V)\\ L &\longmapsto \sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) L_\sigma.\end{aligned}$$

Indeed, we have to show that $\pi_r L$ is an alternating form. Let $(\alpha_1, \dots, \alpha_r) \in V^r$ be such that $\alpha_i = \alpha_j$ for $i \neq j$. We wish to show that $\pi_r L(\alpha_1, \dots, \alpha_r) = 0$. Let $\tau = (ij)$ be the transposition swapping i and j. First observe that the map $S_r \to S_r$ given by $\sigma \mapsto \tau\sigma$ is a bijection. Consequently, if we let $\sigma_1, \dots, \sigma_{\frac{n!}{2}}$ to be any $\frac{n!}{2}$ elements of S_r, then the rest $\frac{n!}{2}$ are given by $\tau\sigma_i$, $i = 1, \dots, n!/2$. Consequently,

$$\begin{aligned}\pi_r L(\alpha_1, \dots, \alpha_r) &= \sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) L(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(r)})\\ &= \sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) L(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(r)})\\ &= \sum_{i=1}^{\frac{n!}{2}} \operatorname{sgn}(\sigma_i) L(\alpha_{\sigma_i(1)}, \dots, \alpha_{\sigma_i(r)}) + \sum_{i=1}^{\frac{n!}{2}} \operatorname{sgn}(\tau\sigma_i) L(\alpha_{\tau\sigma_i(1)}, \dots, \alpha_{\tau\sigma_i(r)})\\ &= \sum_{i=1}^{\frac{n!}{2}} \operatorname{sgn}(\sigma_i) L(\alpha_{\sigma_i(1)}, \dots, \alpha_{\sigma_i(r)}) + \sum_{i=1}^{\frac{n!}{2}} -\operatorname{sgn}(\sigma_i) L(\alpha_{\sigma_i(1)}, \dots, \alpha_{\sigma_i(r)})\\ &= 0.\end{aligned}$$

Hence, π_r is indeed an R-linear map from $M^r(V)$ into $\Lambda^r(V)$.

Finally note that if $L \in \Lambda^r(V)$, then $\pi_r L = r!L$ as $L_\sigma = \operatorname{sgn}(\sigma) L$ for any $\sigma \in S_r$.

Example 22.4.3.11. Let $V = R^n$ be the free R-module of rank n. Let $e_1, \ldots, e_n \in V$ be the standard R-basis of V. Further, let $f_1, \ldots, f_n \in M^1(V)$ be the associated dual basis. Note that for any $\alpha \in V$, we have $\alpha = f_1(\alpha)e_1 + \ldots f_n(\alpha)e_n$. Then, we get an n-form

$$L = f_1 \otimes \ldots \otimes f_n \in M^n(V).$$

Consequently we obtain an alternating n-form given by

$$\pi_r L = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)(f_{\sigma(1)} \otimes \ldots \otimes f_{\sigma(n)}).$$

Observe that for any $(\alpha_1, \ldots, \alpha_n) \in V^n$, we obtain

$$\begin{aligned} \pi_r L(\alpha_1, \ldots, \alpha_n) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left(f_{\sigma(1)} \otimes \ldots \otimes f_{\sigma(n)}\right)(\alpha_1, \ldots, \alpha_n) \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \left(f_{\sigma(1)}(\alpha_1) \cdot \dots \cdot f_{\sigma(n)}(\alpha_n)\right). \end{aligned}$$

This is exactly the determinant of the $n \times n$ matrix over R given by $A = (f_j(\alpha_i))$. That is, $\pi_r L = \det$.

The following properties of π_r will become important later on.

Proposition 22.4.3.12. *Let V be an R-module and $L \in M^r(V)$ and $M \in M^s(V)$ be r and s-forms over V respectively. Then,*

$$\pi_{r+s}(\pi_r(L) \otimes \pi_s(M)) = r!s!\pi_{r+s}(L \otimes M).$$

Proof. ***TODO*** *: Magnum tedium.* □

The above has a very nice and useful corollary.

Corollary 22.4.3.13. *Let V be a free R-module of rank n with $f_1, \ldots, f_n \in V^*$ be a dual basis of V^*. Let $I \in X_r$ and $J \in X_s$ where X_r and X_s are the sets of r and s combinations of $\{1, \ldots, n\}$, respectively, such that I and J are disjoint ($i_k \neq j_l$ for any $1 \leq k \leq r$, $1 \leq l \leq s$). Denote $D_I = \pi_r(f_I)$ and $D_J = \pi_s(f_J)$ where $f_I = f_{i_1} \otimes \ldots \otimes f_{i_r} \in M^r(V)$ and $f_J = f_{j_1} \otimes \ldots \otimes f_{j_s} \in M^s(V)$. Then,*

$$\pi_{r+s}(D_I \otimes D_J) = r!s!D_{I \amalg J}.$$

Proof. Follows immediately from Proposition 22.4.3.12 □

We now come to the main result about alternating forms.

Theorem 22.4.3.14. *Let V be a free module of rank n over R.*

1. *If $r > n$, then $\Lambda^r(V) = 0$.*
2. *If $0 \leq r \leq n$, then rank of $\Lambda^r(V)$ is ${}^nC_r$.*

Proof. (*Sketch*) Using Remark 22.4.3.4, statement 1 is straightforward. For 2, observe that we can write for $(\alpha_1, \dots, \alpha_r) \in V^r$, $r \leq n$ as follows

$$L(\alpha_1, \dots, \alpha_r) = \sum_{J=\{j_1,\dots,j_r\}\in X} L(e_J)(f_{j_1} \otimes \dots \otimes f_{j_r})(\alpha_1, \dots, \alpha_r)$$

where X is the set of all r-permutations of $\{1, \dots, n\}$ (as for any repeatitions, the corresponding term is 0). Now, partitioning the set X into classes in which permutations represent the same combination, we obtain an indexing set $\hat{X}$ of size ${}^nC_r$. Again, by the fact that L is alternating, we observe $\text{sgn}(\sigma)L(e_{j_1}, \dots, e_{j_r}) = L(e_{j_{\sigma(1)}}, \dots, e_{j_{\sigma(r)}})$. Consequntly we may write the above sum as

$$L(\alpha_1, \dots, \alpha_r) = \sum_{J=\{j_1,\dots,j_r\}\in \hat{X}} L(e_{j_1}, \dots, e_{j_r}) \sum_{\sigma\in S_r} \text{sgn}(\sigma) \left(f_{j_{\sigma(1)}} \otimes \dots \otimes f_{j_{\sigma(r)}}\right)(\alpha_1, \dots, \alpha_r).$$

Therefore denote for each $J \in \hat{X}$ the following

$$D_J = \sum_{\sigma\in S_r} \text{sgn}(\sigma) \left(f_{j_{\sigma(1)}} \otimes \dots \otimes f_{j_{\sigma(r)}}\right).$$

One can observe that the D_J for each $J \in \hat{X}$ can alternatively be written as

$$D_J = \pi_r(f_{j_1} \otimes \dots \otimes f_{j_r}).$$

The above shows that D_J is in $\Lambda^r(V)$ and that it spans $\Lambda_r(V)$. The claim now is that these are also linearly independent. Indeed, that follows immediately by using the fact that f_js are dual basis of e_js. □

We can now abstractly obtain the determinant of a linear operator $T : V \to V$ on a free R-module V of rank n.

Corollary 22.4.3.15. *Let V be a free R-module of rank n and $T : V \to V$ be an R-linear operator. Then,*

1. *rank of $\Lambda^n(V) = 1$,*
2. *there exists a unique $c_T \in R$ such that for all $L \in \Lambda^n(V)$,*

$$L \circ T = c_T L.$$

This c_T is defined to be the determinant of the operator T.

Proof. Statement 1 follows from Theorem 22.4.3.14. For statement 2, one need only observe that $L \circ T$ is again an alternating n-tensor and then use statement 1. □

22.4.4 Exterior algebra over characteristic 0 fields

Let us first make the exterior algebra over characteristic 0 fields, before moving to arbitrary ring.

Definition 22.4.4.1. (**Wedge product**) Let K be a field of characteristic 0 and V be an R-vector space. For any $r, s \in \mathbb{N}$, define

$$\begin{aligned}\Lambda^r(V) \times \Lambda^s(V) &\longrightarrow \Lambda^{r+s}(V)\\ (L, M) &\longmapsto L \wedge M := \frac{1}{r!s!}\pi_{r+s}(L \otimes M).\end{aligned}$$

Observe that $D_I \wedge D_J = \frac{1}{r!s!}\pi_{r+s}(\pi_r(f_I) \otimes \pi_s(f_J)) = \frac{r!s!}{r!s!}\pi_{r+s}(f_I \otimes f_J)$ and the latter is either 0 if I and J have a common index or $D_{I \amalg J}$ if they are distinct. This follows from Proposition 22.4.3.12.

In the following result, we see that wedge product is a anti-commutative, distributive and associative operation.

Proposition 22.4.4.2. *Let V be a K-vector space over a field K of characteristic 0.*

1. *Let $\omega, \eta \in \Lambda^k(V), \phi \in \Lambda^l(V)$. Then, wedge product is distributive as*

$$(\omega + \eta) \wedge \phi = \omega \wedge \phi + \eta \wedge \phi,$$

2. *Let $\omega \in \Lambda^k(V), \eta \in \Lambda^l(V)$. Then, wedge product is anti-commutative as*

$$\omega \wedge \eta = (-1)^{kl}\eta \wedge \omega,$$

3. *Let $\omega \in \Lambda^k(V), \eta \in \Lambda^l(V), \phi \in \Lambda^m(V)$. Then, wedge product is associative as*

$$(\omega \wedge \eta) \wedge \phi = \omega \wedge (\eta \wedge \phi).$$

Proof. We need only check these identities on the basis elements $\{D_I\}$ of each $\Lambda^r(V)$.

1. Let $\omega = D_I, \eta = D_J$ and $\varphi = D_M$. Then,

$$\begin{aligned}(D_I + D_J) \wedge D_M &= \pi_{k+l}((D_I + D_J) \otimes D_M) = \pi_{k+l}(D_I \otimes D_M + D_J \otimes D_M)\\ &= \pi_{k+l}(D_I \otimes D_M) + \pi_{k+l}(D_J \otimes D_M) = D_I \wedge D_M + D_J \wedge D_M\end{aligned}$$

as required.

2. **TODO**. □

Using above, we come to the following definition.

Definition 22.4.4.3. (**Exterior algebra**) Let V be a K-vector space where K is a field of characteristic 0. Then the exterior algebra over V is

$$\begin{aligned}\Lambda(V) &= K \oplus \Lambda^1(V) \oplus \Lambda^2(V) \dots\\ &= K \oplus \bigoplus_{k \geq 1} \Lambda^k(V)\end{aligned}$$

where the product is given by wedge product which by Proposition 22.4.4.2 is associative, unital, distributive but non-commutative. This is also sometimes called the Grassmann algebra over V.

Remark 22.4.4.4. Observe that if V is of dimension n, then

$$\Lambda(V) = K \oplus \bigoplus_{k=1}^{n} \Lambda^k(V)$$

as all the higher forms are automatically 0. Consequently, the dimension of $\Lambda(V)$ by Theorem 22.4.3.14 is seen to be

$$\begin{aligned}\dim_K \Lambda(V) &= 1 + \sum_{k=1}^{n} {}^nC_k \\ &= \sum_{k=0}^{n} {}^nC_k \\ &= 2^n.\end{aligned}$$

Remark 22.4.4.5. Let V be a K-vector space of dimension n, where K is of characteristic 0. The exterior algebra $\Lambda(V)$ is a graded K-algebra of dimension 2^n over K. Indeed, the grading is correct as if $\omega \in \Lambda^k(V), \eta \in \Lambda^l(V)$, then $\omega \wedge \eta \in \Lambda^{k+l}(V)$.

22.4.5 Tensor, symmetric & exterior algebras

We now define the three algebras TM, SM and $\wedge M$ associated to a module M over R

Definition 22.4.5.1 (TM, SM **and** $\wedge M$)**.** Let R be a ring and M be an R-module.

1. The tensor algebra over M is defined to be
$$TM = \bigoplus_{n\geq 0} T^n M$$
where $T^nM = M\otimes\ldots\otimes M$ n-times and $T^0M = R$. This is a non-commutative graded R-algebra where the multiplication is given by tensor product.
2. The symmetric algebra over M is defined to be the quotient
$$SM = TM/I = \bigoplus_{n\geq 0} S^n M$$
where I is the two-sided graded ideal of TM given by
$$I = \langle x\otimes y - y\otimes x | x, y \in M\rangle.$$
This is a commutative graded R-algebra where S^nM denotes $T^nM/I \cap T^nM$.
3. The exterior algebra over M is defined to be the quotient
$$\wedge M = TM/J = \bigoplus_{n\geq 0} \wedge^n M$$
where J is the two-sided graded ideal of TM given by
$$J = \langle x\otimes x \mid x \in M\rangle.$$
This is a skew-commutative[5] graded R-algebra where $\wedge^nM$ denotes $T^nM/J \cap T^nM$.

We now give a canonical basis for each of them in the case when M is a free R-module of rank n. **TODO.**

[5] as J contains $x\otimes y + y\otimes x$ by opening $(x+y)\otimes(x+y) \in J$.

22.5 Field theory

22.5.1 Finite and algebraic extensions and compositum

Recall that a field extension K/F is said to be *finite* if K/F is a finite dimensional F-vector space and then we denote $[K : F] := \dim_F K$. It is said to be *algebraic* if for every $\alpha \in K$, there exists $p(x) \in F[x]$ such that $p(\alpha) = 0$, that is, the inclusion $F \hookrightarrow K$ is integral. Let $I = \{p(x) \in F[x] \mid p(\alpha) = 0\} \leq F[x]$ be an ideal. The generating element $m_{\alpha,F}(x)$ of I is called the *minimal polynomial* of $\alpha \in K$. Note that this is irreducible as I is a prime ideal as it is kernel of a map.

The main basic result connecting algebraic and finite extensions is that finitely generated algebraic extensions are equivalent to finite extensions. This is immediate from Proposition 22.6.1.8, but we give an elementary proof. We first begin by elementary observations.

Theorem 22.5.1.1. *Let K/F be a field extension and $\alpha \in K$.*

1. *If K/F is finite, then it is algebraic.*
2. *If $K/L/F$ are extensions, then*
$$[K : F] = [K : L] \cdot [L : F]$$
where $[K : L]$ or $[L : F]$ is infinity if and only if $[K : F]$ is infinity.
3. *If $\alpha_1, \dots, \alpha_n$ are algebraic over F, then $F(\alpha_1, \dots, \alpha_n) = F[\alpha_1, \dots, \alpha_n]$.*
4. *We have $[F(\alpha) : F] = \deg m_{\alpha,F}$.*
5. *The extension $F(\alpha_1, \dots, \alpha_n)/F$ is algebraic if and only if $\alpha_1, \dots, \alpha_n$ are algebraic over F.*
6. *K/F is a finite-type algebraic extension if and only if K/F is finite.*
7. *If K/L and L/F are both algebraic, then K/F is algebraic.*
8. *The set of all algebraic elements in K over F forms a subfield of K containing F denoted $K^{\mathrm{alg}/F}$.*

Proof. 1. Pick any element $x \in K$ and consider $\{1, x, x^2, \dots\}$. Finiteness of K/F makes sure that there is a finite subset of above which is linearly depenedent.

2. Take bases of K/L and L/F and consider their pairwise product. One sees that this new collection is linearly independent and its F-span is K.

3. As $F[\alpha]$ is a field as it is isomorphic to $F[x]/\langle m_{\alpha,F}(x)\rangle$ and $m_{\alpha,F}(x)$ is irreducible. By universal property of quotients, we get $F[\alpha] = F(\alpha)$. By induction, we wish to show that $F(\alpha_1, \dots, \alpha_{n-1})[\alpha_n] = F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) = F(\alpha_1, \dots, \alpha_{n-1}, \alpha_n)$, which completes the proof.

4. We have $F(\alpha) = F[\alpha] = \frac{F[x]}{m_{\alpha,F}(x)}$ and this is of dimension $\deg m_{\alpha,F}(x)$ over F.

5. Forward is immediate. For converse, proceed by induction. Clearly, $F(\alpha_1)/F$ is algebraic as it is finite. Composition of finite is finite, so $F(\alpha_1, \dots, \alpha_n)/F$ is finite, thus algebraic.

6. Forward is the only non-trivial side. Let $K = F(\alpha_1, \dots, \alpha_n)$ and by algebraicity, α_i are algebraic. Now $F(\alpha_1)/F$ is finite as algebraic. By induction, we get the result.

7. Pick $\alpha \in K$ and consider $m_{\alpha,L}(x) \in L[x]$ as $m_{\alpha,L}(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$, $c_i \in L$. Then, consider $F(c_0, \dots, c_{n-1}) \subseteq L$. As L/F is algebraic, thus $c_i \in L$ are algebraic and thus by previous, we get $F(c_0, \dots, c_{n-1})/F$ is algebraic and finite. As

$F(c_0, \dots, c_{n-1})(\alpha)/F(c_0, \dots, c_{n-1})$ is algebraic as it is finite, thus $F(c_0, \dots, c_{n-1}, \alpha)/F$ is algebraic as it is composite of two finite extensions.

8. Indeed, pick any two algebraic elements $\alpha, \beta \in K$ over F. Then $F(\alpha, \beta)$ is an algebraic extension over F and thus $F(\alpha, \beta) \subseteq K^{\mathrm{alg}/F}$. □

Next, we define compositum, the smallest field containing two subfields.

Definition 22.5.1.2 (**Compositum of fields**)**.** Let F, K be two fields in a field L. Then compositum of F and K in L is the smallest field in L containing both F and K. This is denoted by $F \cdot K$.

The following are the main results for compositum. We will see more later when needed.

Theorem 22.5.1.3. *Let K/F be a field extension and $K_1, K_2 \subseteq K$ be two subfields containing F. Then,*

1. *If $K_1 = F(\alpha_1, \dots, \alpha_n)$ and $K_2 = F(\beta_1, \dots, \beta_m)$, then $K_1 \cdot K_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$.*
2. *If K_1/F and K_2/F are algebraic, then $K_1 \cdot K_2/F$ is algebraic.*
3. *If K_1/F and K_2/F are finite, then $K_1 \cdot K_2/F$ is finite.*
4. *If $[K_1 : F]$ and $[K_2 : F]$ are coprime, then $[K_1 \cdot K_2 : F] = [K_1 : F] \cdot [K_2 : F]$.*
5. *We have $[K_1 \cdot K_2 : F] \leq [K_1 : F] \cdot [K_2 : F]$.*

Proof. 1. It is clear that $K_1 \cdot K_2 \supseteq F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ since $K_1 \cdot K_2$ contains both K_1, K_2 and F. For the converse, as $K_1 \cdot K_2$ is the smallest field containing both K_1 and K_2 therefore $K_1 \cdot K_2 \subseteq F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$.

2. Let L be the algebraic closure of F in $K_1 \cdot K_2$. By hypothesis, $L \supseteq K_1, K_2$. Thus $L \supseteq K_1 \cdot K_2$.

3. By Theorem 22.5.1.1, 6, $K_1 = F(\alpha_1, \dots, \alpha_n)$ and $K_2 = F(\beta_1, \dots, \beta_m)$ where α_i, β_j are algebraic elements over F. By item 1, $K_1 \cdot K_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ is a finitely generated algebraic extension, thus finite, as required.

4. Since we have

$$\begin{aligned} [K_1 \cdot K_2 : F] &= [K_1 \cdot K_2 : K_1][K_1 : F] \\ &= [K_1 \cdot K_2 : K_2][K_2 : F]. \end{aligned}$$

By hypothesis, $[K_1 \cdot K_2 : F]$ is a multiple of $[K_1 : F] \cdot [K_2 : F]$. Thus we redude to showing $[K_1 \cdot K_2 : F] \leq [K_1 : F] \cdot [K_2 : F]$. Note by above equations, it suffices to show that

$$[K_1 \cdot K_2 : K_1] \leq [K_2 : F].$$

To this end, let $\alpha_1, \dots, \alpha_n \in K_2$ be an F-basis of K_2. It thus suffices to show that K_1-span of $\alpha_1, \dots, \alpha_n$ is whole of $K_1 \cdot K_2$, that is, we wish to show

$$L := K_1 \cdot \alpha_1 + \dots + K_1 \cdot \alpha_n = K_1 \cdot K_2.$$

Note that it suffices to show that L is a field containing both K_1 and K_2. Indeed, the fact that L contains K_2 is immediate as L contains F and $\alpha_1, \dots, \alpha_n$. Further L contains K_1 as L contains 1 since L contains K_2 and that it is a K_1-vector space. Thus, $L \supseteq K_1, K_2$. We thus reduce to showing that L is a field.

To this end, observe that if $l \in L$, then $l = c_1\alpha_1 + \cdots + c_n\alpha_n$ for $c_i \in K_1$. Now, $l \in K_2(c_1, \dots, c_n)$. Thus $l^{-1} \in K_2(c_1, \dots, c_n) = K_2[c_1, \dots, c_n]$, that is, l^{-1} is a polynomial in c_i with coefficients in K_2. But any element of K_2 is an F-linear combination of $\alpha_1, \dots, \alpha_n$. As $K_1 \supseteq F$, therefore l^{-1} is a linear combination of $\alpha_1, \dots, \alpha_n$ with coefficients in K_1 (powers of c_i multiplied by elements of F, so in K_1). Thus, $l^{-1} \in L$, as needed. The fact that L is multiplicatively closed is immediate. This completes the proof.

5. Follows from proof of item 4 above. □

We now see that a finite algebra over a domain which is a domain induces a finite extension of fraction fields.

Lemma 22.5.1.4. *Let $B \hookrightarrow A$ be a finite B-algebra where both A, B are domains. Then $Q(A)$ is a finite extension of $Q(B)$.*

Proof. Let $\alpha_1, \dots, \alpha_n \in A$ be a generating set of A as a B-module and let $\varphi : B \hookrightarrow A$ be the structure map of the finite B-algebra structure on A. Now let $S = B - \{0\}$. Now we get a map $S^{-1}\varphi : Q(B) \hookrightarrow S^{-1}A$. This is a finite map since $S^{-1}A$ as the $Q(B)$ span of $\alpha_1, \dots, \alpha_n$ in $S^{-1}A$ is $S^{-1}A$. To complete the proof, we need only show that the natural inclusion $S^{-1}A \hookrightarrow Q(A)$ given by $\frac{a}{b} \mapsto \frac{a}{b}$ is a finite map. We see something stronger: $Q(A) = S^{-1}A$. Indeed, this is true because $S^{-1}A$ is a field containing A as $S^{-1}A$ is a domain which is finite over the field $Q(B)$, so that by Lemma 22.6.1.13, we get that $S^{-1}(A)$ is a field. As it contains A, so it also contains $Q(A)$. This completes the proof. □

22.5.2 Maps of field extensions

There are some important results which allow us to extend a field homomorphism from a smaller field to a bigger field. These come in handy while discussing splitting fields and algebraic closures.

Proposition 22.5.2.1 (Extension-I). *Let $\varphi : F \to F'$ be a field isomorphism. Let $p(x) \in F[x]$ be an irreducible polynomial and let $\varphi(p(x)) \in F'[x]$ be the irreducible polynomial in the image. If α is a root of $p(x)$ and β is a root of $\varphi(p(x))$, then there exists a field isomorphism $\tilde{\varphi} : F(\alpha) \to F'(\beta)$ mapping $\alpha \mapsto \beta$ and extending φ:*

$$\begin{tikzcd}
F(\alpha) \arrow[r, "\tilde{\varphi}", "\cong"'] & F'(\beta) \\
F \arrow[u, hook] \arrow[r, "\cong", "\varphi"'] & F' \arrow[u, hook]
\end{tikzcd} .$$

Proof. Since $F(\alpha) = F[x]/p(x)$ and $F'(\beta) = F'[x]/\varphi(p(x))$, therefore we need only construct an isomorphism between them via φ which takes $\bar{x}$ to $\bar{x}$ (as $\bar{x}$ in $F(\alpha)$ is the root of $p(x)$ in $F(\alpha)$ and similarly for $F(\beta)$).

Indeed, consider the map

$$\begin{aligned} \varphi : F[x] &\to F'[x] \\ x &\mapsto x. \end{aligned}$$

Then, we get $\tilde{\varphi} : \frac{F[x]}{\varphi^{-1}(\varphi(p(x)))} \xrightarrow{\cong} \frac{F'[x]}{\varphi(p(x))}$. This completes the proof. □

Corollary 22.5.2.2. *If $p(x) \in F[x]$ is irreducible and $\alpha \neq \beta$ are two roots, then there is an isomorphism*

$$\begin{aligned} F(\alpha) &\longrightarrow F(\beta) \\ \alpha &\longmapsto \beta \end{aligned}$$

which is id *on F.*

Proof. Use $\varphi = \mathrm{id}_F$ with $F' = F$ on Proposition 22.5.2.1 to get the result. □

We next show that transcendental elements are mapped to transcendental elements under a field homomorphism.

Proposition 22.5.2.3. *Let $\varphi : F \to F'$ be a morphism of fields. If K/F is a field extension, $\psi : K \to F'$ is a morphism extending φ, then the following are equivalent:*

1. *$\alpha \in K$ is transcendental over F,*
2. *$\psi(\alpha) \in F'$ is transcendental over $\varphi(F) \subseteq F'$.*

Proof. The main observation is that for transcendental element $\alpha \in K$ over F, we have that $F[\alpha]$ is isomorphic to polynomial ring $F[x]$. Using this, we consider the restriction $\psi : F(\alpha) \to F'$. Note that $\alpha \in F(\alpha)$ is transcendental over F if and only if $\mathrm{Ker}\,(\psi) = 0$. Further $\psi(\alpha)$ is transcendental over $\psi(F)$ if and only if $\mathrm{Ker}\,(\psi) = 0$. We win. □

22.5.3 Splitting fields & algebraic closure

Given a polynomial, we will now construct the smallest field where that polynomial splits into linear factors. We will then see that splitting fields are exactly what are called normal extensions.

Definition 22.5.3.1 (Splitting field). Let $f(x) \in F$ be a field and $f(x) \in F[x]$ be a polynomial. The splitting field of $f(x)$ over F is the smallest field extension K/F such that $f(x) \in K[x]$ is product of linear factors, that is, K is the smallest field containing all roots of $f(x)$.

Theorem 22.5.3.2. *Splitting field exists.*

Proof. Let $f(x) \in F$ be a field and $f(x) \in F[x]$ be a polynomial. We wish to construct the smallest field K/F containing all roots of F. We induct over $\deg f(x) = n$. If $n = 1$, then $K = F$ will do. Suppose for every polynomial $g(x)$ of degree $n - 1$ or lower has a splitting field, which we denote by K_g/F. Pick $f(x) \in F[x]$ be of degree n. We wish to construct the splitting field of $f(x)$. We have two cases. If $f(x)$ is reducible, then $f(x) = g(x)h(x)$ where $\deg g, \deg h < n$. We thus have splitting fields K_g and K_h for g and h respectively. We claim that $K_g \cdot K_h$ is a splitting field of $f(x)$. Indeed, $K_g \cdot K_h$ contains all roots of $f(x)$ so splitting field is a subfield of $K_g \cdot K_h$. But since splitting field of $f(x)$ also contains roots of $g(x)$ and $h(x)$, it follows that it must contain K_g and K_h and thus $K_g \cdot K_h$ as well. Hence splitting field is exactly $K_g \cdot K_h$.

On the other hand if $f(x)$ is irreducible, then let $K = \frac{F[x]}{\langle f(x) \rangle}$ which is a finite extension of F. Now, K has atleast one root of $f(x)$, namely $\bar{x}$, which we label as $\alpha \in K$. Thus, we have that $f(x) = (x - \alpha)g(x)$ in $K[x]$. Thus $g(x) \in K[x]$ is of degree $n-1$. Hence by inductive hypothesis, there exists a field $L_g/K/F$ such that $g(x)$ splits into linear factor/L_g contains all roots of $g(x)$. Thus $L_g(\alpha)$ contains all roots of $f(x)$. We claim that $L_g(\alpha)$ is contains a splitting field of $f(x)$. Indeed, we may take intersection of all sub-fields of $L_g(\alpha)$ which contains all roots of $f(x)$. Such a collection is non-empty as $L_g(\alpha)$ contains all roots of $f(x)$. As intersection of subfields is a subfield, we win the induction step. □

We now show that splitting fields are unique upto isomorphism.

Proposition 22.5.3.3 (Extension-II)**.** *Let $\varphi : F \to F'$ be a field isomorphism and $f(x) \in F[x]$ be a polynomial. Let $\varphi(f(x)) \in F'[x]$ be the image of $f(x)$ under φ. Then, φ lifts to an isomorphism $\tilde{\varphi} : K \to K'$ where K/F is the splitting field of $f(x)$ and K'/F' is the splitting field of $\varphi(f(x))$:*

$$\begin{tikzcd} K \arrow[r, "\tilde{\varphi}", "\cong"'] & K' \\ F \arrow[u, hook] \arrow[r, "\cong", "\varphi"'] & F' \arrow[u, hook] \end{tikzcd} .$$

Proof. We will induct on degree of $f(x)$. If $\deg f(x) = 1$, then F has the root of f and thus we may take $\tilde{\varphi}$ to be φ itself. Let $\deg f = n$ and suppose that for any polynomial of degree $n-1$ or lower over any extension of F, we have the required map. Let $f(x) = p(x)g(x)$ where $p(x) \in F[x]$ is an irreducible factor of $f(x)$. Thus $\deg p(x) \le n-1$. Now, let α be a root of $p(x)$ and α' be a root of $\varphi(p(x))$. Thus by Extension-I (Proposition 22.5.2.1), it follows that we have an extension $\chi : F(\alpha) \to F'(\alpha')$ which extends φ. Now consider $h(x) = f(x)/x - \alpha$ in $F(\alpha)[x]$. Then, $h(x)$ has degree $n-1$ over $F(\alpha)$, so by inductive hypothesis, we get an extension $\tilde{\varphi} : K_h \to K'_h$ where $K_h/F(\alpha)$ and $K'_h/F'(\alpha')$ are splitting fields of $h(x)$ and $\chi(h(x))$ respectively. We claim that K_h is the splitting field of $f(x)$. Indeed, K_h has all roots of $f(x)$, so it contains the splitting field. But roots of $h(x)$ are just those of $f(x)$ except α, so K_h is the splitting field of $f(x)$. This completes the proof. □

Algebraic closure

We now discuss some basic properties of algebraic closure. Note that there is a subtlety to the definition of an extension being algebraically closed.

Definition 22.5.3.4 (**Agebraically closed fields & extensions**)**.** A field K is algebraically closed if every polynomial in $K[x]$ has a root. An extension K/F is called an algebraically closed extension if K/F is algebraic and K is algebraically closed. In this case, K is called the algebraic closure of F.

Remark 22.5.3.5. The linguistic subtlety here is that $\mathbb{C}/\mathbb{Q}$ is not algebraically closed extension as it is not algebraic. But $\bar{\mathbb{Q}}/\mathbb{Q}$ is an algebraically closed extension.

We will omit the statement that an algebraic closed extension of any field exists as it can be found in any standard book. We however state the following important results about equivalence conditions for a field to be algebraically closed.

Theorem 22.5.3.6. *Let F be a field. Then the following are equivalent:*

1. *F is algebraically closed.*
2. *Only irreducible polynomial in $F[x]$ are linear.*
3. *If K/F is algebraic, then $K = F$.*

Proof. The only non-trivial part is that of 3. $\Rightarrow$ 1. Indeed, pick any $f(x) \in F[x]$. Then, consider the splitting field K/F of $f(x)$. As K/F is finite, therefore K/F is algebraic and thus by hypothesis we have $K = F$. It follows that F has all roots of F, as required. □

22.5.4 Separable, normal extensions & perfect fields

Let us begin with definitions.

Definition 22.5.4.1 (**Separable polynomials & extensions**). A polynomial $f(x) \in F[x]$ is said to be separable if $f(x)$ has no repeated roots. That is, there doesn't exists $\alpha \in \bar{F}$ such that $(x-\alpha)^2 | f(x)$. An extension K/F is said to be separable if it is algebraic and for all $\alpha \in K$, the minimal polynomial $m_{\alpha,F}(x) \in F[x]$ is separable.

Definition 22.5.4.2 (**Normal extensions**). An extension K/F is said to be normal if it is algebraic and for all $\alpha \in K$, the minimal polynomial $m_{\alpha,F}(x) \in F[x]$ has all roots in K and is thus a product of linear factors in $K[x]$.

Remark 22.5.4.3. Note that if K/F is normal, then K contains the splitting field of all $f(x) \in F[x]$. Thus every splitting field of some $f(x) \in F[x]$ is an intermediate extension of K/F.

Definition 22.5.4.4 (**Frobenius & perfect fields**). Let K be a field of characteristic $p > 0$. Then the Frobenius is the field map $\mathrm{Fr} : K \to K$ mapping $x \mapsto x^p$. A field K is perfect if either $\mathrm{char}(K) = 0$ or the Frobenius $\mathrm{Fr} : K \to K$ is an isomorphism.

Our goal is to study two questions. First is to understand the relationship between splitting fields and normal extensions (we will see that they are equivalent). Second is to understand the relationship between separability and the automorphisms of the extension.

Understanding these two problems will give us the tool which will allow us to show when a field extension is separable or normal, which will come in handy while doing Galois theory.

Let us begin by the first question.

Theorem 22.5.4.5. *Let K/F be an extension. The following are equivalent:*
1. *K/F is a splitting field of some $S \subseteq F[x]$.*
2. *K/F is a normal extension.*

We now build towards answering the second question.

Definition 22.5.4.6 (**Separable degree**).

There's a tower law for separable degree as well.

Proposition 22.5.4.7. *Let $L/K/F$ be field extensions and L/F be finite. Then,*

$$[L : F]_s = [L : K]_s \cdot [K : F]_s.$$

The following is an easy lemma.

Lemma 22.5.4.8. *Let K/F be a finite extension. Then*

$$[K : F]_s \leq [K : F].$$

Theorem 22.5.4.9. *Let K/F be a field extension. Then the following are equivalent:*

1. *$[K : F]_s = [K : F]$.*
2. *K/F is a separable extension.*

Using the above theorems, we obtain the following useful criterion usually used in induction steps and allows us to reduce to checking the separability and normality for a single element.

Proposition 22.5.4.10. *Let K/F be a field extension and $\alpha \in K$ be an algebraic element. If the minimal polynomial $m_{\alpha,F}(x) \in F[x]$*

1. *is a separable polynomial, then $F(\alpha)/F$ is a separable extension,*
2. *has all roots in $F(\alpha)$, then $F(\alpha)/F$ is a normal extension.*

Proof. 1. Note that since $m_{\alpha,F}(x)$ is separable, we get

$$[F(\alpha) : F]_s = |S(\mathrm{id}, F(\alpha)/F)| = \#\text{conjugates of } \alpha = \deg m_{\alpha,F}(x) = [F(\alpha) : F].$$

By Theorem 22.5.4.9, we win.

2. We claim that $F(\alpha)/F$ is the splitting field of $m_{\alpha,F}(x)$ in this case. Indeed, $F(\alpha)/F$ is the smallest field containing F and α. By hypothesis, it contains all the roots of $m_{\alpha,F}(x)$, of which α is one. It follows that $F(\alpha)/F$ is the smallest field containing all roots of $m_{\alpha,F}(x)$, as required. □

22.5.5 Cyclotomic extensions

We discuss the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ where ζ_n is an n^{th}-root of unity, that is, a solution of $x^n - 1$ in $\mathbb{C}$. We will see that n^{th}-roots of unity form a cyclic group $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$, therefore we define a *primitive* n^{th} root of unity to be a generator of $\mathbb{Z}/n\mathbb{Z}$. Thus, there are $\varphi(n)$ many primitive n-th roots of unity, where φ is the Euler totient function.

We denote the group of n-th roots of unity as μ_n. Some basic facts about μ_n are as follows.

Lemma 22.5.5.1. *Let $n \in \mathbb{N}$. Then,*

1. *μ_n is a finite cyclic group isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*
2. *If $d|n$, then $\mu_d \hookrightarrow \mu_n$.*

Proof. 1. μ_n is finite of size n since its the set of roots of $x^n - 1$ in $\mathbb{C}$. This is a group since product of any two n-th roots of unity is an n-th root of unity. Thus μ_n is a finite subgroup of the multiplicative group $\mathbb{C}^\times$. It follows that μ_n is cyclic.

2. Consider the map

$$\begin{aligned} \varphi : \mu_d &\longrightarrow \mu_n \\ \zeta &\longmapsto \zeta. \end{aligned}$$

This is well-defined since a d-th root of unity is also an n-th root of unity if $d|n$. Further, this is clearly a group homomorphism. □

Thus $\mu_d \leq \mu_n$ is precisely the subgroup of order d-elements of μ_n.

Definition 22.5.5.2 (**n^{th}-cyclotomic polynomial**)**.** Let $n \in \mathbb{N}$. The n^{th}-cyclotomic polynomial is defined to be the polynomial $\Phi_n(x) = \prod_{\zeta \in \mu_n^\times}(x - \zeta)$, that is, the polynomial whose all roots are the primitive n^{th}-roots of unity.

We immediately have the following observations.

Lemma 22.5.5.3. *Let $\Phi_n(x)$ be the n^{th}-cyclotomic polynomial. Then,*

1. $\Phi_n(x)|x^n - 1$.
2. $x^n - 1 = \prod_{d|n}\Phi_d(x)$.

Proof. Follows from the observation that $x^n - 1 = \prod_{\zeta^n=1}(x - \zeta)$. □

Remark 22.5.5.4. Using Lemma 22.5.5.3, we see that we can calculate $\Phi_n(x)$ recursively by finding Φ_d for all $d|n$ and $d \neq n$. In particular,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d\neq n}\Phi_d(x)}.$$

We now state and prove the following theorem, which in particular tells us that cyclotomic polynomial $\Phi_n(x)$ is monic irreducible of degree $\varphi(n)$. Once shown, we would be able to conclude that the the minimal polynomial of a primite n^{th}-root of unity is $\Phi_n(x)$.

Theorem 22.5.5.5. *Let $n \in \mathbb{N}$. Then,*

1. *$\Phi_n(x)$ is a monic polynomial of degree $\varphi(n)$ in $\mathbb{Z}[x]$.*
2. *$\Phi_n(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$.*
3. *$\Phi_n(x)$ is the minimal polynomial of any primitive n^{th}-root of unity $\zeta_n \in \mathbb{C}$.*
4. *If ζ_n is a primitive n^{th}-root of unity, then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a degree $\varphi(n)$ extension.*

Proof. 1. The fact that degree of $\Phi_n)(x)$ is $\varphi(n)$ follows from the fact that in $\mathbb{C}$ it is a product of $\varphi(n)$ many linear factors. This also shows that $\Phi_n(x)$ is a monic polynomial. We need only show that coefficients lie in $\mathbb{Z}$. To this end, we proceed by induction. For $n = 1$, $\Phi_n(x) = x - 1 \in \mathbb{Z}[x]$. For $n = 2$, $\Phi_2(x) = x + 1 \in \mathbb{Z}[x]$. Now suppose that for all $d < n$ $\Phi_d(x) \in \mathbb{Z}[x]$. Then we have

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d\neq n}\Phi_d(x)},$$

thus $f(x) := \prod_{d|n,d\neq n}\Phi_d(x) \in \mathbb{Z}[x]$ by inductive hypothesis. As $f(x)|x^n - 1$ in $\mathbb{Q}[x]$ and $f(x) \in \mathbb{Z}[x]$, therefore by results surrounding Gauss' lemma, we get $f(x)|x^n - 1$ in $\mathbb{Z}[x]$, that is, $\Phi_n(x) \in \mathbb{Z}[x]$.

2. Let $\Phi_n(x) = f(x)g(x)$ in $\mathbb{Z}[x]$ where we assume that $f(x)$ is an irreducible factor of $\Phi_n(x)$ (by $\mathbb{Z}[x]$ being an UFD). We claim that $f(x)$ has all primitive n^{th}-roots of unity as a root over $\mathbb{C}$, so that $f(x) = \Phi_n(x)$ over $\mathbb{Z}$. Indeed, let $\zeta^a \in \mu_n$ be any other primitive root,

then $(a,n)=1$ and so we may write $a=p_1\dots p_k$ where p_i are primes not dividing n. We wish to show that ζ^a is a root of $f(x)$. It suffices to show that if ζ is a root of $f(x)$, then ζ^p is a root of $f(x)$ as well for any prime p not dividing n. This is what we will show now.

Indeed, let $\zeta\in\mu_n$ a primitive n^{th}-root of unity which is a root of $f(x)$. As $f(x)$ is irreducible over $\mathbb{Z}[x]$, therefore irreducible over $\mathbb{Q}[x]$ as well, hence $f(x)$ is the minimal polynomial of ζ over $\mathbb{Q}$. Consider p a prime not dividing n. We wish to show that ζ^p is also a root of $f(x)$. Indeed, as $\Phi_n(x)$ has ζ^p as a root, therefore either $f(\zeta^p)=0$ or $g(\zeta^p)=0$ over $\mathbb{C}$. Suppose the latter is true. Thus $g(x^p)$ has ζ as a root. As $g(x^p)\in\mathbb{Q}[x]$, therefore $f(x)|g(x^p)$ in $\mathbb{Q}[x]$. As $f(x),g(x^p)\in\mathbb{Z}[x]$, therefore by results surrounding Gauss' lemma, we conclude that $f(x)|g(x^p)$ in $\mathbb{Z}[x]$. Let $g(x^p)=f(x)\cdot h(x)$ where $h(x)\in\mathbb{Z}[x]$. Going modulo p, we get that $\bar{g}(x^p)=(\bar{g}(x))^p$. Thus, $(\bar{g}(x))^p=\bar{f}(x)\bar{h}(x)$ in $\mathbb{F}_p[x]$. Thus, $\bar{g}$ and $\bar{f}$ have a common factor in $\mathbb{F}_p[x]$ as both have ζ as a root. Thus, $\bar{\Phi}_n(x)=\bar{f}(x)\bar{g}(x)$ has a repeated factor, thus, $\Phi_n(x)$ is not separable over over $\mathbb{F}_p$. But since $\Phi_n'(x)=nx^{n-1}\neq 0$ has only $x=0$ as a root, therefore $\Phi_n(x)$ is separable. It follows that we have a contradiction to the separability of x^n-1 as $\Phi_n(x)$ is a factor of x^n-1, thus ζ^p cannot be a root of $g(x)$, as required.

3. As $\Phi_n(\zeta_n)=0$ for any primitive n^{th}-root of unity, therefore we get that $m_{\zeta_n,\mathbb{Q}}|\Phi_n(x)$. As $m_{\zeta_n,\mathbb{Q}}$ is irreducible and so is $\Phi_n(x)$, thus $m_{\zeta_n,\mathbb{Q}}=\Phi_n$, as required.

4. As $\Phi_n(x)$ is the minimal polynomial of ζ_n which has degree $\varphi(n)$, the result follows. □

22.5.6 Galois extensions

For simplicity, let us only work with finite Galois extensions.

Definition 22.5.6.1 (**Galois extensions & Galois group**)**.** An extension K/F is Galois if it is finite, separable and normal. That is, for all $\alpha\in K$, the minimal polynomial $m_{\alpha,F}(x)\in F[x]$ has all roots in K and each of them is distinct. The Galois group of a Galois extension K/F, denoted $\mathrm{Gal}\,(K/F)$, is defined to be the automorphism group $\mathrm{Aut}\,(K/F)$.

Let us first see that every splitting field of a separable polynomial is a Galois extension over the base.

Proposition 22.5.6.2. *Let F be a field and $f(x)\in F[x]$ be a separable polynomial. Let K/F be the splitting field of $f(x)$ over F. Then K/F is a Galois extension and* $\mathrm{Gal}\,(K/F)$ *is called the Galois group of the polynomial $f(x)$.*

Proof. We first establish that K/F is Galois. Indeed K/F is finite as it is a splitting field of a polynomial. As it is a splitting field, so it is normal (Theorem 22.5.4.5). To show separability, it suffices to show that the separable degree $[K:F]_s=[K:F]$ (Theorem 22.5.4.9). To this end, we first have $K=F(\alpha_1,\dots,\alpha_n)$ for $\alpha_i\in K$ elements algebraic over F. Consequently, by the tower law for separable degree (Proposition 22.5.4.7), we obtain

$$[K:F]_s=[K:F(\alpha_1,\dots,\alpha_{n-1})]_s\cdot\dots\cdot[F(\alpha_1,\alpha_2):F(\alpha_1)]_s\cdot[F(\alpha_1):F]_s.$$

By Proposition 22.5.4.10, it suffices to show that $m_{\alpha_i,F(\alpha_1,\ldots,\alpha_{i-1})}(x) \in F(\alpha_1,\ldots,\alpha_{i-1})[x]$ is a separable polynomial for each i. Indeed, since $f(\alpha_i) = 0$, thus $m_{\alpha_i,F(\alpha_1,\ldots,\alpha_{i-1})}(x) | f(x)$ in $F(\alpha_1,\ldots,\alpha_{i-1})[x]$. As $f(x)$ is separable, and $\overline{F(\alpha_1,\ldots,\alpha_{i-1})} = \overline{F}$, it follows that $m_{\alpha_i,F(\alpha_1,\ldots,\alpha_{i-1})}(x)$ is separable, as required. □

Théorème fondamental de la théorie de Galois

Theorem 22.5.6.3 (Fundamental theorem)**.** *Let K/F be a Galois extension with Galois group G. Then the maps*

$$\begin{tikzcd}
\{L \mid K/L/F \text{ is an intermediate extension}\} \arrow[d, shift left=2ex, "\mathrm{Gal}(K/-)"] \\
\{H \mid H \leq G \text{ is a subgroup}\} \arrow[u, shift left=2ex, "K^{(-)}"]
\end{tikzcd}$$

establish a bijection. Moreover, we have the following:

1. *For any intermediate $K/L/F$, the extension K/L is a Galois extension.*
2. *Both the maps above are antitone, i.e. they reverse the order.*
3. *For any intermediate extension $K/L/F$, the following are equivalent:*
   (a) *L/F is a Galois extension.*
   (b) *$\mathrm{Gal}\,(K/L)$ is a normal subgroup of G and in this case,*

$$\mathrm{Gal}\,(L/F) \cong \frac{G}{\mathrm{Gal}\,(K/L)}.$$

4. *For any two intermediate extensions $K/L_1, L_2/F$ with $H_i = \mathrm{Gal}\,(()\,K/L_i)$, we have*
   (a) *$\mathrm{Gal}\,(K/L_1 \cdot L_2) = H_1 \cap H_2$ in G,*
   (b) *$\mathrm{Gal}\,(K/L_1 \cap L_2) = \langle H_1, H_2 \rangle$ in G.*

22.5.7 Transcendence degree

Definition 22.5.7.1. (**Transcendence**) Let K/k be a field extension.

1. A collection of elements $\{\alpha_i\}_{i\in I}$ of K is said to be *algebraically independent* if the map

$$\begin{aligned} k[x_i \mid i \in I] &\longrightarrow K \\ x_i &\longmapsto \alpha_i \end{aligned}$$

   is injective.
2. A *transcendence basis* of K/k is defined to be an algebraically independent set $\{\alpha_i \mid i \in I\}$ of K/k such that $K/k(\alpha_i \mid i \in I)$ is an algebraic extension.
3. The extension K/k is said to be *purely transcendental* if $K \cong k(x_i \mid i \in I)$ for some indexing set I.

Lemma 22.5.7.2. *Let K/k be a field extension. Then, $\{\alpha_i\}_{i\in I}$ is a transcendence basis of K/k if and only if $\{\alpha_i\}_{i\in I}$ is a maximal algebraically independent set of K/k.*

Proof. (L $\Rightarrow$ R) If $\{\alpha_i\}_{i\in I}$ is not maximal, then there exists $S \subset K$ containing $\{\alpha_i\}_{i\in I}$ such that S is algebraically independent. Let $\beta \in S \setminus \{\alpha_i\}_{i\in I}$. But since $K/k(\{\alpha_i\}_{i\in I})$ is an algebraic extension and $\beta \notin k(\{\alpha_i\}_{i\in I})$ by algebraic independence of S, therefore we have a contradiction to algebraic nature of the extension $K/k(\{\alpha_i\}_{i\in I})$.
(R $\Rightarrow$ L) Suppose $K/k(\{\alpha_i\}_{i\in I})$ is not algebraic. Then there exists $\beta \in K$ which is transcendental over $k(\{\alpha_i\}_{i\in I})$. Thus the set $\{\alpha_i\}_{i\in I} \cup \{\beta\}$ is a larger algebraically independent set, contradicting the maximality. □

Lemma 22.5.7.3. *Let K/k be a field extension. Then any two transcendence basis have the same cardinality.*

Proof. See Tag 030F of cite[Stacksproject]. □

Definition 22.5.7.4. (**Transcendence degree**) Let K/k be a field extension. The cardinality of any transcendence basis is said to be the transcendence degree, denoted trdeg K/k. Furthermore, if A is a domain containing k, then we define trdeg A/k to be the transcendence degree of A_0, the field of fractions of A, over k.

Remark 22.5.7.5. Let K/k be a field extension. If trdeg $K/k = 1$, then there exists $\alpha \in K$ such that α is not an algebraic element over k but $K/k(\alpha)$ is algebraic. In particular, for any transcendental element $\alpha \in K$ over k, the set $\{\alpha\}$ is algebraically independent over k. Precisely, there is a one-to-one bijection between the set of all singletons which are algebraically independent and all transcendental elements of K/k.

Example 22.5.7.6. There are some basic examples which reader might have encountered. For example, one knows that $\mathbb{Q}(\pi)/\mathbb{Q}$ is transcendental as $\pi \in \mathbb{Q}(\pi)$ is not algebraic over $\mathbb{Q}$. Consequently, trdeg $\mathbb{Q}(\pi)/\mathbb{Q}$ is 1, as $\mathbb{Q}(\pi)/\mathbb{Q}(\pi)$ is algebraic.

For another example, consider the next obvious situation of $\mathbb{Q}(e, \pi)/\mathbb{Q}$. Since $\{e\}$ and $\{\pi\}$ are algebraically independent sets over $\mathbb{Q}$, therefore trdeg in this case is ≥ 1. But it is an unknown problem whether $\{e, \pi\}$ forms an algebraically independent set over $\mathbb{Q}$(!) Consequently, if they do, then trdeg $\mathbb{Q}(e, \pi)/\mathbb{Q} = 2$ and if they don't, then the best we can say is trdeg $\mathbb{Q}(e, \pi)/\mathbb{Q} \geq 1$.

Example 22.5.7.7. We have trdeg $k(x_1, \dots, x_n)/k = n$ as $\{x_1, \dots, x_n\}$ forms a maximal algebraically independent set.

We observe some basic first properties of transcendence degree.

Lemma 22.5.7.8. *Let $A = k[\alpha_1, \dots, \alpha_n]$ be an integral domain where $\alpha_i \in K$ for some field extension K/k. If* trdeg $A/k = r > 0$*, then there exists $\alpha_{i_1}, \dots, \alpha_{i_r}$ which are transcendental over k.*

22.6 Integral dependence and normal domains

The main topic of interest of study in this section is the following question: "*let R be a ring and S be an R-algebra. How do all those elements of S behave like which satisfy a polynomial with coefficients in R?*".

22.6.1 Definitions and basic theory

In order to investigate this further, let us bring some definitions.

Definition 22.6.1.1. (**Integral elements and integral algebra**) Let R be a ring and S be an R-algebra. An element $s \in S$ for which there exists $p(x) \in R[x]$ such that $p(s) = 0$ in S is said to be an *integral element* over R. Further, S is said to be *integral over R* if every element of S is integral over R.

To begin deriving properties, we would need a fundamental result about endomorphisms of finitely generated modules.

Theorem 22.6.1.2. *(Cayley-Hamilton theorem) Let R be a ring, M be a finitely generated R-module generated by n elements and $I \leq R$ be an ideal. If $\varphi : M \to M$ is an R-linear map such that*

$$\varphi(M) \subseteq IM,$$

then there exists a monic polynomial

$$p(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$$

in $R[x]$ such that $p(\varphi) = 0$ in $\operatorname{Hom}_R(M, M)$ and $a_k \in I^k$ for $k = 1, \ldots, n$.

Proof. See Theorem 4.3, pp 120, [cite Eisenbud]. □

There are two immediate corollaries of Cayley-Hamilton which will remind the reader of finite-dimensional vector space case.

Corollary 22.6.1.3. *Let R be a ring and M be a finitely generated R-module. If $\phi : M \to M$ is a surjective R-module homomorphism, then ϕ is an isomorphism.*

Proof. Using ϕ, we may regard M as an $R[z]$-module. Note that M is a finitely generated $R[z]$-module. Let $I = \langle z \rangle \leq R[z]$. Since the action of z on M is by ϕ and ϕ is surjective, therefore $IM = M$. We may use Cayley-Hamilton with $\varphi = \text{id}$ to deduce that there is a polynomial $p(x, z) \in R[x, z]$ such that $p(z, \text{id}) = 0$ and $p(x, z)$ is a monic polynomial in $R[z][x]$. Consequently, we can write $0 = p(z, \text{id}) = 1 + q(z)z$ for some $q(z) \in R[z]$. It follows that $-q(z)$ is the inverse of z in $R[z]$. Since $z \in R[z]$ denotes the endomorphism ϕ, so we have found an R-linear inverse of ϕ, namely the one corresponding to $-q(z)$, as required. □

Corollary 22.6.1.4. *Let R be a ring and M be a finitely generated R-module. If $M \cong R^n$, then any generating set of n elements of M is linearly independent. In particular, any generating set of n elements of M is a basis.*

Proof. Denote $f : M \to R^n$ to be the given isomorphism. Pick $S = \{s_1, \dots, s_n\}$ to be a generating set of M. This yields a surjection $g : R^n \to M$. We wish to show that g is an isomorphim. Observe that $gf : M \to M$ is surjective. It follows from Corollary 22.6.1.3 that gf is an isomorphism. Since f is an isomorphism, hence it follows that g is an isomorphism, as required. □

The fundamental result which drives the basic results about integral algebras is the following equivalence.

Proposition 22.6.1.5. *Let $R \to S$ be an R-algebra and $s \in S$. Then the following are equivalent.*

1. *$s \in S$ is integral over R.*
2. *$R[s] \subseteq S$ is a finite R-algebra.*
3. *$R[s] \subseteq S$ is contained in a finite R-algebra.*
4. *There is a faithful $R[s]$-module M which when restricted to R is finitely generated as an R-module.*

Proof. $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4$ follows at once. We do $4 \Rightarrow 1$. Indeed, let $I = \langle s \rangle \leq R[s]$ be the ideal generated by $s \in R[s]$. Consequently, s induces an endomorphism $m_s : M \to M$ by scalar multiplication. Observe that $m_s(M) = IM$. It follows by Cayley-Hamilton (Theorem 22.6.1.2) that there exists a monic $p(x) \in R[s][x]$ such that $p(m_s) = 0$ as an $R[s]$-linear map $M \to M$. Consequently, for any $a \in M$, we have $p(m_s)(a) = 0$, where upon expanding one sees that $p(m_s) = m_{q(s)}$ for some $q(s) \in R$, $q(x) \in R[x]$. But since M is faithful, therefore $q(s) = 0$, as required. □

Lemma 22.6.1.6. *Let $R \to S$ be an R-algebra and $s_1, \dots, s_n \in S$ be integral over R. Then $R[s_1, \dots, s_n]$ is a finite R-algebra.*

Proof. We proceed by induction over n. Base case follows from Proposition 22.6.1.5. Assume that $R_k = R[s_1, \dots, s_k]$ is a finite R-algebra. Since $s_{k+1} \in S$ is integral over R, therefore it is integral over R_k. It follows from Proposition 22.6.1.5 that $R_k[s_{k+1}]$ is a finite R_k-algebra. Since R_k is a finite R-algebra, therefore $R_k[s_{k+1}] = R[s_1, \dots, s_{k+1}]$ is a finite R-algebra, as required. □

One then obtains that finite generation of an algebra by integral elements as an algebra is equivalent to finite generation as an R-module.

Lemma 22.6.1.7. *Any finite R-algebra is integral over R.*

Proof. Let S be a finite R-algebra and let $s \in S$ be an element. Let $m_s : S \to S$ be the R-linear given by multiplication by s. As S is a finitely generated R-module, then by Cayley-Hamilton (Theorem 22.6.1.2), it follows that there is a monic $p(x) \in R[x]$ such that $p(m_s) = 0$ as an R-linear map. Applying $p(m_s)$ to $1 \in S$ yields $p(s) = 0$, as required. □

Proposition 22.6.1.8. *Let R be a ring and S be an R-algebra. Then the following are equivalent.*

1. *S is a finite R-algebra.*
2. *$S = R[s_1, \dots, s_n]$ where $s_1, \dots, s_n \in S$ are integral over R. In particular, S is integral over R.*

That is, an R-algebra is finite if and only if it is a finite type and integral R-algebra.

Proof. Observe that 2. $\Rightarrow$ 1. is just Lemma 22.6.1.6. For 1. $\Rightarrow$ 2. proceed as follows. By Lemma 22.6.1.7, it follows that S is integral over R. Let $s_1, \dots, s_n \in S$ be a generating set of S as an R-module. It is now clear that $R[s_1, \dots, s_n] = S$ as S is finitely generated. □

The following result show that all integral elements form a subring of S.

Proposition 22.6.1.9. *Let R be a ring and S be an R-algebra. The set of all elements of S integral over R forms a subalgebra of S, called the integral closure of R in S.*

Proof. Let $s, t \in S$ be integral over R. Then $R[s,t]$ is a subalgebra of S. It suffices to show that every element of $R[s,t]$ is integral over R. By Proposition 22.6.1.8, the algebra $R[s,t]$ is integral over R as it is finite by Lemma 22.6.1.6. □

With this, a natural situation is when every element of S is integral over R.

Definition 22.6.1.10. (**Normalization & integral extension**) Let R be a ring and S be an R-algebra. The subalgebra A of all integral elements of S over R is said to be the *integral closure of S over R*. One also calls A the *normalization of R in S*. If S is fraction field of R, then A is also denoted by $\tilde{R}$. Further, if $R \hookrightarrow S$ is a ring extension and every element of S is integral over R, then S is said to be an integral extension of R. If $f : R \to S$ is an integral R-algebra, then the map f is said to be *integral*.

Composition of integral maps is integral.

Lemma 22.6.1.11. *Let $R \to S$ and $S \to T$ be integral maps. Then the composite $R \to S \to T$ is integral.*

Proof. Pick any element $t \in T$. We wish to show that $R[t]$ is contained in a finite R-algebra by Proposition 22.6.1.5. As $S \to T$ is integral, there exists $p(x) \in S[x]$ monic such that $p(t) = 0$. So we have

$$t^n + s_{n-1}t^{n-1} + \cdots + s_1 t + s_0 = 0$$

in T where $s_i \in S$. Let $S' = R[s_0, \dots, s_{n-1}]$. As $R \to S$ is integral, therefore S' is a finite R-algebra by Lemma 22.6.1.6. Note that $R \subseteq S'$. By the above equation, it then follows that $S'[t]$ is a finite S'-algebra. As composition of finite maps is finite, therefore $S'[t]$ is a finite R-algebra containing $R[t]$, as required. □

Another trivial observation is that a map which factors an integral map becomes integral.

Lemma 22.6.1.12. *Let $A \to C$ be an integral map. If there is a map $A \to B$ such that*

$$\begin{tikzcd} A \arrow[r] \arrow[d] & C \\ B \arrow[ur] & \end{tikzcd}$$

commutes, then $B \to C$ is an integral map.

Proof. Pick any element $c \in C$. There exists non-zero monic $p(x) \in A[x]$ such that $p(x)$ is non-zero in $C[x]$ and $p(c) = 0$ in C. Observe that $p(x) \in B[x]$ is also a non-zero monic as if not then $p(x)$ would be zero in $C[x]$ because the above triangle commutes. The result then follows. □

The following observation is simple to see, but comes in very handy while handling intermediate rings that pop-up while subsequent localizations.

Lemma 22.6.1.13. *Let k be a field and A be an integral k-algebra. Then A is a field.*

Proof. Pick any element $a \in A$. By integrality, there exists $c_i \in k$ such that

$$a^n + c_{n-1}a^{n-1} + \cdots + c_1 a + c_0 = 0$$

in A. Consider this equation in the fraction field $Q(A)$ to multiply by a^{-1}, so that we may get

$$a^{n-1} + c_{n-1}a^{n-2} + \cdots + c_2 a + c_1 + c_0 a^{-1} = 0$$

in $Q(A)$. It thus follows that a^{-1} is a polynomial in A with coefficients in k, that is, $a^{-1} \in A$, as required. □

22.6.2 Normalization & normal domains

A special situation in Definition 22.6.1.10 is when R is a domain and S is its fraction field. These domains will play a crucial role later on, especially in arithmetic.

Definition 22.6.2.1. (**Normal domain**) Let R be a domain and S be its fraction field. If the normalization of R in S is R itself, then R is said to be a normal domain.

Example 22.6.2.2. Let R be a domain, K its fraction field and $\tilde{R}$ be the normalization of R in K. It follows that $\tilde{R} \hookrightarrow K$ is a normal domain. Indeed, let $\hat{R}$ be normalization of $\tilde{R}$ in K. Then, we have maps

$$R \hookrightarrow \tilde{R} \hookrightarrow \hat{R}$$

where both inclusions are integral maps by construction. It follows from Lemma 22.6.1.11 that the inclusion $R \hookrightarrow \hat{R}$ is integral, forcing $\hat{R} \subseteq \tilde{R}$ which further implies $\tilde{R} = \hat{R}$.

Further investigation into normal domains lets us identify all UFDs as normal domains.

Proposition 22.6.2.3. *All unique factorization domains are normal domains.*

Proof. Let R be a UFD and K be its fraction field. Let $\frac{a}{b} \in K$ with $\gcd(a, b) = 1$. Suppose $\frac{a}{b}$ is integral over R so that there exists $p(x) = x^n + c_{n-1}x^{n-1} + \ldots c_1 x + c_0 \in R[x]$ such that $p(a/b) = 0$. It follows by rearrangement that

$$a^n + c_{n-1}ba^{n-1} + \ldots c_1 b^{n-1} + c_0 b^n = 0.$$

Hence, $b|a^n$. As $\gcd(a, b) = 1$, hence we deduce thay $b|a$, a contradiction. □

Example 22.6.2.4. Consequently, $\mathbb{Z}$ and $\mathbb{Z}[x_1, \dots, x_n]$ are normal as well. Moreover, as Gauss' lemma states that R is UFD if and only if $R[x]$ is UFD, therefore we deduce that $R[x_1, \dots, x_n]$ is a normal domain if R is UFD.

We have something similar to Gauss' lemma for normal domains.

Proposition 22.6.2.5. *A ring R is normal if and only if $R[x]$ is normal.*

Proof. **TODO.** □

Further, we can obtain a generalization of the fact that a monic irreducible in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$.

Proposition 22.6.2.6. *Let $R \hookrightarrow S$ be a ring extension and let $f \in R[x]$ be a monic polynomial. If $f = gh$ in $S[x]$ where g and h are monic, then the coefficients of g and h are integral over R.*

We also obtain that any monic irreducible in the polynomial ring in one variable over a normal domain is prime.

Lemma 22.6.2.7. *Let R be a ring and $f(x) \in R[x]$ be a monic irreducible. If R is a normal domain, then $f(x)$ is a prime element.*

Thus, for normal domains R, monic irreducible and monic prime polynomials are equivalent concepts.

We now show that normalization is a very hereditary process as it preserves many properties of the original ring. Indeed, we first show that normalization and localization commutes.

Proposition 22.6.2.8. *Let $f : R \to S$ be an R-algebra and $M \subseteq R$ be a multiplicative set. If $A \subseteq S$ is the integral closure of R in S, then $M^{-1}A$ is the integral closure of $M^{-1}R$ in $M^{-1}S$.*

Proof. We may assume that f is inclusion of a subring of S by replacing R by $f(R)$ and M by $f(M)$. Consequently, we have inclusions $R \hookrightarrow A \hookrightarrow S$ which induces inclusions $M^{-1}R \hookrightarrow M^{-1}A \hookrightarrow M^{-1}S$. We wish to show that $M^{-1}A$ is the integral closure of $M^{-1}R$ in $M^{-1}S$. Pick an element $s/m \in M^{-1}S$ where $m \in M$ which is integral over $M^{-1}R$. Consequently, there exists $r_i/m_i \in M^{-1}R$ for $0 \leq i \leq k-1$ such that

$$\left(\frac{s}{m}\right)^k + \frac{r_{k-1}}{m_{k-1}}\left(\frac{s}{m}\right)^{k-1} + \dots \frac{r_1}{s_1}\left(\frac{s}{m}\right) + \frac{r_0}{m_0} = 0$$

in $M^{-1}S$. Multiplying by product of denominators and absorbing coefficients into r_i, we get

$$m's^k + r_{k-1}s^{k-1} + \dots + r_1 s + r_0 = 0$$

which we may multiply by $(m')^{k-1}$ to get

$$(m's)^k + r_{k-1}(m's)^{k-1} + \dots + r_1(m')^{k-2}(m's) + r_0(m')^{k-1} = 0.$$

It follows that $m's \in A$, thus $s/1 \in M^{-1}A$ and thus $s/m \in M^{-1}A$.

Conversely, pick an element $a/m \in M^{-1}A$. We wish to show that it is integral over $M^{-1}R$. As $a \in A$, therefore we have

$$a^n + r_{n-1}a^{n-1} + \dots a_1 r + a_0 = 0$$

for $r_i \in R$. This equation in $M^{-1}S$ can be divided by m^n to obtain

$$\left(\frac{a}{m}\right)^n + \frac{r_{n-1}}{m}\left(\frac{a}{m}\right)^{n-1} + \dots + \frac{r_1}{m^{n-1}}\left(\frac{a}{m}\right) + \frac{r_0}{m^n} = 0.$$

It follows that a/m is integral over $M^{-1}R$, as required. □

An immediate, but important corollary of the above is the following.

Corollary 22.6.2.9. *Let A be a domain, K be its fraction field and $\tilde{A}$ be its normalization. Then, for all $g \in A$, we have $\tilde{A}_g = \widetilde{A_g}$ in K.* □

Another important corollary is that being a normal domain is alocal property.

Proposition 22.6.2.10. *Let R be a domain. Then the following are equivalent:*

1. *R is a normal domain.*
2. *$R_{\mathfrak{p}}$ is a normal domain for each prime $\mathfrak{p} \in \operatorname{Spec}(R)$.*
3. *$R_{\mathfrak{m}}$ is a normal domain for each maximal $\mathfrak{m} \in \operatorname{Spec}(R)$.*

Proof. By Proposition 22.6.2.8, we immediately have that (1. $\Rightarrow$ 2.) and (1. $\Rightarrow$ 3.). The (2. $\Rightarrow$ 3.) is immediate. We thus show (3. $\Rightarrow$ 1.). Let K be the fraction field of R. Observe that each $R_{\mathfrak{m}}$ is a domain and have fraction field K again, where $\mathfrak{m} \in \operatorname{Spec}(R)$ is a maximal ideal. Thus we have $R \hookrightarrow R_{\mathfrak{m}} \hookrightarrow K$. Pick $x \in K$ which satisfies a monic polynomial over R. It follows that x satisifes a monic polynomial over $R_{\mathfrak{m}}$ for each maximal $\mathfrak{m} \in \operatorname{Spec}(R)$. Thus $x \in R_{\mathfrak{m}}$ for each $\mathfrak{m}$ as $R_{\mathfrak{m}}$ is a normal domain. We thus deduce from Lemma 22.1.2.12 that $x \in \bigcap_{\mathfrak{m} \neq R} R_{\mathfrak{m}} = R$, as required. □

Remark 22.6.2.11 (*Normalization is a strongly local construction*)**.** Let A be an arbitrary domain. Then we get an inclusion $\varphi_A : A \hookrightarrow \tilde{A}$ where $\tilde{A}$ is the normalization of A in its fraction field. We claim that the collection of maps $\{\varphi_A : A \hookrightarrow \tilde{A}\}$ one for each domain is a construction which is strongly local on domains (see Definitions 1.6.2.3 & 1.6.2.4).

Indeed, first $\{\varphi_A : A \hookrightarrow \tilde{A}\}$ is a construction on domains as if $\eta : A \to B$ is an isomorphism, then we have an isomorphism $\tilde{\eta} : \tilde{A} \to \tilde{B}$ given as follows: we have an isomorphism $\bar{\eta} : K_A \to K_B$ between their fraction fields, given by $a/a' \mapsto \eta(a)/\eta(b)$. Now $a/a' \in K_A$ is integral over A if and only if $\eta(a)/\eta(a') \in K_B$ is integral over B. This shows that $\bar{\eta} : K_A \to K_B$ restricts to an isomorphism $\tilde{\eta} : \tilde{A} \to \tilde{B}$. Moreover, if $\eta : A \to A$ is id, then so is $\tilde{\eta}$ and it satisfies the square and cocycle condition as well of Definition 1.6.2.3. We now claim that normalization is strongly local.

Indeed, pick $g \in A$ non-zero. Then, the localization of the inclusion $\varphi_A : A \hookrightarrow \tilde{A}$ at element g yields $(\varphi_A)_g : A_g \hookrightarrow \tilde{A}_g = \widetilde{A_g}$ which is equal to the normalization of the domain $\varphi_{A_g} : A_g \hookrightarrow \widetilde{A_g}$. It follows that any integral scheme X admits a *normalization* in light of Theorem 1.6.2.10. Indeed, this is what is the content of Theorem 1.6.6.3.

We have a universal property for normalization of domains.

Proposition 22.6.2.12. *Let A be a domain and $\tilde{A}$ be the normalization of A in its fraction field. Then for any normal domain B and an injective map $A \hookrightarrow B$, there exists a unique map $\tilde{A} \to B$ such that following commutes:*

$$\begin{tikzcd}
\tilde{A} \arrow[r, dashed] & B \\
A \arrow[u, hook] \arrow[ur, hook] &
\end{tikzcd}.$$

Proof. Let $f : A \hookrightarrow B$. This, by universal property of fraction fields, induces a unique injective map $\varphi : K \hookrightarrow L$ from fraction field of A to that of B such that $\varphi|_A = f$. Let $x \in \tilde{A}$. Then

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

holds in K where $a_i \in A$. Applying φ on the above equation yields

$$\varphi(x)^n + f(a_{n-1})\varphi(x)^{n-1} + \cdots + f(a_1)\varphi(x) + f(a_0) = 0$$

in L. It follows that $\varphi(x)$ is an integral element of L over B. As B is normal it follows that $\varphi(x) \in B$. Consequently, we have a unique map

$$\varphi|_{\tilde{A}} : \tilde{A} \to B$$

such that the triangle commutes, as required. □

In certain situations (especially those arising in geometry and arithmetic), normalization preserves noetherian property. **TODO.**

22.6.3 Noether normalization lemma

Finally, as a big use of normalization in geometry, we obtain the following famous result.

Theorem 22.6.3.1. [6] *Let k be a field and A be a finite type k-algebra. Then, there exists elements $y_1, \dots, y_r \in A$ algebraically independent over k such that the inclusion $k[y_1, \dots, y_r] \hookrightarrow A$ is an integral map.*

Proof. Let us assume that k is infinite. Let $x_1, \dots, x_n \in A$ be generators of A as a k-algebra. Suppose there is no algebraically independent subset of $\{x_1, \dots, x_n\}$. Thus, each $x_1, \dots, x_n$ is integral over k. As $A = k[x_1, \dots, x_n]$, therefore by Proposition 22.6.1.8 it follows that A is integral over k, so there is nothing to show here.

Consequently, we may assume that there is a largest algebraically independent subset of $\{x_1, \dots, x_n\}$, denoted $\{x_1, \dots, x_r\}$. It follows that each $x_{r+1}, \dots x_n$ is integral/algebraic over k. If $r = n$, then A is the affine n-ring over k, so there is nothing to show. Consequently, we may assume that $n > r$. We now proceed by induction over n.

In the base case, we have $n = 1$, and thus $r < 1$. It follows that $A = k[x]$ where $x \in A$

[6] Exercise 5.16 of AMD.

is algebraically dependent over k, that is, x is integral over k. Consequently, A is integral over k by Lemma 22.6.1.6 and there is nothing to show. We now do the inductive case.

Assume that every finite type k-algebra $B \subseteq A$ with $n-1$ generators have elements $\{y_1, \dots, y_m\} \subseteq B$ algebraically independent over k such that B is integral over $k[y_1, \dots, y_m]$. Denote $A_{n-1} = k[x_1, \dots, x_{n-1}] \subseteq A$. It now suffices to find a finite type k-algebra $B \subseteq A$ generated by $n-1$ elements not containing x_n such that the following two statements hold about B:

1. $x_n \in A$ is integral over B,
2. $B[x_n] = A$.

For if such a B exists, then we have integral maps $k[y_1, \dots, y_m] \hookrightarrow B$ and $B \hookrightarrow B[x_n] = A$ (Proposition 22.6.1.5). Then, by Lemma 22.6.1.11, it follows that $k[y_1, \dots, y_m] \hookrightarrow A$ is integral, as needed.

Indeed, first observe that since x_n is algebraic over k and $k \subseteq A_{n-1}$, therefore x_n is algebraic over A_{n-1}. Consequently, there is a polynomial $f(z_1, \dots, z_{n-1}, z_n) \in k[z_1, \dots, z_n]$ of total degree N such that $f(x_1, \dots, x_{n-1}, x_n) = 0$. Using this, we now construct the required algebra B as follows. Let F be the highest degree homogeneous part of f and denote it by

$$F(z_1, \dots, z_n) = \sum_{i_1 + \dots + i_n = N} c_{i_1 \dots i_n} z_1^{i_1} \dots z_n^{i_n}$$

where $c_{i_1 \dots i_n}$ and is 0 for those indices which are not present in F and is 1 for those which are present. Let $(\lambda_1, \dots, \lambda_{n-1}) \in k^{n-1}$ be a tuple such that $F(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$. Such a tuple exists because the field is infinite (n might be arbitrarily large). Consequently, for each $0 \leq i \leq n-1$, consider the following elements of A:

$$x_i' = x_i - \lambda_i x_n.$$

Let $B = k[x_1', \dots, x_{n-1}'] \subseteq A$. We now show that above two hypotheses are satisfied by B. This will conclude the proof. First, we immediately have the second hypothesis as $B[x_n] = k[x_1', \dots, x_{n-1}', x_n] = k[x_1, \dots, x_n] = A$. We thus need only show that x_n is integral over B. This also follows by the way of construction of B; consider the polynomial

$$g(z_1, \dots, z_{n-1}, z_n) := f(z_1 + \lambda_1 z_n, \dots, z_{n-1} + \lambda_{n-1} z_n, z_n)$$

in $k[z_1, \dots, z_{n-1}, z_n]$. We wish to show the following two items

1. $g(z_1, \dots, z_{n-1}, z_n)$ is monic in z_n,
2. $g(x_1', \dots, x_{n-1}', x_n) = 0$.

This would suffice as a polynomial in $B[z_n]$ is just a polynomial in $k[x_1', \dots, x_{n-1}', z_n]$.

Indeed, we see that

$$\begin{aligned}
g(z_1,\dots,z_{n-1},z_n) &= f(z_1+\lambda_1 z_n,\dots,z_{n-1}+\lambda_{n-1}z_n,z_n)\\
&= F(z_1+\lambda_1 z_n,\dots,z_{n-1}+\lambda_{n-1}z_n,z_n)+\cdots\\
&= \sum_{i_1+\cdots+i_n=N} c_{i_1\dots i_n}(z_1+\lambda_1 z_n)^{i_1}\dots(z_{n-1}+\lambda_{n-1}z_n)^{i_{n-1}}z_n^{i_n}+\cdots\\
&= \left(\sum_{i_1+\cdots+i_n=N} c_{i_1\dots i_n}\lambda_1^{i_1}z_n^{i_1}\dots\lambda_{n-1}^{i_{n-1}}z_n^{i_{n-1}}z_n^{i_n}\right)+\dots\\
&= z_n^N\left(\sum_{i_1+\cdots+i_n=N} c_{i_1\dots i_n}\lambda_1^{i_1}\dots\lambda_{n-1}^{i_{n-1}}\right)+\cdots\\
&= z_n^N F(\lambda_1,\dots,\lambda_{n-1},1)+\cdots .
\end{aligned}$$

It follows that g is monic in z_n and $g(x'_1,\dots,x'_{n-1},x_n)=f(x_1,\dots,x_{n-1},x_n)=0$. This completes the proof. □

22.6.4 Dimension of integral algebras

We will cover Cohen-Seidenberg theorems about primes in an integral extension. The main theorem will allow us to deduce that, apart from other things, dimension of an integral R-algebra is equal to that of R.

22.7 Dimension theory

We will discuss the notion of dimension of rings and how that notion corresponds to dimension of the corresponding affine scheme. Further, the notion of dimension applied to algebraic geometry will garnish us with a concrete geometric intuition to situations which otherwise may feel completely sterile.

22.7.1 Dimension, height & coheight

As usual, all rings are commutative with 1.

Definition 22.7.1.1. (**Dimension of a ring**) Let R be a ring. Then $\dim R$ is defined as follows

$$\dim R := \sup_r \{\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_r \mid \mathfrak{p}_i \text{ are prime ideals of } R\}.$$

Definition 22.7.1.2. (**Height/coheight of a prime ideal**) Let R be a ring and $\mathfrak{p} \lneq R$ be a prime ideal. Then height of $\mathfrak{p}$ is defined as follows:

$$\text{ht } \mathfrak{p} := \sup_r \{\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_r \mid \mathfrak{p}_i \text{ are prime ideals of } R\}.$$

Similarly, the coheight of $\mathfrak{p}$ is defined by

$$\text{coht } \mathfrak{p} := \sup_r \{\mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r \mid \mathfrak{p}_i \text{ are prime ideals of } R\}$$

Remark 22.7.1.3. Note that the dimension of a prime ideal $\mathfrak{p}$ as a ring may not be same as its height in R, as there might be many more primes in $\mathfrak{p}$ which may fail to be primes in the ring R. But clearly, $\dim \mathfrak{p} \geq \text{ht } \mathfrak{p}$.

Recall that the *dimension of a topological space* X is defined as

$$\dim X = \sup_r \{Z_0 \supsetneq Z_1 \supsetneq \cdots \supsetneq Z_r \mid Z_i \text{ are irreducible closed subsets of } X\}.$$

We now have some immediate observations about height, coheight and dimension.

Lemma 22.7.1.4. *Let R be a ring. Then,*

1. $\text{ht } \mathfrak{p} = \dim R_{\mathfrak{p}}$,
2. $\text{coht } \mathfrak{p} = \dim R/\mathfrak{p}$,
3. $\text{ht } \mathfrak{p} + \text{coht } \mathfrak{p} \leq \dim R$.

Proof. Prime ideals of $R/\mathfrak{p}$ are in one-to-one order preserving bijection with prime ideals of R containing $\mathfrak{p}$. Prime ideals of $R_{\mathfrak{p}}$ are in one-to-one order preserving bijection with prime ideals of R contained in $\mathfrak{p}$. Let Y denote the length of all chains of prime ideals of R passing through $\mathfrak{p}$. Consequently, $\sup Y \leq \dim X$. But $\sup Y = \text{ht } \mathfrak{p} + \text{coht } \mathfrak{p}$. □

Lemma 22.7.1.5. *Let R be a PID. Then,* $\dim R = 1$. *Consequently,* $\mathbb{Z}$ *and* $k[x]$ *are one dimensional rings for any field* k[7].

[7] as the intuition agrees!

Proof. Any chain is either of the form $\langle 0\rangle$ or $\langle x\rangle \supsetneq \langle 0\rangle$. □

Further, by Theorem 22.1.5.3 we see the following.

Lemma 22.7.1.6. *If R is a PID which is not a field, then* $\dim R[x] = 2$.

Proof. Indeed, by Theorem 22.1.5.3, the longest chain of prime ideals of the form $\mathfrak{o} \lneq \langle f(x)\rangle \lneq \langle p, h(x)\rangle$ where $f(x)$ is irreducible and $h(x)$ is irreducible modulo prime $p \in R$, as one can see immediately. □

The following is also a simple assertion, which basically is why one introduces dimension of a ring.

Lemma 22.7.1.7. *Let R be a ring. Then,*

$$\dim \operatorname{Spec}(A) = \dim A.$$

Proof. Immediate from definitions and Lemma 1.2.1.1. □

Let us now give some more helpful notions, especially the dimension of an R-module.

Definition 22.7.1.8. (**Dimension of a module and height of ideals**) Let M be an R-module. Then the dimension of M is defined as

$$\dim M := \dim R/\operatorname{Ann}(M).$$

Further, for an ideal $I \leq R$, we define the height of I as the infimum of heights of all prime ideals above I:

$$\operatorname{ht} I := \inf\{\operatorname{ht} \mathfrak{p} \mid \mathfrak{p} \supseteq I,\ \mathfrak{p} \in \operatorname{Spec}(R)\}.$$

We have the corresponding topological result.

Lemma 22.7.1.9. *Let R be a ring and M be a finitely generated R-module. Then,*

$$\dim M = \dim \operatorname{Supp}(M)$$

where $\operatorname{Supp}(M) \subseteq \operatorname{Spec}(R)$ *is the support of the module M.*

Proof. The result follows as $\operatorname{Supp}(M)$ is the closed subset $V(\operatorname{Ann}M)$ so that any irreducible closed set in $\operatorname{Supp}(M)$ will be irreducible closed in $\operatorname{Spec}(R)$ and then we can use Lemma 1.2.1.1. □

22.7.2 Dimension of finite type k-algebras

In algebraic geometry, one is principally interested in finite type algebras over a field. Thus it is natural to engage in the study of their dimensions. We discuss some elementary results in this direction in this section. See Section 22.1.6 for basics of finite type k-algebras.

The main results are as follows.

Theorem 22.7.2.1. *Let k be a field and A be a finite type k-algebra which is a domain*[8]*. Then,*

$$\dim A = \operatorname{trdeg} A/k.$$

Theorem 22.7.2.2. *Let k be a field and A be a finite type k-algebra which is a domain and let $\mathfrak{p} \lneq A$ be a prime ideal. Then,*

$$\operatorname{ht} \mathfrak{p} + \dim A/\mathfrak{p} = \dim A.$$

We now prove these results.

[8] note that such algebras are exactly the ones which correspond to affine algebraic varieties.

22.8 Completions

Do from Chapter 7 of Eisenbud

22.9 Valuation rings

We begin with the basic theory of valuation rings.

22.9.1 General theory

Definition 22.9.1.1. (**Valuation on a field**) Let K be a field and G be an abelian group. A function $v : K \to G \cup \{\infty\}$ is said to be a valuation of K with values in G if v satisfies

1. $v(xy) = v(x) + v(y)$,
2. $v(x + y) \geq \min\{v(x), v(y)\}$,
3. $v(x) = \infty$ if and only if $x = 0$.

Let $\mathrm{Val}(K, G)$ denote the set of all valuations over K with values in G.

Few immediate observations are in order.

Lemma 22.9.1.2. *Let K be a field, G be an abelian group and $v \in \mathrm{Val}(K, G)$ be a valuation. Then,*

1. *$R = \{x \in K \mid v(x) \geq 0\} \cup \{0\}$ is a subring of K,*
2. *$\mathfrak{m} = \{x \in K \mid v(x) > 0\} \cup \{0\}$ is a maximal ideal of R,*
3. *$(R, \mathfrak{m})$ is a local ring,*
4. *R is an integral domain,*
5. *$R_{\langle 0 \rangle} = K$,*
6. *$\forall x \in K$, $x \in R$ or $x^{-1} \in R$.*

Proof. Items 1 and 4 are immediate from the axioms of valuations. Items 2 and 3 are immediate from the observation that $\{x \in K \mid v(x) = 0\} \cup \{0\}$ is a field in R. For items 5 and 6, we need to observe that $v(1) = 0$ and for any $x \in K^{\times}$, $v(x^{-1}) = -v(x)$. □

Remark 22.9.1.3. We call the subring $R \subset K$ above corresponding to a valuation v over K to be the *value ring of v*.

Definition 22.9.1.4. (**Valuation rings**) Let R be an integral domain. Then R is said to be a valuation ring if it is the value ring of some valuation over $K = R_{\langle 0 \rangle}$.

Definition 22.9.1.5. (**Domination**) Let K be a field and $A, B \subset K$ be two local rings in K. Then B is said to dominate A if $B \supseteq A$ and $\mathfrak{m}_B \cap A = \mathfrak{m}_A$.

There is an important characterization of valuation rings inside a field K with respect to all local rings in K.

Theorem 22.9.1.6. *Let K be a field and $R \subset K$ be a local ring. Denote $\mathrm{Loc}(K)$ to be the set of all local rings in K together with the partial order of domination. Then, the following are equivalent,*

1. *R is a valuation ring.*
2. *R is a maximal element of the poset $\mathrm{Loc}(K)$.*

Furthermore, for every local ring $S \in \mathrm{Loc}(K)$, there exists a valuation ring $R \in \mathrm{Loc}(K)$ which dominates S.

Proof. See Tag 00I8 of cite[Stacksproject]. □

An important type of valuation rings are where the value group is the integers.

Definition 22.9.1.7. (**Discrete valuation rings**) Let R be a domain. Then R is said to be a discrete valuation ring (DVR) if the value group of R is the integers $\mathbb{Z}$.

It turns out that noetherian local domains of dimension 1 have some important characterizations.

Theorem 22.9.1.8. *Let A be a noetherian local domain of dimension 1. Then the following are equivalent*

1. *A is a DVR,*
2. *A is a normal domain,*
3. *A is a regular local ring,*
4. *the maximal ideal of A is principal.*

Proof. Do it from Atiyah-Macdonald page 94. □

22.9.2 Absolute values

We discuss the basics of absolute values and places, which will be used to state Ostrowski's theorem which classifies the places of $\mathbb{Q}$.

22.10 Dedekind domains

We will now discuss a class of rings which forms the right context for number theory. We give here the barebones, rest will be developed as needed elsewhere.

Definition 22.10.0.1 (**Dedekind domain**)**.** A noetherian normal domain of dimension 1 is defined to be a Dedekind domain.

Theorem 22.10.0.2. *Let R be a noetherian domain of dimension 1. Then the following are equivalent:*

1. *R is normal (equivalently, Dedekind).*
2. *Every primary ideal $\mathfrak{q}$ of R is of the form $\mathfrak{q} = \mathfrak{p}^n$ for some prime ideal $\mathfrak{p}$ and $n \geq 0$.*
3. *$R_{\mathfrak{p}}$ is a DVR for each non-zero prime $\mathfrak{p}$.*

Proof. **TODO**. □

22.11 Tor and Ext functors

Start doing from Appendix 3 of Eisenbud.

22.11.1 Some computations

Do exercises from Bruzzo.

22.12 Projective and injective modules

In this section we define an important object in the study of algebraic K-theory, projective modules. These generalize finitely generated free R-modules. This notion is further used in a very important geometric concept called depth and Cohen-Macaulay condition. In order to reach there, we would need a concept called projective dimension, which we cover here.

22.12.1 Divisible modules and Baer's criterion

Baer's criterion gives a characterization of injective R-modules. It consequently helps to show that divisible modules are injective in $\mathbf{Mod}(R)$ and thus that $\mathbf{Mod}(R)$ has enough injectives.

Definition 22.12.1.1 (Divisible modules). An R-module M is said to be divisible if for every $r \in R$, the multiplication by r map $\mu_r : M \to M$ is surjective.

Theorem 22.12.1.2. *(Baer's criterion) Let R be a ring and M be an R-module. The following are equivalent:*

1. *M is an injective R-module.*
2. *For any ideal $\mathfrak{a} \leq R$ and any map $f : \mathfrak{a} \to M$, there exists an extension $g : R \to M$ such that the following commutes:*

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{a} \arrow[r] \arrow[d, "f"'] & R \arrow[dl, dashed, "g"] & . \\
& M &
\end{tikzcd}$$

That is, one needs to check injectivity condition along inclusions of submodules of R.

Proof. 1. $\Rightarrow$ 2. is immediate from definition. For 2. $\Rightarrow$ 1. we proceed as follows. Pick $i : A \to B$ an injection of submodule $A \leq B$ and a map $f : A \to M$. We wish to extend this to $g : B \to M$. Indeed, consider the poset $\mathcal{P}$ of tuples (A', f'), $f' : A' \to M$ an extension of f with $(A', f') \leq (A'', f'')$ such that $A' \subseteq A''$ and f'' extends f'. By Zorn's lemma, we have a maximal extension $\bar{f} : \bar{A} \to M$. We reduce to showing that $\bar{A} = B$. If not, then there is $b \in B \setminus \bar{A}$. Consider $\tilde{A} = Rb + \bar{A}$. We claim that there is a map $\tilde{f} : \tilde{A} \to M$ extending f. Indeed, consider the ideal $\mathfrak{a} = \{r \in R \mid rb \in \bar{A}\}$. The map $\bar{f}$ defines a map $\mathfrak{a} \to M$ given by $r \mapsto \bar{f}(rm)$. By hypothesis, this has an extension, say $\kappa : R \to M$. Thus, we may define $g : \tilde{A} \to M$ as $rb + \bar{a} \mapsto \kappa(r) + \bar{f}(\bar{a})$. This extends f as if $rb + \bar{a} \in A$, then $rb \in \bar{A}$. Consequently, $\kappa(r) + \bar{f}(\bar{a}) = \bar{f}(rb) + \bar{f}(\bar{a}) = \bar{f}(rb + \bar{a}) = f(rb + \bar{a})$, as needed. □

As a corollary, we see that injective R-modules are divisible.

Corollary 22.12.1.3. *Let R be a ring and M be an R-module. If M is injective, then M is divisible.*

Proof. Pick any $m \in M$ and $r \in R$. Then, we have an R-linear map $\mu_r : \langle r \rangle \to M$ given by $r \mapsto m$. By Theorem 22.12.1.2, 2, this extends to an R-linear homomorphism $g : R \to M$ where $\mu_r(r) = g(r) = rg(1) = m$, Thus $g(1) \in M$ is such that $rg(1) = m$, as needed. □

22.13 Multiplicities

22.14 Kähler differentials

22.15 Depth and Cohen-Macaulay

22.16 Filtrations

Do from Chapter 5 of Eisenbud

22.17 Flatness

Complete this from Eisenbud Chapter 7 and appendix of Sernesi on Flatness, especially Proposition A.2.

This is one of the important parts of commutative algebra, as this notion corresponds to the idea of a continuous family of schemes, in some sense, as is discussed in the respective part above.

Definition 22.17.0.1. (**Flat modules and flat map of rings**) Let R be a ring. An R-module M is said to be flat if for any short exact sequence of R-modules

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

the following sequence is exact

$$0 \longrightarrow M \otimes_R N_1 \longrightarrow M \otimes_R N_2 \longrightarrow M \otimes_R N_3 \longrightarrow 0\ .$$

A map $\varphi : A \to B$ is a flat map if B is a flat A-module. In this case one also calls B to be a flat A-algebra.

Remark 22.17.0.2.

1. By right exactness of tensor products, it is sufficient to check that the s.e.s. $0 \to N_1 \to N_2$ is taken to s.e.s $0 \to M \otimes_R N_1 \to M \otimes_R N_2$.
2. Since localisation is an exact functor (Lemma 22.1.2.2), thus the natural map $A \to S^{-1}A$ is a flat map for any multiplicative set $S \subseteq A$.

22.18 Lifting properties : Étale maps

22.19 Lifting properties : Unramified maps

22.20 Lifting properties : Smooth maps

22.21 Simple, semisimple and separable algebras

These algebras are at the heart of the Galois phenomenology, i.e. all things related to polynomials splitting in a bigger field or not. Our study of these objects will thus motivate the study of the corresponding geometrical picture.

and write more
these algebras,
er 22.

22.21.1 Semisimple algebras

Definition 22.21.1.1. (**Semisimple algebras over a field** k) Let A be a k-algebra. Then A is a semisimple k-algebra if the Jacobson radical of A is 0.

22.21.2 Separable algebras

We will first study a rather special type of separable algebras, which are finitely generated and free as modules. Let us first give an example of such an algebra which is motivating our definition given later.

Example 22.21.2.1. Consider a ring A and the A-algebra A^n. There is something special about A^n; it is "separated" into finitely pieces which looks like A. This can be formalized. Indeed, we have the most obvious fact about such algebras that the obvious map

$$\begin{aligned} \varphi : A^n &\longrightarrow \operatorname{Hom}_A(A^n, A) \\ (a_1, \dots, a_n) &\longmapsto e_i \mapsto a_i \end{aligned}$$

is an isomorphism of A-algebras. More specifically, the map φ takes $(a_i) = (a_1, \dots, a_n)$ to the following mapping

$$\begin{aligned} \varphi((a_i)) : A^n &\longrightarrow A \\ (b_1, \dots, b_n) &\longmapsto a_1 b_1 + \cdots + a_n b_n. \end{aligned}$$

We now wish to generalize this. That is to say, taking above phenomenon as a definition we want to generalize when an A-algebra B "separates" into simple pieces. For this to work, we need to find an alternate characterization of the above phenomenon. For this, a little bit of thought shows that the above map is obtained as the dual map of the $\phi \in \operatorname{Hom}_A(A^n, \operatorname{Hom}_A(A^n, A))$ under the $\otimes$-Hom adjunction

$$\operatorname{Hom}_A(A^n \times A^n, A) \cong \operatorname{Hom}_A(A^n, \operatorname{Hom}_A(A^n, A))$$

where the isomorphism is given by

$$(A^n \times A^n \xrightarrow{f} A) \longmapsto ((a_i) \mapsto ((b_i) \mapsto f((a_i), (b_i)))) .$$

Now, consider the map

$$\begin{aligned} \tilde{\phi} : A^n \times A^n &\longrightarrow A \\ ((a_i), (b_i)) &\longmapsto \sum_{i=1}^{n} a_i b_i. \end{aligned}$$

The tensor-hom isomorphism tells us that $\tilde{\phi}$ is the dual map of ϕ above. Now notice that this dual map $\tilde{\phi}$ has a very simple description; it is given by the following commutative diagram:

$$\begin{tikzcd}
A^n \times A^n \arrow[r, "\tilde{\phi}"] \arrow[d] & A \\
\operatorname{Hom}_A\left(A^n, A^n\right) \arrow[ru, "\mathrm{Tr}"'] &
\end{tikzcd}.$$

It is this dual map that we shall generalize to the setting of arbitrary A-algebra B which is finitely generated and free of rank n. Indeed, for any A-algebra B and chose any generating set of B as an A-module, so that for any element $b \in B$, we can write $b = (b_1, \ldots, b_n) \in A^n$. We thus get a natural map $\tilde{\phi}$ as in the diagram below

$$\begin{tikzcd}
(b,c) \arrow[d] & B \times B \arrow[r, "\tilde{\phi}"] \arrow[d, "\kappa"'] & A \\
(b_i c_j)_{1\le i,j\le n} & \operatorname{Hom}_A\left(B, B\right) \arrow[ru, "\mathrm{Tr}"'] &
\end{tikzcd}.$$

Now, consider the tensor-hom dual of $\tilde{\phi}$ to obtain

$$\begin{aligned}
\phi : B &\longrightarrow \operatorname{Hom}_A\left(B, A\right) \\
b &\longmapsto \left(c \mapsto \tilde{\phi}(b,c)\right).
\end{aligned}$$

In order to mimic the case of A^n, we would require the map ϕ to be an isomorphism. Indeed, this is what we do in the definition given below.

Before defining a nice class of separable algebras, let us define an A-algebra B to be *finitely free* if B is finitely generated and free as an A-module.

Definition 22.21.2.2. (**Free separable algebras**) Let A be a ring and B be a finitely free A-algebra of rank n and chose a generating set of B, so for $b \in B$, we can write $b = (b_1, \ldots, b_n)$ for $b_i \in A$. Define $\tilde{\varphi}$ to be the following map

$$\begin{tikzcd}
(b,c) \arrow[d] & B \times B \arrow[r, "\tilde{\varphi}"] \arrow[d, "\kappa"'] & A \\
(b_i c_j)_{1\le i,j\le n} & \operatorname{Hom}_A\left(B, B\right) \arrow[ru, "\mathrm{Tr}"'] &
\end{tikzcd}.$$

Then B is said to be a separable A-algebra if the tensor-hom dual map $\varphi : B \to \operatorname{Hom}_A\left(B, A\right)$ is an isomorphism of A-algebras.

We would now like to show how separable algebras become familiar in the case of algebras over a field.

Proposition 22.21.2.3. *Let k be a field and A be an k-algebra. Then, the following are equivalent*

1. *A is a free separable k-algebra.*

2. *$A = \prod_{i=1}^n K_i$ where K_i are finite separable extensions of field k.*

Proof. □

Important exerc
Chapter 22.

Another characterization of separable algebras is as follows.

Lemma 22.21.2.4. *Let A be a ring and B be a finitely free A-algebra. Then the following are equivalent.*

1. *B is a separable A-algebra.*
2. *For all $\{w_1, \dots, w_n\}$ in B which is a generating set of free A-module B, we have*

$$\det\left(\mathrm{Tr}(w_i w_j)_{1\le i,j\le n}\right) \in A^\times.$$

tant exercise,
er 22.

Proof. □

22.22 Miscellaneous

We collect in this section results which so far doesn't fit in any other prior section. Perhaps this means our arrangement of material is not optimal.

The following result is a generalization of Lagrange interpolation formula.

Lemma 22.22.0.1. *Let K/F be an algebraic field extension. Then for any $\alpha_1, \dots, \alpha_n \in K$, such that α_i is not equal to any α_j nor any of its conjugate, and for any choice $\beta_1, \dots, \beta_n \in K$, there exists a polynomial $f(x) \in F[x]$ such that $f(\alpha_i) = \beta_i$ for all $i = 1, \dots, n$.*

Proof. Let $\alpha_1, \dots, \alpha_n \in K$ be such that α_j is not equal to α_i nor any of its conjugates for any $j \neq i$. Let $\beta_1, \dots, \beta_n \in K[\alpha_i]$. We wish to find a polynomial $f(x) \in F[x]$ such that $f(\alpha_i) = \beta_i$ for each $i = 1, \dots, n$.

We first observe that as K is an algebraic extension of F, therefore there exists $p_i(x) \in F[x]$ which is the minimal polynomial of $\alpha_i \in K$. This polynomial is obtained by looking at the kernel of evaluation at α_i, $\varphi_i : F[x] \to K$ where $x \mapsto \alpha_i$. Consequently, $p_i(x)$ is a monic irreducible polynomial of least degree in $F[x]$ such that $p_i(\alpha_i) = 0$, for each $i = 1, \dots, n$.

As $\mathfrak{m}_i := \langle p_i(x) \rangle \le F[x]$ are maximal ideals and $p_i(x) \neq p_j(x)$ because $\alpha_i \neq \alpha_j, \overline{\alpha_j}$[9], therefore $\mathfrak{m}_i + \mathfrak{m}_j = F[x]$ for all $i \neq j$. Hence $\mathfrak{m}_i$ are comaximal. Consequently, we obtain by Chinese remainder theorem that

$$\begin{tikzcd}
F[x] \arrow[r, two heads] & \frac{F[x]}{\mathfrak{m}_1\dots\mathfrak{m}_n} \arrow[r, "\cong"] & \frac{F[x]}{\mathfrak{m}_1} \times \dots \times \frac{F[x]}{\mathfrak{m}_n} \arrow[r, "\cong"] & F[\alpha_1] \times \dots \times F[\alpha_n] . \\
f(x) \arrow[r, maps to] & f(x) + \mathfrak{m}_1 \dots \mathfrak{m}_n \arrow[r, maps to] & (f(x) + \mathfrak{m}_i)_i \arrow[r, maps to] & (f(\alpha_1), \dots, f(\alpha_n))
\end{tikzcd}$$

Consequently, by above diagram, for the elements $(\beta_,1 \dots, \beta_n) \in F[\alpha_1] \times \dots \times F[\alpha_n]$, there exists a polynomial $f(x) \in F[x]$ such that $(f(\alpha_1), \dots, f(\alpha_n)) = (\beta_1, \dots, \beta_n)$. Hence $f(\alpha_i) = \beta_i$ for each $i = 1, \dots, n$. This completes the proof. □

The following is a general exercise in basic ideal theory.

[9] because conjugates have same minimal polynomials.

Lemma 22.22.0.2. *Let R be a commutative ring with unity. Let $\mathfrak{p} \lneq R$ be a prime ideal and $I, J \leq R$ be ideals. Then,*

1. *$I^k \subseteq \mathfrak{p}$ for some $k \geq 0$ implies $I \subseteq \mathfrak{p}$,*
2. *the following are equivalent:*
   (a) *$\sqrt{I} + \sqrt{J} = R$,*
   (b) *$I + J = R$,*
   (c) *$I^k + J^l = R$ for all $k, l > 0$.*

Proof. 1. Let $I \leq R$ be an ideal and $\mathfrak{p} \lneq \mathbb{R}$ be a prime ideal. Then, we wish to show that $I^k \subseteq \mathfrak{p} \implies I \subseteq \mathfrak{p}$ for any $k \in \mathbb{N}$.

Indeed, pick any $x \in I$. As $x^k \in I$, therefore $x^k \in \mathfrak{p}$. As $x^k = x \cdot x^{k-1} \in \mathfrak{p}$, therefore either $x \in \mathfrak{p}$ of $x^{k-1} \in \mathfrak{p}$. If the former, then we are done. If the latter, then we have $x^{k-1} = x \cdot x^{k-2} \in \mathfrak{p}$. Continuing in this manner, we eventually reach to the conclusion that $x \in \mathfrak{p}$.

2. ((a) $\Rightarrow$ (b)) : As we have $x \in \sqrt{I}$ and $y \in \sqrt{J}$ such that $x + y = 1$, therefore for some $n, m \in \mathbb{N}$ we have $x^n \in I$ and $y^m \in J$. Now, observe that

$$\begin{aligned} 1 = 1^{n+m} = (x+y)^{n+m} &= \sum_{r=0}^{n+m} {}^{n+m}C_r x^r y^{n+m-r} \\ &= \sum_{r=0}^{n} {}^{n+m}C_r x^r y^{n+m-r} + \sum_{r=n+1}^{n+m} {}^{n+m}C_r x^r y^{n+m-r}. \end{aligned}$$

If $0 \leq r \leq n$, then $y^{n+m-r} \in J$ and if $n+1 \leq r \leq n+m$, then $x^r \in I$. Hence $\sum_{r=0}^{n} {}^{n+m}C_r x^r y^{n+m-r} \in J$ and $\sum_{r=n+1}^{n+m} {}^{n+m}C_r x^r y^{n+m-r} \in I$. This shows that there exists $a \in I$ and $b \in J$ then $a + b = 1$.

((b) $\Rightarrow$ (c)) : As we have $x \in I$ and $y \in J$ such that $x + y = 1$, thus writing $1 = 1^{k+l}$ again, we see

$$\begin{aligned} 1 &= 1^{k+l} = (x+y)^{k+l} \\ &= \sum_{r=0}^{k+l} {}^{k+l}C_r x^r y^{k+l-r} \\ &= \sum_{r=0}^{k} {}^{k+l}C_r x^r y^{k+l-r} + \sum_{r=k+1}^{k+l} {}^{k+l}C_r x^r y^{k+l-r}. \end{aligned}$$

If $0 \leq r \leq k$, then $y^{k+l-r} \in J^l$ and if $k+1 \leq r \leq k+l$, then $x^r \in I^k$. Consequently, we have $\sum_{r=0}^{k} {}^{k+l}C_r x^r y^{k+l-r} \in J^l$ and $\sum_{r=k+1}^{k+l} {}^{k+l}C_r x^r y^{k+l-r} \in I^k$. Hence there exists $a \in I^k$ and $b \in J^l$ such that $a + b = 1$.

((c) $\Rightarrow$ (a)) : Setting $k = l = 1$, we have that there exists $x \in I$ and $y \in J$ such that $x + y = 1$. As $\sqrt{I} \supseteq I$ and $\sqrt{J} \supseteq J$, therefore $x \in \sqrt{I}$ and $y \in \sqrt{J}$ such that $x + y = 1$. Hence $\sqrt{I} + \sqrt{J} = R$. This completes the proof. □

The following is a counterexample to the claim that a sub-algebra of a finite type algebra is a finite type algebra.

Lemma 22.22.0.3. *Let R be a ring. The ring $R[t, tx, tx^2, \dots, tx^i, \dots]$ is neither a finite type R-algebra nor a finite type $R[t]$-algebra.*

Proof. Let $S = R[t, tx, tx^2, tx^3, \dots]$. We wish to show that S is not a finitely generated R or $R[t]$ algebra.

a) We first show that S is not finitely generated R-algebra. Indeed, let $p_1, \dots, p_n \in S$ be generators of S as an R-algebra. Then, we have that $p_i \in R[t, tx, \dots, tx^{m_i}]$ as a polynomial can atmost be in finitely many indeterminates. Hence, letting $M = \max_i m_i$, we obtain that $p_1, \dots, p_n \in R[t, tx, \dots, tx^M]$. It then follows that the R-algebra generated by $p_1, \dots, p_n$ will only be inside $R[t, tx, \dots, tx^M]$. We consequently reduce to showing that $R[t, tx, \dots, tx^M] \neq S$.

Let $tx^{M+1} \in S$. We claim that $tx^{M+1} \notin R[t, tx, \dots, tx^M]$. Assuming to the contrary, we have that for some $a_{k_0,\dots,k_M} \in R$

$$\begin{aligned} tx^{M+1} &= \sum_{k_0,\dots,k_M} a_{k_0,\dots,k_M} t^{k_0} \dots (tx^M)^{k_M} \\ &= \sum_{k_0,\dots,k_M} a_{k_0,\dots,k_M} t^{k_0+\dots+k_M} \cdot x^{k_1+2k_2+\dots+Mk_M}. \end{aligned}$$

We thus deduce that $a_{k_0,\dots,k_M} \neq 0$ if and only if $k_0 + \dots + k_M = 1$. As $k_i \in \mathbb{Z}_{\geq 0}$, we further deduce that the only non-zero coefficients are $a_{1,0,\dots,0}, a_{0,1,\dots,0}, \dots, a_{0,0,\dots,1}$. Hence, the above equation reduces to

$$tx^{M+1} = a_{1,0,\dots,0}t + a_{0,1,\dots,0}tx + \dots + a_{0,0,\dots,1}tx^M.$$

Clearly, for no choice of coefficients $a_{1,0,\dots,0}, a_{0,1,\dots,0}, \dots, a_{0,0,\dots,1}$ in R can we make both sides equal in $R[t, x]$. This is a contradiction.

b) We now wish to show that S is not finitely generated as an $R[t]$-algebra. Assuming to the contrary, there exists $p_1, \dots, p_n \in S$ such that S is generated by them as an $R[t]$-algebra. Again for the same reason as in a), we see that $p_1, \dots, p_n \in R[t, tx, \dots, tx^M]$ for some $M \in \mathbb{Z}_{>0}$. Now, as $R[t, tx, \dots, tx^M] = R[t][tx, tx^2, \dots, tx^M]$, therefore the $R[t]$-algebra generated by $p_1, \dots, p_n$ will only be inside $R[t][tx, tx^2, \dots, tx^M]$. Hence, we reduce to showing that $R[t][tx, tx^2, \dots, tx^M] \neq S$. To this end, the exact same technique as in part a) works verbatim, as we need only show that $tx^{M+1} \notin R[t][tx, tx^2, \dots, tx^M] = R[t, tx, \dots, tx^M]$.

This completes the proof. □

The following result characterizes all ideals of $F[[x]]$, yielding that $F[[x]]$ is a local PID, i.e. a DVR, and tells us that localization of $F[[x]]$ at the local parameter x yields the Laurent series ring, i.e. the fraction field of $F[[x]]$.

Proposition 22.22.0.4. *Let F be a field and $R = F[[x]]$.*

1. *An element in $a = a_0 + a_1x + \dots \in R$ is a unit if and only if $a_0 \neq 0$.*
2. *Every non-zero ideal of R is of the form x^kR.*
3. *$R[x^{-1}] = Q(R) = F((x))$.*

Proof. 1. ($\Rightarrow$) Since $\sum_{i\geq 0} a_ix^i$ is a unit in $F[[x]]$, therefore there exists $\sum_{i\geq 0} b_ix^i$ which is an inverse of $\sum_{i\geq 0} a_ix^i$. Consequently, we have

$$\begin{aligned} (a_0 + a_1x + \dots) \cdot (b_0 + b_1x + \dots) &= 1 \\ (a_0b_0 + (a_1b_0 + a_0b_1)x + \dots) &= 1. \end{aligned}$$

Comparing the degree 0 term both sides, we obtain $a_0b_0 = 1$. Therefore, if $a_0 = 0$, then $a_0b_0 = 0$ and we would thus obtain a contradiction.
($\Leftarrow$) Suppose $a_0 \neq 0$. We wish to find $\sum_{i\geq 0} b_ix^i$ such that $\left(\sum_{i\geq 0} a_ix^i\right) \cdot \left(\sum_{j\geq 0} b_jx^j\right) = 1$. We can calculate what b_is should be by observing the following:

$$\left(\sum_{i\geq 0} a_ix^i\right) \cdot \left(\sum_{j\geq 0} b_jx^j\right) = \sum_{k\geq 0} c_kx^k$$

where $c_k = \sum_{i+j=k} a_ib_j$. We now claim that there exists a unique solution for each b_i in the equations given by setting $c_0 = 1$ and $c_k = 0$ for all $k \geq 1$. We show this by strong induction. Indeed, for $c_0 = a_0b_0 = 1$ yields that $b_0 = a_0^{-1}$. For $k = 1$, we have $c_1 = a_1b_0 + a_0b_1 = 0$ which thus yields $b_1 = -a_0^{-1}a_1b_0$. We now wish to show that if b_l has a unique solution for all $l = 0, \dots k-1$, then b_k has a unique solution as well. Indeed, b_k satisfies the following equation coming from $c_k = 0$:

$$\begin{aligned} 0 &= \sum_{i+j=k} a_ib_j \\ &= a_0b_k + \sum_{i+j=k, j<k} a_ib_j. \end{aligned}$$

By inductive hypothesis, for all $0 \leq j < k$, b_j has a unique solution. Consequently by the above, b_k has a unique solution as well. This completes the induction which yields the required formal power series.

$\sum_{j\geq 0} b_jx^j$ which acts as the inverse of $\sum_{i\geq 0} a_ix^i$. 2. We wish to show that any non-zero ideal $I \leq R$ is of the form $I = x^kR$ where $k \in \mathbb{N}$. Pick any ideal $I \leq R$. For any power series $p(x) = c_nx^n + c_{n+1}x^{n+1} + \dots$ where $c_n \neq 0$, we define n to be the ***co-degree*** of $p(x)$. Then, let $p(x) = c_kx^k + c_{k+1}x^{k+1} + \dots$ be the element of I with least co-degree (such an element exists by virtue of well-ordering of $\mathbb{N}$). Consequently, we obtain $p(x) = x^k(c_k + c_{k+1}x + \dots)$.

We thus claim that $I = x^kR$. Indeed, pick any $f(x) \in I$. Then, $f(x) = d_nx^n + d_{n+1}x^{n+1} + \dots$ where $d_n \neq 0$. Hence, we may write $f(x) = x^n(d_n + d_{n+1}x + \dots)$. By item 1, we know that $d_n + d_{n+1}x + \dots$ is a unit in R, so that we may write $f(x) = x^nu$, $u \in R$ is a unit. Now, as $f(x) \in I$, thus co-degree of f is atleast k as $p(x) \in I$ with co-degree k is the least co-degree element. Consequently, we may write $f(x) = x^kx^{n-k}u$. Hence $f(x) \in x^kR$. Conversely, pick any $x^kg(x) \in x^kR$. Since $p(x) = x^k(c_k + c_{k+1}x + \dots)$ where $c_k \neq 0$, therefore $c_k + c_{k+1}x + \dots$ is a unit, hence $p(x) = x^kv$ for some unit $v \in R$. Thus, $x^k \in I$ and hence $x^kg(x) \in I$. This completes the proof.

3. We wish to show that $R[\frac{1}{x}] = Q(R)$, the fraction field of R, i.e. $F((x))$. Indeed, as $x \in R$ is a non-zero element, therefore $1/x \in Q(R)$ and consequently, $R[\frac{1}{x}] \subseteq Q(R)$. We now wish to show that converse also holds.

Pick any $\frac{f(x)}{g(x)} \in Q(R)$ where $f(x), g(x) \in R$ are power series. Let $f(x)$ have co-degree n and $g(x)$ have co-degree m. We may then write

$$\frac{f(x)}{g(x)} = \frac{c_nx^n + c_{n+1}x^{n+1} + \dots}{d_mx^m + d_{m+1}x^{m+1} + \dots}$$

where $c_n, d_m \neq 0$. We may further write above as

$$\frac{f(x)}{g(x)} = \frac{x^n u}{x^m v}$$

for units $u = c_n + c_{n+1}x + \dots, v = d_m + d_{m+1}x + \dots \in R$ (by item 1).

If $n > m$, then $\frac{f(x)}{g(x)} = \frac{x^{n-m}w}{1}$ for some unit $w \in R$ and we know that $\frac{x^{n-m}}{1} \in R[\frac{1}{x}]$. If $n < m$, then $\frac{f(x)}{g(x)} = \frac{w}{x^{m-n}}$ for some unit $w \in R$ and we know that $\frac{1}{x^{m-n}} \in R[\frac{1}{x}]$. Finally if $n = m$, then $\frac{f(x)}{g(x)}$ is a unit of R and hence of $R[\frac{1}{x}]$.

Hence in all cases, $\frac{f(x)}{g(x)} \in R[\frac{1}{x}]$. We thus conclude $Q(R) \subseteq R[\frac{1}{x}]$, completing the proof. □

In the following theorem, we show some important properties of the ring $\mathbb{Z}[\omega]$, where ω is a third root of unity.

Theorem 22.22.0.5. *Let $R = \mathbb{Z}[\omega]$ where $\omega = e^{\frac{2\pi i}{3}}$ is a cube root of unity.*

1. *R is a Euclidean domain.*
2. *The function given by*

$$\begin{aligned} f : \operatorname{Spec}(\mathbb{Z}[\omega]) &\longrightarrow \operatorname{Spec}(\mathbb{Z}) \\ \pi &\longmapsto \begin{cases} p & \textit{if } \pi = p \textit{ upto associates,} \\ \pi\bar{\pi} & \textit{else.} \end{cases} \end{aligned}$$

   is surjective such that $f^{-1}(p)$ is either $\{\pi, \bar{\pi}\}$ or $\{p\}$ (upto associates) for any prime $p \in \operatorname{Spec}(\mathbb{Z})$.
3. *Let $p \in \mathbb{Z}$ be a prime. The following are equivalent:*
   - *(i) p splits in $\mathbb{Z}[\omega]$, that is $p = \alpha\bar{\alpha}$ for some $\alpha \in \mathbb{Z}[\omega]$,*
   - *(ii) $x^2 \pm x + 1$ has a root in $\mathbb{F}_p$, that is, $\exists a \in \mathbb{F}_p$ such that $a \neq 1$ and $a^3 = \pm 1$,*
   - *(iii) either $p = 3$ or $p = 1 \mod 3$.*
4. *Take any $n \in \mathbb{Z}$. The following are equivalent:*
   - *(i) $n = a^2 \pm ab + b^2$ for some $a, b \in \mathbb{Z}$,*
   - *(ii) primes $2 \mod 3$ occurs evenly many times in the prime factorization of n.*

Proof. 1. We first wish to show that R is a Euclidean domain. We claim that the following function

$$\begin{aligned} d : R \setminus \{0\} &\longrightarrow \mathbb{N} \cup \{0\} \\ \alpha = a + b\omega &\longmapsto \alpha\bar{\alpha} = a^2 + b^2 - ab \end{aligned}$$

satisfies the axiom of size function for R. Indeed, pick any $\alpha, \beta \in R$ where $\beta \neq 0$. We may then write

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = \frac{\alpha\bar{\beta}}{c} = a + ib$$

where $a, b \in \mathbb{Q}$. As any rational $x \in \mathbb{Q}$ can be written as $x = n + q$ where $n \in \mathbb{Z}$ and $0 \leq q \leq 1/2$, therefore we may write

$$\frac{\alpha}{\beta} = a + ib = (n_1 + r_1) + \omega(n_2 + r_2)$$

where $n_1, n_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 \leq 1/2$. Thus,

$$\alpha = \beta(n_1 + \omega n_2) + \beta(r_1 + \omega r_2) \tag{1.1}$$

As $\alpha, \beta(n_1 + \omega n_2) \in R$, therefore by (1.1) we deduce that $\beta(r_1 + \omega r_2) \in R$.
Note that since the size function d is the norm map, which is actually a multiplicative map defined on whole of $\mathbb{C}$ as

$$\begin{aligned} \mathbb{C} &\longrightarrow \mathbb{R} \\ z &\longmapsto z\bar{z}, \end{aligned}$$

hence, we see that

$$\begin{aligned} d(\beta(r_1 + \omega r_2)) &= \beta\bar{\beta}(r_1^2 + r_2^2 - r_1 r_2) \\ &\leq \beta\bar{\beta}\left(\frac{1}{2^2} + \frac{1}{2^2}\right) \\ &= \frac{\beta\bar{\beta}}{2} \\ &< \beta\bar{\beta} \\ &= d(\beta). \end{aligned}$$

Thus, Eq. (1.1) is the required division of α by β. This proves that R is a Euclidean domain.

2. Let R be an arbitrary Euclidean domain and let Spec (R) denote the set of all prime ideals of R. As R is a Euclidean domain, therefore it is a PID. Consequently, Spec (R) is in one-to-one bijection with prime/irreducible elements of R together with 0. Hence, we write $p \in \text{Spec}\,(R)$ to mean a prime element of R. We know that $\mathbb{Z}[\omega]$ and $\mathbb{Z}$ are Euclidean domains.
We wish to show that there is a surjective map

$$\begin{aligned} f : \text{Spec}\,(\mathbb{Z}[\omega]) &\longrightarrow \text{Spec}\,(\mathbb{Z}) \\ \pi &\longmapsto \begin{cases} p & \text{if } \pi = p \text{ upto associates,} \\ \pi\bar{\pi} & \text{else.} \end{cases} \end{aligned}$$

such that $f^{-1}(p)$ is either $\{\pi, \bar{\pi}\}$ or $\{p\}$ (upto associates) for any prime $p \in \text{Spec}\,(\mathbb{Z})$ where $\pi \in \text{Spec}\,(\mathbb{Z}[\omega])$ is a prime element.
We first observe that $\mathbb{Z}[\omega]$ has a non-trivial automorphism given by $\alpha = a + b\omega \mapsto \bar{\alpha} = a + b\omega^2$. Pick $\pi \in \text{Spec}\,(\mathbb{Z}[\omega])$ a non-zero prime element. Observe that automorphisms takes a prime element to a prime element. As $\mathbb{Z}$ is a UFD, therefore for $p_1, \dots, p_l \in$

Spec$(\mathbb{Z})$ non-zero primes, and $\pi_1, \dots, \pi_k \in$ Spec$(\mathbb{Z}[\omega])$ non-zero primes, we may write

$$\begin{aligned}\pi\bar{\pi} &= a^2 + b^2 - ab\\ &= p_1 \dots p_l\\ &= \pi_1 \dots \pi_k\end{aligned}$$

where the last equality comes from writing prime factorization of each p_i in $\mathbb{Z}[\omega]$. Now, as $\mathbb{Z}[\omega]$ is a UFD, therefore $k = 2$ and hence $l \leq 2$. We now have two cases

(i) If $l = 2$, then $\pi\bar{\pi} = p_1 p_2$. Expanding each p_i into product of primes in $\mathbb{Z}[\omega]$, we immediately deduce by unique factorization in $\mathbb{Z}[\omega]$ that $p_1 = \pi$ and $p_2 = \bar{\pi}$ upto associates (wlog). Hence, $\bar{\pi} = p_2 = p_1$. That is,

$$\pi\bar{\pi} = p^2.$$

(ii) If $l = 1$, then

$$\pi\bar{\pi} = p$$

for some non-zero prime $p \in$ Spec$(\mathbb{Z})$.

This defines the function $f :$ Spec$(\mathbb{Z}[\omega]) \to$ Spec$(\mathbb{Z})$. Next, we wish to show that this is surjective. Indeed, pick any non-zero $p \in$ Spec$(\mathbb{Z})$. Using prime factorization in $\mathbb{Z}[\omega]$, we obtain primes $\pi_1, \dots, \pi_k$ in $\mathbb{Z}[\omega]$ such that

$$p = \pi_1 \dots \pi_k.$$

Again using the conjugation automorphism yields us

$$p^2 = (\pi_1\bar{\pi_1}) \dots (\pi_k\bar{\pi_k}).$$

Note $\pi_i\bar{\pi_i} \in \mathbb{Z}$. Hence, by unique factorization of $\mathbb{Z}$, we obtain $k \leq 2$. We now have two cases

(i) If $k = 2$, then $p^2 = (\pi_1\bar{\pi_1})(\pi_2\bar{\pi_2})$. As π_i are not units, we deduce that $p = \pi_1\bar{\pi_1}$ and $p = \pi_2\bar{\pi_2}$. Consequently, we have $\pi_1\bar{\pi_1} = \pi_2\bar{\pi_2}$. Thus, by unique factorization of $\mathbb{Z}[\omega]$, we further deduce that $\pi_1 = \pi_2$ or $\bar{\pi_2}$. Hence, $p = \pi\bar{\pi}$ for a unique $\pi \in$ Spec$(\mathbb{Z}[\omega])$.

(ii) If $k = 1$, then

$$p^2 = \pi\bar{\pi}$$

for some $\pi \in$ Spec$(\mathbb{Z}[\omega])$. Writing p as a product of primes in $\mathbb{Z}[\omega]$, we immediately deduce of unique factorization of $\mathbb{Z}[\omega]$ that $p = \pi'$ upto units for some non-zero prime $\pi' \in$ Spec$(\mathbb{Z}[\omega])$. Consequently, $p^2 = \pi'\bar{\pi'} = \pi\bar{\pi}$. Again by unique factorization of $\mathbb{Z}[\omega]$, we immediately deduce that $\pi = \pi'$ upto units.

This shows the surjectivity of the map f.

3. (i) $\iff$ (ii) : By part b), p splits in $\mathbb{Z}[\omega]$ iff p is not prime in $\mathbb{Z}[\omega]$. This happens iff $\mathbb{Z}[\omega]/p$ is not a domain. We now observe

$$\begin{aligned}\frac{\mathbb{Z}[\omega]}{p\mathbb{Z}[\omega]} &\cong \frac{\frac{\mathbb{Z}[x]}{\langle x^2+x+1\rangle}}{\frac{\langle p,x^2+x+1\rangle}{\langle x^2+x+1\rangle}}\\ &\cong \frac{\mathbb{Z}[x]}{\langle p, x^2+x+1\rangle}\\ &\cong \frac{\frac{\mathbb{Z}[x]}{p\mathbb{Z}[x]}}{\frac{\langle p,x^2+x+1\rangle}{p\mathbb{Z}[x]}}\\ &\cong \frac{\mathbb{F}_p[x]}{\langle x^2+x+1\rangle}.\end{aligned}$$

Hence, p is not prime in $\mathbb{Z}[\omega]$ iff x^2+x+1 is reducible in $\mathbb{F}_p[x]$. As a polynomial of degree 2 or 3 over a field is reducible iff it has a root in the field, therefore p is not prime in $\mathbb{Z}[\omega]$ iff x^2+x+1 has a root in $\mathbb{F}_p$. Similarly, since ω^2 has minimal polynomial x^2-x+1 and $\mathbb{Z}[\omega]=\mathbb{Z}[\omega^2]$, hence repeating the above yields p is not prime in $\mathbb{Z}[\omega]$ iff x^2-x+1 has a root in $\mathbb{F}_p[x]$.

(ii) $\Rightarrow$ (iii) : If $p=2$, then $x^2 \pm x+1$ has no roots in $\mathbb{F}_2$. Consequently, let $p\neq 2,3$. We then wish to show that $p=1 \mod 3$. Let $a\in\mathbb{F}_p$ be the root of $f(x)=x^2\pm x+1$. Thus, $a^3=\pm 1$. Observe that $a\neq\pm 1$ as if $a=1$, then $f(1)$ and $f(-1)$ are either 1 or 3 and since $p\neq 3$, therefore $f(1), f(-1)\neq 0$, a contradiction.
As $a^3=\pm1$ and $a\neq\pm1$, therefore the order of $a\in\mathbb{F}_p^*$ is either 3 or 6. In either case, as $\left|\mathbb{F}_p^*\right| = p-1$, therefore by Lagrange's theorem, $3|p-1$ or $6|p-1$. But in both cases, we have $p=1 \mod 3$.

(iii) $\Rightarrow$ (ii) : If $p=3$, then $1\in\mathbb{F}_3$ is root of x^2+x+1 and 2 is the root of x^2-x+1. If $p=1 \mod 3$, then we proceed as follows. As $\mathbb{F}_p^*$ is a cyclic group of order $p-1$ and since $p-1=3k$ for some $k\in\mathbb{Z}$, hence there exists an element $a\in\mathbb{F}_p$ of order 3. Consequently, we have $a^3=1$ and thus x^3-1 in $\mathbb{F}_p[x]$ has a root. As $x^3-1=(x-1)(x^2+x+1)$ and $a\neq 1$, hence a is a root of x^2+x+1.
Now since

$$\frac{\mathbb{F}_p[x]}{\langle x^2+x+1\rangle} \cong \frac{\mathbb{F}_p[x-1]}{\langle (x-1)^2+(x-1)+1\rangle} = \frac{\mathbb{F}_p[x]}{\langle x^2-x+1\rangle}$$

therefore if x^2+x+1 has a root in $\mathbb{F}_p$, then so does x^2-x+1.

4. (i) $\Rightarrow$ (ii) : Write the prime factorization of n in $\mathbb{Z}[\omega]$ as follows

$$\begin{aligned}n &= (a+b\omega)(a+b\omega^2)\\ &= (\pi_1\ldots\pi_k)(\bar{\pi_1}\ldots\bar{\pi_k})\\ &= (\pi_1\bar{\pi_1})\ldots(\pi_k\bar{\pi_k}).\end{aligned}$$

From parts b) and c), we know that for any prime element $\pi\in\mathbb{Z}[\omega]$, we have $\pi\bar{\pi}=p$ iff $p=3$ or $1 \mod 3$ and $\pi\bar{\pi}=p^2$ iff $p=2 \mod 3$. Consequently, we have

$$n = (p_1\ldots p_m)(p_{m+1}^2\cdots p_k^2)$$

where we call primes $p_1, \dots, p_m$ which are either 3 or $1 \mod 3$ of ***split type***. Similarly, we call the primes $p_{m+1}, \dots, p_k$ which are $2 \mod 3$ of ***unsplit type***. From above it is clear that unsplit type primes appear evenly many times (they appear in squares) in the prime factorization of n.

(ii) $\Rightarrow$ (i) : Let $n \in \mathbb{Z}$ be such that its prime factorization in $\mathbb{Z}$ is as follows

$$n = (p_1 \dots p_m)(q_1^{2k_1} \dots q_n^{2k_n})$$

where q_i are primes of unsplit type, that is, $q_i = 2 \mod 3$ and p_i are of split type, that is, 3 or $1 \mod 3$. Now, by part b), we may write $p_i = \pi_i \bar{\pi_i}$ as they split in $\mathbb{Z}[\omega]$ and $q_i = \xi_i$, where ξ_i, π_i are primes in $\mathbb{Z}[\omega]$.
It follows that we may write

$$\begin{aligned} n &= (\pi_1 \bar{\pi_1} \dots \pi_m \bar{\pi_m}) \left(\xi_1^{2k_1} \dots \xi_n^{2k_n}\right) \\ &= (\xi_1^{k_1} \dots \xi_n^{k_n})(\pi_1 \dots \pi_m) \cdot (\xi_1^{k_1} \dots \xi_n^{k_n})(\bar{\pi_1} \dots \bar{\pi_m}) \\ &= \alpha\bar{\alpha} \end{aligned}$$

where $\alpha = (\xi_1^{k_1} \dots \xi_n^{k_n})(\pi_1 \dots \pi_m) = a + b\omega$, as required.
This completes the proof. □

Example 22.22.0.6. As an example use of above we may now find all ordered tuples $(a, b) \in \mathbb{Z}^2$ such that $2100 = a^2 - ab + b^2$.

Observe that

$$\begin{aligned} 2100 &= 2^2 \cdot 3 \cdot 5^2 \cdot 7 \\ &= 2^2 \cdot 5^2 \cdot (2 + \omega)(2 + \omega^2)(3 + \omega)(3 + \omega^2). \end{aligned}$$

We now wish to find the distinct $\alpha \in \mathbb{Z}[\omega]$ such that $2100 = \alpha\bar{\alpha}$. For this, we first need to find all units of $\mathbb{Z}[\omega]$.

Indeed, we claim that the units of $\mathbb{Z}[\omega]$ are $1, -1, \omega, -\omega, 1 + \omega, -1 - \omega$. We give a terse proof of this fact as follows. Let $a + b\omega \in \mathbb{Z}[\omega]$ be a unit, so that there exists $c + d\omega$ such that $(a + b\omega)(c + d\omega) = 1$. Then, the multiplicative map

$$\begin{aligned} \mathbb{Z}[\omega] &\to \mathbb{Z} \\ \alpha &\mapsto \alpha\bar{\alpha} \end{aligned}$$

yields in $\mathbb{Z}$ that $(a^2 + b^2 - ab)(c^2 + d^2 - cd) = 1$. This forces $a^2 + b^2 - ab = 1 = c^2 + d^2 - cd$. From these equations one can deduce that $c + d\omega = (a - b) - b\omega$. Hence, $a + b\omega$ is a unit iff $a^2 + b^2 - ab = 1$. It follows by AM-GM inequality on a^2 and b^2 that $ab \leq 1$. Hence, we deduce that $a = 1, b = 1$ or $a = -1, b = -1$ or $a = 0$ or $b = 0$. Correspondingly, we get the six units of $\mathbb{Z}[\omega]$ as mentioned above.

In order to count the number of distinct pairs $(a, b) \in \mathbb{Z}^2$ such that $n = a^2 + b^2 - ab = (a + b\omega)(a + b\omega^2)$ properly, let us bring some notations. Let $X_n = \{(a + b\omega) \mid (a + b\omega)(a + b\omega^2) = n\} \subseteq \mathbb{Z}[\omega]$. Denote $f : \mathbb{Z}[\omega] \to \mathbb{Z}$ to be the multiplicative map $\alpha \mapsto \alpha\bar{\alpha}$. We thus have $X_n = f^{-1}(n)$. Now observe that

1. for each $a + b\omega \in X_n$, we have $b + a\omega \in X_n$,
2. for each $a + b\omega \in X_n$, we have $a + b\omega^2 \in X_n$,
3. for each $a + b\omega \in X_n$ and $u \in \mathbb{Z}[\omega]$ a unit, we have $u(a + b\omega) \in X_n$. This is because in $\mathbb{Z}[\omega]$, inverse of a unit is its conjugate.

Our goal is to count ordered tuples $(a, b) \in \mathbb{Z}^2$ such that $n = a^2 + b^2 - ab$. Immediately, we see that such ordered tuples are in bijection with X_n. Hence, we reduce to counting X_n.

From the above discussion, we see the elements in X_n obtained by multiplying by units are

- $2 \cdot 5 \cdot 1 \cdot (2 + \omega)(3 + \omega) = 50 + 40\omega$,
- $2 \cdot 5 \cdot -1 \cdot (2 + \omega)(3 + \omega) = -50 - 40\omega$,
- $2 \cdot 5 \cdot \omega \cdot (2 + \omega)(3 + \omega) = -40 + 10\omega$,
- $2 \cdot 5 \cdot (-\omega) \cdot (2 + \omega)(3 + \omega) = 40 - 10\omega$,
- $2 \cdot 5 \cdot (1 + \omega) \cdot (2 + \omega)(3 + \omega) = 10 + 50\omega$,
- $2 \cdot 5 \cdot (-1 - \omega) \cdot (2 + \omega)(3 + \omega) = -10 - 50\omega$,
- $2 \cdot 5 \cdot 1 \cdot (2 + \omega^2)(3 + \omega) = 40 - 10\omega$.
- $2 \cdot 5 \cdot -1 \cdot (2 + \omega^2)(3 + \omega) = -40 + 10\omega$,
- $2 \cdot 5 \cdot \omega \cdot (2 + \omega^2)(3 + \omega) = 10 + 50\omega$,
- $2 \cdot 5 \cdot (-\omega) \cdot (2 + \omega^2)(3 + \omega) = -10 - 50\omega$,
- $2 \cdot 5 \cdot (1 + \omega) \cdot (2 + \omega^2)(3 + \omega) = 50 + 40\omega$,
- $2 \cdot 5 \cdot (-1 - \omega) \cdot (2 + \omega^2(3 + \omega) = -50 - 40\omega$.

Similarly, those obtained by swapping are

- $40 + 50\omega$,
- $-40 - 50\omega$,
- $10 - 40\omega$,
- $50 + 10\omega$,
- $-50 - 10\omega$.

Hence, there are 12 such ordered tuples $(a, b) \in \mathbb{Z}^2$ given by $(40, 50), (-40, -50), (10, -40)$, $(50, 10), (-50, 10), (50, 40), (-50, -40), (-40, 10), (10, 50), (-10, -50)$.

The following is a simple but powerful lemma about certain type of k-algebras.

Lemma 22.22.0.7. *Let k be a field and A be a k-algebra such that there is a maximal ideal $\mathfrak{m} \lneq A$ for which $A/\mathfrak{m} \cong k$. Then,*

$$A \cong k \oplus \mathfrak{m}$$

where $k \oplus \mathfrak{m}$ obtains the k-algebra structure from A.

Proof. Consider the triangle

$$\begin{tikzcd} A \arrow[d, two heads, "\pi"'] & k \arrow[l, hook'] \arrow[dl, "\cong"] \\ A/\mathfrak{m} & \end{tikzcd}.$$

Pick any $a \in A$. We have $\pi(a) \in A/\mathfrak{m} \cong k$, so let $\pi(a) \in k$ by identifying under that isomorphism. Consequently, we may write $a = \pi(a) + (a - \pi(a))$. Note since $\pi(a - \pi(a)) = \pi(a) - \pi(\pi(a)) = \pi(a) - \pi(a) = 0$ by the commutativity of the above, therefore $a \in \mathfrak{m}$.

Furthermore $\mathfrak{m} \cap k = 0$ is immediate as $\mathfrak{m}$ is a proper ideal. It follows that $A = k \oplus \mathfrak{m}$ as k-linear subspaces, and thus $k \oplus \mathfrak{m}$ is a k-algebra as well, isomorphic to A, where, since $(k_1 + m_1) \cdot (k_2 + m_2) = k_1k_2 + k_1m_2 + k_2m_1 + m_1m_2$ inside of A, hence we may define the k-algebra structure on $k \oplus \mathfrak{m}$ as

$$(k_1, m_1) \cdot (k_2, m_2) = (k_1k_2, k_1m_2 + k_2m_1 + m_1m_2)$$

for $(k_i, m_i) \in k \oplus \mathfrak{m}$. □

The following proposition shows that any submodule of a free module over a PID is free (which is not true in general).

Proposition 22.22.0.8. *Let R be a PID and X an indexing set. Then any submodule of $R^{\oplus X}$ is free.*

Proof. Let $M \leq R^{\oplus X}$ be a submodule. For each $Y \subseteq X$, consider the submodule

$$M_Y := M \cap R^{\oplus Y}.$$

Denote by $\mathbb{T}$ the following partially ordered set

$$\mathbb{T} = \left\{(B, Y) \mid Y \subseteq X,\ B \subseteq M \text{ s.t. } M_Y = \bigoplus_{b \in B} Rb\right\}$$

where $(B_1, Y_1) \leq (B_2, Y_2)$ if and only if $B_1 \subseteq B_2$ and $Y_1 \subseteq Y_2$.

We first claim that $\mathbb{T}$ is non-empty. Indeed, consider any finite subset $Y \subseteq X$. We claim that $M \cap R^{\oplus Y}$ is free. To this end, first observe that $M \cap R^{\oplus Y} \leq R^{\oplus Y}$. As finite direct sum of noetherian modules is noetherian, therefore $R^{\oplus Y}$ is noetherian. As a module is noetherian if and only if every submodule is finitely generated, therefore $M \cap R^{\oplus Y}$ is finitely generated.

By structure theorem of finitely generated modules over a PID, we deduce that

$$M \cap R^{\oplus Y} \cong \frac{R}{d_1R} \oplus \cdots \oplus \frac{R}{d_kR} \oplus R^n. \tag{5.1}$$

As R is a PID, so in particular a domain, therefore $R^{\oplus Y}$ has no R-torsion element. Consequently, in Eq. (5.1), we conclude that $d_i = 1$ for each $i = 1, \dots, k$, that is, $M \cap R^{\oplus Y} \cong R^n$. Hence, $M \cap R^{\oplus Y}$ is free, as required. More generally this argument shows that any submodule of R^X where X is finite is free. This shows that $\mathbb{T}$ is non-empty.

We next wish to show that $\mathbb{T}$ has a maximal element. We will use Zorn's lemma on $\mathbb{T}$ for this. Pick any totally ordered subset $\mathcal{T} \subseteq \mathbb{T}$. We wish to show that $\mathcal{T}$ has an upper bound. Indeed, denote

$$C = \bigcup_{(B,Y) \in \mathcal{T}} B \ \&\ Z = \bigcup_{(B,Y) \in \mathcal{T}} Y.$$

We claim that

$$M_Z := M \cap R^{\oplus Z} = \bigoplus_{c \in C} Rc.$$

For $(\subseteq)$, pick an element $m \in M_Z$. We may write

$$m = (m_\alpha)_{\alpha \in Z}$$

where $m_\alpha \in R$ for each $\alpha \in Z$ and $m_{\alpha_i} \neq 0$ only for $i = 1, \dots, k$. As $\alpha_i \in Z$ and $\mathcal{T}$ is totally ordered, therefore for some $(B, Y) \in \mathcal{T}$, we have $\alpha_i \in Y$ for each $i = 1, \dots, k$. Thus, $m \in M \cap R^Y = \bigoplus_{b \in B} Rb$. In particular, $m \in \bigoplus_{b \in B} Rb \subseteq \bigoplus_{c \in C} Rc$ as $B \subseteq C$. This shows $(\subseteq)$. For $(\supseteq)$, pick any $(m_c)_{c \in C} \in \bigoplus_{c \in C} Rc$. Then $m_c = 0$ for all but finitely many $c_1, \dots, c_k$. As $\mathcal{T}$ is totally ordered and $m_{c_i} \in Rc_i$, therefore there exists $(B, Y) \in \mathcal{T}$ such that all $c_i \in B$ for $i = 1, \dots, k$. We then conclude that $m \in \bigoplus_{b \in B} Rb = M \cap R^{\oplus Y} \subseteq M \cap R^{\oplus Z}$, as needed. This shows that $(C, Z) \in \mathbb{T}$.

It is clear that for any $(B, Y) \in \mathcal{T}$, we have $(B, Y) \leq (C, Z)$ by construction. Hence we have produced an upper bound for any toset of $\mathbb{T}$. It follows by Zorn's lemma that $\mathbb{T}$ has a maximal element. Let it be denoted by $(\tilde{B}, \tilde{Y})$.

It now suffices to show that $\tilde{Y} = X$ as it would imply $M = M \cap R^{\oplus X} \in \mathbb{T}$, and hence is free. To this end, suppose $\tilde{Y} \subsetneq X$. Then there exists $\tilde{Y} \subsetneq Y'$ such that $Y' \setminus \tilde{Y}$ is finite. We shall now construct an element $(B', Y') \in \mathbb{T}$ such that $(\tilde{B}, \tilde{Y}) \leq (B', Y')$ and $(\tilde{B}, \tilde{Y}) \neq (B', Y')$, thus contradicting the maximality of $(\tilde{B}, \tilde{Y})$.

We first have the following exact sequence

$$0 \longrightarrow M \cap R^{\oplus \tilde{Y}} \xhookrightarrow{i} M \cap R^{\oplus Y'} \xrightarrow{\pi} \mathrm{CoKer}\,(()i) \longrightarrow 0 \tag{5.2}$$

We claim that $\mathrm{CoKer}\,(()i)$ is a free module. To this end, we first claim that

$$\mathrm{CoKer}\,(i) = \frac{M \cap R^{\oplus Y'}}{M \cap R^{\oplus \tilde{Y}}} \cong K$$

where $K \leq R^{\oplus Y' \setminus \tilde{Y}}$ is a submodule. Indeed, consider the map $\tilde{\varphi}$ obtained by the universal property of quotients

$$\begin{tikzcd}
M \cap R^{\oplus Y'} \arrow[r, "\varphi"] \arrow[d, two heads] & R^{\oplus Y' \setminus \tilde{Y}} \\
\frac{M \cap R^{\oplus Y'}}{M \cap R^{\oplus \tilde{Y}}} \arrow[ur, dashed, "\tilde{\varphi}"'] &
\end{tikzcd}$$

where φ is the R-linear map which takes $(m_\alpha)_{\alpha \in Y'} \mapsto (m_\alpha)_{\alpha \in Y' \setminus \tilde{Y}}$. It is clear that $\mathrm{Ker}\,(\varphi) = M \cap R^{\oplus \tilde{Y}}$. Consequently, $\tilde{\varphi}$ is an inclusion and let $K \leq R^{\oplus Y' \setminus \tilde{Y}}$ be its image.

As $Y' \setminus \tilde{Y}$ is finite and we showed above that every submodule of a finitely generated free module is free, therefore

$$K = \bigoplus_{z \in Z} Rz \cong R^{\oplus Z}.$$

where $Z \subseteq R^{\oplus Y' \setminus Y}$. This shows that $\mathrm{CoKer}\,(()i) \cong R^{\oplus Z}$ is a free R-module. In particular, it is projective. Consequently, the exact sequence of (5.2) is split exact so that there exists $j : \mathrm{CoKer}\,(()i) \hookrightarrow M \cap R^{\oplus Y'}$ such that $\pi j = \mathrm{id}_{\mathrm{CoKer}(()i)}$. It now follows immediately that

$$\begin{aligned} M \cap R^{\oplus Y'} &= \mathrm{Ker}\,(\pi) \oplus j\,(\mathrm{CoKer}\,(()i)) \\ &= \left(M \cap R^{\oplus \tilde{Y}}\right) \oplus j\,(\mathrm{CoKer}\,(()i)) \end{aligned}$$

where $j\left(\operatorname{CoKer}\left(()i\right)\right) \cong R^{\oplus Z}$ so it is free. Hence, we see that $B' \supseteq \tilde{B}$. This shows that $(B', Y') \geq (\tilde{B}, \tilde{Y})$, completing the proof. □

Statistics:-

- # Parts = 6
- # Chapters = 28
- # Definitions = ??
- # Remarks = ??
- # Lemmas = ??
- # Propositions = ??
- # Theorems = ??

Milestones:-

- Started : Somewhere in middle of December 2022.
- First 100 pages of Chapter 1 : 24th September, 2023.
- Total 400 pages : 8th October, 2023.
- The Arithmetic Viewpoint initiated on : 24th December, 2023.
- First 500 pages : 30th December, 2023.