McGill University - Winter 2019

Lecture Notes - MATH 571

Ralph Sarkis, David Marcil

January 24, 2026

Contents

Prerequisites

We recall some basic notions for completeness and to introduce the notation.

Definitions 1 (Basic definitions)**.** Let R be a commutative ring.

- An element $x \in R$ is a **unit** if it has a multiplicative inverse.
- An element $x \in R$ is **irreducible** if it is not a unit and it cannot be written as the product of two non-units.
- An element $x \in R$ is **prime** if for any $a, b \in R$, $x \mid ab$ implies $x \mid a$ or $x \mid b$.
- A subset $I \subseteq R$ is an **ideal** if $0 \in I$ and for any $a, b \in I$, $r \in R$, $a + rb \in I$. We denote $I \lhd R$.

- An ideal $I \lhd R$ is **prime** if $I \neq R$ and for any $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.
- An ideal $I \lhd R$ is **maximal** if $I \neq R$ and for any ideal $J \lhd R$ with $I \subseteq J \subseteq R$, either $I = J$ or $J = R$.
- We say that R is an **integral domain** if for any $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$ (equivalently, the ideal 0 is prime).
- R is a **principal ideal domain** (PID) if any ideal is generated by one element.
- R is a **unique factorization domain** (UFD) if any element can be written as a product of irreducible elements uniquely up to units and ordering.
- R **Noetherian** if all of its ideals are finitely generated.
- R **local** if it has a unique maximal ideal, or equivalently if the set $R - R^\times$ is an ideal of R.
- [1] Given a multiplicative set $S \subset R - \{0\}$, we can consider the **localization**

  $$R[S^{-1}] = S^{-1}R = \{\frac{r}{s} : r \in R, s \in S\}/\sim,$$

  where $\frac{r_1}{s_1} \sim \frac{r_2}{s_2}$ if $\exists\ s \in S$ such that $s(r_1 s_2 - r_2 s_2) = 0$. One can verify that $S^{-1}R$ is a commutative ring.
- If R is an integral domain, we denote $\mathrm{Frac}(R)$ to be the **fraction field** of R (i.e.: the localization R at the prime ideal 0).
- Let K be a field, a **field extension** is a field L containing K. The **degree** of the extension, denoted $[L : K]$ is the dimension of L as a K-vector space.
- A field extension L/K is **algebraic** if every element of L is a root of some polynomial in $K[x]$.
- A field extension L/K is **separable** if for every $\alpha \in L$, the minimal polynomial of α over K is separable in L (it splits in linear factors).
- Let R be a ring and M be a (left) R-module, the annihilator of an element $m \in M$ is $\mathrm{Ann}_M(m) = \{r \in R \mid rm = 0\}$. It is an ideal of R.

Facts 2 (Basic properties)**.**

Proposition 3. *Given a commutative ring R, the following conditions are equivalent :*

a) R is Noetherian

b) Every ascending chain of ideals

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n \subset \cdots,$$

there exists some $N \geq 1$ such that for all $m \geq N$, $\mathfrak{a}_m = \mathfrak{a}_N$.

[1] In general, the natural homomorphism $R \to S^{-1}R$ is not injective. It will be if and only if S does not contain zero divisors of R. In class, we only used in on integral domains, so this condition is always satisfied.

c) Every nonempty set S of ideals in R has a maximal element.

Definitions 4. A module M is said to be **Noetherian** if every submodule is finitely generated.[2]

Proposition 5. *Let R be a Noetherian ring. Every finitely generated R-module is Noetherian.*

In the first part of the course, we will only work with commutative rings (and mostly with integral domains), so all the rings will be commutative until we mention otherwise.

Rings of Dimension One

The main reference for this section is J.S. Milne's *Algebraic Number Theory*, chapter 1-3.

Krull dimension

Definition 6 (Krull dimension)**.** Let R be a ring, its **Krull dimension** is the maximal length[3] of a strict chain of inclusions of prime ideals in R.

Examples 7.

1. Let R be an integral domain. If its Krull dimension is zero, then R is a field. Indeed, since 0 is a prime ideal in an integral domain and every prime ideal is maximal when the Krull dimension is zero, we get $R/0 \cong R$ is a field.

2. The Krull dimension of $\mathbb{Z}$ is one. Since $\mathbb{Z}$ is a PID, we can write a chain of length two as $(a_1) \subset (a_2) \subset (a_3)$, where the a_i's are distinct prime and $a_2, a_3 \neq 0$ because no prime ideal is properly contained (0). Thus, we have two non-zero primes a_2 and a_3 with $a_3 \mid a_2$ which is absurd. An example of a chain of length one in $\mathbb{Z}$ is $0 \subset (2)$.

3. Let k be a field, then the Krull dimension of $k[x_1, \ldots, x_n]$ is n.

4. The ring $\mathbb{Z}[i]$[4] has Krull dimension one. We still have the chain $0 \subset (2)$ of length one, thus it is enough to show that if $\mathfrak{p}$ is a non-zero prime idea, then it is maximal. Pick some non-zero $a + bi \in \mathfrak{p}$ and let $n = (a+bi)(a-bi) \in \mathfrak{p}$, it is also non-zero, so $\mathbb{Z}[i]/(n) \cong \mathbb{Z}/n\mathbb{Z}[i]$ is finite. Moreover, since $(n) \subseteq \mathfrak{p}$, we infer that $\mathbb{Z}[i]/(n)$ maps surjectively onto $\mathbb{Z}[i]/\mathfrak{p}$ and then conclude the latter is a finite integral domain, hence a field.[5]

5. All the previous examples are UFDs but it is not true that a Krull dimension equal to one implies unique factorization. We can easily see that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD as $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are two decompositions in irreducibles. However, the same argument as for $\mathbb{Z}[i]$ works to show this ring has Krull dimension one.

Proposition 8. *If R has Krull dimension one and is a UFD, then it is a PID.*

Proof. Let I be a prime ideal of R, $r \in I$ and $r = p_1 \cdots p_t$ be the unique decomposition into primes. Without loss of generality, since I is prime, $p_1 \in I$ and we get a

[2] This definition and the following proposition are crucial in our proof of the algebraic statement of the Nullstellensatz.

[3] The length of a chain $I_0 \subset \cdots \subset I_n$ is n, i.e.: the number of inclusions (not the number of ideals).

[4] This is the ring $\mathbb{Z}$ adjoined with an element i that satisfies $i^2 = -1$. Equivalently, $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$.

[5] Pick any $a \neq 0$ in a finite integral domain R, then the multiplication map $x \mapsto ax$ must be injective, and by cardinality, it must also be surjective, yielding $ax = 1$ for some x. Note that this argument also holds when R is a finite dimensional vector space over a field because the multiplication map is linear and injectivity still implies surjectivity.

prime ideal $(p_1) \subseteq I$. Because R has Krull dimension one, (p_1) is maximal and we conclude $I = (p_1)$.

The proposition follows after a simple argument showing that if every prime ideal of R is principal, then R is a PID. Assume towards a contradiction that R is not a PID, then it has some non-principal ideals. Every chain of such ideals has an upper bound,[6] therefore, by Zorn's lemma, there exists a maximal non-principal ideal I.

We claim that I is prime. Suppose that $ab \in I$ and $a, b \notin I$, then (I, a) is strictly larger than I, hence principal, yielding $(I, a) = (c)$ for $c \in R$. Also, the set $I : a := \{r \in R \mid ra \in I\}$ is an ideal containing I and b, thus it is principal and we have $I : a = (d)$ for $d \in R$. Now, pick any $i \in I \subseteq (I, a) = (c)$, it can be written as uc, hence $u \cdot (c) \subseteq I$. In particular, we have $ua \in I$, or equivalently $u \in I : a = (d)$. We obtain $u = vd$ and $i = vcd$ which means $I \subseteq (cd)$.

However, we also have $(cd) \subseteq I$ because $da \in I$ implies $d(I, a) = d(c) \subseteq I$. We conclude that $I = (cd)$, but this contradicts the definition of I. □

Integrality

For the following, let R be an integral domain, $K = \mathrm{Frac}(R)$ and L be a field containing K.

Definition 9. An element $\alpha \in L$ is said to be **integral** over R if α is the root of a monic polynomial with coefficients in R.

Example 10. Say $R = \mathbb{Z}, K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. The element i is integral over $\mathbb{Z}$ since it solves $x^2 + 1 = 0$. The element $\frac{i}{2}$ is not integral because the minimal polynomial is $x^2 - \frac{1}{4} = 0$ and theorem 17.

Theorem 11. *The set of elements of L which are integral over R is a subring of L.*

We will give two different proofs of this theorem based on two different lemmas.

Lemma 12 (Newton). *Let $\{e_0, \dots, e_n\}$ be the elementary symmetric polynomials in n variables, namely,*

$$e_i(x_1, \dots, x_n) = \sum_{1 \le a_1 < \cdots < a_i \le n} x_{a_1} \cdots x_{a_i}.$$

All the symmetric polynomials[7] in $R[x_1, \dots, x_n]$ are R-generated by the elementary symmetric polynomials.

First proof of theorem 11. Let α and β be integral over R. Let $f \in R[x]$ be a monic polynomial that α satisfies. We can write

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - \alpha_1) \cdots (x - \alpha_n),$$

where $\forall 1 \le i \le n$, $a_i \in R$, the α_i's are in the splitting field of f and $\alpha = \alpha_1$. If we expand the R.H.S., we obtain

$$f(x) = \sum_{i=0}^{n} e_{n-i}(\alpha_1, \dots, \alpha_n) x^i,$$

so we have[8]

$$\forall 0 \le i \le n, e_{n-i}(\alpha_1, \dots, \alpha_n) = a_i \in R.$$

[6] Let $\{I_\alpha\}_{\alpha \in A}$ be a chain of non-principal ideals and let $I = \cup_{\alpha \in A} I_\alpha$, it is an upperbound for the chain because if I were principal, then $I = (x)$ would imply $x \in I_i$ and furthermore $I = (x) \subseteq I_i \subseteq I$, contradicting the non-principality of I.

[7] A polynomial p in several variables is said to be symmetric if $p \circ \sigma = p$ for any permutation σ of the variables.

[8] In words, applying elementary symmetric polynomials to $\alpha_1, \dots, \alpha_n$ yields elements of R.

By Newton's lemma, we infer that for any symmetric polynomial $p \in R[x_1, \dots, x_n]$, $p(\alpha_1, \dots, \alpha_n) \in R$.

Let g be the monic polynomial of $R[x]$ that β satisfies and write $g = (x - \beta_1) \cdots (x - \beta_m)$. We can conclude in the same way that for any symmetric polynomial $p \in R[x_1, \dots, x_m]$, $p(\beta_1, \dots, \beta_m) \in R$.

Let

$$h(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - (\alpha_i + \beta_j)).$$

Note that the coefficients of h are symmetric polynomials in $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_m$, and, by appropriately regrouping the terms, we can see them as symmetric polynomials in $\alpha_1, \dots, \alpha_n$ with coefficients being symmetric polynomials in $\beta_1, \dots, \beta_m$. By the previous observation, we conclude $h(x) \in R[x]$. Since h is monic and has $\alpha + \beta$ as a root, we have shown that $\alpha + \beta$ is integral. A similar construction works to show $\alpha\beta$ is integral. □

Corollary 13. *More generally, for any polynomial $g \in R[x_1, \dots, x_n]$ and integral elements $\alpha_1, \dots, \alpha_n \in L$, $g(\alpha_1, \dots, \alpha_n)$ is integral.*

Lemma 14. *An element $\alpha \in L$ is integral over R if and only if there exists a finitely generated R-submodule M of L such that $\alpha M \subseteq M$.*

Proof. ($\Rightarrow$) Let $f \in R[x]$ be a monic polynomial, say of degree n, that α satisfies. Observe that $M = R[\alpha]$ is finitely generated as a module because it is generated by $1, \alpha, \dots, \alpha^{n-1}$.[9] It is clear that $\alpha M \subseteq M$.

($\Leftarrow$) Suppose that $M = Re_1 + \cdots + Re_m$ is a finitely generated R-module and $\alpha M \subseteq M$. Since for any $1 \leq i \leq n$, αe_i can be written as an R-linear combination of the e_j's, we have a matrix $A \in M_n(R)$ such that $A[e_1, \dots, e_n]^t = \alpha[e_1, \dots, e_n]^t$. Let $f_A = \det(xI_n - A)$ be the characteristic polynomial of A, it is a monic polynomial in $R[x]$ by definition. Moreover, we know that $f_A(\alpha) = 0$ because α is an eigenvalue of A, so we conclude that α is integral. We may also conclude this from Cayley-Hamilton which tells us that $f_A(A)$ is identically the zero map, then evaluating $f_A(A)$ at any non-zero $v \in M$ yields $f_A(\alpha) = 0$. □

Second proof of theorem 11. Let α and β be integral over R and let $M = Re_1 + \cdots + Re_n$ and $N = Rf_1 + \cdots + Rf_m$ be the modules that satisfy the condition of the lemma for α and β respectively.

It is clear that $MN = \{xy \mid x \in M, y \in N\}$ is stable under multiplication by both α and β and MN is clearly generated by $\{e_i f_j \mid i \in [n], j \in [m]\}$. Therefore, $\alpha + \beta$ and $\alpha\beta$ are integral over R. □

Definition 15. The ring of elements of L which are integral over R is called the **integral closure** of R in L.

Definition 16. An integral domain R is said to be **integrally closed** if the integral closure of R in $\mathrm{Frac}(R)$ is R itself.

Proposition 17. *Assume that R is integrally closed. An element $\alpha \in L$ is integral over R if and only if its minimal polynomial is contained in $R[x]$.*

[9] If we isolate α^n in $f(\alpha)$, we see that all higher powers of α are R-generated by the powers less than n.

Proof. ($\Leftarrow$) Follows from the definition of integrality and the fact that the minimal polynomial is monic.

($\Rightarrow$) Let f be the minimal polynomial of α over K. For any root β of f, we know[10] that there exists an isomorphism $\phi : K[\alpha] \to K[\beta]$ such that $\phi(\alpha) = \beta$ and $\phi|_K = \mathrm{id}_K$. Let $p \in R[x]$ be the monic polynomial that α satisfies, we see from applying ϕ to p that β also satisfies it and hence any root of f is integral over R. Finally, writing $f = (x - \alpha_1) \cdots (x - \alpha_n)$ and expanding, we see that the coefficients of f, being polynomials of integral elements, are integral as well (by corollary 13). As R is assumed to be integrally closed and the coefficients lie in K, it follows that they are contained in R, hence we conclude that $f \in R[x]$ as desired. □

Proposition 18. *Assume L/K is an algebraic extension. If S is the integral closure of R in L, then L/S is a torsion R-module.*

Proof. We will show that if $\alpha \in L$, then there exists $d \in R$, such that $d\alpha \in S$. If $\alpha \in L$, then there is a monic polynomial with coefficients in K satisfied by α (since L is algebraic), $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in K$. We can find a non-zero $d \in R$ such that $da_i \in R$ for all $1 \leq i \leq n$.[11] We see that $d\alpha$ satisfies

$$y^n + da_{n-1}y^{n-1} + \cdots + d^{n-1}a_1 y + d^n a_0$$

which is monic and has coefficients in R. The proposition follows. □

Corollary 19. *The field of fractions of S is L.*[12]

Proposition 20. *If R is a UFD, then R is integrally closed.*

Proof. Let $\alpha = \frac{a}{b} \in K$ be an integral element, since R is a UFD, we can assume that a and b have no common irreducible factors. If $b \in R^\times$, then $\alpha \in R$.

Otherwise, there exists an irreducible element $\pi \in R$ such that $\pi \mid b$. By integrality of α, we have

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\frac{a}{b} + c_0 = 0$$

If we multiply this by b^n, we see that π divides the R.H.S. and all terms other than the first in the L.H.S., and this leads to a contradiction.[13] We conclude that α being integral implies $\alpha \in R$. □

Examples 21.

1. By the last result, $\mathbb{Z}$ and $\mathbb{Z}[i]$ are integrally closed because they are UFDs.

2. By the contrapositive of the last proposition, any ring which is not integrally closed is not a UFD. For instance, $\mathbb{Z}[2i]$ is not integrally closed (because $i \notin \mathbb{Z}[2i]$ is integral over $\mathbb{Z}$) one can indeed verify that it is not a UFD. [14]

3. Let us find for which n, $R = \mathbb{Z}[\sqrt{n}]$ is integrally closed. The field of fraction is $K = \mathbb{Q}(\sqrt{n})$ and every element is of the form $a + b\sqrt{n}$ with $a, b \in \mathbb{Q}$.

   If n is a square, then $R = \mathbb{Z}$ nad $K = \mathbb{Q}$, so R is integrally closed.

[10] This is an important fact usually proved in an introduction to Galois theory course.

[11] For instance, we can let d be the product of the denominators of the a_i's.

[12] Any element $\alpha \in L$ can be identified with $\frac{d\alpha}{d} \in \mathrm{Frac}(S)$ as seen above. The corollary then follows because $\mathrm{Frac}(S)$ is the smallest field containing S.

[13] Observe that $\pi \mid 0$ always holds and all terms but the first in the L.H.S. are multiples of b, hence multiples of π. However, the first term is a^n and π cannot divided, or a and b would have common factors.

[14] Recall that if p is prime and $p \equiv 1 \pmod 4$, then there exists $a \in 2\mathbb{Z}$ and $b \notin 2\mathbb{Z}$ such that $p = a^2 + b^2$. In other words, we have $a + bi \notin \mathbb{Z}[2i]$ and $|a + bi| = p$.

Let $p_1, \ldots, p_n$ be such primes with decompositions $p_j = a_j^2 + b_j^2$. Then,

$$\alpha_{j,k} = (a_j + ib_j)(a_k + ib_k) \in \mathbb{Z}[2i]$$

is irreducible because it factorizes in irreducible elements in the bigger ring $\mathbb{Z}[i]$. It is clear that

$$\alpha_{1,2}\alpha_{3,4} = \alpha_{1,3}\alpha_{2,4},$$

so $\mathbb{Z}[2i]$ does not have a unique factorization.

If $n = d^2m$ with $d > 1$, then $\sqrt{m} = \frac{\sqrt{d^2m}}{d} \in \mathbb{Q}(\sqrt{n})$ is a root of $x^2 - m \in \mathbb{Z}[x]$, but $\sqrt{m} \notin \mathbb{Z}[\sqrt{n}]$. Hence, $\mathbb{Z}[\sqrt{n}]$ is not integrally closed.

Assume n is square-free.

Definition 22. A ring extension S/R is **integral** if $\forall \alpha \in S$, α is integral over R.

Proposition 23. *If S/R is integral and finitely generated as an R-algebra, then S is finitely generated as an R-module.*

Proof. We proceed by induction on n, the number of generators of S as an R-algebra. If $n = 1$, then $S = R[\alpha]$, but α is integral, so S is finitely generated as a module (it is generated by $1, \alpha, \ldots, \alpha^{n-1}$).

Suppose it is true for n and write $S = R[\alpha_1, \ldots, \alpha_n][\alpha_{n+1}]$. By induction hypothesis, we have $R[\alpha_1, \ldots, \alpha_n] = R\beta_1 + \cdots + R\beta_N$ as an R-module. Moreover, since α_{n+1} is integral, S is finitely generated as a $R[\alpha_1, \ldots, \alpha_n]$-module. It follows that S is finitely generated R-module. □

Remark 24. If S_2 is a finitely generated integral extension of S_1 and S_1 is a finitely generated integral extension of R, then S_2 is a finitely generated integral extension of R.

Example 25. We want to illustrate the connection between integrality and smoothness.

Let $R = k[x]$, where k is algebraically closed of characteristic 0. Formally, we have $\text{Spec}(R) = \mathbb{A}^1_k = \{(x-a) : a \in k\} \cup \{(0)\}$, but one can simply see $\mathbb{A}^1_k = k \cup \{*\}$ by identifying $(x-a)$ with a and (0) with $*$.[15] Thus, $\text{Spec}(R) = k \cup \{*\}$ can geometrically be seen as a 1-dimensional k-line, with an extra point "at infinity". Formally, the point at infinity certainly has its importance, but for this example, think nothing of it. We see that R is integrally closed and that $\text{Spec}(R)$ is smooth.

In contrast, let $S = k[x,y]/(p(x,y))$ for some polynomial p, of degree d in y. The structure of $\text{Spec}(S)$ is slightly more complicated now (it is a variety V_p in $\mathbb{A}^2_k$), but we can think of it geometrically as the zero locus of $p(x,y) = 0$ in k^2. As $R \subset S$, we have that V_p is related to $\text{Spec}(R)$ from the projection $\text{Spec}(S) = V_p \to \mathbb{A}^1_R = \text{Spec}(R)$ that maps $(a,b) \mapsto a$. Since k is algebraically closed, we know that given any point $a \in k$, there exists d solutions (counting multiplicities) of $p(a,y) = 0$, so we can think of V_p as a d-sheeted cover of $\mathbb{A}^1_k$ (i.e. there are d points of V_p above any given point of $\mathbb{A}^1_k$).

If we pick the concrete example $S = k[x,y]/(y^2 - x^2(x+1))$, we want to show that it is not integrally closed. This is not hard as $\frac{y}{x}$ satisfies $t^2 - (x+1)$. Moreover, the solution set V_p of $y^2 = x^2(x+1)$ (i.e. $\text{Spec}(S)$) is not a smooth curve since the point $(0,0)$ is a singularity[16].

As an exercise, one can try to show that the integral closure of $R = k[x]$ in $\text{Frac}(S)$ is $\tilde{S} = k[x][\sqrt{x+1}] = k[x,y]/(y^2 - (x+1)) \cong k[y]$. This would again provide evidence of an integrally closed ring $\tilde{S}$ such that $\text{Spec}(\tilde{S}) = \mathbb{A}^1_k = k$ is smooth. Moreover, one can check that the natural inclusion $S \subset \tilde{S}$ now provides the map $\text{Spec}(\tilde{S}) = \mathbb{A}^1_k \to \text{Spec}(S) = V_p$ as $a \mapsto (a^2 - 1, a(a^2-1))$. [17] In algebraic geometry, we say that this map provides is the *resolution of singularity* of $\text{Spec}(S)$. One can take $k =$ and plot the "$\mathbb{R}$ part" of $a \mapsto (a^2 - a, a(a^2-1))$ to see that this essentially takes

[15] The spectrum of a ring R, denoted $\text{Spec}(R)$, is the set of prime ideals of R, it will be further studied in a later section. We will learn to see $\text{Spec}(R)$ as a geometric object associated to R. In general, an inclusion $R \subset S$ corresponds to a map $\text{Spec}(S) \to \text{Spec}(R)$. We want to give evidence here that the integral closure of R ensures the smoothness of $\text{Spec}(R)$ and vice-versa.

[16] Namely, $\frac{\partial F}{\partial x}(0,0) = \frac{\partial F}{\partial y}(0,0) = 0$ for $F = y^2 - x^2(x+1)$

[17] This example is trying to motivate the notion of integrality, but one does not really need to understand it to move on in the notes.

the real line and "loops it" to cover the "nodal curve" $y^2 = x^2(x+1)$ (plot in Desmos to understand this name). This cover is one-to-one, except over the singularity $(0,0)$ where both $0, 1 \in \mathbb{R}$ map to it, so this map can be seen as pulling apart both branches of the "nodal curve", creating a smooth line. This motivates the name for "resolution of singularity".

Our next big goal is motivated by the following construction. Let K be a finite extension of $\mathbb{Q}$ (resp. of $k(x)$, with k a finite field). The integral closure of $\mathbb{Z}$ (resp. of $k[x]$) in K is called the ring of integers of K and denoted $\mathcal{O}_K$. More generally, if L is a finite extension of K, then $\mathcal{O}_K \subset \mathcal{O}_L$. We know that $L \cong K^n$ as a K-module, where $n = [L : K]$.

Question 26. *Is it true that $\mathcal{O}_K \cong \mathbb{Z}^n, n = [K : \mathbb{Q}]$ or $\mathcal{O}_L \cong \mathcal{O}_K^m, m = [L : K]$?*

We will see that the answers are yes and no respectively.

Definition 27. Let R be an integral domain. An R-module M is said to be **free** if M has an R-basis.[18]

Remark 28. Let S be an R-algebra which is free of finite rank over R. For an element $\alpha \in S$, we can define $m_\alpha : S \to S$ to be the endomorphism sending x to αx. If $e_1, \ldots, e_n$ forms an R-basis for S, then we can see m_α as an $n \times n$ matrix with entries in R.

Definition 29. In the setting of the above remark, we define the **trace** of α as the sum of the diagonal elements of the matrix m_α and denote it $\mathrm{Tr}_{S/R}(\alpha)$. The **norm** of α is the determinant of this matrix and we denote it $\mathrm{Nm}_{S/R}(\alpha)$. Note that the trace and norm are invariant on the choice of basis.

Example 30. Consider the Hamilton quaternion $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$. Given an element $\alpha = a + bi + cj + dk \in \mathbb{H}$, one can define $\mathrm{Tr}(\alpha) = 2a$ and $\mathrm{Nm}(\alpha) = a^2 + b^2 + c^2 + d^2$. On the other hand, recall that there is an embedding $\mathbb{H} \subset M_2()$ given from

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \;\; ; \;\; i \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \;\; ; \;\; j \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \;\; ; \;\; k \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

then one readily verifies that the trace of an element corresponds to its trace as a matrix, and its norm is its determinant. This can serve as motivation for our definitions above.

Proposition 31. *[Some properties of the trace and norm] For any $\alpha_1, \alpha_2 \in S$ and $a \in R$, we have*

$$\begin{aligned} \mathrm{Tr}_{S/R}(\alpha_1 + \alpha_2) &= \mathrm{Tr}_{S/R}(\alpha_1) + \mathrm{Tr}_{S/R}(\alpha_2) \\ \mathrm{Tr}_{S/R}(a\alpha_1) &= a\,\mathrm{Tr}_{S/R}(\alpha_1) \\ \mathrm{Nm}_{S/R}(\alpha_1\alpha_2) &= \mathrm{Nm}_{S/R}(\alpha_1)\,\mathrm{Nm}_{S/R}(\alpha_2) \\ \mathrm{Nm}_{S/R}(a\alpha_1) &= a^n\,\mathrm{Nm}_{S/R}(\alpha_1). \end{aligned}$$

Definition 32. Let $K < L$ be an extension of fields, we define the **trace form** on L/K as $\langle a, b \rangle = \mathrm{Tr}_{L/K}(ab)$ for any $a, b \in L$. Using the properties in proposition 31, one can show that $\langle \cdot, \cdot \rangle$ is K-bilinear.

Proposition 33. *Suppose that L/K is separable, then $\langle \cdot, \cdot \rangle$ is non-degenerate, i.e.:*

$$\{a \in L \mid \langle a, x \rangle = 0, \forall x \in L\} = \{a \in L \mid \langle x, a \rangle = 0, \forall x \in L\} = \{0\}.$$

[18] i.e.: there exists a set $\{e_\alpha\}_{\alpha \in I}$ that is linearly independent and generates M. If, in addition, M is finitely generated, then $M \cong R^n$ where $n = |I|$.

We need the following lemma that we state without proof.

Lemma 34. *A field extension $L < K$ is separable if and only if* $\mathrm{Tr}_{L/K} \not\equiv 0$.

Proof of proposition 33. Assume towards a contradiction that $0 \neq a \in L$ is such that $\langle a, x \rangle = 0$ for all $x \in L$, then $aL \subseteq \{\ell \in L \mid \mathrm{Tr}_{L/K}(\ell) = 0\}$. On the other hand, since the multiplication map $a : L \to L$ is an isomorphism of K-vector spaces (its inverse being multiplication by a^{-1}), we have $aL = L$. Thus, all elements have trace zero, but this contradicts the lemma. □

As a consequence of this result, we get a K-vector space isomorphism $L \to \mathrm{Hom}(L, K)$ that sends a to $\langle a, \cdot \rangle$.[19] If $\{\gamma_1, \dots, \gamma_d\}$ is a basis for L as a K-vector space, then we write $\gamma_1^*, \dots, \gamma_d^*$ for the dual basis of L^* where $\gamma_j^*(\gamma_k) = \delta_{j,k}$ (Kronecker delta). The isomorphism lets us think of these basis elements as living in L and write

$$\left\langle \gamma_i, \gamma_j^* \right\rangle = \delta_{i,j}.$$

Proposition 35. *Let L/K be an extension of fields of degree n, and let $\beta \in L$ with minimal polynomial f over K. Say that $\beta_1, \dots, \beta_m$ are the disctinc roots of f in L. Then,*

$$\mathrm{Tr}_{L/K}(\beta) = r(\beta_1 + \cdots + \beta_m) \quad \text{and} \quad \mathrm{Nm}_{L/K}(\beta) = (\beta_1 \cdots \beta_m)^r$$

where $r = [L : K[\beta]] = n/m$.

Corollary 36. *Let L/K and β be as above. If L/K is separable, with* $\mathrm{Aut}(L/K) = \{\sigma_1, \dots, \sigma_n\}$, *then*

$$\mathrm{Tr}_{L/K}(\beta) = \sigma_1\beta + \cdots + \sigma_n\beta) \quad \text{and} \quad \mathrm{Nm}_{L/K}(\beta) = \sigma_1\beta \cdots \sigma_n\beta$$

and so, if we also have that R is integrally closed and $\beta \in L$ is integral over R, then both $\mathrm{Tr}_{L/K}(\beta)$ *and* $\mathrm{Nm}_{L/K}(\beta)$ *are in R.*

Proposition 37. *Assume that R is integrally closed in $K = \mathrm{Frac}(R)$, let $K < L$ be a separable field extension of degree d and S be the integral closure of R in L. Then, there exist free R-modules Ω and Ω^* of rank d in L such that $\Omega \subseteq S \subseteq \Omega^*$.*

Proof. Let $\gamma_1, \dots, \gamma_d$ be a basis for L/K. By proposition 18, there exists some $0 \neq a \in R$ such that $a\gamma_i \in S$ for all i. Set $\gamma_i = a\gamma_i$, they still form a linearly independent set over K, hence $\Omega = R\gamma_1 \oplus \cdots \oplus R\gamma_d$ is a free R-submodule of L and clearly $\Omega \subseteq S$.

Let $\Omega^* = R\gamma_1^* \oplus \cdots \oplus R\gamma_d^*$ (with the identification of γ_i^* in L). We claim that $S \subseteq \Omega^*$. If $\alpha \in S$, then we can write $\alpha = x_1\gamma_1^* + \cdots + x_d\gamma_d^*$ where $x_i \in K$, since $\{\gamma_1^*, \dots, \gamma_d^*\}$ also provides a K-basis of L. Since $\langle \cdot, \cdot \rangle$ is K-bilinear, we have

$$\mathrm{Tr}_{L/K}(\alpha \cdot \gamma_j) = \langle \alpha, \gamma_j \rangle = \sum_{i=1}^{d} x_i \left\langle \gamma_i^*, \gamma_j \right\rangle = x_j.$$

As α, $\gamma_j \in S$, we know that $x_i = \mathrm{Tr}(\alpha\gamma_j) \in R$ from corollary 36. The proposition follows. □

Corollary 38. *If R is Noetherian, then S is a finitely generated R-module. If R is a PID, then $S = R^d$.*

Theorem 39. *Let S be the integral closure of R in a separable extension L/K of degree d. Then, S be a finitely generated R-module and if R is PID, then S is free of rank d over R.*

[19] The fact that the trace form is bilinear and non-degenerate yields injectivity and surjectivity follows because both sides have the same dimension.

Dedekind Domains

Definition 40. An integral domain R is a **Dedekind domain** if

(i) R is Noetherian (finiteness),

(ii) R is integrally closed (smoothness), and

(iii) Every non-zero prime ideal of R is maximal.[20]

Example 41. We have already seen that $\mathbb{Z}[i]$ satisfy theses three properties,[21] so they are Dedekind domains.

Proposition 42. *If R is a Dedekind domain and $S \subseteq R \setminus \{0\}$ is a multiplicative set, then $R[S^{-1}]$ is also a Dedekind domain.*

Proof. We will prove that if R satisfies any property from the definition above, then $R[S^{-1}]$ also satisfies it.

(i) Suppose R is Noetherian and let $\mathfrak{a} \lhd R[S^{-1}]$, we have $\mathfrak{a} = (\mathfrak{a} \cap R)[S^{-1}]$. Moreover, since R is Noetherian, $\mathfrak{a} \cap R$ is finitely generated by $x_1, \dots, x_n \in R$, but then $x_1, \dots, x_n$ also generate $\mathfrak{a}$ as an $R[S^{-1}]$ module. We conclude that any ideal of $R[S^{-1}]$ is finitely generated, so $R[S^{-1}]$ is Noetherian.

(ii) Suppose R is integrally closed and let $\alpha \in \text{Frac}(R) = \text{Frac}(R[S^{-1}])$ be integral over $R[S^{-1}]$, then α satisfies the polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in R[S^{-1}]$. By the construction of $R[S^{-1}]$, there exists $s \in S$ such that $sa_i \in R$ for every i. Multiplying the polynomial by s^n, we find that $s\alpha$ satisfies a monic polynomial with coefficients in $R[x]$.[22] Since R is integrally closed, $sa \in R$, implying $a \in R[S^{-1}]$. We conclude that $R[S^{-1}]$ is integrally closed.

(iii) Suppose R has Krull dimension one. Recall that $\text{Spec}(R[S^{-1}]) = \text{Spec}(R) \setminus I_S$ where I_S is the set of prime ideals of R that intersect S. Moreover, we have the following natural correspondence for $a \in \text{Spec}(R[S^{-1}])$: $R[S^{-1}]/a \cong R/(a \cap R)$. However, $a \cap R$ is a non-zero prime ideal, so it must be maximal. This implies the R.H.S. is a field, so the L.H.S. is also a field, yielding that a is a maximal ideal. We conclude that $R[S^{-1}]$ has Krull dimension one.

□

Corollary 43. *If $\mathfrak{p}$ is a prime ideal of a Dedekind domain R, then $R_{\mathfrak{p}}$[23] is a Dedekind domain with a unique non-zero prime ideal $\mathfrak{p}R_{\mathfrak{p}}$.*

Proof. We just saw that $R_{\mathfrak{p}}$ is a Dedekind domain. Assume towards a contradiction that there is a non-zero prime ideal other than $\mathfrak{p}R_{\mathfrak{p}}$, by one-dimensionality, it cannot be contained or contain $\mathfrak{p}R_{\mathfrak{p}}$. Hence, it contains some $0 \neq x \in R_{\mathfrak{p}} \setminus \mathfrak{p}R_{\mathfrak{p}}$. We can write $x = \frac{a}{b}$ where $a, b \in R \setminus \mathfrak{p}$ are non-zero, thus x is a unit with inverse $\frac{b}{a}$, thus this ideal is the whole ring, contradicting its primeness. □

Definition 44. A Dedekind domain which is local (i.e.: has a unique non-zero prime ideal) is called a discrete valuation ring (DVR).

[20] Note that a Dedekind can have Krull dimension zero or one. In the former, the last property is vacuously satisfied.

[21] They are Noetherian because they are the quotient of the Noetherian ring $\mathbb{Z}[x]$, they are integrally closed by examples 21 and they have Krull dimension one by examples 7.

[22]
$$s^n\alpha^n + s^n a_{n-1}\alpha^{n-1} + \cdots + s^n a_0 = 0$$
$$(s\alpha)^n + sa_{n-1}(s\alpha)^{n-1} + \cdots + s^n a_0 = 0$$

[23] If $\mathfrak{p}$ is a prime ideal, then $R - \mathfrak{p}$ is a multiplicative set not containing 0 and $R_{\mathfrak{p}}$ denotes the localization of R at $R - \mathfrak{p}$.

Proposition 45. *Assume R is Noetherian.*[24] *If all the localizations at non-zero prime ideals of R are DVR's, then R is a Dedekind domain.*

Proof. We need to show that $R_{\mathfrak{p}}$ being Dedekind for all $\mathfrak{p} \in \operatorname{Spec}(R)$ implies R is Dedekind. Suppose all the localizations at prime ideals are Dedekind domains, then we show R satisfies each property.

(i) By assumption.

(ii) Let $\alpha \in \operatorname{Frac}(R)$ be integral over R and $\mathfrak{a} = \{x \in R \mid x\alpha \in R\} \lhd R$. For all prime ideals $\mathfrak{p}$, α is integral over $R_{\mathfrak{p}}$ (since $R \subseteq R_{\mathfrak{p}}$), so $\alpha \in R_{\mathfrak{p}}$ because $R_{\mathfrak{p}}$ is integrally closed. Then, there exists $s \in R - \mathfrak{p}$ such that $s\alpha \in R$, thus the ideal $\mathfrak{a}$ is not contained in $\mathfrak{p}$. Letting $\mathfrak{p}$ vary over $\operatorname{Spec}(R)$, we conclude that $\mathfrak{a}$ is not contained in any maximal ideal implying $\mathfrak{a} = R$. Since $1 \in \mathfrak{a}$, $1\alpha = \alpha \in R$, so R is also integrally closed.

(iii) Assume $\mathfrak{p}$ be a non-zero prime ideal that is not maximal, then it is contained in another prime ideal $\mathfrak{q}$. However, we observe that $\mathfrak{p}R_{\mathfrak{q}} \subset \mathfrak{q}R_{\mathfrak{q}}$ are also non-zero prime ideals of $R_{\mathfrak{q}}$ and this contradicts the fact $R_{\mathfrak{q}}$ is a DVR.

□

Theorem 46. *Let A be a DVR (and not a field) and $\mathfrak{p} \lhd R$ be the unique prime ideal, then $\mathfrak{p}$ is a principal ideal.*

Proof. Let $0 \neq c \in A \setminus A^{\times}$. Observe that $A/(c)$ is a non-zero A-module so we can choose $0 \neq b + (c) \in A/(c)$ such that $I = \operatorname{Ann}_{A/(c)}(b + (c)) \lhd A$ is maximal among all choices of b.[25] In other words, we choose b such that there is no proper ideal of A which arises as $\operatorname{Ann}_{A/(c)}(x + (c))$ for some $x \in A$ and properly contains I.

First, we claim that I is a non-zero prime ideal. Suppose $x, y \in A$ and $xy \in I$, namely, $xyb \in (c)$. If $x \notin I$, then $xb \notin (c)$ and $xb + (c)$ is non-zero in $A/(c)$. Let $I' = \operatorname{Ann}_{A/(c)}(xb + (c))$, we clearly have $I' \supseteq I$ and $I' \supseteq (y)$.[26] Therefore, $I' = I$ by maximality of I and we obtain $y \in I$. We conclude that I is prime (it is not the whole ring by definition and it is non-zero because $c \in I$).

Second, we must have $\mathfrak{p} = I$, so it is enough to show that I is principal. Since c is not a unit, $\frac{b}{c} \in \operatorname{Frac}(A)$ is not in A. Furthermore, by definition of I, $\frac{b}{c}I \lhd A$. Assume towards a contradiction that $\frac{b}{c}I \subseteq I$, then since I is a finitely generated A-module[27], we find that $\frac{b}{c}$ is integral (by proposition 14) and $\frac{b}{c} \in A$ by integral closure, so we get a contradiction. Thus, we must have $\frac{b}{c}I = A$, then $I = (\frac{c}{b})$. In particular, b divides c and $\pi = \frac{c}{b}$ is a generator for $I = \mathfrak{p}$. □

Proposition 47. *If A is a DVR, then A is a PID.*

Proof. Let π be a generator of $\mathfrak{p}$, the unique non-zero prime ideal of A and let $I \lhd A$. We will show that I is generated by one element. Consider the sequence $I \subseteq \pi^{-1}I \subseteq \pi^{-2}I \subseteq \cdots$ in the fraction field $K = \operatorname{Frac}(A)$. We claim that $\pi^{-j}I \neq \pi^{-(j+1)}$ for any j, otherwise $\pi^{-1}(\pi^{-j}I) \subseteq \pi^{-j}I$ implies that π^{-1} is integral[28] and hence $\pi^{-1} \in A$ contradicting the primeness of $\mathfrak{p} = (\pi) = A$. We conclude that this sequence is

[24] This assumption is necessary as there exists non-Noetherian domains with all their localizations being DVR's. Instead of assuming R is Noetherian, one could also assume every non-zero element of R is contained in finitely many maximal ideals.

[25] This choice can be made because A is Noetherian, thus every collection of ideals (in our case $\{\operatorname{Ann}_{A/(c)}(m) \mid m \in A/(c) \setminus \{0\}\}$) has a maximal element.

[26] If $ab \in (c)$, then $axb \in (c)$, so

$$I' = \operatorname{Ann}_{A/(c)}(xb + (c)) \supseteq \operatorname{Ann}_{A/(c)}(b + (c)) = I,$$

and since $yxb + (c) = 0$, we have $(y) \in \operatorname{Ann}_{A/(c)}(xb + c)$.

[27] Since A is Noetherian.

[28] It follows from proposition 14 and the fact that $\pi^{-j}I$ is finitely generated because A is Noetherian.

strictly increasing. Since A is Noetherian, there must be some j such that $\pi^{-j}I \subseteq A$ and $\pi^{-1}(\pi^{-j}I) \not\subseteq A$, thus $\pi^{-j}I \not\subseteq (\pi)$. However, (π) is the only maximal ideal, so we must have $\pi^{-j}I = A$ and we obtain $I = \pi^j A = (\pi^j)$. □

Corollary 48. *Every ideal of a DVR is generated by π^j where $j \in \mathbb{N}$ and π is the generator of the unique prime ideal.*

Corollary 49. *If A is a DVR, then every $a \in A$ can be written as $u\pi^n$ where $n \geq 0$ and $u \in A^\times$.*

Proof. Write $(a) = (\pi^j)$ for some j and conclude that a and π^j must be associates.[29] □

Corollary 50. *Every element of $K = \operatorname{Frac}(A)$ can be written as $u\pi^j$ where $j \in \mathbb{Z}$ and $u \in A^\times$.*

Definition 51. We define j to be the valuation of a in A and write $v(a) = j$. We also write $v(a) = \operatorname{ord}_\pi(a)$.

Proposition 52. *$v(ab) = v(a) + v(b)$ and $v(a+b) \geq \min\{v(a), v(b)\}$.*[30]

Example 53. Recall that $A = \mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain but $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are two decompositions of 6 into irreducibles, so it is not a UFD. We can also write the prime ideal decomposition $(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{5})(3, 1-\sqrt{5})$.

Let $\mathfrak{p} = (3, 1+\sqrt{-5})$, it is a prototypical example of a non-principal ideal in $\mathbb{Z}[\sqrt{-5}]$. Consider the localization of A at $\mathfrak{p}$ and the ideal that $\mathfrak{p}$ generates. It is now principal because $1+\sqrt{-5}$ divides both $1+\sqrt{-5}$ and 3 (as $3 = \frac{1-\sqrt{-5}}{2} \cdot (1+\sqrt{-5})$).

Exercise 54. Show that $(2, 1+\sqrt{-5})$ is principal in $A_\mathfrak{p}$ with $\mathfrak{p} = (2, \sqrt{-5})$, but $(2, 1+\sqrt{-5}) \neq (2)$.

Our next goal is to show that ideals have unique decompositions as prime ideals in Dedekind domains.

Lemma 55. *Suppose A is a Noetherian integral domain, then any ideal $I \lhd A$ contains a product of prime ideals.*

Proof. Let Σ be the set of ideals $I \lhd A$ which do not contain a product of prime ideals. Assume towards a contradiction that Σ is not empty, let J be a inclusion-wise maximal in Σ.[31] In particular, J is not prime, so there exists $a, b \notin J$, $ab \in J$. Let $J_1 = (a) + J$ and $J_2 = (b) + J$, by maximality, we can find prime ideals $p_1, \dots, p_r$ and $q_1, \dots, q_s$ such that $J_1 = p_1 \cdots p_r$ and $J_2 = q_1 \cdots q_s$, thus $J \supset J_1 J_2 \supseteq p_1 \cdots p_r q_1 \cdots q_s$, which contradicts $J \in \Sigma$. □

Lemma 56. *If I and J are relatively prime ideals*[32]*, then so are I^m and J^n for any $m, n \in \mathbb{N}$.*

Proof. Since $I + J = A$, there exists $i \in I$ and $j \in J$ such that $1 = i + j$ and we can write

$$1 = 1^{m+n} = (i+j)^{m+n} = \sum_{k=0}^{m+n} i^{m+n-k} j^k.$$

[29] i.e.: there exists $u \in A^\times$ such that $a = u\pi^n$.

[30] Write $a = u\pi^i$ and $b = u'\pi^j$, without loss of generality, $i \leq j$. Then,

$$ab = u\pi^i u'\pi^j = u''\pi^{i+j},$$

so $v(ab) = i + j = v(a) + v(b)$. Also,

$$a + b = \pi^i(u + u'\pi^{j-i}) = \pi^i(u''\pi^k) = u''\pi^{i+k},$$

hence $v(a+b) \geq \min\{v(a), v(b)\}$.

[31] A being Noetherian guarantees the existence of J.

[32] i.e.: $I + J = A$.

Notice that every term of the R.H.S. is either divisible by i^m or by j^n, thus $1 \in I^m + J^n$. The lemma follows. □

Lemma 57. *Let A be a Dedekind domain. For any prime ideal $\mathfrak{p} \lhd A$, the inclusion $A \hookrightarrow A_{\mathfrak{p}}$ induces an isomorphism $A/\mathfrak{p}^n \cong A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}$ for any $n \in \mathbb{N}$.*

Proof. Fix $n \in \mathbb{N}$, let $f : A \to A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}$ be the composition of the inclusion with the projection $A_{\mathfrak{p}} \twoheadrightarrow A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}$ and note that

$$\ker(f) = A \cap \mathfrak{p}^n[(R - \mathfrak{p})^{-1}] = \mathfrak{p}^n.$$

Moreover, to see that f is surjective, observe that for any $\frac{a}{s} \in A_{\mathfrak{p}}$, we have $\mathfrak{p}^n + (s) = A$,[33] so there exists $x \in \mathfrak{p}^n$ and $y \in A$ such that $x + sy = 1$. Consequently, y is sent to $\frac{1}{s} \pmod{\mathfrak{p}^n}$ and ay to $\frac{a}{s} \pmod{\mathfrak{p}^n}$. The lemma follows from the first isomorphism theorem. □

Theorem 58. *If A is a Dedekind domain, then every non-zero ideal I can be uniquely written (up to permutations) as $I = p_1^{e_1} \cdots p_r^{e_r}$ where $e_j \geq 0$ and p_j are prime ideals.*

Proof. Let $I \lhd A$, lemma 55 yields $J = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} \subseteq I$. By the Chinese Remainder Theorem (CRT), lemma 56 which says that $\mathfrak{p}_i^{r_i}$ is coprime to $\mathfrak{p}_j^{r_j}$ for all $i \neq j$ and lemma 57, we obtain[34]:

$$A/J = A/\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} \cong A/\mathfrak{p}_1^{r_1} \times \cdots \times A/\mathfrak{p}_n^{r_n} \cong A_{\mathfrak{p}_1}/\mathfrak{p}_1^{r_1} \times \cdots \times A_{\mathfrak{p}_n}/\mathfrak{p}_n^{r_n}.$$

The map $A \to A/J$ induces a bijection between the ideals of A containing J and the ideals of I/J. The image of I in $A_{\mathfrak{p}_1}/\mathfrak{p}_1^{r_1} \times \cdots \times A_{\mathfrak{p}_n}/\mathfrak{p}_n^{r_n}$ is of the form

$$\pi_1^{e_1} A_{\mathfrak{p}_1}/\mathfrak{p}_1^{r_1} \times \cdots \times \pi_n^{e_n} A_{\mathfrak{p}_n}/\mathfrak{p}_n^{r_n},$$

where $e_i \leq r_i$ [35]. On the other hand, the ideal $\mathfrak{p}_1^{e_1} \times \cdots \times \mathfrak{p}_r^{e_r}$ is another ideal containing J which has the same image in A/J, so this is the decomposition of I. Furthermore, the exponents depend only on I. □

Many properties of ideals in Dedekind domains can be checked "locally".

Corollary 59.

$$I = J \Leftrightarrow IA_{\mathfrak{p}} = JA_{\mathfrak{p}}, \forall \mathfrak{p} \in \operatorname{Spec}(A) - 0$$
$$I \subseteq J \Leftrightarrow IA_{\mathfrak{p}} \subseteq JA_{\mathfrak{p}}, \forall \mathfrak{p} \in \operatorname{Spec}(A) - 0$$

Proof. □

Corollary 60. *If a Dedekind domain A has finitely many prime ideals, then A is a PID.*

Proof. Suppose $\operatorname{Spec}(A) = \{0, \mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, it is enough to show $\mathfrak{p}_i$ is principal for every i.[36] Choose $a \in A$ which is congruent to π_i modulo π_i^2 where π_i generates $\mathfrak{p}_i A_{\mathfrak{p}_i}$ and congruent to 1 modulo $\mathfrak{p}_k$ for any $k \neq i$. By the CRT, we can find such an a and it is clear that $(a) = \mathfrak{p}_i$. □

Lemma 61. *If $I \supseteq J$ are two ideals of A, then there exists $a \in I$ such that $I = (a) + J$.*

[33] Since s is not in the unique maximal ideal $\mathfrak{p}$, s and $\mathfrak{p}$ must generate A otherwise $\mathfrak{p}^n + (s)$ would sit in a different maximal ideal.

[34] Abusing notation, we write $\mathfrak{p}_i^i$ for both the ideal in A and the ideal generated by $\mathfrak{p}_i^i$ in $A_{\mathfrak{p}_i}$.

[35] Because each $A_{\mathfrak{p}_i}$ is a DVR where every ideal is generated by some power of π_i (the generator of the unique prime ideal), recall corollary 48. To see that $e_i \leq r_i$, observe that $\pi_i \in \mathfrak{p}_i$, so it vanishes in $A_{\mathfrak{p}_i}/\mathfrak{p}_i^{r_i}$ when raised to the power r_i.

[36] Recall the proof of proposition 8.

Proof. Consider the decompositions

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \qquad J = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_r^{f_r}, \forall 1 \leq i \leq r, e_r \leq f_r,$$

where some e_i can be zero. Choose $a \in \pi_j^{e_j} \setminus \mathfrak{p}_j^{e_j+1}$ for $j = 1, \dots, r$. □

Proposition 62. *Any ideal in a Dedekind domain A can be generated by at most two elements of A.*

Proof. Choose an element $0 \neq b \in I$, we have $I \supseteq (b) \neq 0$ and by lemma 61, $\exists a \in I$, $(a) + (b) = I$. □

Proposition 63. *If I is a non-zero ideal of A, then there exists an ideal (far from unique) J such that IJ is principal.*

Proof. Write $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and pick $a \in I$, then $(a) = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_r^{f_r}$[37] with $e_j \leq f_j$. Let $J = \mathfrak{p}_1^{f_1 - e_1} \cdots \mathfrak{p}_r^{f_r - e_r}$. The proposition follows. □

Definition 64. For a Dedekind domain A, we define the multiplication monoid of ideals of A as $I_A = \{0 \neq I \lhd A\}$ with operation being multiplication of ideal. We denote P_A to be the submonoid of non-zero principal ideal, it corresponds exactly to $(A - \{0\})/A^\times$.[38]

Theorem 65. *Let A be a Dedekind domain, $K = \mathrm{Frac}(A)$, and B be the integral closure of A in L, a finite extension of K. Then, B is a Dedekind domain.*

Proof.

(i) We already showed B is finitely generated as an A-module in theorem 39. Consequently, any ideal of B is finitely generated as an A-module[39] and, a fortiori, as a B-module. We conclude that B is Noetherian.

(ii) B is integrally closed by definition.

(iii) Let β be a non-zero prime ideal of B. Let $b \in \beta$ be non-zero, it is integral over A, so it satisfies

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

where $a_i \in A$ and $a_0 \neq 0$. After isolating a_0, we see that a_0 is A-generated by powers of b, so that $a_0 \in \beta \cap A =: \mathfrak{p} \lhd A$, it is clear that $\mathfrak{p}$ is a non-zero prime ideal[40]. Consider B/β as an $A/\mathfrak{p}$-algebra, the containment map being

$$a + \mathfrak{p} \mapsto a + \beta : A/\mathfrak{p} \hookrightarrow B/\beta.$$

The fact that B is a finitely generated A-module implies that $B/\mathfrak{p}$ is a finitely generated $(A/\mathfrak{p})$-module and hence B/β is finitely generated over $(A/\mathfrak{p})$. Now, we also have that $\mathfrak{p}$ is maximal because A is Dedekind, so $A/\mathfrak{p}$ is a field and we obtain that B/β is a finite dimensional vector space. Moreover, since B/β is an integral domain[41], multiplying by any non-zero element yields a full rank linear map. Therefore, we can find an inverse to any non-zero element and we can conclude that B/β is a field and that β is maximal.

□

[37] Although it was used before the choice of a, the index r is determined by it. Indeed, (a) might have more primes in its decomposition than I, but for simplicity, we assume that some e_j's might be zero.

[38] A corollary of this last proposition is that I_A/P_A is an abelian group (any element has an inverse) it is called the class group of A.

[39] Recall that a ring R is Noetherian if and only if any submodule of a finitely generated R-module is finitely generated.

[40] It is non-zero because it contains a_0 and it is prime because β was prime in the bigger ring B.

[41] Because β is prime.

Until the end of this section, we will work in the following setting. Let A be a Dedekind domain, $K = \mathrm{Frac}(A)$, $K < L$ be a field extension of degree n and B be the integral closure of A in L such that B is locally free over A.[42]

Definition 66. If β is a non-zero prime ideal of B, then $\dim_{A/(\beta \cap A)}(B/\beta)$ is called the residue degree of β and denoted f_β. If there exists some prime ideal $\mathfrak{p} \lhd A$ such that $\mathfrak{p}B$ decomposes uniquely as $\beta_1^{e_1} \cdots \beta_t^{e_t}$ where $\beta_1 = \beta$, e_1 is called the ramification index of β in B/A, it is denoted e_β.[43]

Lemma 67. *A prime ideal β divides $\mathfrak{p}B$ if and only if $\mathfrak{p} = \beta \cap K$.*

Proof. ($\Rightarrow$) It is clear that $\mathfrak{p} \subseteq \beta \cap K$ because any element in $\mathfrak{p}$ is in a product of ideals including β and thus in β. Also, since $\mathfrak{p}$ is maximal and $\beta \cap K$ is an ideal, we have $\mathfrak{p} = \beta \cap K$.

($\Leftarrow$) If $\mathfrak{p} \subseteq \beta$, then $\mathfrak{p}B \subseteq \beta$, thus $\mathfrak{p}B_\beta \neq B_\beta$[44]. However, if β did not divide $\mathfrak{p}B$, then we would get all of B_β when localizing at β. □

Theorem 68. *For any prime ideal $\mathfrak{p} \lhd A$ with $\mathfrak{p}B = \beta_1^{e_1} \cdots \beta_t^{e_t}$, if f_i is the residue degree of β_i in B/A, then $\sum_{i=1}^t e_i f_i = n$.*

Proof. On one hand, from the following derivation[45], we see that $B/\mathfrak{p}B$ is isomorphic to $(A/\mathfrak{p})^n$:

$$\begin{aligned} B/\mathfrak{p}B &\cong B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} && \text{(by lemma 57)} \\ &\cong A_\mathfrak{p}^n/(\mathfrak{p}A_\mathfrak{p}^n) && \text{(by local freeness}^{46}\text{)} \\ &\cong (A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})^n \\ &\cong (A/\mathfrak{p})^n && \text{(by lemma 57).} \end{aligned}$$

On the other hand, from the CRT, we know that

$$B/\mathfrak{p}B \cong B/\beta_1^{e_1} \times \cdots \times B/\beta_t^{e_t},$$

as vector spaces over $(A/\mathfrak{p})$. Therefore, it is enough to show that for all $1 \leq i \leq t$, the dimension of $B/\beta_i^{e_i}$ is $e_i f_i$. We will show this by induction on e_i.

First, observe that for any $1 \leq k \leq e_i - 1$, β_i^k/β_i^{k+1} is a (B/β_i)-module of dimension one. One can easily check that $(a + \beta_i)(b + \beta_i^{k+1}) := (ab + \beta_i^{k+1})$ for any $a \in B$ and $b \in \beta_i^k$ is a suitable scalar multiplication. Furthermore, by the fourth isomorphism theorem, any non-trivial strict subspace of β_i^k/β_i^{k+1} must come from an ideal $\beta_i^{k+1} \subset V \subset \beta_i^k$. However, no such ideal can exist because β_i is prime, so β_i^k/β_i^{k+1} must have dimension one.

Our base case (when $e_i = 1$) follows from the definition of f_i. Suppose that $B/\beta_i^{e_i - 1}$ has dimension $(e_i - 1)f_i$ over $A/\mathfrak{p}$. Then, we have the following short exact sequence of modules

$$0 \to \beta_i^{e_i-1}/\beta_i^{e_i} \to B/\beta_i^{e_i} \to B/\beta_i^{e_i-1} \to 0.$$

By a basic result from the study of modules, we get that the dimension of $B/\beta_i^{e_i}$ is $(e_i - 1)f_i + f_i = e_i$. □

[42] i.e.: for any prime ideal $\mathfrak{p} \lhd A$, $B_{\mathfrak{p}B}$ is free over $A_\mathfrak{p}$.

[43]

[44] Because no element of β has an inverse in B_β.

[45] Where the isomorphisms are as vector spaces over $(A/\mathfrak{p})$.

[46] We know from the proof of proposition 37 that B is both contained and contains free A-modules of rank n. After localizing at $\mathfrak{p}$, we get that $B_\mathfrak{p}$ is between two free $(A_\mathfrak{p})$-modules of rank n, but by local freeness, it is also finitely generated, so it must be isomorphic to $(A_\mathfrak{p})^n$.

Theorem 69. *If L/K is a Galois extension with Galois group G, then G acts transitively on the set of prime ideals dividing $\mathfrak{p}B$. In particular, for all $\beta \mid \mathfrak{p}B$, the ramification number $e_\beta = e$ depends only on $\mathfrak{p}$ and likewise for $f_\beta = f$. Hence, $n = t \cdot f \cdot e$.*[47]

Proof. Suppose G does not act transitively, then there exists $\beta_0 \mid \mathfrak{p}$ and $\beta_1 \mid \mathfrak{p}$ such that $\beta_0 \neq \sigma\beta_1$ for all $\sigma \in G$. Hence, there exists an element $a \in \beta_0$ such that $a \notin \sigma\beta_1$ for all $\sigma \in G$, equivalently, $\sigma^{-1}a \notin \beta_1$. Since β_1 is prime, we have

$$\mathrm{Nm}(a) = \prod_{\sigma \in G} \sigma^{-1}a \notin \beta_1.$$

However, we also know that $\mathrm{Nm}(a) \in \beta_0 \cap A = \mathfrak{p} \subseteq \beta_1$[48], so we have a contradiction. □

Definition 70. Let $\mathfrak{p} \lhd A$ be prime. If, for some prime ideal $\beta \lhd B$, $\beta^2 \mid \mathfrak{p}B$, then we say that $\mathfrak{p}$ ramifies (or is ramified) in B/A.

Our last goal in this section is to show that there are only finitely many primes that ramify in B/A.

Definition 71 (Discriminant)**.** If $B \cong A^n$ as an A-module, then we define

$$\mathrm{disc}(B/A) = \det\left(\left(\mathrm{Tr}_{L/K}(e_ie_j)\right)_{i,j}\right) \in A,$$

where $\{e_1, \dots, e_n\}$ is an A-basis for B. Otherwise, we still have that B is locally free over A, so $\mathrm{disc}(B_{\mathfrak{p}B}/A_\mathfrak{p}) = u \cdot \pi^{e_\mathfrak{p}} \in A_\mathfrak{p}$.[49] Thus, we can define, in general,

$$\mathrm{disc}(B/A) = \prod_{\mathfrak{p}\text{ prime}} \mathfrak{p}^{e_\mathfrak{p}} \lhd A.$$

Remark 72. The general definition is compatible with the definition for PIDs because if $B = Ae_1 \oplus \cdots \oplus Ae_n$, then $B_\mathfrak{p} = A_\mathfrak{p}e_1 \oplus \cdots \oplus A_\mathfrak{p}e_n$.

Theorem 73. *A prime ideal $\mathfrak{p} \lhd A$ is ramified in B/A if and only if $\mathfrak{p} \mid \mathrm{disc}(B/A)$.*

Proof. We claim that

$$\mathrm{disc}(B/A) \equiv \mathrm{disc}(B_\mathfrak{p}/A_\mathfrak{p}) \pmod{\mathfrak{p}} \equiv \mathrm{disc}((B_\mathfrak{p}/\mathfrak{p})/(A_\mathfrak{p}/\mathfrak{p})) \pmod{\mathfrak{p}}.$$

By the previous remark, we also have $(B_\mathfrak{p}/\mathfrak{p}) = (A_\mathfrak{p}/\mathfrak{p})\bar{e}_1 \oplus \cdots \oplus (A_\mathfrak{p}/\mathfrak{p})\bar{e}_n$. [50]

On the other hand, $\mathfrak{p} = \beta_1^{e_1} \times \cdots \times \beta_t^{e_t}$, thus $B_\mathfrak{p}/\mathfrak{p} = B_\mathfrak{p}/\beta_1^{e_1} \times \cdots \times B_\mathfrak{p}/\beta_t^{e_t}$ as $(A_\mathfrak{p}/\mathfrak{p})$-algberas. Moreover, if $B = B_1 \times \cdots \times B_t$ as k-algebras, then $\mathrm{disc}(B/k) = \mathrm{disc}(B_1/k) \cdots \mathrm{disc}(B_t/k)$ (matrix that is considered in the discriminant and we can write it as block matrix).

It remains to understand the discriminant of $B_\mathfrak{p}/\beta^e$ where β is a prime ideal of B. Note that this algebra is isomorphic to a field if $e = 1$, but it has non-zero nilpotent elements if $e > 1$. The discriminant of a field extension is non-zero (because the trace form is non-degenerate). However, when there are nilpotent elements, the trace form is degenerate, so the discriminant is zero. □

Corollary 74. *There are finitely many ramified primes in B/A.*

[47] t is the number of distinct prime ideals dividing $\mathfrak{p}$.

[48] We know that $\mathrm{Nm}(a) \in \beta_0$ because it is a multiple of $a \in \beta_0$. We know that $\mathrm{Nm}(a) \in A$ because B is integral over A. We know that $\beta_0 \cap A = \mathfrak{p}$ by lemma 67.

[49] Recall that $A_\mathfrak{p}$ is a DVR, so we have this decomposition where π is the generator of the unique non-zero prime ideal and u is a unit.

[50] Argue that they are linearly independent. If B is an A-algebra which is free of rank N as an A-module, the discriminant is really an eliment of A/A^{times^2}

Examples 75.

1. Let $B = \mathbb{Z}[i]$ and $A = \mathbb{Z}$, their fraction fields are $\mathbb{Q}(i)$ and $\mathbb{Q}$ respectively and they fit in the general set-up of this section with $n = [\mathbb{Q}(i) : \mathbb{Q}] = 2$. Let the A-basis for B be $\{1, i\}$, we can readily compute

   $$\operatorname{disc}(\mathbb{Z}[i]/\mathbb{Z}) = \det \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} = -4.$$

   Let $p \in \mathbb{Z}$ be prime, we will investigate the factorization of (p) in $\mathbb{Z}[i]$. If $p = 2$, then we notice $(2) = (1+i)(1-i) = (1+i)^2$, thus $t = 1$ and $e = 2$. Also, because $\mathbb{Z}[i]/(2)$ identifies $1 = -1 = i^2$, we find that it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, so $f = 1$. Otherwise, we have $\mathbb{Z}[i]/(p) = \mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$ and we consider two cases.

   If $p \equiv 1 \pmod 4$, then -1 has a square root $a \in \mathbb{Z}/p\mathbb{Z}$ and $x^2 + 1 = (x-a)(x+a)$ is reducible, thus

   $$\mathbb{Z}[i]/(p) \cong \mathbb{Z}/p\mathbb{Z}[x]/(x-a) \times \mathbb{Z}/p\mathbb{Z}[x]/(x+a) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z},$$

   and $f = 2$. Furthermore, we now see that $p = (p, i-a)(p, i+a)$, so $t = 2$ and $e = 1$ which confirms that (p) does not ramify because it does not divides -4.

   If $p \equiv 3 \pmod 4$, then x^2+1 is irreducible, so $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1) \cong \mathbb{F}_{p^2}$ and (p) is prime in $\mathbb{Z}[i]$, we obtain $t = 2$, $e = 1$, $f = 2$.

2. Let $R = \mathbb{Z}[\sqrt[3]{2}] \subset B = O_{\mathbb{Q}(\sqrt[3]{2})}$. We can compute

   $$\operatorname{disc}(R/\mathbb{Z}) = \det \begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{bmatrix} = -3^3 \cdot 2^2.$$

   We get that $R_{(p)} = B_{(p)}$ for any $p \neq 2, 3$. For such a p, we have

   $$B/(p) = B_{(p)}/(p) = R_{(p)}/(p) = R/(p) = \mathbb{Z}[x]/(x^3-2)/(p) = \mathbb{Z}/p\mathbb{Z}[x]/(x^3-2)$$

   We are now in a nicer ring (a UFD), so the strucutre is really nice. $\alpha = \sqrt[3]{2}$ On the other hand, we have $(2) = (\sqrt[3]{2})^3$ and $(3) = (\sqrt[3]{2}+1)^3$ in $R_{(3)}$ [51]. We have $(5) = (5, \alpha+2)(5, \alpha^2+3\alpha+4)$ because $(x^3-2) \equiv (x+2)(x^2+3x+4) = \mathfrak{p}_1\mathfrak{p}_2 \pmod 5$. We see that $B/\mathfrak{p}_1 = \mathbb{Z}/5\mathbb{Z}$, but $B/\mathfrak{p}_2 = \mathbb{F}_p5$. So $f_1 = 1$ and $f_2 = 2$.

   In (7), (x^3-2) is irreducible, so $f = 3$. For $(11) = (11, \alpha+4)(11, \alpha^2+7\alpha+5)$ and $(13) = (13)$. Interestingly, $(31) = (31, \alpha+11)(31, \alpha+24)(31, \alpha+27)$. Doing this for many primes, we see that 50% of the time, $f_1 = 1$ and $f_2 = 2$ occurs. $f = 3$ occurs 33% of the time. $f_1 = f_2 = f_3 = 1$ occurs 16.6% of the time. Notice that this happens because $\mathbb{Q}(\alpha)$ is not Galois.

   Remark: these proportions are predicted by the Chebotarev density theorem. In particular, if $K/\mathbb{Q}$ is a cyclic Galois extension of degree 3 with polynomial $f(x)$, then $f(x) \pmod p$ factors either into three linear factors or is irreducible. Interesting questions, are there any patterns satisfied by the function $p \mapsto (f_1, f_2, \ldots, f_t)$.

[51] detail this

$\mathbb{Z}$	$[t]$
$\mathbb{Q}$	(t)
$K > \mathbb{Q}$, $[K : \mathbb{Q}] < \infty$	$(t)[x]/(x^n + a_{n-1}(t)x^{n-1} + \cdots + a_1(t)x + a_0(t))$ where $a_i(t) \in [t]$, so we indeed have $p(t,x) \in [t,x]$.

Remark 76. Explaination of the terminology of ramification. The first appearance of this theory was motivated by the study of Riemann surfaces. Let $p(t,x) \in [t,x]$ and $S = \{(t,x) \in^2 \mid p(t,x) = 0\}$ is a curve in because it is one dimension but topologically it is more of a surface because we are in . We have the following analogies. The function $S \to = (t,x) \mapsto t$ is generically n-to one except for $t \in R := \{t \in \mid x^n + a_{n-1}(t)x^{n-1} + \cdots a_1(t)x_1 + a_0(t)$ has multiple roots $= \{t \mid \delta(t) = 0, \delta = \operatorname{disc}_x(P_t(x))\}$ is called the ramification locus.

Commutative Algebra and Algebraic Geometry

The main objects studied in algebraic geometry are algebraic varieties, we first introduce two kinds of such objects in the two following sections and then move to a more abstract setting.

The main reference for this section is Ernst Krunz's *Introduction to Commutative Algebra and Algebraic Geometry*, chapter 1-4.

Affine Varieties

Definition 77. Let k be a fields, we denote $\mathbb{A}^n(k)$ to be the **affine n-space** isomorphic to k^n.[52] If k is algebraically closed, then $\mathbb{A}^n(k)$ can be identified with the maximal ideals of $k[x_1, \ldots, x_n]$.

Definition 78. A **variety** V over k is a system of polynomial equations of the form

$$\left\{ \begin{matrix} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{matrix} \right\},$$

where $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$. For a k-algebra L, we denote $V(L)$ to be the set of solutions of this system in L^n.

Examples 79. Here are a few brief examples that we might study more in depth in this section. In the context of the above definition:

- We talk about a **linear** variety if $\deg f_1 = \cdots = \deg f_m = 1$.
- We talk about **hypersurfaces** when $m = 1$.
- We talk about **quadric hypersurfaces** when $\deg f_1 = 2$ and $m = 1$, they are a generalization of conic surfaces.
- More generally, if $\deg f_1 = \cdots = \deg f_m = 2$, then V is a **quadric variety**.
- We say that V is a **cone** when $f_1, \ldots, f_m$ are homogeneous[53]. Such varieties have a nice scaling property, namely,

$$(a_1, \ldots, a_n) \in V(L) \implies (\lambda a_1, \ldots, \lambda a_n) \in V(L), \qquad \forall \lambda \in L.$$

[52] In this class, we will always view the affine n-space as k^n.

[53] We say that a polynomial is homogeneous if all of its monomials have the same degree.

- With more generality, one can consider **quasi-homogeneous** varieties, they satisfy that for some fixed $\{m_i\}_{i\in[n]} \subset \mathbb{N}$ and $m \in \mathbb{N}$ and for all monomials $cx_1^{r_1}\cdots x_n^{r_n}$ of the polynomial f_j, $\sum_{i=1}^n r_i m_i = m$. We then have
$$(a_1,\dots,a_n) \in V(L) \implies (\lambda^{m_1}a_1,\dots,\lambda^{m_n}a_n) \in V(L), \qquad \forall\lambda \in L.$$
- If V_1 is a system $\{f_1,\dots,f_m\}$ and V_2 is a system $\{g_1,\dots,g_l\}$, then we can build another variety[54]
$$V_1 \cap V_2 = \{f_1,\dots,f_m,g_1,\dots,g_l\}.$$
The variety $V_1 \times V_2$ arises from considering the same set but viewing the polynomials in $k[x_1,\dots,x_n,y_1,\dots,y_n]$ where $f_j \in k[x_1,\dots,x_n]$ and $g_j \in k[y_1,\dots,y_n]$.[55]
- We can look at some common groups with the point of view of varieties. For instance, we can see GL_n as a subset of $\mathbb{A}^{n^2+1}$ with the variables $x_{i,j}$ for $i,j \in [n]$ and t. Observe that $\det((x_{i,j}))$ is a polynomial of degree n in n^2 variables and that the solutions in L^{n^2+1} of the equation $t\det(x_{i,j}) - 1 = 0$ are precisely matrices with invertible determinants in L, namely $GL_n(L)$, where L is any k-algebra. It has a natural group structure arising from the multiplication of matrices. This is what we call an **algebraic group**.

Definition 80. To a variety $V \subseteq \mathbb{A}^n$ over k, we can associate two related ring theoretic invariants. First, the ideal $I(V) \lhd k[x_1,\dots,x_n]$ of polynomials that are identically 0 on V. Second, the coordinate ring of V, denoted $\mathcal{O}_V$, is the quotient $k[x_1,\dots,x_n]/I(V)$. We can think of the latter as polynomially defined functions on V.

The general problem that is studied in this section is to understand the relation between the collection $\{V(L) \mid L \text{ is a } k\text{-algebra}\}$ and $I(V)$ or $\mathcal{O}_V$. We start with a very useful fact about the map $L \mapsto V(L)$. It will use Hilbert's basis theorem, so we prove it for completeness.[56]

Theorem 81. *If R is Noetherian, then $R[x]$ is Noetherian.*

Proof. We show the contrapositive. Suppose $I \lhd R[x]$ is not finitely generated. Let $f_1(x)$ be a non-zero element of I of minimal degree d_1 and a_1 be its leading coefficient. Let f_2 be the element of smallest degree in $I - (f_1)$, it has degree $d_2 \geq d_1$ and leading coefficient a_2. Inductively, let f_j be the element of smallest degree in $I - (f_1,\dots,f_{j-1})$ with degree d_j and leading coefficient a_j. Since I is not finitely generated, we will always find non-zero elements, so we get an infinitely many a_i's. We claim that
$$(a_1) \subset (a_1,a_2) \subset \cdots \subset (a_1,\dots,a_j) \subset \cdots.$$
Suppose one inclusion is not strict at some point j, then we can write $a_{j+1} = \lambda_1 a_1 + \cdots + \lambda_j a_j$. Therefore, the degree of
$$f_{j+1} - \lambda_1 x^{d_{j+1}-d_1} f_1 + \cdots + \lambda_j x^{d_{j+1}-d_j} f_j \in I$$
is strictly less than d_{j+1}, so this polynomial belongs to $(f_1,\dots,f_j)$. However, this implies that $f_{j+1} \in (f_1,\dots,f_j)$ which is a contradiction. We conclude that R is not Noetherian as it has an infinite ascending chain of ideals. □

[54] The notation $\cap$ is justified because for any $L > k$, we have $(V_1 \cap V_2)(L) = V_1(L) \cap V_2(L)$.

[55] The notation $\times$ has the same justification as $\cap$.

[56] In fact, we prove a more general statement.

Corollary 82 (Hilbert's basis theorem)**.** *For any $n \in \mathbb{N}$, $k[x_1, \dots, x_n]$ is Noetherian.*

Remark 83. Hilbert's basis theorem also justifies the fact that varieties can be defined by an ideal. Indeed, if $I \lhd k[x_1, \dots, x_n]$, it is finitely generated by $f_1, \dots, f_m$, then we define $V(I)$ to be the variety defined by $f_1 = \dots = f_m = 0$, we also say it is the variety corresponding to the ideal I. One can verify that $V(I(V)) = V$ is true for any V, but $I(V(I)) = I$ is not true for any I.

Proposition 84. *A variety V determines a functor (the functor of points) from $V : \mathbf{Alg}_k \rightsquigarrow \mathbf{Sets}$ associating $L \mapsto V(L)$.*

Proof. The action of V on a morphism[57] $f : L \to M$ is the natural map

$$L^n \ni (a_1, \dots, a_n) \mapsto (f(a_1), \dots, f(a_n)) \in M^n.$$

We first need to verify that if the L.H.S. vanishes on the polynomials defining V, then the R.H.S. also does. This is easy to see because properties of f are such that applying a polynomial and then f is the same as applying f and then the polynomial and $f(0) = 0$. The remaining functoriality properties obviously hold. □

Theorem 85. *A functor $F : \mathbf{Alg}_k \rightsquigarrow \mathbf{Sets}$ is representable[58] if and only if it arises from some variety V over k.*

Proof. ($\Leftarrow$) Let V be defined by $f_1 = \dots = f_m = 0$ and let $R = k[x_1, \dots, x_n]/(f_1, \dots, f_m)$. We claim that $V(L) \cong \mathrm{Hom}_{\mathbf{Alg}_k}(R, L)$. This is clear because to define a function ϕ in the R.H.S., we need to specify where it sends $x_1, \dots, x_n$ in L such that

$$f_i(\phi(x_1), \dots, \phi(x_n)) = \phi(f_i(x_1, \dots, x_n)) = \phi(0) = 0, \qquad \forall i \in [m].$$

This happens precisely when $(\phi(x_1), \dots, \phi(x_n)) \in V(L)$.

($\Rightarrow$) Let R be the k-algebra that represents F, then because R is finitely generated, we can write $R = k[x_1, \dots, x_n]/I$, where I is generated by the relations between the generators of R. Since I is finitely generated,[59] we can write $I = (f_1, \dots, f_m)$. Then, as in the converse direction, we have $\mathrm{Hom}_{\mathbf{Alg}_k}(R, L) \cong V(L)$, where V is the variety defined by $f_1 = \dots = f_m = 0$. □

Question 86. *To what extent is a variety V (equivalently, $I(V)$ or $\mathcal{O}_V$) determined by $V(k)$?*

It is obviously not *completely* determined by $V(k)$, for example: let $V_1 = \{x^2 + y^2 + 1 = 0\}$ and $V_2 = \{x^2 + y^2 + 2 = 0\}$ with $k = \mathbb{R}$. It is clear that $I(V_1) \neq I(V_2)$ but both $V_1(\mathbb{R})$ and $V_2(\mathbb{R})$ are empty. One might think that this situation gets better when k is algebraically closed. However, this is still not enough. For instance, if we have $V_1 = \{x = 0\}$ and $V_2 = \{x^2 = 0\}$, then if L is any field, $V_1(L) = V_2(L) = \{0\}$, but these varieties have different defining ideals. We will see that looking at more general algebras will help us greatly towards distinguishing different varieties. Coming back to the previous example, if we let $L = k[\epsilon], \epsilon^2 = 0$[60], we see that $V_1(L) = \{(0)\}$ and $V_2(L) = \{\lambda\epsilon \mid \lambda \in k\}$ are different.

Our next main result is Hilbert's Nullstellensatz. We will first prove a proposition that is equivalent to it (sometimes called the field theoretic Nullstellensatz). This proposition needs two simple but very general lemmas.

Lemma 87. *The field of rational functions $k(x_1, \dots, x_n)$ is not finitely generated as a k-algebra.*

[57] Recall that objects in the $\mathbf{Alg}_k$ are k-algebras and morphisms are ring homomorphisms that restrict to the identity on k.

[58] We say a functor $F : \mathbf{Alg}_k \rightsquigarrow \mathbf{Sets}$ is representable if there is a finitely generated algebra R such that $F \cong \mathrm{Hom}_{\mathbf{Alg}_k}(R, -)$.

[59] Because $k[x_1, \dots, x_n]$ is Noetherian.

[60] We can also write

$$L = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in k \right\}.$$

Proof. Let $\alpha_1 = \frac{p_1}{q_1}, \dots, \alpha_t = \frac{p_t}{q_t}$ be a finite collection of elements of this field. We claim that there is a strict inclusion

$$k[\alpha_1, \dots, \alpha_t] \subset k(x_1, \dots, x_n).$$

Any element of the L.H.S. can be written as $\frac{p(x)}{q_1^{r_1} \cdots q_t^{r_t}}$, hence if $q \in k[x_1, \dots, x_n]$ is relatively prime to each q_i,[61] then $\frac{1}{q} \notin k[\alpha_1, \dots, \alpha_n]$ and the lemma follows. □

Lemma 88. *Let R be a Noetherian ring, T be a finitely generated R-algebra and S be a subring of T containing R. If T is finitely generated as an S-module, then S is a finitely generated as an R-algebra.*

Proof. Let $w_1, \dots, w_r$ be the S-module generators of T and assume[62] that this spanning set also includes a set of R-algebra generators of T. Then, we can write

$$w_i w_j = \sum_{k=1}^{r} a_{i,j}^{(k)} w_k, \qquad \forall i, j, k \in [r], a_{i,j}^{(k)} \in S.$$

Let S' be the R-algebra generated by all the coefficients $a_{i,j}^{(k)}$. We have the inclusions $R \subseteq S' \subseteq S \subseteq T$. Since R is Noetherian, then S' is also Noetherian since it is finitely generated as an R-algebra. This implies that S, being a submodule of a finitely generated S'-module (namely T), is finitely generated as an S'-module. We conclude that S is finitely generated as an R-algebra.[63] □

Proposition 89. *If L/k is an extension of fields and L is finitely generated as a k-algebra, then L is algebraic over k.*

Proof. From general field theory, we know that there exists $x_1, \dots, x_n \in L$ such that $k(x_1, \dots, x_n)$ (we adjoin $x_1, \dots, x_n$ to k) is purely transcendental and $L/k(x_1, \dots, x_n)$ is algebraic.[64] Our goal is to show that $n = 0$, i.e.: there are no transcendental elements in L.[65]

Since L is finitely generated as a module over $k(x_1, \dots, x_n)$ and as a k-algebra, we can use lemma 88 to conclude that $k(x_1, \dots, x_n)$ is finitely generated as a k-algebra, contradicting lemma 87 if $n > 0$. □

Remark 90. One might think that the proposition follows from the first paragraph of the previous proof and lemma 87, because $k(x_1, \dots, x_n)$ is not finitely generated over k while L is, leading to a contradiction. However, in general, sub-algebras of finitely generated algebras are not necessarily finitely generated hence the need for lemma 88.

For example, let k be a field and R be the k-algebra generated by the set $\{x^i y^j \mid i < j\}$ where x and y are commuting formal variables. It is a subalgebra of $k[x, y]$ which is finitely generated over k. Suppose that $g_1, \dots, g_t \in R$ and let $\{v_1, \dots, v_m\}$ be the set of degrees of monomials appearing in the generators.[66] Now, any degree (i, j) appearing in a monomial in $g_1^{d_1} \cdots g_t^{d_t}$ is a positive linear combinations of $v_1, \dots, v_m$. Since $v_1, \dots, v_m$ are above the diagonal $x = y$ when seen as points of the lattice $\mathbb{N}^2$, this linear combination is also above the diagonal.

[61] We can always find such q by the CRT.

[62] We do not loose generality because any set of R-algebra generators of T can be extended to be a spanning S-module generators.

[63] It is generated by the R-algebra generators of S' and the S'-module generators of S.

[64] We say that $x_1, \dots, x_n$ is a transcendental basis of L and n is the transcendence degree of L over k.

[65] Why do we know $[L : k(x_1, \dots, x_n)] < \infty$? We can prove this because L is finitely generated as a k-algebra.

[66] We view the degree of the monomial $x^i y^j$ as the tuple $(i, j) \in \mathbb{N}^2$.

In fact, letting v_1 be the closest (out of $v_1, \ldots, v_m$) to the diagonal, we see that the degree (i, j) is above the line going through the origin and v_1. However, we can always find a point below this line and above the diagonal, it represents the degree of a monomial in R that cannot be generated by this finite set.

Corollary 91 (Hilbert's Nullstellensatz). *If $I(V) \neq k[x_1, \ldots, x_n]$ and k is algebraically closed, then $V(k)$ is not empty.*

Proof. Let M be a maximal ideal containing $I(V)$ and $L = k[x_1, \ldots, x_n]/M$. Note that L is a field extension of k. Moreover, it is finitely generated as k-algebra by $\{x_1 + M, \ldots, x_n + M\}$. By proposition 89, L is contained in the algebraic closure of k, but since $k = \bar{k}$, they must be equal. Let $\phi : k[x_1, \ldots, x_n]/M \cong k$ and $(a_1, \ldots, a_n) = (\phi(x_1), \ldots, \phi(x_n)) \in k^n$. Since ϕ is a homomorphism, we have $f(a_1, \ldots, a_n) = 0$ for all $f \in M$. In particular, this is true for all $f \in I$, thus $(a_1, \ldots, a_n)$ belongs to $V(k)$. As desired, we conclude that $V(I)(k) \neq \emptyset$. □

Remark 92. We also note that Hilbert's Nullstellensatz implies proposition 89.

Proof. If L/k is a field extension that is finitely generated as a k-algebra, then $L = k[x_1, \ldots, x_n]/M$,[67] where M is maximal because L is a field. Let V be the variety corresponding to M, the Nullstellensatz implies that $V(\bar{k})$ is non-empty, hence there exists $\phi \in \mathrm{Hom}_{\mathbf{Alg}_k}(L, \bar{k})$, hence L is algebraic.[68] □

We will now refine Hilbert's Nullstellensatz.

Definition 93. Let $I \lhd R$ be an ideal in a ring. The radical of I is the set

$$\sqrt{I} := \{f \in R \mid \exists m \in \mathbb{N}, f^m \in I\}.$$

If $I = \sqrt{I}$ we say that I is a radical ideal.

Fact 94. *$R/\sqrt{I}$ has no nilpotent elements*[69] *and $\sqrt{I}$ is the smallest ideal containing I with this property.*

Question 95. *When is an ideal $I \lhd k[x_1, \ldots, x_n]$ of the form $I(V(\bar{k}))$ for a variety V?*

We will see that the condition that $I = \sqrt{I}$ is necessary and sufficient.

Theorem 96. *Let $I \lhd k[x_1, \ldots, x_n]$, then $I(V(I)(\bar{k})) = \sqrt{I}$.*

Proof. ($\supseteq$) It is clear because if $f^d \in I$,then $f^d \equiv 0$ on $V(I)(\bar{k})$, so $f \equiv 0$ as well.

($\subseteq$) Let f be in the L.H.S which is generated by $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ and consider the ideal $J = (f_1, \ldots, f_m, tf - 1) \lhd k[x_1, \ldots, x_n, t]$. Observe that

$$V(J)(\bar{k}) = \left\{(x_1, \ldots, x_n, t) \in \bar{k}^{n+1} \mid f_i(x_1, \ldots, x_n) = 0, \forall i, tf(x_1, \ldots, x_n) - 1 = 0\right\}$$

is empty because any points that vanish on $f_1, \ldots, f_m$ also vanish on f, thus we have $f(x_1, \ldots, x_n) = 0$ and the last equation cannot be satisfied. Consequently, Hilbert's Nullstellensatz implies that $J = k[x_1, \ldots, x_n, t]$, in particular

$$1 = \sum_{i=1}^{m} r_i f_i + s(tf - 1), \text{ for some } r_i, s \in k[x_1, \ldots, x_n, t]. \qquad (*)$$

[67] M is generated by the relations between the generators of L.

[68] Any ring homomorphism $\phi : L \to \bar{k}$ is injective, so L is a subfield of $\bar{k}$ and we conclude any element of L is algebraic over k.

[69] We often called this a reduced algebra.

Consider now a homomorphism $\phi : k[x_1, \dots, x_n, t] \to k[x_1, \dots, x_n][f^{-1}]$ with $x_j \mapsto x_j$, $t \mapsto f^{-1}$ and $\phi \mid_k = \text{id}$. Applying ϕ to $(*)$, we get

$$1 = \phi(1) = \sum_{i=1}^{m} \phi(r_i) f_i, \qquad \phi(r_i) = \frac{g_i(x_1, \dots, x_n)}{f^{d_i}}.$$

Let d be the maximum of the d_i's and multiply by f^d to obtain

$$f^d = \sum_i g(x_1, \dots, x_n) f^{d-d_i} f_i,$$

so $f^d \in I$ and $f \in \sqrt{I}$. □

Corollary 97. *The maps $V \mapsto I(V(\bar{k}))$ and $I \mapsto V(I)$ are mutual inverses*[70]

$$\{\textit{varieties over } k\} \leftrightarrow \{\textit{radical ideals of } k[x_1, \dots, x_n]\}.$$

To end this section, we will talk about decomposition of varieties in irreducible components and we will need to take a small detour in topology.[71]

Definition 98. The Zariski topology on $\mathbb{A}^n(\bar{k})$ with respect to k is the topology where the closed sets are the sets of the form $V(\bar{k})$ for V a variety over k.

Proposition 99. *The Zariski topology makes $\mathbb{A}^n(\bar{k})$ into a topological space, i.e.:*

1. *$\emptyset$ and $\mathbb{A}^n(\bar{k})$ are closed.*

2. *If $\{V_\alpha\}_{\alpha \in A}$ are closed, then $\bigcap_{\alpha \in A} V_\alpha$ is closed.*

3. *If $\{V_\alpha\}_{\alpha \in A}$ are closed and A is finite, then $\bigcup_{\alpha \in A} V_\alpha$ is closed.*

Proof. 1. The empty set is always the variety defined by $1 = 0$. The whole space is the variety defined by $0 = 0$.

2. Let $F_\alpha = I(V_\alpha)$ and $F = \sum_{\alpha \in A} F_\alpha$, F is an ideal that is finitely generated by some polynomials $f_1, \dots, f_m$ and it is clear that the variety they define is the intersection of all the V_α's.

3. Let $F_\alpha = I(V_\alpha)$ and $F = \prod_{\alpha \in A} F_\alpha$[72], F is an ideal that is finitely generated by some polynomials $f_1, \dots, f_m$ and it is clear that the variety they define is the union of all the V_α's.

□

Definition 100. A topological space X is **irreducible** if for any decomposition $X = A_1 \cup A_2$ where A_1 and A_2 are closed, $A_1 = X$ or $A_2 = X$.[73]

Remark 101. Observe that this definition applied to the Zariski topology coincides with the definition of irreducibility of varieties.

Lemma 102. *The following properties of a topological space X are equivalent:*

(i) X is irreducible.

[70] In remark 83, we said that $I(V(I)) = I$ does not always hold. This corollary states that it holds if and only if I is radical.

[71] We assume some basic knowledge about topological spaces.

[72] While arbitrary sum of ideals is well defined. Products are only well defined when A is finite.

[73] Same for open or closed.

(ii) If U_1 and U_2 are open non-empty subsets of X, then $U_1 \cap U_2 \neq \emptyset$.

(iii) Any non-empty open subset of X is dense in X.

Proof. (i $\Leftrightarrow$ ii) The contrapositive of this equivalence follows from DeMorgan's laws, namely, let U_1 and U_2 be subsets of X and $V_1 = X - U_1$ and $V_2 = X - U_2$, then

$$\emptyset \neq U_1, U_2 \text{ are open and } U_1 \cap U_2 = \emptyset \Leftrightarrow X \neq V_1, V_2 \text{ are closed and } V_1 \cup V_2 = X.$$

(ii $\Leftrightarrow$ iii) Again, we show the contrapositive. If U is a non-empty open subset of X, then

$$\exists \emptyset \neq V \text{ open}, U \cap V = \emptyset \Leftrightarrow \exists x \in X - U, \exists V \text{ open}, U \cap V = \emptyset \Leftrightarrow U \text{ is not dense.}$$

□

Corollary 103. *If $S \subseteq X$ is irreducible, then so is $\overline{S}$ (its closure in the topology).*

Definition 104. An **irreducible component** of X is a maximal irreducible subset.

Corollary 105. *The irreducible components of X are closed.*

Proposition 106. *Let X be a topological space, then we have*

(i) Any irreducible subset of X is contained in an irreducible component.

(ii) X is the union of its irreducible components.

Proof. (i) Follows from Zorn's lemma. Let $S \subseteq X$ be irreducible and M be the set of all irreducible subsets of X containing S. If $\{S_i \in M\}_{i \in I}$ is a chain of inclusions, then let $Y = \cup_{i \in I} S_i$. We claim that Y is also in M, implying the chain has an upper bound.

It is obvious that Y contains S. To see that Y is irreducible, observe that any two open sets U_1 and U_2 that intersect Y non-trivially must intersect some element S_0 of the chain non-trivially.[74] Thus, we have

$$\emptyset \neq U_1 \cap U_2 \cap S_0 \subseteq U_1 \cap U_2 \cap Y,$$

and, by lemma 102 part (ii), Y is also irreducible.

The maximal element of M is an irreducible component of X containing S.

(ii) Follows from a): the union of the irreducible components of X is the same as the union of the irreducible components containing $x \in X$ (they exist because x is irreducible) which clearly yields the whole space.

□

Definition 107. A topological space X where every descending chain of closed sets stabilizes is said to be **Noetherian**.

Example 108. Consider $\mathbb{A}^n(k)$ with the Zariski topology, a descending chain of closed sets is a descending chain of varieties which in turn corresponds to an ascending chain of ideals of $k[x_1, \ldots, x_n]$. Since $k[x_1, \ldots, x_n]$ is Noetherian, these chains must stabilize and we conclude that $\mathbb{A}^n(k)$ is Noetherian. Moreover if V is a variety, $V(\bar{k})$ with the induced topology is also Noetherian.

Proposition 109. *A Noetherian topological space has finitely many components. Moreover, no component is contained in the union of the others.*

[74] U_1 intersects some S_1 and U_2 intersects som S_2, since one of the S_i must be contained in the other (they are in a chain), we can let S_0 be the bigger one.

Proof. Let M be the set of closed subsets of X that are not equal to a finite union of irreducible subsets. Suppose $M \neq \emptyset$ and let Y be a minimal element[75]. It is not irreducible[76], hence $Y = Y_1 \cup Y_2$, where Y_1 and Y_2 are closed. By minimality of Y, Y_1 and Y_2 cannot be in M. Thus, each of Y_1 and Y_2 can be written as a finite union of irreducible components and it follows that Y can also be written as a finite union of irreducible components. This contradicts the fact that $Y \in M$.

In particular, we obtain $X = \cup_{i=1}^{n} X_i$, where X_i are distinct irreducible components.[77] Suppose Y is an irreducible component of X, then $Y = \cup_{i=1}^{n} Y \cap X_i$ and by irreducibility, we can assume $Y = Y \cap X_1$, namely $Y = X_1$. This shows that all irreducible components are in the X_i's, so there are finitely many.

For the second part of the proposition, assume towards a contradiction that $X_i \subseteq \cup_{i \neq j} X_i$, then intersecting with X_i and using irreducibility of X_i yields $X_i = X_i \cap X_j$ for some $j \neq i$, which means X_i and X_j are not distinct. □

Corollary 110. [78] *If $I \lhd k[x_1, \dots, x_n]$, then there are only finitely many minimal prime ideals that contain I and they are called the associated primes of I. Moreover, if I is radical, then $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$, where the $\mathfrak{p}_i$'s are its associated primes.*

Proof. □

Projective varieties

It is useful to consider more general classes of varieties obtained by "gluing together" affine varieties. This section is concerned by such objects, which we call projective varieties. They are defined on the projective space.

Definition 111. The n-dimensional projective space $\mathbb{P}_n(k)$ is the set of all lines in k^{n+1} that go through the origin. It can be described as $(k^{n+1} - 0)/\sim$ where the $\sim$ is the following relation[79]

$$(x_0 : x_1 : \cdots : x_n) \sim (y_0 : y_1 : \cdots : y_n) \Leftrightarrow \exists \lambda \in k^\times, \forall 0 \leq i \leq n, \lambda x_i = y_i.$$

We can also see $\mathbb{P}_n$ as the functor $\mathbf{Fields}_k \to \mathbf{Sets}$ sending a field $L > k$ to the set

$$(L^{n+1} - 0)/\sim .$$

One often writes $\mathbb{P}^n$ for $\mathbb{P}_n$ even though $\mathbb{P}_n \neq (\mathbb{P}_1)^n$ in general.

Lemma 112 (Hilbert's Satz 90)**.** *Let k be a field. If $\lambda : \mathrm{Gal}(\bar{k}/k) \to \bar{k}^\times$ is a continuous crossed homomorphism* [80]*, then there exits $a \in \bar{k}$ such that for any $\sigma \in \mathrm{Gal}(\bar{k}/k)$, $\lambda_\sigma = \frac{a}{\sigma(a)}$.*

Proof. To be seen later in □

Proposition 113. *Let k be a field, then*

$$\{x \in \mathbb{P}_n(\bar{k}) \mid \forall \sigma \in \mathrm{Gal}(\bar{k}/k), \sigma(x) = x\} =: \mathbb{P}_n(\bar{k})^{\mathrm{Gal}(\bar{k}/k)} = \mathbb{P}_n(k).$$

Proof. It is clear that $\mathbb{P}_n(k)$ maps injectively into $\mathbb{P}_n(\bar{k})^{\mathrm{Gal}(\bar{k}/k)}$ with the inclusion map.[81] Moreover, for any $(a_0 : \cdots : a_n) \in \mathbb{P}_n(\bar{k})^{\mathrm{Gal}(\bar{k}/k)}$ and any $\sigma \in \mathrm{Gal}(\bar{k}/k)$, we

[75] It exists because X is Noetherian.

[76] Otherwise it would be a finite union of irreducible subsets (namely, just Y) and it wouldn't be in M.

[77] The first part only yields a finite union of irreducible subsets X_i', but in the decomposition of the whole space, we can take the irreducible components that contain the X_i''s and call them X_i and get rid of duplicates.

[78] This result can be seen as a ring-theoretic version of proposition 109.

[79] We denote the tuples with colons to distinguish these from the usual tuples of affine spaces. This relation says that two elements are equal if one of them is the scaled version of the other. It is clear that all points on the same line going through the origin are equal, hence the first sentence of this definition.

[80] Let G and H be groups with an action $*$ of G on H. A map $\phi : G \to H$ is said to be a **crossed homomorphism** if it is a homomorphism that satisfies $\phi(g_1 g_2) = \phi(g_1)(g_1 * \phi(g_2))$ for any $g_1, g_2 \in G$. Furthermore, we say that it is **continuous** if ??? $\lambda : \mathrm{Gal}(L/k) \to L^\times$

[81] Any element $(x_0 : \cdots : x_n) \in \mathbb{P}_n(k)$ will be invariant under $\mathrm{Gal}(\bar{k}/k)$ because each coordinate is invariant.

know that $(\sigma a_0 : \cdots : \sigma a_n) = (a_0 : \cdots : a_n)$, or equivalently, there is $\lambda_\sigma \in \bar{k}^\times$ such that $(\sigma a_0 : \cdots : \sigma a_n) = \lambda_\sigma (a_0 : \cdots : a_n)$. We obtain a map $\lambda : \mathrm{Gal}(\bar{k}/k) \to \bar{k}^\times = \sigma \mapsto \lambda_\sigma$.[82]

Observe that λ is a crossed homomorphism because if $\sigma, \tau \in \mathrm{Gal}(\bar{k}/k)$, then $\lambda_{\sigma\tau} = \lambda_\sigma \sigma(\lambda_\tau)$. Then, by Hilbert's Satz 90, we obtain some $a \in k^\times$ such that

$$\forall \sigma \in \mathrm{Gal}(\bar{k}/k), \sigma(a_0 : \cdots : a_n) = \frac{a}{\sigma(a)}(a_0 : \cdots : a_n),$$

so $\sigma(aa_0 : \cdots : aa_n) = (aa_0 : \cdots : aa_n)$. We found elements of $aa_j \in \bar{k}$ that are invariant under automorphisms of $\mathrm{Gal}(\bar{k}/k)$, this means that they belong to k and we conclude that $(a_0 : \cdots : a_n)$ is the image of $(aa_0 : \cdots : aa_n) \in \mathbb{P}_n(k)$, yielding surjectivity of the inclusion map. □

Remark 114. The ring of polynomial functions on $\mathbb{P}_n$ is poor. If $f(x_0, \ldots, x_n)$ gives rise to a function on $\mathbb{P}_n$, then it would have to be invariant under scaling, i.e.: $f(\lambda x_0, \ldots, \lambda x_n) = f(x_0, \ldots, x_n)$, but when k is infinite, this only happens when f is constant.[83] Although $f(a_0 : \cdots : a_n)$ is not well-defined when $\deg(f) > 0$, if f is homogeneous of non-zero degree, then $f(a_0 : \cdots : a_n) = 0$ is a well-defined conditions for $(a_0 : \cdots : a_n) \in \mathbb{P}_n$. This is because $f(x) = 0$ implies $f(\lambda x) = \lambda^d f(x) = 0$.

Definition 115. A ***k*-projective variety** V in $\mathbb{P}_n$ is the zero locus of a finite system of homogeneous polynomials in $k[x_1, \ldots, x_n]$:

$$F_1(x_0 : \cdots : x_n) = \cdots F_m(x_0 : \cdots : x_n) = 0.$$

We can view V as a functor

$$\mathbf{Fields}_k \rightsquigarrow \mathbf{Sets} = L \mapsto V(L) = \{x \in \mathbb{P}_n(L) \mid \forall i \in [m], F_i(x) = 0\}.$$

Remark 116. The main justification for working with projective varieties is that the intersection theory is much nicer as we will show.

Example 117. In $\mathbb{P}_2$ (the projective plane), lines corresponds to the solutions of a homogeneous polynomial of degree one ($ax_0 + bx_1 + cx_2 = 0$). Considering the natural map $\mathbb{A}^3 \setminus \{0\} \to \mathbb{P}_2$, we see that any lines in $\mathbb{P}_2$ is the image of a plane in $\mathbb{A}^3$ through the origin. We can conclude that the fact that any two such planes in $\mathbb{A}^3$ intersect only at a common line is equivalent to the fact that any two lines in $\mathbb{P}_2$ intersect in a common point.

Definition 118. We say that a variety in $\mathbb{P}_n$ is **linear** if it is defined by a collection of linear equations [84]. If the set of solutions in $\mathbb{A}^{n+1}$ is a vector space of dimension $d+1$, then d is the dimension of the linear variety.

Definition 119. A **hypersurface** of degree $d > 0$ is a variety defined by a single polynomial equation of degree d. The terms linear hypersurface (or hyperplane) and quadric hypersurfaces are used to describe hypersurfaces of degree one and two respectively.

[82] It measures the obstruction to $(a_0 : \cdots : a_n)$ being defined over k.

[83] Decompose f into its homogeneous components f_d of degree d and fix $x \in k^{n+1}$. Then, for all $\lambda \in k^\times$, we have

$$\sum_{d=0}^{\deg(f)} f_d(x) = \lambda f(x) = f(x) = \sum_{d=0}^{\deg(f)} \lambda^d f_d(x)$$

This is satisfied for infinitely many λ's if and only if f is constant.

[84] Systems of the form $Ax = 0$ for $A \in M_{m \times n}(k)$.

Proposition 120. *Let k be algebraically closed, V be a linear variety in $\mathbb{P}_n(k)$ of dimension $d \geq 1$ and S be a hypersurface. Then, V and S have a non-empty intersection.*[85]

Proof. We can assume without loss of generality that the dimension of the linear variety is 1 (otherwise take a line inside it) and that V is given by the equation $x_2 = x_3 = \cdots = x_n = 0$. Indeed, we can always rotate the whole space so that V becomes this linear variety. More generally, the group of symmetries of $\mathbb{P}_n$ is $GL_{n+1}(k)$, so we can perform lots of transformations while keeping the same structure.

Let S be given by $F(x0 : \cdots : x_n) = 0$. $S \cap L$ is given by the equations $F(x_0 : x_1 : 0 : \cdots : 0) = 0$ which is still homogeneous because all terms with $x_2, \dots x_n$ are killed. This clearly still has zeros (when one of x_0 and x_1 are zero)[86], so we are done. □

Proposition 121. *If $n > 1$, then any two hypersurfaces in $\mathbb{P}_n$ have non trivial intersection over $\bar{k}$.*

Proof. Let V_1 defined by $F(x_0 : \cdots : x_n) = 0$ and V_2 defined by $G(x_0 : \cdots : x_n) = 0$ be the two hypersurfaces, we will show that $V_1(\bar{k}) \cap V_2(\bar{k}) \neq \emptyset$.

Assume without loss of generality that the point $(0 : \cdots : 0 : 1)$ lies neither on $V_1(\bar{k})$ nor $V_2(\bar{k})$[87]. This implies that F has $x_n^{d_1}$ as a monomial and G has $x_n^{d_2}$, where d_1 and d_2 are the degrees of F and G respectively. Moreover, we can also assume that V_1 and V_2 are both irreducible (otherwise we replace them by the irreducible component that contains them) and that neither is contained in the other (otherwise the result is trivial).

Now, we can view F and G as elements of $k(x_0, \dots, x_{n-1})[x_n]$ that are relatively prime in this ring, by our previous assumptions. Thus, we obtain

$$\exists A, B \in k[x_0, \dots, x_n], \exists N \in k[x_0, \dots, x_{n-1}], \quad \frac{A}{N}F + \frac{B}{N}G = 1 \Leftrightarrow AF + BG = N,$$

where $\frac{A}{N}$ and $\frac{B}{N}$ are in lowest terms. Observe that for any irreducible factor ϕ of N, if $\phi \mid A$, then $\phi \mid BG$, but as G is irreducible, we get $\phi \mid B$, implying the fractions are not in lowest terms. Similarly, we can show that if $\phi \mid B$, then $\phi \mid A$ which leads to the same contradiction. Hence, ϕ divides neither A nor B. Moreover, after dividing A by G, we can assume $\deg_{x_n}(A) < \deg_{x_n}(G)$.[88]

Let φ be an irreducible divisor of N, we know that $V((\varphi)) \nsubseteq V(A)$ and $V((\varphi)) \nsubseteq V(B)$, so we can find $(a_0, \dots, a_{n-1}) \in \bar{k}^n$ such that $\varphi(a_0, \dots, a_{n-1}) = 0$ and

$$A(a_0, \dots, a_{n-1}, x_n), B(a_0, \dots, a_{n-1}, x_n) \neq 0.$$

Therefore, if we partially evaluate both sides of $AF + BG = N$ at $(a_0, \dots, a_{n-1})$, we obtain[89]

$$A(a_0, \dots, a_{n-1}, x_n)F(a_0, \dots, a_{n-1}, x_n) = -B(a_0, \dots, a_{n-1}, x_n)G(a_0, \dots, a_{n-1}, x_n),$$

and since $\deg_{x_n}(A) < \deg_{x_n}(G)$, there exists a factor $(x_n - a_n)$ of $F(a_0, \dots, a_{n-1}, x_n)$ that also divides $G(a_0, \dots, a_{n-1}, x_n)$. We conclude that $(a_0, \dots, a_n) \in V_1 \cap V_2$. □

Our main result in this section is the analog of the decomposition of affine varieties into irreducible for their projective counterpart. We will start with a bit more generality.

[85] More intuitively, this result says that any two spaces of co-dimension one and dimension one respectively will intersect. This is clearly not the case in $\mathbb{A}_n$, for instance, take two parallel lines in $\mathbb{A}_2$.

[86] Notice that $F(\cdot : \cdot : 0 : \cdots : 0)$ cannot be constant unless it is zero, otherwise F would have had a non-zero constant coefficient.

[87] We can always do that by using the numerous symmetries of $\mathbb{P}_n(\bar{k})$, we just need at least one point in $\bar{k}^{n+1}$ that does not vanish on either of F and G. If it does not exist, then $(F, G) = \bar{k}[x_0, \dots, x_n]$, but if two homogeneous polynomials generate 1, then one of them must be constant, a case that is not allowed for hypersurfaces.

[88] The Euclidean algorithm in $k[x_0, \dots, x_{n-1}][x_n]$ yields $A = GQ + A'$ with $\deg_{x_n}(A') < \deg_{x_n}(G)$, so we have

$$(GQ + A')F + BG = N \text{ or } A'F + (B + FQ) = N.$$

[89] It is important to note that both sides are non-zero because both F and G have a monomial involving only x_n and $(a_0, \dots, a_{n-1})$ was constructed so that the partial evaluation of A and B are non-zero as well.

Definition 122. A ring R is said to be graded if it is isomorphic (as an additive group) to $\oplus_{d \in \mathbb{N}} R_d$ and if for any $d_1, d_2 \in \mathbb{N}$, $R_{d_1} R_{d_2} \subseteq R_{d_1 d_2}$. We denote π_d to be the projection of R onto its d-th coordinate.

Definition 124. An ideal in a graded ring is said to be homogeneous if it is generated by homogeneous elements (i.e.: elements of R_d for some $d \in \mathbb{N}$).

Example 123. The ring $R = k[x_0, \dots, x_n]$ has the natural grading

$$R = \bigoplus_{d \in \mathbb{N}} R_d,$$

where R_d is the group of homogeneous polynomials of degree d. It is clear that $R_{d_1} R_{d_2} \subseteq R_{d_1 d_2}$. Moreover, the projection π_d collects all the monomials of degree d of its argument.

Theorem 125. *Let $R = \oplus_{d \in \mathbb{N}} R_d$ be a graded ring and $I \lhd R$, the following are equivalent:*

1. *I is homogeneous.*
2. *If $f \in I$, then all of its homogeneous components lie in I.*
3. *R/I is also a graded ring and $R/I = \oplus_{d \in \mathbb{N}} (R_d + I)/I$.*

Proof. Write $I = (f_1, \dots, f_t)$ where each f_i is homogeneous in R_{d_i}.

($1 \implies 2$) If $f \in I$, then for some $\lambda_i \in R$, we can write

$$f = \lambda_1 f_1 + \cdots + \lambda_t f_t,$$

which implies that for any $d \in \mathbb{N}$,

$$\pi_d(f) = \pi_{d-d_1}(\lambda_1) f_1 + \cdots + \pi_{d-d_t}(\lambda_t) f_t \in I.$$

($2 \implies 1$) Write $I = (f_1, \dots, f_t)$ where the f_i's are not a priori homogeneous. If we let D be the highest degree of a monomial of an f_i, we obtain $I = (\pi_1 f_1, \dots, \pi_D f_t)$.[90]

($2 \implies 3$) Clearly, we already have $R/I = \sum_{d \in \mathbb{N}} (R_d + I)/I$. It remains to show that this is in fact a direct sum. If $0 = \sum_{d=0}^{m} \lambda_d$ where $\lambda_d \in (R_d + I)/I$, then, letting $\widetilde{\lambda}_d$ be a preimage of λ_d from the quotient map, this means $\sum_{d=0}^{m} \widetilde{\lambda}_d \in I$. However, this can only happen if each $\widetilde{\lambda}_d$ is in I,[91] so for each d, $\lambda_d = 0$. This shows we indeed have a direct sum.

($3 \implies 2$) Is similar. □

Definition 126. A projective variety $V \subseteq \mathbb{P}_n$ naturally gives rise to an affine variety $\widetilde{V} \subseteq \mathbb{A}^{n+1}$ (by forgetting the quotient).[92] It is called the **affine cone** attached to V. This can be seen as the union of lines that are in the variety seen in the affine space.

Proposition 127 (Projective Nullstellensatz)**.** *Let k be algebraically closed, the assignment $V \mapsto I(V(k))$ gives a bijection*[93]

$$\{\textit{projective varieties over } k\} \leftrightarrow \{\textit{homogeneous radical ideals in } k[x_0, \dots, x_n]\}.$$

Corollary 128. *A system of homogeneous polynomial equations $F_1 = \cdots F_t = 0$ has no solutions over an algebraically closed k if and only if $\sqrt{(F_1, \dots, F_t)} = (x_0, \dots, x_n)$.*

Remark 129. We can decompose the projective space as $\mathbb{P}_n = \Sigma_0 \amalg \cdots \amalg \Sigma_n$, where $\Sigma_j = \{(x_0 : \cdots : x_n) \mid x_j \neq 0\}$. Observe that we have the bijection $\Sigma_j \cong \mathbb{A}^n$:

$$(x_0 : \cdots : x_n) \mapsto (x_0/x_j, \dots, x_{j-1}/x_j, x_{j+1}/x_j, \dots, x_n/x_j),$$

and that clearly $\mathbb{P}_n - \Sigma_j = \mathbb{P}_{n-1}$, so $\mathbb{P}_n = \mathbb{A}^n \amalg \mathbb{P}_{n-1}$.[94] Moreover, for a projective

[90] This holds because all homogeneous components of polynomials in I are in I and I is generated by the homogeneous components of its polynomials.

[91] If $\widetilde{\lambda}_d = r + i \in R_d + I$, then $\sum_{d=0}^{m} \widetilde{\lambda}_d - i$ is in I but has r as its homogeneous component, so $r \in I$ and $\widetilde{\lambda}_d \in I$.

[92]

[93] Note that the empty variety is is mapped to $(x_0, \dots, x_n)$ because 0 is not considered in the projective variety.

[94] Another way to view the projective space is as a compactification of the affine space and this decomposition illustrates this idea.

variety V in $\mathbb{P}_n$, we can write $V = V_0 \cup \cdots \cup V_n$, where $V_j = V \cap \Sigma_j$. To obtain the equations that define V_j, replace x_j by 1 in each F_i. This operation does not preserve homogeneity of the F_i's, but still we get the affine variety V_j.

Conversely, if $V_0 \subseteq \mathbb{A}^n$ is an affine variety defined by $F_1 = \cdots = F_t = 0$. We claim that there exists $V \subseteq \mathbb{P}_n$ such that $V_0 = V \cap \Sigma_0$.[95] Let D_i be the maximum degree of a monomial in one of the F_i's, then define

$$F_i' = \sum_{d=0}^{D_i} x_0^{D_i - d} \pi_d(F_i).$$

F_i' is called the homogeneous completion of F_i by x_0 and one can verify that the F_i''s define the suitable variety V.

Recall that for affine varieties, their decomposition into a finite union of irreducible components $V = V_1 \cup \cdots \cup V_s$ translated to the ring-theoretic fact that any radical ideal is the intersection of a finite collection of minimal prime ideals containing I. We now want to talk about decomposition but for projective varieties and we will work in the opposite direction, namely, from a ring-theoretic argument to the geometric result).

Lemma 130. *If $\mathfrak{p}$ is a prime ideal of a graded ring R, and $\mathfrak{p}^*$ is the ideal generated by the homogeneous elements of $\mathfrak{p}$, then $\mathfrak{p}^*$ is also a prime ideal.*[96]

Proof. Suppose there exists $a, b \notin \mathfrak{p}^*$ such that $ab \in \mathfrak{p}^*$ for a $d \in \mathbb{N}$ sufficiently large, write

$$a = \pi_0(a) + \cdots + \pi_d(a) \text{ and } b = \pi_0(b) + \cdots + \pi_d(b).$$

Let i and j be the greatest integers such that $\pi_i(a) \notin \mathfrak{p}^*$ and $\pi_j(b) \notin \mathfrak{p}^*$, namely, we have $\pi_{i+t}(a), \pi_{j+t}(b) \in \mathfrak{p}^*$ for all $t > 0$.[97]

By construction, $\mathfrak{p}^*$ is a homogeneous ideal, so for each k, $\pi_k(ab) \in \mathfrak{p}^*$ (by theorem 125). Then, we have

$$\pi_{i+j}(ab) = \pi_i(a)\pi_j(b) + \sum_{t=-i}^{j} \pi_{i+t}(a)\pi_{j-t}(b),$$

and since the L.H.S. is in $\mathfrak{p}^*$ and every element of the sum is in $\mathfrak{p}^*$ (by maximality of i and j), we infer that $\pi_i(a)\pi_j(b) \in \mathfrak{p}^*$. Therefore, $\pi_i(a)\pi_j(b)$ is also in $\mathfrak{p}$ and by primality either $\pi_i(a) \in \mathfrak{p}$ or $\pi_j(b) \in \mathfrak{p}$, so either $\pi(a)_i \in \mathfrak{p}^*$ or $\pi_j(b) \in \mathfrak{p}^*$ (because they are homogeneous). □

Proposition 131. *Let $R = \oplus_{j \in \mathbb{N}} R_j$ be a graded ring and $I \lhd R$ be homogeneous. Then, all minimal prime divisors*[98] *of I are homogeneous.*

Lem implies prop. If $\mathfrak{p} \supseteq I$ is a minimal prime, then, since I is homogeneous, it is generated by some homogeneous elements of $\mathfrak{p}$. Thus,we have $\mathfrak{p} \supseteq \mathfrak{p}^* \supseteq I$ and by the previous lemma $\mathfrak{p}^*$ is prime, so $\mathfrak{p} = \mathfrak{p}^*$ by minimality. We conclude that $\mathfrak{p}$ is also homogeneous. □

Remark 132. The minimality condition is a key condition. Geometrically, consider the usual ring $k[x_0, \ldots, x_n]$ and an affine cone $\widetilde{V} \subseteq \mathbb{A}^n$, we see that every irreducible subset of an affine cone is not necessarily affine cones.

Corollary 133. *Every irreducible component of an affine cone is an affine cone and every irreducible component of a projective variety is a projective variety.*

[95] This is called the projective closure of V.

[96] Geometrically, $\mathfrak{p}$ corresponds to a variety and $\mathfrak{p}^*$ to the affine cone generated by this variety.

[97] These indices exist because $a, b \notin \mathfrak{p}^*$.

[98] In the sense that it contains no other prime divisor of I.

Introduction to Spec and Schemes

The motivation for this section is that the mapping from an ideal $I \lhd k[x_1, \dots, x_n]$ to $V(I)$ does not carry all the information. Recall that if the radical of I_1 is equal to the radical to I_2, then $V(I_1) = V(I_2)$. More precisely, we are forgetting about some quotients that contain nilpotent elements, but these are important. This section is aimed at positively answering the following:

Question 134. *Is there a geometric object corresponding to general ideals of $k[x_1, \dots, x_n]$?*

We will indeed see that non-radical ideals have a geometric meaning, as informally shown by these simple examples.

Examples 135.

1. Consider $I = (x^2) \lhd k[x]$, we know $\sqrt{I} = (x)$ and $V(I) = \{(0)\}$ in every affine space over an extension of k. We also have the notion of the coordinate ring $\mathcal{O}_{V(I)}$ which is $k[x]/(x) = k$. If we "redefine" a new object $\widetilde{V}$ such that its coordinate ring of is $\mathcal{O}_{\widetilde{V}(I)} = k[x]/(x^2)$. Recall that f vanishes on $V(I)$ if and only if $f = 0 \in \mathcal{O}_V$, so we analogously define that f vanishes on $\widetilde{V}(I)$ if and only if $f = 0 \in \mathcal{O}_{\widetilde{V}(I)}$. The former holds if and only $f(0) = 0$ while the latter holds if and only if $f(0) = f'(0) = 0$, we have recovered the lost information.[99]
2. Consider $I = (x^2, xy, y^2) \lhd k[x, y]$. Then, $V(I)$ still only contain the origin in any affine space. However, in $\widetilde{V}(I)$, we have a thickened origin with vectors representing each first order partial derivative.
3. The "double line": Let $I = (x^2) \lhd k[x, y]$, we have $\mathcal{O}_{\widetilde{V}(I)} = k[x, y]/(x^2) = k[y] \oplus k[y]x$ with $x^2 = 0$. Also, we can write $f(x, y)$ in $\mathcal{O}_{\widetilde{V}(I)}$ as $f(0, y) + \frac{\partial}{\partial x} f(0, y)x$.

The formalization of these examples will use the notion of spectrum of rings.

Definition 136. The spectrum of a ring R is $\operatorname{Spec}(R) := \{\mathfrak{p} \lhd R \mid \mathfrak{p} \text{ is prime}\}$.

Proposition 137. *Denote $V(I) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid I \subseteq \mathfrak{p}\}$[100], then the collection of closed sets $\{V(I) \mid I \lhd R\}$ defines a topology on $\operatorname{Spec}(R)$, we refer to it as the **Zariski topology**.*

Proof. 1. We have $\emptyset = V(R)$ and $\operatorname{Spec}(R) = V(0)$, so both sets are closed.

2. If $\{I_\alpha\}_{\alpha \in A}$ is a collection of prime ideals, then it is clear that

$$\begin{aligned} \bigcap_{\alpha \in A} V(I_\alpha) &= \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \forall \alpha \in A, \mathfrak{p} \supseteq I_\alpha\} \\ &= \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supseteq \sum_{\alpha \in A} I_\alpha\} = V\left(\sum_{\alpha \in A} I_\alpha\right). \end{aligned}$$

3. If I_1 and I_2 are prime ideals, then we claim that[101]

$$V(I_1) \cup V(I_2) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supseteq I_1 \text{ or } \mathfrak{p} \supseteq I_2\} = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supseteq I_1 \cap I_2\}.$$

[99] Geometrically, we can think of the points of $\widetilde{V}(I)$ as thickened points with tangent vectors associated.

[100] When I is principal, say generated by p, we also write $V(p)$ for simplicity.

[101] The reasoning will work for any finite collection of ideals (or one could use induction), but it is not valid for infinite collections because it would require taking an infinite product.

The $\subseteq$ inclusion is clear. For $\supseteq$, assume that $\mathfrak{p} \supseteq I_1 \cap I_2$ does not contain I_1 nor I_2, then there exists $a_1 \in I_1 - \mathfrak{p}$ and $a_2 \in I_2 - \mathfrak{p}$. However, this yields $a_1 a_2 \in I_1 \cap I_2 \subseteq \mathfrak{p}$, which contradicts the primeness of $\mathfrak{p}$.

□

Examples 138. 1. The spectrum of $\mathbb{Z}$ consists of the zero ideal and all the ideals generated by primes p. The closed sets are $V(n) = \{(p) \mid p \text{ is a prime factor of } n\}$, if $n \neq 0$ and $V(0) = \operatorname{Spec}(\mathbb{Z})$.

2. The spectrum of $k[x]$ consists of the zero ideal and the ideals generated by irreducible polynomials. If k is algebraically closed, then $\mathbb{A}^1(k)$ is in bijection with $\operatorname{Spec}(R) - \{(0)\}$ by sending a to $(x-a)$.[102] Otherwise, $\operatorname{Spec}(k[x])$ contains many more points.

3. The spectrum of $k[x,y]$ is quite more complicated even when k is algebraically closed, i.e.: the inclusion $\mathbb{A}^2(k) \hookrightarrow \operatorname{Spec}(k[x,y]) = (a,b) \mapsto (x-a, y-b)$ is not a bijection. This happens because $f(x,y)$ can be irreducible without being in this kind of ideal. For such an f, the closure of $\{(f)\}$ is $\{(f), 0\} \cup \{(x-a, y-b) \mid f(a,b) = 0\}$.

Definition 139. Given $A \subseteq \operatorname{Spec}(R)$, the **vanishing ideal** of A is $I(A) := \cap_{\mathfrak{p} \in A} \mathfrak{p}$.

Proposition 140. *If $A \subseteq \operatorname{Spec}(R)$, then $V(I(A)) = \overline{A}$ (the closure of A).*

Proof. Clearly $A \subseteq V(I(A))$ and $V(I(A))$ is closed, thus $\overline{A} \subseteq V(I(A))$. Conversely, if $V(I)$ contains A, then for all $\mathfrak{p} \in A$, $\mathfrak{p} \supseteq I$, implying $I \subseteq \cap_{\mathfrak{p} \in A} = I(A)$. We obtain that $V(I(A)) \subseteq V(I)$[103] and we conclude that $V(I(A))$ is the smallest closed set containing A, namely that $V(I(A)) = \overline{A}$. □

Lemma 141 (Krull)**.** *Let S be a multiplicative subset of R not containing 0. If I is an ideal of R that trivially intersects S, then there exists a prime $\mathfrak{p} \supseteq I$ such that $\mathfrak{p} \cap S = \emptyset$ as well.*[104]

Proof. Let M be the collection of ideals $J \supseteq I$ such that $J \cap S = \emptyset$. We know that M is not empty because it contains I and that it satisfies the maximal chain condition, because if $\{J_\alpha\}_{\alpha \in A}$ is a chain in M, then $\cup_{\alpha \in A} J_\alpha$ is clearly in M and is an upper bound. Thus, by Zorn's lemma, M contains a maximal element $\mathfrak{p}$.

We claim that $\mathfrak{p}$ is prime. Assume towards a contradiction that $a, b \notin \mathfrak{p}$ and $ab \in \mathfrak{p}$, then both $\mathfrak{p} + (a)$ and $\mathfrak{p} + (b)$ are strictly greater than $\mathfrak{p}$, so they must intersect with S (by maximality of $\mathfrak{p}$). Then, we can find $p_1, p_2 \in \mathfrak{p}$ and $r_1, r_2 \in R$ such that $p_1 + r_1 a$ and $p_2 + r_2 b$ are both in S, hence, so is their product $p_1 p_2 + p_2 r_1 a + p_1 r_2 b + r_1 r_2 ab$. However, we see that each term in this sum is in $\mathfrak{p}$, so this contradicts $\mathfrak{p} \cap S = \emptyset$. □

Corollary 142. [105]

1. *$\cap_{\mathfrak{p} \in \operatorname{Spec}(R)} = \sqrt{0}$, namely the intersection of the prime ideals is precisely the nilpotent elements.*

2. *For any ideal $I \lhd R$, $\cap_{\mathfrak{p} \in V(I)} = \sqrt{I}$.*

[102] In fact, this map is a homeomorphism with respect to the Zariski topology. Indeed, the inverse image of $V(I)$ is precisely the variety defined by I (hence the notation), while the image of a variety X is $V(I(X))$.

[103] It is true in general that $I \subseteq J$ implies $V(J) \subseteq V(I)$.

[104] Note that Krull's lemma implies the fact that every ideal is contained in a maximal ideal, taking $S = \{1\}$.

[105] The second part can be seen as a Nullstellensatz and works for more general polynomial rings. The traditional approach in algebraic geometry was to work over $\bar{k}$, so the old Nullstellensatz was enough. In the modern approach, one replaces $V(I) \subseteq \mathbb{A}^n(k)$ by $\operatorname{Spec}(k[x_1, \ldots, x_n]/I)$, hence the need for this more general statement.

Proof.

1. It is clear that $\sqrt{(0)} \subseteq \cap_{\mathfrak{p}\in\mathrm{Spec}(R)}$.[106]

   For the other inclusion, suppose that x is not nilpotent, then let $S = \{x^m \mid m \in \mathbb{N}\}$, it does not contain 0, so we can use Krull's lemma with $I = (0)$ to conclude that there is a prime ideal with $x \notin \mathfrak{p}$.

2. This is a simple application of the first part to the quotient ring R/I.[107]

□

Theorem 143. *Any ring homomorphism $\varphi : R \to S$ induces a continuous map*

$$\varphi^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R) = \mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}).$$

Proof. If $\mathfrak{p} \lhd S$ is prime, then it is trivial to show that $\varphi^*(\mathfrak{p})$ is an ideal of R, to see it is prime, note that $R/\varphi^{-1}(\mathfrak{p}) \cong \varphi(R)/\mathfrak{p} \subseteq S/\mathfrak{p}$.[108]

The continuity of φ^* follows from the following derivation (for any ideal $I \lhd R$):

$$\begin{aligned}(\varphi^*)^{-1}(V(I)) &= (\varphi^*)^{-1}\{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq I\}\\ &= \{\mathfrak{p} \in \mathrm{Spec}(S) \mid \varphi^{-1}(\mathfrak{p}) \supseteq I\}\\ &= \{\mathfrak{p} \in \mathrm{Spec}(S) \mid \mathfrak{p} \supseteq \varphi(I)\}\\ &= V(\varphi(I)).\end{aligned}$$

Moreover, it is clear that $\varphi^*\psi^* = (\psi\varphi)^*$ and $\mathrm{id}^* = \mathrm{id}$, so we conclude that the maps $R \mapsto \mathrm{Spec}(R)$ and $\varphi \mapsto \varphi^*$ form a contravariant functor **Rings** $\rightsquigarrow$ **Top**.[109] □

Remark 144. This functor is not injective on objects. For instance, if R is a ring and $I = \sqrt{0}$, then the continuous map $\mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$ induced by the quotient map is a homeomorphism. Hence, we can't distinguish between the two spaces and we lost the information about the nilpotent elements.

The notion of scheme which we will cover next will add extra structure on $\mathrm{Spec}(R)$ in order to regain this information. The basic principle is that an element $f \in R$ can be viewed as a "function" on $\mathrm{Spec}(R)$, with $f(\mathfrak{p})$ being the image of f in $R/\mathfrak{p}$. Note that the codomain of f depends on the argument, so it is not truly a function. What is more, f need not be determined by its values, namely, if f is a nilpotent element of R, then $\forall \mathfrak{p} \in \mathrm{Spec}(R), f(\mathfrak{p}) = 0$,[110] but we do not want to think of f as 0 (otherwise, we would not have gained any information).

We start developing the formal concepts.

Definition 145. A sheaf of rings (we will often simply say sheaf) on a topological space X is a contravariant functor $\mathcal{O}_X : T(X) \rightsquigarrow$ **Rings**[111] with two additional properties listed below.

Unpacked, this definition says that for each open $U \subseteq X$, we have a ring $\mathcal{O}_X(U)$ and for each inclusion of open sets $U \subseteq V$, then we have a ring homomorphisms[112] $|^V_U$: $\mathcal{O}_X(V) \to \mathcal{O}_X(U)$ satisfying the following properties:

1. For any open set U, $|^U_U$ is the identity on $\mathcal{O}_X(U)$.

[106] Any ideal contains 0, thus if $x^m = 0$ for some m, then $x^m \in \mathfrak{p}$ which implies $x \in \mathfrak{p}$ by primeness.

[107] By the fourth isomorphism theorem, $V(I)$ in R is in correspondence with $V(0)$ in R/I. Moreover, the preimage of nilpotent elements in R/I is precisely $\sqrt{I}$. We conclude with the fact that the preimage of $\cap_{\mathfrak{p}\in V(I)}\overline{\mathfrak{p}}$ is $\cap_{\mathfrak{p}\in V(I)}\mathfrak{p}$.

[108] Since the R.H.S. is an integral domain (by primality), so is the L.H.S. and we conclude that $\varphi^*(\mathfrak{p})$ is prime.

[109] The objects of **Top** are topological spaces and morphisms are continuous maps.

[110] Recall that nilpotent elements are in the intersection of the prime ideals by corollary 142.

[111] The category $T(X)$ has all the open sets of X as its objects and the morphisms can be described for any open sets U, V as

$$\mathrm{Hom}(U,V) = \begin{cases} i_{U,V} & U \subseteq V \\ \varnothing & \text{o/w} \end{cases}.$$

[112] They are called the restriction maps. And we use them with the suffix notation, namely $|^V_U\,(f) = f\,|^V_U$.

2. For any open sets $U \subseteq V \subseteq W$, $|^W_U = |^V_U \circ |^W_V$.

3. For any open cover $\{U_\alpha\}$ of an open set U, if $f \in \mathcal{O}_X(U)$ is such that $\forall \alpha, f |^U_{U_\alpha} = 0$, then $f = 0$.

4. For any open cover $\{U_\alpha\}$ of an open set U and any collection $\{f_\alpha \in \mathcal{O}_X(U_\alpha)\}$ such that
$$\forall \alpha, \beta, \quad f_\alpha |^{U_\alpha}_{U_\alpha \cap U_\beta} = f_\beta |^{U_\beta}_{U_\alpha \cap U_\beta},$$
there is an element $f \in \mathcal{O}_X(U)$ with $f_\alpha = f |^U_{U_\alpha}$ for all α's.[113]

Remark 146. One can infer from the third property that the restriction maps are always injective and we will see later that it follows from the fourth that $\mathcal{O}_X$ is determined by where it sends an open basis of X. Moreover, we can use the third property to see that the glued data f in the fourth property is unique. In fact, one can also define sheaves by requiring that the glued data is unique and dropping the third property.

Definition 147. The sheaves on X form a category where if $\mathcal{O}_X$ and $\mathcal{O}'_X$ are sheaves on X, then a morphism $\pi : \mathcal{O}_X \to \mathcal{O}'_X$ is a natural transformation between the two functors. Explicitly, it associates to any open set U, a homomorphism $\pi_U : \mathcal{O}_X(U) \to \mathcal{O}'_X(U)$ such that for any $U \subseteq V$, the following diagram commutes, where the restriction maps are coming from the appropriate functors.

$$\begin{tikzcd}
\mathcal{O}_X(V) \arrow[r, "\pi_V"] \arrow[d, "|^V_U"'] & \mathcal{O}'_X(V) \arrow[d, "|^V_U"] \\
\mathcal{O}_X(U) \arrow[r, "\pi_U"] & \mathcal{O}'_X(U)
\end{tikzcd}$$

Definition 148. Let $X = \text{Spec}(R)$, for any $f \in R$, we define $U_f = \{\mathfrak{p} \in \text{Spec}(R) \mid f(\mathfrak{p}) \neq 0\}$, equivalently $\mathfrak{p} \in U_f$ if and only if $f \notin \mathfrak{p}$. We call these sets **distinguished** open sets.

Proposition 149. *The collection of distinguished open sets is a basis for X for the Zariski topology on* Spec(R).

Definition 150. The structure sheaf on Spec(R) is defined by $\mathcal{O}_X(U_f) = R[f^{-1}]$.[114]

With the same intuition, we can see that $\mathcal{O}_X(U_f \cap U_g) = R[f^{-1}, g^{-1}]$. Moreover, by injectivity, we get that $\mathcal{O}_X(U_f \cup U_g)$ is a subring of $\mathcal{O}_X(U_f) \times \mathcal{O}_X(U_g)$. More precisely, since both projections need to restrict to the same thing on $\mathcal{O}_X(U_f \cap U_g)$, we have

$$\mathcal{O}_X(U_f \cup U_g) = \{(\alpha_f, \alpha_g) \mid \text{the images of } \alpha_f \text{ and } \alpha_g \text{ in } R[f^{-1}, g^{-1}] \text{ are the same}\}.$$

This is a fiber product and is denoted $R[f^{-1}] \times_{R[f^{-1}, g^{-1}]} R[g^{-1}]$.

Fact 151. *The restriction maps are well-defined, i.e.: if $U_g \subseteq U_f$, then $R[f^{-1}] \subseteq R[g^{-1}]$.*

[113] The last two properties are not part of the functoriality of $\mathcal{O}_X$. Informally, they describe the locality of the sheaf, namely, the first one says that if f is locally zero, then it zero and the second one says that local data can be glued together.

[114] The intuition for this definition is that for any $g \in R[f^{-1}]$ and $\mathfrak{p} \in U_f$, $g \pmod{\mathfrak{p}}$ is well-defined. Note that f cannot be nilpotent for $R[f^{-1}]$ to be well defined, but if it is, then U_f is empty, so $\mathcal{O}_X(U_f)$ need not be defined.

Proof. Taking the complements, we see that

$$U_g \subseteq U_f \Leftrightarrow \{\mathfrak{p} \in \text{Spec}(R) \mid g \in \mathfrak{p}\} \supseteq \{\mathfrak{p} \in \text{Spec}(R) \mid f \in \mathfrak{p}\}.$$

Thus, intersecting the primes in the two sets on the R.H.S., we obtain by corollary 142, $\sqrt{(g)} \subseteq \sqrt{(f)}$. In particular, there exists $n > 0$ such that $g^n = fh$, or equivalently, $f^{-1} = hg^{-n}$, so $R[f^{-1}] \subseteq R[g^{-1}]$. □

Examples 152. 1. The spectrum of a field is a single point $*$ and the structure sheaf assigns the whole field to $\{*\}$.

2. Let k be a field and $R = k[\varepsilon]/(\varepsilon^2)$, then $\text{Spec}(R) = \{*\}$, so it has the same topological space as the first example. However, the structure sheaf is different since it assigns $k[\varepsilon]$ to $\{*\}$. We see that the "functions" we obtain have more structure, namely, they can be "evaluated" and "differentiated" once.

3. Recall that $\text{Spec}(\mathbb{Z}) = \{p \mid p \text{ is prime}\} \cup \{*\}$. For $f \in \mathbb{Z}$, we have $U_f = \{p \text{ prime} \mid p \nmid f\}$ and $\mathcal{O}_X(U_f) = \mathbb{Z}[f^{-1}]$.

Definition 153. Let $\mathcal{O}_X$ be a sheaf of rings on X and $x \in X$. Then, the stalk of $\mathcal{O}_X$ at X is[115]

$$\mathcal{O}_{X,x} = \varinjlim_{U \subseteq X, x \in U} \mathcal{O}_X(U) = \bigcup_{U_f \ni x} \mathcal{O}_X(U_f) = \bigcup_{f \in R, f \notin x} R[f^{-1}].$$

Definition 154. A morphism of affine schemes $\pi : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a continuous map $\pi : X \to Y$ along with a morphism of sheaves $\pi^{\#} : \mathcal{O}_Y \to \pi_* \mathcal{O}_X$, where $\pi_* \mathcal{O}_X$ is the pushforward of the structure sheaf on x, i.e.: $\pi_* \mathcal{O}_X(U) = \mathcal{O}_Y(\pi^{-1}(U))$.

Proposition 155. *Every morphism* $\pi : (\text{Spec}(S), \mathcal{O}_Y) \to (\text{Spec}(R), \mathcal{O}_X)$ *is completely determined by the associated map* $\pi^{\#} : \mathcal{O}_X(X) \to \mathcal{O}_Y(Y) = \pi_* \mathcal{O}_Y(X) = R \to S$.

Corollary 156. *The functor* Spec : ***Rings*** $\rightsquigarrow$ ***Schemes*** *is an anti-equivalence of categories.*[116]

The passage from R to $(\text{Spec}(R), \mathcal{O}_X)$ interprets morphisms of rings geometrically. If S is a multiplicative set generated by some $f \in R$ not nilpotent. Then, the inclusion $R \hookrightarrow R[f^{-1}]$ induces the morphism $\text{Spec}(R[f^{-1}]) \hookrightarrow \text{Spec}(R)$. This map is called an open embedding or open inversion. If $I \lhd R$, then the quotient map $R \to R/I$ induces $\text{Spec}(R/I) \to \text{Spec}(R)$. This map is a closed embedding of $V(I)$ in $\text{Spec}(R)$.

Everything here is fairly formal. There is an extensive dictionary between objects/concepts/constructions in ring theory and corresponding geometric notions in scheme theory.

Non-commutative algebras

General examples

We start with a general construction of a non-commutative ring. Let R be a commutative ring and M be a module over R, then we denote $\text{End}_R(M)$ the ring[117] of

[115] The last two equalities hold when $X = \text{Spec}(R)$. If x corresponds to a prime ideal $\mathfrak{p} \lhd R$ (when $X = \text{Spec}(R)$), then $\mathcal{O}_{X,x}$ corresponds to the localization of R at $\mathfrak{p}$.

[116] In other words, Spec induces a bijection between the objects of the categories and bijections between the appropriate Hom sets, i.e.: for any R, S, $\text{Hom}_{\textbf{Schemes}}(\text{Spec}(S), \text{Spec}(R)) \cong \text{Hom}_{\textbf{Rings}}(R, S)$.

[117] Addition is defined point-wise and multiplication is composition of functions, i.e.: for any $\phi, \psi \in \text{End}_R(M)$ and $x \in M$,

$$(\phi + \psi)(x) = \phi(x) + \psi(x)$$
$$(\phi \cdot \psi)(x) = \phi(\psi(x)).$$

endomorphisms of M that preserve the R-module structure, it is not commutative in general. A prototypical example of such rings that is thoroughly studied studied in linear algebra is when R is a field and $M \cong R^n$, then endomorphisms of M are precisely the $n \times n$ matrices over R, denoted $M_n(R)$.

Our goal for the third part of this course is to arrive at the classification of a particular kind of rings. Unsurprisingly, the class of all rings is not amenable to classification, so we will focus on a soon defined subset of **Rings**. We start our focus on a particular setting, namely, when R is an algebra over a field k.[118]

Examples 157. Here are some examples of such rings:

1. We have already seen the ring of $n \times n$ matrices over k, but it is also a k-algebra where the inclusion $k \hookrightarrow M_n(k)$ sends λ to the scalar matrix λI_n. Also, we remark that, even for general rings R, the assignment $R \mapsto M_n(R)$ is a functor **Rings** $\rightsquigarrow$ **Rings**.

2. With the underlying field k being the real numbers, we can define the algebra of Hamiltonian quaternions $\mathbb{H} := \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ with the relations

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij = -ji &= k \\ ki = -ik &= j \\ jk = -kj &= i. \end{aligned}$$

   Surprisingly, $\mathbb{H}$ is a division algebra, i.e.: every element has an inverse. [119]

3. Let G be a finite group and k a field, the group ring is defined as

$$k[G] := \left\{ \sum_{g \in G} a_g g \mid \forall g \in G, a_g \in k \right\},$$

   where addition and multiplication are extended in a natural way from the field addition and group operation respectively. These rings are particularly interesting because k-linear representations of G are equivalent to modules over $k[G]$ (in the categorical sense).

4. Let k be a field and consider the ring $k[x, \frac{d}{dx}]$ of polynomials in x and $\frac{d}{dx}$ viewed as operators on $k[x]$. Specifically, we want $\frac{d}{dx}P(x) = P'(x)$ for any polynomial in x.[120] It is non-commutative because we have

$$\left(\frac{d}{dx}x - x\frac{d}{dx}\right)P(x) = \frac{d}{dx}xP(x) - x\frac{d}{dx}P(x) = xP'(x) + P(x) - xP'(x) = P(x),$$

   which implies $\frac{d}{dx}x - x\frac{d}{dx} = 1$.

Definition 158. A module M over a ring R is said to be **simple** if it has no non-trivial submodule. A module M is **semisimple** if it is a direct sum of simple submodules.

[118] Notice that we can also view R as a k-vector space by forgetting the ring structure and keeping only addition and multiplication by scalars (elements of k). When we want to emphasize this structure, we will write V_R.

[119] For $a, b, c, d \in \mathbb{R}$, we have

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

Warning: in general it is ambiguous to write fractions in a non-commutative division algebra because $\frac{x}{y}$ can be interpreted as xy^{-1} or $y^{-1}x$. Fractions are well-defined precisely when the denominators are in the center, ($\mathbb{R}$ is the center of $\mathbb{H}$, so the inverse described above is well-defined).

[120] Note that the polynomial $P(x)$ lives in $k[x]$ as a polynomial ring, it does not live in the ring of operators we are considering.

Examples 159. 1. Let k be a field, $R = M_n(k)$ and $M = k^n$ (viewed as column vectors), then M is simple (as a left $M_n(k)$-module). To see this, let $N \subseteq M$ be a non-zero submodule, then N contains some vector $v_1 = (d_1, \ldots, d_n)$ where some d_i is non-zero, without loss of generality, we can say $d_1 = 1$ and $d_i = 0$ for $i > 1$.[121] Then, letting $v_i = M_i v_1 \in N$ where M_i is the permutation matrix corresponding to $(1\ i)$, we see that $\{v_1, \ldots, v_n\} \subseteq N$ is the standard basis, so we conclude $N = M$.

2. Any module over a field is semi-simple. This follows from a basic result in linear algebra, namely, that any vector space has a basis (even infinite dimensional vector spaces).

3. Let k be a field and G a finite group:

   Proposition 160 (Mascke). *If* $\operatorname{char}(k) \nmid |G|$, *then every module over* $k[G]$ *is semisimple.*

   Proof. We will show that if $N \subseteq M$, then there exists a complementary submodule N', i.e.: $N' \subseteq M$ such that $N \oplus N' = M$, then the result will follow because you can take a minimal non-zero submodule N, write $M = N \oplus N'$ and recurse on N'.[122]

   Since N and M are k-vector spaces, we know that there is a projection $\pi : M \to N$ (idempotent and surjective). Observe that $\ker \pi$ is the complement of N as a k-vector space, but it is not necessarily a $k[G]$-module. Define the following $k[G]$-module homomorphism[123]

   $$\widetilde{\pi} = \frac{1}{|G|} \sum_{g \in G} g \circ \pi \circ g^{-1}, \text{ where } g \text{ is the (left) multiplication map by } g.$$

   We claim that $\operatorname{Im}(\widetilde{\pi}) = N$. $\subseteq$ is trivial because π always projects onto N and $\supseteq$ is clear because $\widetilde{\pi}$ is the identity on N. We conclude that $N' = \ker \widetilde{\pi}$ is the complementary $k[G]$-submodule to N. □

4. Let us construct a counter example to the previous proposition when $\operatorname{char}(k) \mid |G|$. Let $k = \mathbb{F}_2$ and $C_2 = \{1, \tau\}$ be the cyclic group of order two, then we have

   $$\begin{aligned} \mathbb{F}_2[G] &\cong \mathbb{F}_2[\tau]/(\tau^2 - 1) \\ &= \mathbb{F}_2[\tau]/((\tau - 1)^2) \\ &= \mathbb{F}_2[\tau - 1]/((\tau - 1)^2) \\ &= \mathbb{F}_2[\epsilon]/(\epsilon^2) \end{aligned}$$

   This is not semisimple over itself because $N = \mathbb{F}_2\epsilon$ is a simple submodule, but if N' is its complementary submodule, then it must contain $1 + a\epsilon$ and hence $\epsilon(1 + a\epsilon) = \epsilon \in N$ contradicting $N' \cap N = \emptyset$.

Definition 161. A ring R is (left)[124] semisimple if it is semisimple as a left module over itself, i.e.: R is a direct sum of minimal left ideals.

[121] First, multiply v_1 by a permutation matrix so that the first coordinate is non-zero, then apply projection onto the first coordinate and a rescaling by d_1^{-1}.

[122] Argue why we can find the minimal.

[123] It is clearly a homomorphism because it is the sum of compositions of homomorphisms. Also, notice that $\frac{1}{|G|}$ is only well-defined when $\operatorname{char}(k) \nmid |G|$, hence the assumption in the statement.

[124] We will see that left semisimplicity is equivalent to right semisimplicity in corollary 171 but until then, we omit the adjective left for brevity and never work with right semisimple rings.

Examples 162. 1. A division ring (or skew field) D is a non-commutative k-algebra in which every non-zero element has an inverse. Such a D is obviously simple over itself,[125] hence semisimple.

2. Let k be a field, $R = M_n(k)$ and denote V_j the set of matrices with non-zero entries only in the j-th column. The latter is clearly stable under left multiplication by elements of R,[126] and we have $R = V_1 \oplus \cdots \oplus V_n$. A similar argument to example 159.1 yields that each V_i is minimal/simple, thus R is semisimple.

3. We can extend the previous example and be slightly more abstract. Let k be a field, V a finite dimensional k-vector space and $R = \mathrm{End}_k(V)$. Let $\varphi_1, \dots, \varphi_n$ be a basis for V^* and $V_i = \ker(\varphi_i) \subseteq V$, then we can write
$$\mathrm{End}_k(V) \cong \mathrm{Hom}(V/V_1, V) \oplus \cdots \oplus \mathrm{Hom}(V/V_n, V),$$
where $\mathrm{Hom}(V/V_j, V)$ embeds naturally in $\mathrm{Hom}(V, V)$.[127] Each summand is clearly stable under left composition by any endomorphism because the kernel of a linear map can only grow after composition.

4. A direct product of semisimple rings is semisimple.

Wedderburn's classification

We now list several simple lemmas that will lead to Wedderburn's classification.

Lemma 163. *Let $R = M_n(D)$ where D is a division algebra over a field k and $M = D^n$ viewed as a left R-module (we already saw it is simple), then $\mathrm{End}_R(M) \cong D^{op}$.*[128]

Proof. Define
$$\phi : D^{\mathrm{op}} \to \mathrm{End}_R(D^n) = d \mapsto (\cdot)d,$$
where $(\cdot)d$ is the coordinate-wise multiplication by d on the right. It is clear that
$$\phi(d_1 + d_2)(v) = \phi(d_1)(v) + \phi(d_2)(v) \text{ and } \phi(d_1 d_2)(v) = \phi(d_2) \circ \phi(d_1)(v),$$
so ϕ is indeed a homomorphism. Moreover, ϕ is injective because the kernel, being an ideal of D^{op}, must be the zero ideal.[129] For surjectivity, observe that knowing where a given $f \in \mathrm{End}_R(D^n)$ sends $(1, 0, \cdots, 0)^t$ is enough to understand the complete action of f (by the action of R). For instance, if $f(e_1) = (d, d_2, \dots, d_n)$ and P is the projection onto the first coordinate, $f(e_1) = f(Pe_1) = Pf(e_1)$, thus for each $i > 1$, $d_i = 0$. Furthermore, for each M_i corresponding to the permutation $(1\ i)$, $f(e_i) = f(M_i e_1) = M_i f(e_1) = de_i$. We conclude that $f = \phi(d)$. □

Lemma 164. *Let R be a ring and view $M = R$ as a free left R-module of rank one, then $\mathrm{End}_R(M) \cong R^{op}$.*

Proof. For any $\varphi \in \mathrm{End}_R(M)$ and $a \in M$, we have $\varphi(a) = \varphi(a \cdot 1) = a \cdot \varphi(1)$. Thus, the map $\varphi \mapsto \varphi(1)$ is a bijection from $\mathrm{End}_k(M)$ to R and it is clear that addition is preserved and multiplication is just reversed. □

[125] Any submodule of D is an ideal, but D cannot have any non-trivial ideal because $x \in D$ implies $xx^{-1} = 1 \in D$.

[126] Not true for right multiplication.

[127] Send a linear map $T : V/V_j \to V$ to the operator $v \mapsto T(v + V_j)$.

[128] Where D^{op} has the ring structure opposite to D, namely, $a^{\mathrm{op}} b^{\mathrm{op}} = (ba)^{\mathrm{op}}$ for any $a, b \in D$. Note that it retains the usual algebra structure because k embeds in the center of D which is the same as the center of D^{op}. We often omit the $\cdot^{\mathrm{op}}$ notation for elements of D^{op}.

[129] Recall that D^{op} has no non-trivial ideal and any non-zero d is mapped to a non-zero map, so $\ker \phi$ cannot be the whole ring.

Lemma 165. *If V is a simple R-module, then $D = \mathrm{End}_R(V)$ is a division ring.*

Proof. Let $\varphi \in D$, then since V is simple, $\ker(\varphi)$ is either V or 0. The former leads to $\varphi = 0$ and the latter leads to φ being injective. It is also easy to check φ is surjective arguing similarly with $\mathrm{Im}(\varphi)$. We conclude that φ is a bijection and hence has an inverse.[130] □

Lemma 166. *If V is a simple R-module, then $\mathrm{End}_R(V^n) \cong M_n(\mathrm{End}_R(V)) = M_n(D)$.*

Proof. To see why the first equality holds, first note that any $\phi \in \mathrm{End}_R(V^n)$ can be decomposed into a sum of R-module homomorphisms $\phi_i : V^n \to V$, where $\phi_i = P_i \circ \phi$ and P_i is the projection onto the i-th coordinate. Moreover, denote $\phi_{i,j}$ to be the restriction of ϕ_i to vectors with only the j-th coordinate being non-zero, then $\phi_i = \oplus_{j=1}^n \phi_{i,j}$ and it is clear that the matrix $\phi_{i,j}$ will act on V^n just as ϕ does. Checking that $\phi \mapsto (\phi_{i,j})_{i,j\in[n]}$ is an isomorphism is left as an exercise.

The second equality follows from the previous lemma. □

Lemma 167. *If $M \cong V_1^{n_1} \oplus \cdots \oplus V_r^{n_r}$, where the V_i are pairwise non-isomorphic simple modules, then $\mathrm{End}_R(M) \cong \oplus_{i=1}^r M_{n_i}(D_i)$ where $D_i = \mathrm{End}_R(V_i)$.*

Proof. If we restrict an element $\phi \in \mathrm{End}_R(M)$ to one of the direct summand, then we get a map $\phi_j : V_j^{n_j} \to M$ and we claim that $\mathrm{Im}(\phi_j) \subseteq V_j^{n_j}$. □

Theorem 168 (Wedderburn's classification)**.** *If R is a semisimple ring, then there exists $r, n_1, \ldots, n_r \in \mathbb{N}$ and division rings $D_1, \ldots, D_r$ such that $R \cong \oplus_{i=1}^r M_{n_i}(D_i)$.*

Proof. By semisimplicity, we can write $R = \oplus_{j\in S} I_j$, where the I_j's are minimal left ideals. First, observe that we can assume S is finite because $1 \in R$ can be written uniquely as a finite sum of elements in the I_j's. Namely, for some finite $S' \subseteq S$, $1 = \sum_{j\in S'} a_j$, where $a_j \in I_j$ and this implies $R = \oplus_{j\in S'} I_j$.

We obtain a simpler decomposition $R = I_1^{n_1} \oplus \cdots \oplus I_r^{n_r}$,[131] where each I_j are simple submodules of R and pairwise non-isomorphic. Thus, by lemma 164 and 167, we conclude

$$R^{\mathrm{op}} \cong \mathrm{End}_R(R) \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r),$$

and the theorem follows.[132] □

Remark 170. A refinement of this theorem is that, given a semisimple ring R, the objects $r, n_1, \ldots, n_r, D_1, \ldots, D_r$ are well-defined invariants of R. This is a consequence of the Jordan-Holder theorem for R-modules.

Corollary 171. *R is left semisimple if and only if it is right semisimple.*

Proof. Observe that the functor $(-)^{\mathrm{op}} : \textbf{Rings} \rightsquigarrow \textbf{Rings}$ maps left semisimple rings to right semisimple rings and vice-versa, but by remark 169, it does not change the structure of their decomposition. Thus, R is left semisimple if and only it has a decomposition as in Wedderburn's theorem if and only if it is right semisimple. □

Corollary 172. *If R is a semisimple finite dimensional algebra over a field k, then the decomposition becomes $R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r)$ where the D_i's are finite dimensional over k. Moreover, if $k = \bar{k}$, then $R = M_{n_1}(k) \oplus \cdots \oplus M_{n_r}(k)$.*[133]

[130] Checking the inverse is R-linear is an easy exercise.

[131] We have regrouped the isomorphic terms toegethers, i.e.: the exponent means a direct product of I_j with itself n_j times as a module (not the n_j-th power of the ideal I_j).

[132]

Remark 169. It remains to show that applying $^{\mathrm{op}}$ will not modify the relevant structure of the R.H.S. This can be decomposed into three easy checks, namely that for any R-module A and B, $n \in \mathbb{N}$ and division ring D:

$$(A \oplus B)^{\mathrm{op}} \cong A^{\mathrm{op}} \oplus B^{\mathrm{op}},$$
$$M_n(D)^{\mathrm{op}} \cong M_n(D^{\mathrm{op}}),$$
$$D^{\mathrm{op}} \text{ is a division algebra.}$$

[133] An important instance of this specific case is the group ring:

$$[G] = M_{n_1}() \oplus \cdots \oplus M_{n_r}(),$$

where $n_1, \ldots, n_r$ are the dimensions of the irreducible k-linear representations of G. It follows by dimensionality check that $|G|$ is the sum of the squares of the dimensions of its irreducible representation, a useful result in representation theory.

Proof. Finite dimensionality of the D_i's is clear and the claim that $D_i = k$ holds because if $\alpha \in D_i$, then $k(\alpha)$ is finite dimensional over k and still commutative because α commutes with all of k and its powers. Therefore, $k(\alpha)$ is a finite dimensional field extension, thus α is algebraic and $\alpha \in k$. We conclude $D_i = k$. □

Semisimple Algebras

Definition 173. A ring R is **simple** if it has no proper non-trivial two-sided ideals.

Remark 174. The motivation for this definition is that the kernel of a homomorphism is a two-sided ideal, thus if R is simple then any non-zero $\phi : R \to S$ is injective. This fact will be used in lots of arguments, often with the additional fact that R and S have the same dimension over some field yielding that ϕ is an isomorphism.

Examples 175. 1. Any field is simple and if R is commutative and simple, then it has no non-trivial ideal so it is a field.

2. If D is a division ring and $n \in \mathbb{N}$, then $M_n(D)$ is simple.

   Proof. Let I be a non-zero two-sided ideal of $M_n(D)$, pick a non-zero $X \in I$ and $s, t \in [n]$ such that $X_{s,t} \neq 0$. We can assume that $X_{s,t} = 1$ because we can rescale by any element of D. Let $E_{i,j} \in R$ be the matrix which has a one in its (i, j)-th entry and zeros everywhere else. One can verify that $E_{s,s}XE_{t,t} = X_{s,t}E_{s,t} = E_{s,t} \in I$.[134] Then, we conclude $E_{i,j} \in I$ for any $i, j \in [n]$ because we can apply any permutation to the columns and rows by multiplying by permutation matrices on the left and right respectively. Since these matrices generate $M_n(D)$, we conclude $I = M_n(D)$. □

3. Recall the ring $R = [x, \frac{d}{dx}]$ with $x\frac{d}{dx} - \frac{d}{dx}x = -1$ from example 157.4. We claim that R is simple.

   Proof. Let I be a non-zero two-sided ideal, it contains a non-zero element

   $$\alpha = P_r(x)\frac{d^r}{dx} + \cdots + P_1(x)\frac{d}{dx} + P_0(x).$$

   One can check that $[\frac{d}{dx}, P(x)] = P'(x)$, $[\frac{d}{dx}, P(x)\frac{d^t}{dx}] = P'(x)\frac{d^t}{dx}$ and $[\frac{d^r}{dx}, x] = r\frac{d^{r-1}}{dx}$. Thus, if we let $m = \max\{\deg P_j \mid 0 \leq j \leq r\}$, we can compute

   $$...m\ times[\frac{d}{dx}, [\frac{d}{dx}, \alpha]] = a_t\frac{d^t}{dx} + \cdots + a_1\frac{d}{dx} + a_0 = \beta,$$

   where $a_i \in$ and $0 \leq t \leq r$. Now apply the commutator with $[\beta, x]$ r times to obtain $t!a_t \in I$. Thus, I has a unit and $I = R$. □

   Remarkably, we can also show that R is not semisimple.

[134] We first recall that

$$E_{a,b}E_{c,d} = \delta_{b,c}E_{a,d},$$

and that we can decompose X as

$$X = \sum_{k,\ell \in [n]} X_{k,\ell}E_{k,\ell}X_{k,\ell}.$$

Thus, it follows that

$$\begin{aligned} E_{i,i}XE_{j,j} &= \sum_{k,\ell \in [n]} \delta_{i,k}X_{k,\ell}E_{i,\ell}E_{j,j} \\ &= \sum_{k,\ell \in [n]} \delta_{i,k}X_{k,\ell}\delta_{\ell,j}E_{i,j} = X_{i,j}E_{i,j}. \end{aligned}$$

Proof. Consider the chain $R \supseteq R\frac{d}{dx} \supset R\frac{d^2}{dx} \supset \cdots$. We claim that these inclusions are all proper, namely, for any t, $R\frac{d^t}{dx} \supset R\frac{d^{t+1}}{dx}$. Notice that $\frac{d^t}{dx} \notin R\frac{d^{t+1}}{dx}$ because $\frac{d^t}{dx}x^t = t! \neq 0$ whereas for any $P \in R$, $P(x, \frac{d}{dx})\frac{d^{t+1}}{dx}x^t = 0$.

We have shown that R has an infinite composition series and this implies R is a not a finite direct sum. □

In order to avoid examples such as $[x, \frac{d}{dx}]$ where a simple ring is not semisimple, we can impose some type of finiteness condition on R. We explore two different options.

Theorem 176. *If R is a finite dimensional k-algebra which is simple, then $R \cong M_n(D)$ for some division k-algebra D and hence is semisimple.*

Proof. Let V be a minimal non-zero left ideal of R.[135] If $r \in R$, then since the right multiplication map $(-)r : V \to V \cdot r$ is a homomorphism of left R-modules, it has a trivial kernel because V is minimal, thus $V \cdot r$ is either 0 or isomorphic to V as a left R-module. Therefore, $\sum_{r \in R} V \cdot r$ is a non-zero two-sided ideal,[136] and hence must be equal to R.

Now, each of these $V \cdot r$ are minimal ideals, so we have written R as a sum of simple submodules. Furthermore, this sum can be made finite with a similar argument as in the proof of 168 and it is a direct sum because the intersection of any two distinct minimal ideal is a smaller ideal, so it must be trivial. From Wedderburn's classification, we infer that $R \cong M_n(D)$ because if there were more terms in the sum, R would not be simple. □

Corollary 177. *Every finite dimensional simple k- algebra is semisimple and every finite dimensional semisimple k-algebra is a direct sum of simple k-algebras.*

Definition 178. A ring R is (left) Artinian if any strictly descending chain of left ideals is finite.[137]

Examples 179. 1. Any finite ring is trivially Artinian. (e.g.: $\mathbb{Z}/n\mathbb{Z}$, $M_m(\mathbb{Z}/n\mathbb{Z})$, etc.)

2. PID's are Noetherian but usually not Artinian (e.g.: $\mathbb{Z}$ contains the infinite decreasing chain $(2) \supseteq (4) \supseteq (8) \supseteq \cdots$).

3. A finite dimensional k-algebra is both left and right Noetherian and Artinian (e.g.: $[G]$, where G is finite). Recall that ideals will be subspaces of that algebra and infinite decreasing or increasing chains cannot exist in finite dimensional vector spaces.

4. A semisimple ring R is both left and right Noetherian and Artinian.

   Proof. We will show that left semisimple implies left Noetherian and Artinian. The argument for the "right" counterpart of this statement is similar and since left semisimple and right semisimple is equivalent, the claim will be proven.

   □

[135] Minimal non-zero ideals exist because of finite dimensionality. Indeed, left ideals can be seen as k-subspaces of R, so you cannot have a strictly decreasing chain os left ideals if R is finite dimensional.

[136] It is clear that it is a left ideal because each $V \cdot r$ is a left ideal. Now, multiplying on the right by any $r' \in R$ yields

$$\sum_{r \in Rr'} V \cdot r \subseteq \sum_{r \in R} V \cdot r,$$

so it is indeed a right ideal.

[137] Note the parallel with Noetherian rings. We will usually refer to left Artinian rings simply as Artinian rings and we will be precise when talking about both kinds at the same time. Just as Noetherian rings have maximal ideals, Artinian rings always contains minimal non-zero ideals.

5. The ring $[x, \frac{d}{dx}]$ is neither left nor right Artinian.

   Proof. Consider the chain $(x) \supseteq (x^2) \supseteq \cdots$ as left ideals and as right ideals separately.[138] □

6. Triangular rings: Let R and S be two rings, an (R, S)-bimodule ${}_RM_S$ is an abelian group (with operation $+$) equipped with a left R-module and a right S-module structure such that $r(ms) = (rm)s$ for any $r \in R$, $s \in S$, $m \in M$.[139] The **triangular** ring associated to a bimodule ${}_RM_S$ is

   $$A = \left\{ \begin{bmatrix} r & m \\ 0 & s \end{bmatrix} \mid r \in R, s \in S, m \in M \right\},$$

   where addition and multiplication are the usual matrix addition and multiplication.[140] In the following, we denote

   $$e_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad e_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

   Observe that the subset Me_2 is a two-sided ideal of A because

   $$\begin{bmatrix} r_1 & m_1 \\ 0 & s_1 \end{bmatrix} \begin{bmatrix} 0 & m \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & r_1 m \\ 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & m \\ 0 & 0 \end{bmatrix} \begin{bmatrix} r_2 & m_2 \\ 0 & s_2 \end{bmatrix} = \begin{bmatrix} 0 & ms_2 \\ 0 & 0 \end{bmatrix}.$$

   Moreover, we have a clear isomorphism $A/Me_2 \cong R \times S$.

   Proposition 180. *If R and S are left Artinian, then A is left Artinian if and only if M is finitely generated over R.*

7. In the setting of the last item, let $R = \mathbb{Q}(x)$, $S = \mathbb{Q}$ and $M = \mathbb{Q}(x)$ with the natural bimodule structure, then A is left Noetherian and Artinian but neither right Noetherian nor right Artinian.

   Proof. Let I be a left ideal of A we will show that it finitely generated, showing A is left Noetherian. Consider first the case where

   $$I \subseteq \begin{bmatrix} \mathbb{Q}(x) & \mathbb{Q}(x) \\ 0 & 0 \end{bmatrix}$$

   and notice that the R.H.S. is also a left ideal and that it has the left $\mathbb{Q}(x)$-module structure of $\mathbb{Q}(x)^2$ where multiplication by $q \in \mathbb{Q}(x)$ is simulated by multiplication by qe_1 on the left, i.e.:

   $$\begin{bmatrix} q_1 & r_1 \\ 0 & 0 \end{bmatrix} + qe_1 \cdot \begin{bmatrix} q_2 & r_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} q_1 + qq_2 & r_1 + qr_2 \\ 0 & 0 \end{bmatrix}.$$

   Since $\mathbb{Q}(x)$ is a PID, we see that I is generated by at most two elements as a module[141] and hence as an ideal.

[138] More precisely, we can see (x^k) as the left ideal generated by x^k or the right ideal generated by x^k.

[139] Example of bimodule: If V_1 and V_2 are k-vector spaces, then $\mathrm{Hom}_k(V_1, V_2)$ is naturally $(\mathrm{End}_k(V_2), \mathrm{End}_k(V_1))$-bimodule with the actions being function composition.

[140] We note that order of multiplication is important and having a bimodule structure on M is necessary to make the multiplication well-defined:

$$\begin{bmatrix} r_1 & m_1 \\ 0 & s_1 \end{bmatrix} \begin{bmatrix} r_2 & m_2 \\ 0 & s_2 \end{bmatrix} = \begin{bmatrix} r_1 r_2 & r_1 m_2 + m_1 s_2 \\ 0 & s_1 s_2 \end{bmatrix}.$$

[141] Any submodule B of a free module A over a PID is a free module of rank at most the rank of A.

In the second case, we know there exists a non-zero $a \in \mathbb{Q}$ such that

$$\begin{bmatrix} q_1 & q_2 \\ 0 & a \end{bmatrix} \in I,$$

then for any $q \in \mathbb{Q}(x)$, multiplying the element above on the left by $\frac{q}{a}e_2$ yields qe_2, so we conclude

$$\mathbb{Q}e_2 := \left\{ \begin{bmatrix} 0 & q \\ 0 & 0 \end{bmatrix} \mid q \in \mathbb{Q} \right\} \subset I.$$

Then, the projection that forgets about the top right coordinate maps into $\mathbb{Q}(x) \times \mathbb{Q}$ and has $\mathbb{Q}(x)e_2$ as its kernel., so we conclude that $A/\mathbb{Q}(x)e_2 \cong \mathbb{Q}(x) \times \mathbb{Q}$. The R.H.S. being Noetherian, we can see that $I/\mathbb{Q}(x)e_2$ is finitely generated in $A/\mathbb{Q}(x)e_2$ and hence so is I in A.

We now find an infinite ascending strict inclusion chain of right ideals in A to show it is not right Noetherian. For any $n \in \mathbb{N}$, let

$$I_n = x^{-n}\mathbb{Q}e_2 = \left\{ \begin{bmatrix} 0 & \frac{q}{x^n} \\ 0 & 0 \end{bmatrix} \mid q \in \mathbb{Q} \right\},$$

it is a right ideal of A because for any $q_1, q_2 \in \mathbb{Q}(x)$ and $a \in \mathbb{Q}$,

$$\begin{bmatrix} 0 & \frac{q}{x^n} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} q_1 & q_2 \\ 0 & a \end{bmatrix} = \begin{bmatrix} 0 & \frac{aq}{x^n} \\ 0 & 0 \end{bmatrix} \in I_n.$$

Moreover, it is clear that $I_1 \subsetneq I_2 \subsetneq \cdots$, but each inclusion is proper because $\frac{1}{x^{n+1}}e_2 \in I_{n+1} - I_n$. Thus, we get the desired chain of ideals. □

Proposition 181. *Finitely generated modules over a left Artinian ring R satisfies the descending chain conditions for left R-modules.*

Proof. Exercise. □

Theorem 182 (Artin). *Let R be a simple ring, then the following are equivalent:*

i. R is left Artinian.

ii. R has a minimal non-zero left ideal.

iii. R is semisimple.

iv. $R \cong M_n(D)$, where D is a division ring.

Proof. (i $\implies$ ii) Follows from the definition of Artinian.

(ii $\implies$ iii)[142] Let I be a minimal left ideal in R and recall that for any r, $I \cdot r$ is either 0 or a minimal left ideal isomorphic to I. Moreover, we have that $\sum_{r \in R} I \cdot r$ is a non-zero two-sided ideal, so is equal to R. We can then conclude R is semisimple.

(iii $\implies$ iv) From the classification of semisimple rings, R is isomorphic to a direct sum of matrix rings over division rings. If there were more than one summand, R would not be simple, so iv follows.

[142] We use a generalization of the argument from theorem 176's proof.

(iv $\implies$ i) Observe that $M_n(D)$ is a free left module over D and has rank n^2[143], thus left ideals correspond to submodules and an infinite strict chain of submodules cannot occur (because of finite dimensionality). □

Definition 183. An ideal I in a ring R is said to be **nilpotent** if there exists k such that $I^k = 0$, i.e.: $a_1 \cdots a_k = 0$ for all $a_1, \dots, a_k \in I$.[144]

Lemma 184. *If I_1 and I_2 are nilpotent left ideals, then $I_1 + I_2$ is also nilpotent.*

Proof. Let $r, s \in \mathbb{N}$ be such that $I_1^r = I_2^s = 0$, then consider the general $r+s$-fold product of elements of $I_1 + I_2$

$$(a_1 + b_1) \cdots (a_{r+s} b_{r+s}); \forall 1 \leq i \leq r+s, a_i \in I_1, b_i \in I_2.$$

Observe that a any monomial in this product has either more than r a_i's or more than s b_i's, and since I_1 and I_2 are left modules, we can see this monomial as a product of at least r elements of I_1 or s elements of I_2.[145] We conclude that all monomials are zero and hence the product is zero and this implies $I_1 + I_2$ is nilpotent. □

Lemma 185. *If I is a nilpotent left ideal in an Artinian ring, then it is contained in a nilpotent two-sided ideal.*

Proof. Let $J = \sum_{r \in R} I \cdot r = IR$, note that J is still nilpotent[146] and is a two-sided ideal that contains I. □

Lemma 186. *If R is an Artinian ring and I is a nil left ideal, then I is nilpotent.*

Proof. Consider the infinite chain of ideals $I \supseteq I^2 \supseteq \cdots$. Since R is Artinian, the chain must become constant at some $k \in \mathbb{N}$. We will prove that $J := I^k = 0$. Suppose it is not and let K_0 be the minimal ideal such that $JK_0 \neq 0$,[147] then since $J^2 = I^{2k} = I^k = J$ is non-zero, we obtain $K_0 \subseteq J$.

Now, fix $a \in K_0$ such that $Ja \neq 0$, we have $Ja \subseteq K_0$ and $J(Ja) = J^2 a = Ja \neq 0$, thus by minimality of K_0, we must have $Ja = K_0$. This implies there exists $x \in J$ such that $xa = a$ and hence $x^n a = a \neq 0$ for any $n \in \mathbb{N}$. This contradicts the fact that x is nilpotent. □

Theorem 187. *If R is an Artinian ring, then there is a unique maximal nilpotent two-sided ideal of R.*

Proof. Let J be the sum of all nilpotent left ideals in R, then J is clearly a left ideal and we claim that it is two-sided. Indeed, for any $a \in I$, a can be written as a finite sum, so there are ideals $I_1, \dots, I_n$ such that $a \in \sum_{i=1}^n I_i = K$. Since K is a nilpotent left ideal, we can infer that a is nilpotent and that it is contained in a two-sided nilpotent ideal K^+. We infer that $aR \subseteq K^+ \subseteq J$,[148] so we conclude that J is a two-sided ideal.

Furthermore, observe that any element in J is nilpotent because it is contained in a finite sum of nilpotent left ideals. Thus, by lemma 186, we have that J is nilpotent. Uniqueness and maximality follows trivially because any other nilpotent two-sided ideal is a nilpotent left ideal and hence contained in J. □

[143] The action of D is multiplication by scalar matrices and generators are $\{E_{i,j} \mid i, j \in [n]\}$.

[144] Note that, in general, every element in an ideal being nilpotent does not imply the ideal is nilpotent. We call ideals satisfying this property **nil** ideals.

[145] For instance, if $r = 3$ and the monomial is $b_1 a_1 b_2 b_3 a_4 a_5$, then we can collapse it into $a'_1 a'_2 a'_3$ where $a'_1 = b_1 a_2$, $a'_2 = b_2 b_3 a_4$ and $a'_3 = a_5$. We notice that each a'_i is in I_1, so this monomial is zero. This argument is not necessary in commutative rings as we can rearrange the product to have all the a'_i together and we get a zero in the product.

[146] Indeed, if $I^k = 0$, then we can prove $J^k = 0$ by using the same collapsing trick as in lemma **??**, namely, we have

$$i_1 r_1 \cdots i_k r_k = i_1 i'_2 \cdots i'_k = 0.$$

[147] It exists because R is Artinian.

[148] The first inclusion holds because K^+ is two-sided and the second holds because K^+ is a nilpotent left ideal, so it is a summand in J.

Definition 188. This unique maximal nilpotent two-sided ideal is called the Artin-Wedderburn radical.

Lemma 189 (Brauer). *If I is a minimal left ideal, then either $I^2 = 0$ or $\exists e \in R$ such that $e^2 = e$ and $I = Re$.*

Proof. Recall that for any $a \in R$, $I \cdot a$ is either 0 or isomorphic to I by the minimality of I. If $I^2 \neq 0$, then $\exists a \in I$ such that $Ia \neq 0$, then $Ia = I$ and right multiplication by a is an isomorphism from I to itself.[149] Hence, there exists $e \in I$ such that $ea = a$ and we infer that $(e^2 - e)a = 0$ and since $e^2 - e \in I$ and a is a bijection (its kernel is trivial), we must have $e^2 - e = 0$. In other words, e is idempotent and furthermore, it is obvious that $Re \subseteq I$ and then $I = Re$ follows from minimality of I. □

Theorem 190. *If R is Artinian and its Artin-Wedderburn radical is zero, then R is semisimple.*

Proof. Let I_1 be a minimal left ideal of R. If $I_1^2 = 0$, then I_1 is contained in the Artin-Wedderburn radical (use the lemmas), so $I_1 = 0$ which is a contradiction. Thus, $I_1^2 \neq 0$ and by Brauer's lemma, there exists an idempotent $e \in I$ that generates I, namely $I = Re$. Observe that $R = Re + R(1-e)$. Moreover, if $x \in Re$, then $xe = x$ and if in addition $x \in R(1-e)$, then $xe = y(1-e)e = 0$. We conclude that $Re \cap R(1-e) = \{0\}$ and that R is a direct sum.

We found that $R = I_1 \oplus I_1'$ where I_1' is a left ideal. If I_1' is minimal, we are done. Otherwise, we can apply the same argument on I_1' to get a decomposition $I_2 \oplus I_2'$ and the recursion is guaranteed to terminate because R is Artinian. The end result is a decomposition of R into minimal left ideals and we conclude R is semisimple. □

Corollary 191. *If R is an Artinian ring and J is its A-W radical, then R/J is semisimple.*[150]

For completeness, we will state Wedderburn's main theorem that refines the last result, but we will not prove it. The results needed to prove it are covered in chapter II.5 of Knapp.

Theorem 192. *If R is a finite dimensional k-algebra and J its Artin-Wedderburn radical, then there is a semisimple k-algebra $S \subseteq R$ such that $R \cong S \oplus J$ as k-vector spaces.*[151]

Examples 194. 1. Let R be the ring of upper triangular 2×2 matrices with entries in a division ring D. A simple computation shows that if the diagonal entries of an element are non-zero, then any power of this element will be non-zero. Thus, we can see the Artin-Wedderburn radical is

$$I = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \mid b \in D \right\}.$$

It is also easy to show that we have a decomposition $R/I = D \oplus D$.

2. Let R be the ring of upper triangular $(n+1) \times (n+1)$ matrices with entries in a division ring D. Similarly to above, we can infer that the Artin-Wedderburn radical J is the set of matrices with a zero diagonal. One can further observe that $J^n = 0$, but $J^k \neq 0$ for $1 \leq k < n$.

[149] *Ia* is a subset of *I* isomorphic to *I*, so it must be *I*.

[150] Prove this.

[151]

Remark 193. We have proved already that there is an exact sequence

$$0 \to J \to R \to S \to 0,$$

where S is semisimple and this finer theorem states that there is a splitting $S \to R$.

3. Let A be the triangular ring associated to ${}_RM_S$, this gives a generalization of the first example. The A-W radical is the set of matrices of the form $\begin{bmatrix} 0 & m \\ 0 & 0 \end{bmatrix}$ and we have the decomposition $A/J = R \oplus S$.

Remark 195. The converse of theorem 190 is also true, namely, if an Artinian ring R is semisimple, then its Artin-Wedderburn radical is zero. To see this, recall Wedderburn's classification that states if R is semisimple, then

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_t}(D_t).$$

Moreover, we know from example 175.2 that $M_n(D)$ is simple for any $n \in \mathbb{N}$ and division algebra D, so any two sided ideal must contain a full summand of R,[152] and hence it cannot be nilpotent. We conclude that the Artin-Wedderburn radical is zero.

Fact 196. *The following are equivalent.*

1. *B is semisimple as a module over itself $B = \oplus I b_i$.*
2. *Every left B-module is isomorphic to a sum of modules isomorphic to I.*

   If M is a left B-module and M' is a submodule, then there exists M'' submodule such that $M = M' \oplus M''$.

Our final goal for this course is to delve more deeply into the structure of simple k-algebras.

Central simple algebras

In this section, we let k be a field and A and B be finite dimensional k-algebras. Recall the usual definition $A \otimes_k B$ for k-vector spaces where elements are of the form[153]

$$\sum_i a_i \otimes b_i, \text{ with } a_i \in A, b_i \in B.$$

We also have $\dim_k(A \otimes_k B) = \dim_k(A)\dim_k(B)$.[154] Moreover, $A \otimes_k B$ inherits the structure of k-algebra by setting $(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1a_2 \otimes b_1b_2)$.[155]

Remark 197. A is naturally a sub-algebra of $A \otimes_k B$ by sending a to $a \otimes 1$ and similarly for B. This is clear when consider the definition of $A \otimes_k B$ as the pushout of the following diagram in the category of k-algebras.

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

Fact 198. *For any $A, B, C \in \textbf{Alg}_k$, we have*

1. *$A \otimes_k (B \oplus C) \cong A \otimes_k B \oplus A \otimes_k C$ (distributivity),*

[152] To obtain this, one has to argue that the projection of a two-sided ideal on any of the summand is also a two-sided ideal of the summand.

[153] Note that this representation is not unique.

[154] There is a natural basis for the tensor product of two vector spaces. That is, if $\{a_i \mid i \in [n]\}$ and $\{b_i \mid i \in [m]\}$ are k-bases for A and B respectively, then $\{a_i \otimes b_j \mid i \in [n], j \in [m]\}$ is a basis for $A \otimes_k B$.

[155] We leave the cumbersome task of verifying this is a well-defined operation to the reader. Alternatively, we refer the reader to the Higher Algebra I lecture notes written by Prof. Eyal Goren for a more general and thorough study of tensor products.

2. *$A \otimes_k (B \otimes_k C) \cong (A \otimes_k B) \otimes_k C$ (associativity), and*

3. *$A \otimes_k B \cong B \otimes_k A$ (commutativity).*

Examples 199. 1. If L is any k-algebra and $n \in \mathbb{N}$, then $M_n(k) \otimes_k L \cong M_n(L)$.

Proof. As k-vector spaces, we have

$$M_n(k) \cong kE_{1,1} \oplus \cdots \oplus kE_{n,n},$$

then if we tensor by L and apply the isomorphisms[156] $kE_{i,j} \otimes_k L \to LE_{i,j} = kE_{i,j} \otimes \ell \mapsto k\ell E_{i,j}$, we get

$$M_n(k) \otimes_k L \cong (kE_{1,1} \otimes_k L) \oplus \cdots \oplus (kE_{n,n} \otimes_k L) \cong LE_{1,1} \oplus \cdots \oplus LE_{n,n} \cong M_n(L).$$

□

2. A special case of the above yields $M_{n_1}(k) \otimes_k M_{n_2}(k) \cong M_{n_1}(M_{n_2}(k)) \cong M_{n_1 n_2}(k)$.

3. Let $\mathbb{H}$ be the Hamiltonian quaternions then $\mathbb{H} \otimes_{\mathbb{R}} \cong M_2()$.

Proposition 200. *If F and L are finite field extensions of k with F/k separable, then $F \otimes_k L$ is a finite product of field extensions of k.*[157]

Proof. The primitive element theorem implies that $F = k[\alpha] = k[x]/(p(x))$, where $p(x)$ is the minimal polynomial of $\alpha \in k$. Taking the tensor, we obtain

$$F \otimes_k L \cong k[x]/(p(x)) \otimes_k L \cong (k[x] \otimes_k L)/(p(x) \otimes 1) \cong L[x]/(p(x)).$$

Note that there is no reason that $p(x)$ stays irreducible in $L[x]$, but it is still separable, so $p(x)$ factors into distinct irreducible factors $p(x) = p_1(x) \cdots p_n(x)$, thus we can use CRT to get the finite product of field extensions. □

Question 201. *If A and B are simple/semisimple algebras over k, what can we say about $A \otimes_k B$?*

To answer this question, we will need to understand the structure of two-sided ideals of $A \otimes_k B$. Moreover, we will assume from now on that all algebras are finite dimensional.

Definition 202. A k-algebra A is **central** if the center of A is exactly k.

Examples 203. 1. $\mathbb{H}$ is central simple over $\mathbb{R}$. Even though it contains copies of they do not commute with each other.

2. $M_n(k)$ is central simple over k. The only matrices in the center are the scalar matrices ($\text{diag}(\lambda, \dots, \lambda)$ for $\lambda \in k$).

3. If L is a field extension of k, then L is central over k if and only if $L = k$ because the center of L is L itself.

[156] Explain why they are isomorphisms.

[157] Separability is crucial in this statement as is witnessed by the following. Let $k = \mathbb{F}_p(t)$ and $F = Lk[x]/(x^p - t) = \mathbb{F}_p[t^{1/p}]$. What is $F \otimes_k F$? By our argument beside, it is isomorphic to

$$F[x]/(x^p - t) = F[x]/(x - t^{1/p})^p,$$

and this cannot be a product of fields because it has nilpotent elements, namely $(x - t^{1/p})$.

Proposition 204. *Suppose that A and B k-algebras with B central simple over k. Then, the two-sided ideals of $A \otimes_k B$ are precisely the ones of the form $I \otimes_k B$ where I is a two-sided ideal of A.*

Proof. Clearly, $I \otimes_k B$ is a two-sided ideal if I is a two-sided ideal of A. Conversely, let J be a two-sided ideal of $A \otimes_k B$ and $I = \{a \in A \mid a \otimes 1 \in J\}$, it is easy to check that I is a two-sided ideal of A and $I \otimes_k B \subseteq J$,[158] we claim this is in fact an equality.

Let $x_1, \ldots, x_n$ be a k-basis for A chosen so that $x_1, \ldots, x_m$ is a k-basis for I and $x_{m+1}, \ldots, x_n$ is the completion of the basis. Then, we can write

$$A \otimes_k B = \{\sum_{i=1}^{n} x_i \otimes b_i \mid b_1, \ldots, b_n \in B\}.$$

We need to show if $\sum_{i=1}^{n} x_i \otimes b_i \in J$, then $b_i = 0$ for all $i > m$. Equivalently, we need to show if $\sum_{i=m+1}^{n} x_i \otimes b_i \in J$, then $b_i = 0$.[159] Let t be minimal for the property that there exists a subset $\{y_1, \ldots, y_t\} \subseteq \{x_{m+1}, \ldots, x_n\}$ with $0 \neq \sum y_i \otimes b_i \in J$. By minimality, all the b_i's are non-zero. Consider the set $\{b_1 \in B \mid \exists \sum y_i \otimes b_i \in J\}$. It is clearly a two-sided ideal which is non-zero by definition of t, but since B is simple, it must be all of B, in particular it contains one. Therefore, there exists $\beta = y_1 \otimes 1 + \sum y_i \otimes b_i \in J$. For any $b \in B$, since J is a two-sided ideal, we have

$$J \ni (1 \otimes b)\beta - \beta(1 \otimes b) = y_2 \otimes bb_2 - b_2 b + \cdots + y_t \otimes bb_t - b_t b.$$

The minimality of t implies that $bb_j - b_j b = 0$ for $j = 2, ..., t$. In other words, $b_2, ..., b_t$ are in the center in B, namely in k. Finally, we set $y_i' = y_i b_i$ to find

$$\sum_{i=1}^{t} y_i' \otimes 1 \in J,$$

thus $\sum y_i' \in I$ and this contradicts our construction of the y_i's.[160] □

Corollary 205. *If A is simple over k and B is central simple over k, then $A \otimes_k B$ is also simple over k.*[161]

Proposition 206. *If k has characteristic 0, A is semisimple over k and F is a finite separable extension of k, then $A \otimes_k F$ is also semisimple over k.*

Proof. By Wedderburn's classification, we can write A as direct sum of simple k-algebras, so we will first prove the case where A is simple. Let Z be the center of A, it is clear that A is a central simple algebra over Z and we have[162]

$$A \otimes_k F = (A \otimes_Z Z) \otimes_k F = A \otimes_Z (Z \otimes_k F) = A \otimes_Z (K_1 \oplus \cdots \oplus K_s),$$

where K_i's are finite extensions of Z that arise from proposition 200.[163] The tensor product also distributes so we obtain $A \otimes_Z K_1 \oplus \cdots \oplus A \otimes_Z K_s$. Since each $A \otimes_Z K_i$ is simple because A is central simple over Z and K_j is simple over Z, we conclude that $A \otimes_k F$ is semisimple. □

Definition 207. If B is a subalgebra of A, then the centralizer of B in A, denoted $\mathcal{Z}_A(B)$, is the set of all elements of A that commute with all of B. For instance, $\mathcal{Z}(A) := \mathcal{Z}_A(A)$ is the center of A. The centralizer is in fact a subalgebra.

[158] The first part is true because

$$ar \in A \Leftrightarrow ar \otimes 1 \in J \Leftrightarrow (a \otimes 1)(r \otimes 1) \in J,$$

and similarly for right multiplication. The second part is true because if $a \otimes 1 \in J$, then $a \otimes b \in J$ for any $b \in B$.

[159] We already know $\sum_{i=1}^{m} x_i \otimes b_i \in J$, so we can subtract by it.

[160] They were a subset of $\{x_{m+1}, \ldots, x_n\}$ of which, none are in I.

[161] If A is simple, then the only two-sided ideals of $A \otimes_k B$ are $0 \otimes_k B = 0$ and $A \otimes_k B$, so there is no non-trivial two-sided ideal.

[162] In facts 198, we mentioned that the tensor product was associative when done over the same algebra, but the version of associativity used here is slightly more complex and uses the fact that Z is a (Z, k)-bimodule.

[163] To use this result, we only need to argue that Z is a finite field extension because any field extensions over a finite field of characteristic 0 is separable. Since A is simple and finite dimensional, we can write it as $M_n(D)$ for a finite dimensional division k-algebra D. Then, it is easy to see the center is the center of D and hence is a finite field extension of k.

Lemma 208. *Let A and B be k-algebras with B central, then*

i. $\mathcal{Z}_{A\otimes_k B}(1\otimes_k B) = A\otimes_k 1$, *and*

ii. $\mathcal{Z}(A\otimes_k B) = \mathcal{Z}(A)\otimes_k 1$.

Proof. i. $(\supseteq)$ is trivial.[164]

$(\subseteq)$ Let $a_1,\dots,a_n$ be a basis for A/k, and recall that every element of $A\otimes_k B$ can be written uniquely in the form $a_1\otimes b_1+\cdots+a_n\otimes b_n$ for some $b_1,\dots,b_n\in B$. In other words, after having chosen a basis for A, $A\otimes_k B$ can be identified by B^n.[165] Let $\alpha\in\mathcal{Z}_{A\otimes_k B}(1\otimes_k B)$, then $(1\otimes b)\alpha=\alpha(1\otimes b)$ and we can write

$$a_1\otimes bb_1+\cdots+a_n\otimes bb_n = a_1\otimes b_1b+\cdots+a_n\otimes b_nb,$$

where $\alpha=a_1\otimes b_1+\cdots+a_n\otimes b_n$. By uniqueness, we get $b_ib=b_ib$ for any b, so each b_i is in the center of B, namely, in k. Then, we have

$$\alpha = a_1b_1\otimes 1+\cdots+a_nb_n\otimes 1 = \left(\sum_i a_ib_i\right)\otimes 1\in A\otimes_k 1.$$

ii. Part i implies that the center is contained in $A\otimes_k 1$ and it is obvious that $(a'\otimes 1)\alpha=\alpha(a'\otimes 1)$ for all α's if and only if $a\in\mathcal{Z}(A)$ (it is even enough to take $\alpha\in A\otimes_k 1$).

□

Corollary 209. *If A and B are central simple algebras, then $A\otimes_k B$ is central simple.*[166]

Example 210. If A is central simple over k, then certainly A^{op} is also central simple[167] and in fact $A\otimes_k A^{\mathrm{op}}\cong M_n(k)$. More precisely, $A\otimes_k A^{\mathrm{op}}$ is canonically identified with $\mathrm{End}_k(V_A)$ by sending $a\otimes a'$ to the linear map $v\mapsto ava'$.[168] This map is injective because its kernel is a two-sided ideal and $A\otimes_k A^{\mathrm{op}}$ is simple, surjectivity follows from counting dimensions ($\dim_k(A)^2=\dim_k(A)^2$).

Corollary 211. *If A is central simple over k and L is a field extension of k, then $A\otimes_k L$ is central simple over L.*

Proof. We already know it is simple by corollary 205. Moreover, lemma 208 yields

$$\mathcal{Z}(A\otimes_k L) = 1\otimes_k\mathcal{Z}(L) = 1\otimes_k L = L.$$

□

Proposition 212. *If A/k is central simple, then* $\dim_k(A)$ *is a square.*

Proof. Let $\bar{k}$ be the algebraic closure of k, then the previous corollary says that $A\otimes_k\bar{k}$ is a central simple algebra over $\bar{k}$ and from Wedderburn's classification, we know $A\otimes_k\bar{k}=M_n(D)$ where D is a finite dimensional division $\bar{k}$-algebra. In addition, note that such a D must be equal to $\bar{k}$[169] an therefore $\dim_{\bar{k}}(A\otimes_k\bar{k})=\dim_{\bar{k}}(M_n(k))=n^2$. But, we also have that this is equal to $\dim_k(A)$ (why?) □

[164] For any $a\in A$ and $b,b'\in B$,

$$(a\otimes b)(1\otimes b') = (1\otimes b')(a\otimes b)$$

if and only if $bb'=b'b$, so $a\otimes b$ is in the center of $1\otimes_k B$ if and only if b is in the center of B, namely, $b\in k$. This implies that

$$a\otimes b = ab\otimes 1\in A\otimes_k 1.$$

[165] Addition and multiplication behave just like in B^n:

$$\sum_i a_i\otimes b_i+\sum_i a_i\otimes b_i' = \sum_i a_i\otimes(b_i+b_i'), \text{and}$$

$$b\left(\sum_i a_i\otimes b_i\right) = (1\otimes b)\left(\sum_i a_i\otimes b_i\right) = \sum_i a_i\otimes bb_i.$$

[166] Simplicity comes from corollary 205 and according to the previous theorem, the center of $A\otimes_k B$ will be $1\otimes 1=k$.

[167] The center and two-sided ideals of the opposite alebra are the exactly the same.

[168] By tedious verifications, one can show that this is a k-algebra homomorphism.

[169] Since D is a finite extension, it is algebraic and hence cannot be bigger than $\bar{k}$.

Corollary 213. *If D is a finite dimensional central division algebra over k, then $\dim_k(D) = n^2$ for some n.*[170]

Theorem 214 (Skolem-Noether)**.** *Let A be a central simple algebra over k and B be a simple subalgebra of A. If $f, g : B \to A$ are k-algebra homomorphisms, then there exists $x \in A^\times$ such that $f(b) = xg(b)x^{-1}$ for all $b \in B$.*

Proof. Consider first the case where $A = M_n(k)$. Notice that $f : B \to A$ endows $V_f := k^n$ with the structure of a left B-module, namely, for $v \in k^n$ and $b \in B$, $b * v = f(b) \cdot v \in k^n$ (with matrix vector multiplication). Because B is simple, there is a unique simple left B-module V_B up to isomorphism. [171] In particular, $V_f \cong V_B^t$ for some $t \in \mathbb{N}$ (as left modules), and likewise, V_g is also isomorphic to V_B^t as left B-modules.[172] Thus, there exists an isomorphism of left B-modules $\phi : V_f \to V_g$, and it must satisfy $\phi(f(b) \cdot v) = g(b) \cdot \phi(v)$. Equivalently, for all $v \in V_g$, $f(b) = \phi^{-1} g(b) \phi$.[173]

For the more general case, we consider the maps

$$f \otimes 1, g \otimes 1 : B \otimes_k A^{\text{op}} \to A \otimes_k A^{\text{op}} = M_n(k).$$

Since A^{op} is CSA and B is simple, $B \otimes_k A^{\text{op}}$ is simple by corollary 205. Then, by applying our first case, we find an element $X \in (A \otimes_k A^{\text{op}})^\times$ such that $f \otimes 1 = X(g \otimes 1)X^{-1}$. More explicitly, for all $b \otimes a' \in B \otimes A^{\text{op}}$, we have

$$f(b) \otimes a' = X(g(b) \otimes a')X^{-1}.$$

Setting $b = 1$, we observe that $(1 \otimes a')X = X(1 \otimes a')$ for all $a' \in A^{\text{op}}$, thus $X \in \mathcal{Z}_{B \otimes_k A^{\text{op}}}(1 \otimes_k A^{\text{op}})$. We can conclude from lemma 208 that $X \in B \otimes 1$. Thus, our more general equation becomes

$$f(b) \otimes a' = (x \otimes 1)(g(b) \otimes a')(x^{-1} \otimes 1) = (xg(b)x^{-1} \otimes a'),$$

and we conclude $f(b) = xg(b)x^{-1}$. □

Corollary 215. *If A is a CSA over k, then every non-zero k-algebra homomorphism $\phi : A \to A$ is inner, i.e.: there exists $x \in A^\times$ such that $\phi(a) = xax^{-1}$.*[174]

Example 216. As a further corollary, we obtain that any element of $\text{Aut}(M_n(k))$ is realized by a conjugation of an invertible matrix. In other words, any automorphism of $M_n(k)$ is a change of basis.

Remark 217. Recall that any simple k-algebra A will be a CSA over its center $\mathcal{Z}(A)$, thus, in the corollary above, we can drop the centrality assumption and instead assume ϕ is a $\mathcal{Z}(A)$-algebra automorphism.

Lemma 218. *Let $B \subseteq A$ and $B' \subseteq A'$ where A and A' are CSA over k and B and B' are simple over k and let $C = \mathcal{Z}_A(B)$ and $C' = \mathcal{Z}_{A'}(B')$. Then,*

$$\mathcal{Z}_{A \otimes_k A'}(B \otimes_k B') = C \otimes_k C'.$$

Proof. Clearly $C \otimes_k C'$ commutes with $B \otimes_k B'$, therefore $\supseteq$ is trivial. Moreover, obvious properties of centers yield

$$\mathcal{Z}_{A \otimes_k A'}(B \otimes_k B') \subseteq_k \mathcal{Z}_{A \otimes_k A'}(B \otimes_k 1) \cap \mathcal{Z}_{A \otimes_k A'}(1 \otimes_k B').$$

[170] This is a trivial application of the proposition using the fact that division algebras are simple. Note that a particular application of this corollary is the fact that there are no central division algebras of dimension three over $\mathbb{R}$. In fact, we will later see Frobenius' theorem that shows there are only two central division algebras over $\mathbb{R}$ up to isomorphism.

[171] Why is this true? Is this an app of (Jordan-Holder)? V_B is minimal left ideal unique up to isomorphism.

[172] They are of the same dimension, so they are isomorphic.

[173] To conclude that $\phi \in A = M_n(k)$, we have to show ϕ is a k-linear map from $V_f = k^n$ to $V_g = k^n$. To see this, first note that $\phi(v + w) = \phi(v) + \phi(w)$ follows from the properties of a B-module homomorphism. Second, the k-algebra homomorphism properties imply that for any $\lambda \in k$,

$$f(\lambda) = g(\lambda) = \text{diag}(k, \cdots, k).$$

Therefore, ϕ is an element of $M_n(k)$.

[174] Apply the Skolem-Noether theorem with $B = A$, $f = \phi$ and $g = 1$.

It is easy to check that the R.H.S. is equal to $C \otimes_k A' \cap A \otimes_k C'$,[175] and furthermore the latter is equal to $C \otimes C'$ because if $c \otimes a' = a \otimes c'$ is in the intersection, then it commutes with $B \otimes_k 1$ and $1 \otimes_k B$, so we infer $a \in C$ and $a' \in C'$. □

Lemma 219. *Let B be a simple k-algebra and let $A = \operatorname{End}_k(V_B)$, where V_B is B viewed as a k-vector space.*[176] *Then, $\mathcal{Z}_A(\ell(B)) = r(B^{op})$.*

Proof. We can think of $\mathcal{Z}_{\operatorname{End}_k(V_B)}(\ell(B))$ as endomorphisms of V_B that commute with the left action of B, namely, the left B-module endomorphisms of V_B. Let ϕ be an element of $\operatorname{End}_B(V_B)$, then $\phi(b) = b \cdot \phi(1)$, hence ϕ is the image of $\phi(1)$ under r. We get that $r : B^{\text{op}} \to \operatorname{End}_B(V_B)$ is surjective, it is injective because B^{op} is simple.[177] □

Theorem 220 (Double centralizer)**.** *Let A be a CSA over k, B a simple subalgebra and $C = \mathcal{Z}_A(B)$, then*

1. *C is simple.*
2. *$\dim_k(B)\dim_k(C) = \dim_k(A)$.*
3. *$B = \mathcal{Z}_A(C)$.*

Proof. Consider the k-algebra $\operatorname{End}_k(V_B)$, it is also central simple,[178] hence $A \otimes_k \operatorname{End}_k(V_B)$ is a central simple k-algebra. Consider the maps $f, g : B \to A \otimes_k \operatorname{End}_k(V_B)$ defined by $f(b) = b \otimes 1$ and $g(b) = 1 \otimes \ell(b)$. By the Skolem-Noether theorem, these two maps can be conjugated into each other by an invertible element of $A \otimes_k \operatorname{End}_k(V_B)$, namely, there exists $x \in (A \otimes_k \operatorname{End}_k(V_B))^\times$ such that $f = xgx^{-1}$. In particular, $f(B) = xg(B)x^{-1} \Leftrightarrow B \otimes 1 = x(1 \otimes \ell(B))x^{-1}$. Then, it is obvious that

$$\mathcal{Z}_{A \otimes_k \operatorname{End}_k(V_B)}(B \otimes_k 1) = x\mathcal{Z}_{A \otimes_k \operatorname{End}_k(V_B)}(1 \otimes_k \ell(B))x^{-1}.$$

Using the previous lemmas, we can compute that the L.H.S. is $\mathcal{Z}_A(B) \otimes_k \operatorname{End}_k(V_B)$ and the R.H.S. is a conjugate of $A \otimes_k r(B^{\text{op}})$, we infer that[179]

$$C \otimes_k \operatorname{End}_k(V_B) \cong A \otimes_k r(B^{op}), \quad \text{as } k\text{-algebras.}$$

We are now ready to prove each part of the statement using this isomorphism.

1. Because the R.H.S. is simple, the L.H.S. also is and it is clear that C must also be simple as any non-trivial two-sided ideal of C would give rise to a non-trivial two-sided ideal of $C \otimes_k \operatorname{End}_k(V_B)$.

2. By computing the dimensions of both sides, we get

$$\dim_k(C) \cdot \dim_k(B)^2 = \dim_k(A) \cdot \dim_k(B).$$

   The result then follows by dividing by $\dim_k(B)$.

3. Clearly B centralizes C, so $B \subseteq \mathcal{Z}_A(C)$ and part two of the theorem applied to C implies that $\dim_k(C)\dim_k(\mathcal{Z}_A(C)) = \dim_k(A)$ and, so $\dim_k(B) = \dim_k(\mathcal{Z}_A(C))$ and we conclude B must equal $\mathcal{Z}_A(C)$.

[175] For any $a \otimes a' \in A \otimes_k A'$, $(ab \otimes a') = (ba \otimes a')$ if and only if $a \in \mathcal{Z}_A(B)$ and similarly for the symmetric case.

[176] There are two k-algebra homomorphism $\ell : B \to \operatorname{End}_k(V_B) = b \mapsto b(-)$ and $r : B^{\text{op}} \to \operatorname{End}_k(V_B) = (-)b$.

[177] Checking that this map preserves the k-algebra structure is left as a simple exercise.

[178] Since B is finite dimensional, we can pick a basis for B over k and identify $\operatorname{End}_k(V_B)$ with $M_{\dim_k(B)}(k)$, we have already seen why the latter is a CSA over k.

[179] We use the fact that conjugation by x is a k-algebra homomorphism.

□

Examples 221.

1. Let $A = M_n(D)$ where D is a central division algebra over k and $B = M_n(k)$. Then we claim $\mathcal{Z}_A(B) = D \cdot I_n$ (the scalar diagonal matrices). Clearly $DI_n \subseteq \mathcal{Z}_A(B)$ and the double-centralizer theorem implies $DI_n = \mathcal{Z}_A(B)$ by dimensionality: $\dim_k(D)\dim_k(M_n(k)) = \dim_k(M_n(D))$.

2. Let $A = M_n(k)$ and B a field extension of k of degree n. We can view B as a subalgebra of $M_n(k)$ by choosing a basis $e_1, \dots, e_n$ of B over k.[180]. This time, $\mathcal{Z}_A(B)$ clearly contains B because B is a field and commutes. The double centralizer yields $B = \mathcal{Z}_A(B)$ by dimensionality again.

3.

There are two important complementary settings where theorem 220 is used.

Corollary 222. *In the same setting as the theorem, if B is central simple over k, then $B \otimes_k C = A$.*

Proof. Since B is central simple and C is simple, $B \otimes_k \mathcal{Z}_A(B)$ is simple and there is a natural homomorphism $B \otimes_k C \to A$ sending $b \otimes c$ to bc.[181] Because the L.H.S. is simple, the map is injective and by dimension counting (recall part ii of the double centralizer), it must be an isomorphism. □

Corollary 223. *In the same setting as the theorem, if B is a maximal abelian subfield*[182] *of A, then $C = B$ and* $\dim_k(B)^2 = \dim_k(A)$.[183]

Remark 224. Note that the last corollary does not necessarily apply here. For instance if A is non-commutative, we cannot have $B \otimes_k B = A$ because the L.H.S. is commutative.

Proof. It is obvious that C contains B because B is commutative. Moreover, if C contains an element not in B, adjoining it to B yields a bigger field contradicting the maximality of B, thus we conclude $B = C$. The result for the dimension is a trivial application of the double centralizer.[184] □

Example 225. Let $A = M_n(k)$, it contains many subfields of degree n and we claim that if E is a field of degree n over k, then E is isomorphic to a subfield of A. To see this, fix a basis for E, and recall that $\mathrm{End}_k(E) \cong M_n(k)$, so the embedding[185] $\ell : E \to \mathrm{End}_k(E)$ extends to an embedding into $M_n(k)$.

Corollary 226. *If D is a division algebra over k, then any maximal subfield F of D satisfies $[F : k]^2 = [D : k]$.*

Corollary 227. *Let A be a CSA over k and K be a subfield, then the following are equivalent:*

1. $K = \mathcal{Z}_A(K)$.

2. $[K : k]^2 = \dim_k(A)$.

[180] There is a natural map $B \mapsto \mathrm{End}_k(B) = M_n(k)$ that sends $b \in B$ to the left multiplication by b.

[181] Note that this is well-defined precisely because C commutes with B. It is a module homomorphism by k-bilinearity and algebra homomorphism by commutation of B and C.

[182] We mean a subalgebra that is a field.

[183] This is one way to see that the dimension of a CSA is a square, but it requires the existence of a maximal abelian subfield. Finite dimensionality guarantees that, but it is not true in the general case.

[184] After noting that B is simple because it is a field.

[185] It sends e to the left multiplication by e.

3. *K is a maximal commutative subalgebra of A.*

Proof. Easy application of the earlier results. □

Classification of Central Simple Algebras

As a first goal, we would like to classify all the central division algebras over a given field k (up to isomorphism). We will denote $DA(k)$ to be the set of central division k-algebras modulo the isomorphism relation and denote $CSA(k)$ to be the set of central simple k-algebras modulo the isomorphism relation. Note that the former is contained in latter and by Wedderburn's classification we can write

$$CSA(k) = \{M_n(D) \mid D \in DA(k), n \geq 1\}.$$

We first consider the case when k is finite.

A result in field theory states that finite fields are completely determined, up to isomorphism, by their cardinality. More precisely, if $n \in \mathbb{N}$, p is prime and $q = p^n$, then there exists a unique field $\mathbb{F}_q$ of size q. In particular finite field extensions of finite fields are isomorphic if and only if they have the same dimension over the base field. To classify finite division ring, we need a general group theoretic lemma.

Lemma 228. *If G is a finite group and H is a proper subgroup, then $G \neq \cup_{x \in G} xHx^{-1}$.*

Proof. Suppose this were true, then we could also range the union over representatives of G/H and preserve equality.[186] This union involves $|G|/|H|$ subsets of size $|H|$, but each subset is not disjoint (they all contain the identity), hence the size of the union is strictly less than $|G|$. □

Theorem 229 (Wedderburn)**.** *Any finite division ring is commutative, i.e.: it is a field.*

Proof. Let D be a finite division ring and $k = \mathcal{Z}(D)$ its center. Since k is a commutative division ring, it is a field and by finiteness, it is isomorphic to $\mathbb{F}_q$ for q a power of a prime. Let K be a maximal commutative k-subalgebra of D,[187] it is a field extension of k. By corollary 223, we have $\dim_k(K)^2 = \dim_k(D)$ and all other maximal commutative subalgebras must be isomorphic to K[188] and hence conjugate (by Skolem-Noether). Therefore, since every $\alpha \in D$ generates a commutative algebra $k[\alpha]$ over k, we infer that $k[\alpha]$ is contained in a maximal commutative algebra of the form xKx^{-1} for some $x \in D^\times$. We conclude that

$$D = \bigcup_{x \in D^\times} xKx^{-1} \text{ and furhtermore } D^\times = \bigcup_{x \in D^\times} xK^\times x^{-1}.$$

This contradicts the previous lemma if $K^\times$ is a proper subset of $D^\times$, so we conclude $D = K$ and hence D is a field. □

Corollary 230. *If k is a finite field and A is a finite dimensional CSA over k, then $A \cong M_n(k)$ for some n.*[189]

Next, we study the case when $k = \mathbb{R}$.

[186] This is because if $xH = yH$, then $xHx^{-1} = yHy^{-1}$.

[187] The existence of K is guaranteed by the finiteness of D.

[188] The equation for dimension yields that all such subalgebras have the same dimension as K and we saw that this imply they are isomorphic when over finite fields.

[189] Might also be true if A is not finite dimensional.

Theorem 231 (Frobenius)**.** *If D is a division algebra over $\mathbb{R}$, then D is either isomorphic to $\mathbb{R}$, or $\mathbb{H}$.*

Proof. If D is commutative, then it follows from the fundamental theorem of algebra that D is either $\mathbb{R}$ or .[190]

Otherwise, the center of D has to be equal to $\mathbb{R}$ since there are no finite dimensional division algebra over .[191] Let E be a maximal commutative subalgebra of D, then E is a non-trivial field extension of $\mathbb{R}$, so $E =$ and by corollary 223, we have $\dim_{\mathbb{R}}(D) = [E : \mathbb{R}]^2 = 4$.

Observe that D is a two dimensional vector space under left multiplication and for any $w \in D-$, $\{1, w\}$ forms a -basis for D. We proceed to choose a particular w that will help us understand the multiplication in D. Consider the maps $f, g :\to D$ where $f = \mathrm{id}$[192] and $g = z \mapsto f(\bar{z})$. By Skolem-Noether, $\exists w \in D^\times$ such that $wzw^{-1} = \bar{z}$ for any $z \in$ and we infer that w does not commute with , hence it is in $D-$ and is independent of 1. Thus, we got a basis and[193]

$$D = 1 + w = \{z_1 + z_2 w \mid z_1, z_2 \in\}.$$

Notice that since $wz = \bar{z}w$ for any z, we have

$$w^2 z = w\bar{z}w = zw^2,$$

therefore w^2 commutes with . We infer that w^2 commutes with all of D,[194] namely, $w^2 \in Z(D) = \mathbb{R}$. Furthermore, we claim that $w^2 < 0$. Suppose otherwise, then there would exists $r \in \mathbb{R}$ such that $r^2 = w^2$, or equivalently, $(w - r)(w + r) = 0$. This would imply D has zero-divisors because $D- \ni w \neq r, -r$ and contradict the fact that D is an integral domain.

Finally, replacing w by λw with $\lambda \in \mathbb{R}$ will not change its properties (because $\mathbb{R}$ commutes with D), so we can assume $w^2 = -1$. We conclude that the multiplication in D is now completely determined: for any $z_1, z_2, y_1, y_2 \in$,

$$(z_1 + z_2 w)(y_1 + y_2 w) = z_1 y_1 + z_1 y_2 w + z_2 \bar{y}_1 w + z_2 \bar{y}_2 w^2 = z_1 y_1 - z_2 \bar{y}_2 + (z_1 y_2 + z_2 \bar{y}_1) w.$$

Hence, there can only be one non-commutative division algebra over $\mathbb{R}$.[195] □

Although the two previous settings (k finite and $k = \mathbb{R}$) resulted in a simple classification, this is not always the case and we now turn to the more general question.

Recall from corollary 209 that $CSA(k)$ is closed under the tensor product over k, and this operation is associative and commutative. Moreover, since tensoring with k does not change the structure, i.e.: $A \otimes_k k \cong A$, we can see $CSA(k)$ as a monoid under the operation $\otimes_k$.

Remark 232. The set $T(k) = \{k, M_2(k), M_3(k), \ldots, \}$ is submonoid of $(CSA(k), \otimes_k)$ and is isomorphic to $(\mathbb{N}^*, \cdot)$. We use it in the followin definition.

Definition 233 (Brauer group)**.** We say that two elements A_1 and A_2 of $CSA(k)$ are Brauer equivalent if $\exists n_1, n_2 \geq 1$ such that $M_{n_1}(A_1) \cong M_{n_2}(A_2)$, or equivalently $A_1 \otimes M_{n_1}(k) \cong A_2 \otimes M_{n_2}(k)$. The Brauer group of k, denoted $\mathrm{Br}(k)$ is the set of Brauer equivalence classes in $CSA(k)$, i.e.: $\mathrm{Br}(k) \cong CSA(k)/T(k)$.

[190] Recall that we are only considering finite dimensional algebras, and along with commutativity, it implies D is an algebraic extension of $\mathbb{R}$.

[191] Recall the argument in corollary 172.

[192] More precisely, f is the isomorphism $\cong E \subseteq D$.

[193] The equalities are as vector spaces.

[194] It obviously commutes with w.

[195] Indeed, if D and D' are two non-commutative division $\mathbb{R}$-algebras, then we find the distinguished elements $w \in D$ and $w' \in D'$ and what we have show is that the map sending 1_D to $1_{D'}$ and w to w' (extend it with -linearity) is an $\mathbb{R}$-algebra isomorphism.

Remark 234. Wedderburn's classification implies that the following composite is a bijection[196]:

$$DA(k) \hookrightarrow CSA(k) \to \mathrm{Br}(k) = D \mapsto D \mapsto [D] = \{M_n(D) \mid n \geq 1\}.$$

In other words, every Brauer equivalence class has a unique central division algebra.

Examples 235. 1. If k is finite, then theorem 229 shows $\mathrm{Br}(k) = \{k\}$.

2. Frobenius' theorem implies $\mathrm{Br}(\mathbb{R}) = \{\mathbb{R}, \mathbb{H}\}$. Moreover, we can infer from the group structure that $[\mathbb{H}] \otimes [\mathbb{H}] = [\mathbb{R}]$ and this implies (by comparing dimensions) that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_4(\mathbb{R})$.

3. If k is algebraically closed, $\mathrm{Br}(k) = \{k\}$.[197]

4. Compared to the previous examples $\mathrm{Br}(\mathbb{Q})$ is way more complex, it is infinite and in fact not even finitely generated.

The next proposition justifies the name "Brauer group".

Proposition 236. *The operation $\otimes_k$ makes $\mathrm{Br}(k)$ into an abelian group.*

Proof. We just need to argue that any element $[A] \in \mathrm{Br}(k)$ has an inverse.[198]

We claim that $[A^{\mathrm{op}}]$ is that inverse. Recall from example 210 that $A \otimes_k A^{\mathrm{op}} \cong \mathrm{End}_k(A) \cong M_n(k)$ and this clearly implies $[A] \otimes [A^{\mathrm{op}}] = [k]$. □

Proposition 237. *The assignment $k \mapsto \mathrm{Br}(k)$ is a functor* ***Fields*** $\rightsquigarrow$ ***AbGrps****.*

Proof. More precisely, if $k \to K$ is a morphism of fields, then we get a map $\mathrm{Br}(k) \to \mathrm{Br}(K)$ sending $[A]$ to $[A \otimes_k K]$. □

Definition 238. The relative Brauer group of an extension K/k is the kernel of the map defined above. We denote it $\mathrm{Br}(K/k)$.

Proposition 239. *The Brauer group of k is the union of the relative Brauer groups of all finite extensions $K > k$, i.e.: $\mathrm{Br}(k) = \bigcup_{[K:k]<\infty} \mathrm{Br}(K/k)$.*

Proof. Given X in $\mathrm{Br}(k)$, let D be the unique central division algebra in X. We want to find a finite extension K/k such that $D \in \mathrm{Br}(K/k)$, that is $D \otimes_k K \cong M_n(K)$. If K is any maximal subfield of D, we know that $n^2 = \dim_k K^2 = \dim_k D$.[199] We claim that for such a K, $D \otimes_k K \cong M_n(K)$.

View D as a K-vector space V_D via right multiplication, it has dimension n, and observe that D acts on V_D K-linearly by left multiplication. Furthermore, since both actions clearly commute and right and left multiplication by k coincide, we obtain a k-algebra homomorphism[200] $D \otimes_k K \to \mathrm{End}_K(V_D) = M_n(K)$ that sends $d \otimes \lambda$ to $v \mapsto dv\lambda$. It is enough then to observe that the dimensions of both sides is n^3 because the L.H.S. is simple, hence the map must be an isomorphism. □

Definition 240. A field K/k is said to split a CSA A if $A \otimes_k K \cong M_n(K)$.

[196] Surjectivity is obvious because every class contains at least one CSA which can be written as $M_n(D)$ for some central division algebra and it follows that this also class contains D. The uniqueness of the decomposition implies that if D and D' are central division k-algebras such that $M_n(D) = M_m(D')$ for some $n, m \in \mathbb{N}$, then $D = D'$ and $n = m$, so the map is injective.

[197] Recall corollary 172.

[198] Because $\mathrm{Br}(k)$ is already the quotient of a commutative monoid, hence a commutative monoid.

[199] Since D is a division algebra, any commutative subalgebra is a subfield. Hence K is a maximal commutative subalgebra and we can use corollary 227.

[200] Checking the properties is left as an exercise.

Example 241. Let $k = \mathbb{Q}$ and $D = \mathbb{Q}(i, j, k)$.[201] Every maximal subfield is quadratic and it is easy to construct them because for any $x \in D - \mathbb{Q}$, $\mathbb{Q}(x)$ is a field of degree two over k. For instance, it is easy to see that $\mathbb{Q}(i) \cong \mathbb{Q}(j) \cong \mathbb{Q}(k)$ because i, j and k all satisfy the same minimal polynomial, namely $x^2 + 1$.

A less obvious fact is that $\mathbb{Q}(i + j) \cong \mathbb{Q}(\sqrt{-2})$. To see this, we note that[202]

$$\mathrm{Nm}(i + j) = \mathrm{Nm}(\sqrt{-2}) = -2 \text{ and } \mathrm{Tr}(i + j) = \mathrm{Tr}(\sqrt{-2}) = 0.$$

We can infer that no field of the form $\mathbb{Q}(\sqrt{d})$ for $d > 0$ is in $\mathbb{Q}(i, j, k)$. Moreover $\mathbb{R}$ cannot arise because it is infinite dimensional, thus $D \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$ is not isomorphic to $M_2(\mathbb{R})$.[203]

The proof of proposition 239 implies that all these fields are examples of splitting fields for D.

The next (and last) theorem of this class is motivated by the study of k-linear representations. An important result in representation theory is the decomposition of the group ring for a finite group G. In the well-studied case $k =$, we have

$$[G] \cong \oplus_{i=1}^{t} M_{d_i}(),$$

where t is the number of distinct irreducible representations of G and $d_1, \dots, d_t$ are their dimensions. We can read off a lot of information from this.

1. By comparing the dimensions, we get $|G| = d_1^2 + \cdots + d_t^2$.

2. The number of conjugacy classes of G is t.

Proof. We will take the center on both sides. On the R.H.S. we obtain a copy of for each summand and hence the center is ^{t}. On the L.H.S., we note that the center is precisely the elements which have the same coefficients in front of elements of the same conjugacy class. Indeed, if $a \in \mathcal{Z}([G])$, we can decompose its sum in conjugacy classes and write

$$a = \sum_{X \in \mathrm{Conj}(G)} \sum_{g \in X} a_g \cdot g.$$

Then, since for any $h \in G$, $hah^{-1} = a$, we have

$$a = \sum_{X \in \mathrm{Conj}(G)} \sum_{g \in X} a_g \cdot hgh^{-1},$$

and we infer[204] that the coefficients of all elements of a single conjugacy class must be the same. It is obvious that the dimension of $\mathcal{Z}([G])$ (t) is the number of conjugacy classes. □

In order to attain more generality, we can ask what happens if is replaced by a field k with $\mathrm{char}(k) \nmid |G|$.[205] Since the study of -linear representations is so well understood, we use it to understand $\mathbb{Q}$-linear representations in the following examples.

[201] The relations between i, j, k are as in $\mathbb{H}$ but we restrict the coefficients to lie in $\mathbb{Q}$.

[202] Recall example 30 to compute the norms and traces.

[203] But we already knew that because $\mathbb{H}$ is a division algebra and $M_2(\mathbb{R})$ is not.

[204] Also using the fact that for any $g_1, g_2 \in G$, there exists $h \in G$ such that $hg_1h^{-1} = g_2$ if and only if g_1 and g_2 are in the same conjugacy class.

[205] We saw in Mascke's theorem that this restriction on k ensures that $k[G]$ is semisimple, namely $k[G] = A_1 \oplus \cdots \oplus A_s$ where the A_i's are simple.

Examples 242.

1. Let p be a prime and $G = \mathbb{Z}/p\mathbb{Z}$. Since G is abelian, it has $|G| = p$ conjugacy classes and we obtain the decomposition
$$[G] \cong \oplus \overset{p}{\cdots} \oplus.$$
Another way to obtain this decomposition is to view $\mathbb{Z}/p\mathbb{Z}$ as the set $\{1, \sigma, \ldots, \sigma^{p-1}\}$ and then we clearly have[206]
$$[G] \cong [x]/(x^p - 1) \cong \oplus_{n=1}^{p}[x]/\left(x - \exp\left(\frac{2\pi i n}{p}\right)\right).$$
However, $x^p - 1$ does not split in $\mathbb{Q}$ and instead we get the decomposition
$$\mathbb{Q}[G] \cong \mathbb{Q}[x]/(x^p - 1) \cong \mathbb{Q}[x]/(x-1)(x^{p-1} + \cdots + x + 1) \cong \mathbb{Q} \oplus \mathbb{Q}(\zeta),$$
where $\zeta = \exp\left(\frac{2\pi i}{p}\right)$.[207]

2. Let Q be the quaternion group, we know from computing the character table[208] of G that
$$[G] = \oplus \oplus \oplus \oplus M_2().$$
By inspecting the two-dimensional representation, we find that Q is realized as a subgroup of $GL_2()$ where all the traces are rational, thus one might wonder if we can realize Q as a subgroup of $GL_2(\mathbb{Q})$. The answer is negative.

   In decomposing $\mathbb{Q}[Q]$, we trivially get the first four terms[209], but the last term is (for now) unknown:
$$\mathbb{Q}[Q] \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus D.$$
We know that $\dim_{\mathbb{Q}}(D) = 4$ and D must be central because if its center were bigger than $\mathbb{Q}$, then the dimension over that would be at least four (it has to be a square and it cannot be one because $\mathbb{Q}[G]$ is not commutative)and hence the dimension over $\mathbb{Q}$ would be too big. We can see that $D = \mathbb{Q}(i, j, k) \subseteq \mathbb{H}$ by defining a map $\phi : \mathbb{Q}[Q] \to D$ that sends $a[x]$ to ax for any $x \in Q$.

   We conclude with the following proposition.

Proposition 243. *The two-dimensional irreducible representation of Q can be realized over $K/\mathbb{Q}$ if and only if K splits $\mathbb{Q}(i, j, k)$.*[210]

This proposition in turns motivates the following question which we answer right away.

Question 244. *Given a CSA A over a field k, how can we understand the collection of all splitting fields for A?*

Theorem 245. *Let $X \in \mathrm{Br}(k)$, then X belongs to $\mathrm{Br}(K/k)$ if and only if there exists a CSA $A \in X$ such that K is contained in A and $[K : k]^2 = \dim_k(A)$.*

[206] The polynomial $x^p - 1$ splits into irreducible linear factors and then we can apply the Chinese remainder theorem.

[207] Note that both summands are field and in particular they are simple, thus, we found the decomposition on $\mathbb{Q}[G]$.

[208] Here is the character table for Q. We only use the dimension of the representations (namely the first column) to obtain the decomposition.

	1	-1	$i_{[2]}$	$j_{[2]}$	$k_{[2]}$
χ_1	1	1	1	1	1
χ_2	1	1	1	−1	−1
χ_3	1	1	−1	1	−1
χ_4	1	1	−1	−1	1
χ_5	2	−2	0	0	0

[209] The one-dimensional -representations are also $\mathbb{Q}$-representations.

[210] It is clear thata $K[Q] = \mathbb{Q}[Q] \otimes_{\mathbb{Q}} K$. Using the decomposition above we see that the decomposition of $K[Q]$ will be composed of matrix rings if and only if $D \otimes_{\mathbb{Q}} K$.

Proof. ($\Leftarrow$) If $\exists A$ with these properties, then we can repeat the argument in proposition 239 to conclude K splits A.

($\Rightarrow$) Suppose that K splits A, namely $A \otimes_k K = M_n(K)$. We can apply the opposite functor and obtain $A^{\text{op}} \otimes_k K \cong M_n(K)$.[211] There is a natural embedding of $A^{\text{op}} \otimes_k 1$ in the L.H.S. and composing with the injective map described above,[212] we get an embedding $A^{\text{op}} \otimes_k 1 \to M_n(K) = B$, where B is a CSA over k.

Let $C = \mathcal{Z}_B(A^{\text{op}} \otimes_k 1)$, the double centralizer theorem implies that C is simple because B is CSA and A^{op} is simple.[213] It also states $\dim_k(C)\dim_k(A^{\text{op}}) = \dim_k(B) = ([K:k]n)^2$, and since $\dim_k(A^{\text{op}}) = n^2$, we infer $\dim_k(C) = [K:k]^2$. It remains to show K sits inside C and $C \in [A]$.

The first part is true because

$$1 \otimes_k K \subseteq \mathcal{Z}_{A^{\text{op}} \otimes_k K}(A^{\text{op}} \otimes_k 1) \subseteq \mathcal{Z}_B(A^{\text{op}}) = A.$$

The second part is true because[214]

$$C \otimes_k A^{\text{op}} \cong B = M_{[K:k]n}(K),$$

thus C is Brauer equivalent to the inverse of A^{op} which is A. □

Corollary 246. *If K splits a central division algebra D and $\dim_k(D) = d^2$, then $d \mid [K:k]$.*

[211] This holds because matrix algebras over a field are isomorphic to their opposites (by taking transposes for instance) and the opposite of K is K.

[212] It is injective by simplicity of $A^{\text{op}} \otimes_k K$ and non-triviality.

[213] We dropped the tensor with 1 because it is unnecessary.

[214] In general if $A \subseteq B$ are both CSA over k, then $C = \mathcal{Z}_B(A)$ commutes with A and $A \otimes_k C \to B$. The L.H.S. is simple over k by the double centralizer, so the map is injective and hence an isomorphism by dimension counting (we can use the double centralizer for that as well).

Review Questions

Exercise 247. Consider the ring $\mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-23}}{2}$ and its ideal $I = (2, \alpha)$. Show that I and I^2 is not principal by I^3 is. This ring is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-23})$.

Proof. Note that α is a root of $x^2 - x + 6$. To show that I is not principal, we need to show that 2 and α have no common divisor but one and that one is not in I. If we write $2 = uv$, then taking norms on both sides yields $4 = \operatorname{Nm}(u)\operatorname{Nm}(v)$, so $\operatorname{Nm}(u) = \operatorname{Nm}(v) = 2$ because the norms cannot be one.

However, we observe that $\operatorname{Nm}(x + y\alpha) = x^2 + xy + 6y^2 = (x + \frac{1}{2}y)^2 + 23(\frac{y}{2})^2$, we conclude that the equation above have no solutions. Thus, the only divisors of 2 are ± 1 and ± 2. Since ± 2 does not divide α, the only common divisor is one.

Finally, we claim that $I \neq (1)$, namely, $2R + \alpha R \neq R$. An element of the L.H.S. is of the form $2u + \alpha v$ and its norm is

$$(2u + \alpha v)(2\bar{u} + \bar{\alpha}\bar{v}) = 4u\bar{u} + 2\bar{\alpha}u\bar{v} + 2\alpha\bar{u}v + 6v\bar{v}.$$

This belongs to $2\mathbb{Z}$, hence $1 \notin I$.

For the second part, we write $I^2 = (4, 2\alpha, \alpha^2) = (4, 2\alpha, \alpha - 6)$. Since we can write $2\alpha = 2(\alpha - 6) + 3 \cdot 4$, we obtain $I^2 = (4, \alpha - 6) = (4, \alpha - 2)$. We claim that $R/I^2 \cong \mathbb{Z}/4\mathbb{Z}$ because $a + b\alpha \mapsto a + 2b$ is surjective and has I^2 as its kernel. We conclude that $I \neq (1)$.

Furthermore, we find the divisors of 4. If $4 = uv$, then taking norms yields $\operatorname{Nm}(u)\operatorname{Nm}(v) = 16$, but no elment has norm two (why?), so we get $\operatorname{Nm}(u) = \operatorname{Nm}(v) = 4$. Using the calculations above, we must find a solution of $4 = (\frac{a}{2})^2 + 23(\frac{b}{2})^2$ or equivalently of $16 = a^2 + 23b^2$. Hence the only divisors of 4 are ± 1, ± 2 and ± 4. But the only divisors of $\alpha - 2$ are ± 1 and hence I^2 cannot be principal.

When we calculate I^3, we get

$$(2, \alpha)(4, \alpha - 2) = (8, 2\alpha - 4, 4\alpha, \alpha^2 - 2\alpha) = (8, 2\alpha - 4, 4\alpha, \alpha + 6).$$

We can remove both terms in the middle, so $I^3 = (8, \alpha - 2)$ and we notice that $\operatorname{Nm}(-2 + \alpha) = 8$, thus $-2 + \alpha$ divides 8 and hence $I^3 = (\alpha - 2)$ is principal. □

Exercise 248. Prime ideals of Dedekind domain are locally principle (because any localization is a DVR). We would like to understand how to find the generator of the localization of an ideal.

Fact 249. *If I is a prime ideal in a Dedekind R. Let $R = \mathbb{Z}[\alpha]$ as above and $\mathfrak{p} = (2, \alpha)$ is a prime ideal because $R/\mathfrak{p} = \mathbb{Z}/2\mathbb{Z}$. What is a generator for $\mathfrak{p}R_{\mathfrak{p}}$. If we try to divide 2 by α, we get*

$$\frac{2}{\alpha} = \frac{2\bar{\alpha}}{\alpha\bar{\alpha}} = \frac{2\bar{\alpha}}{6} = \frac{\bar{\alpha}}{3},$$

thus $2 = \alpha\frac{\bar{\alpha}}{3}$ implying α divides 2, thus $(\alpha) = \mathfrak{p}R_{\mathfrak{p}}$.

Note that this will not work if we tried dividing α by 2. In fact, $R/(\alpha) = \mathbb{Z}/6\mathbb{Z}$ and $R/(2) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ because we can write $R = \mathbb{Z}[x]/(x^2 - x + 6)$, so $R/(2) = \mathbb{Z}/2\mathbb{Z}[x]/(x(x-1)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 250. If $R = [x]$, what is the spectrum of R?.

Proof. As a set: it is the set of prime ideals of $[x]$ which are precisely $(x - a)$ for $a \in$ and (0). So, we can naturally identify $\operatorname{Spec}(R)$ with $\cup\{*\}$, where $*$ represents the generic point (0).

As a topological space: Recall that the closed sets are $V(I) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supset I\}$ and that any I is generated by finitely many polynomials which will have finitely many common roots. If $I = (f_1, \ldots, f_n)$ with common roots $a_1, \ldots, a_m$, then $V(I) = \{a_1, \ldots, a_m\}$. If $I = 0$, then $V(0) = \cup\{*\}$. Hence, the open sets are co-finite sets containing $\{*\}$ together with $\emptyset$.

What is the sheaf $\mathcal{O}$ on $\operatorname{Spec}(R)$. Let $U_S = \operatorname{Spec}([x]) - \{a_1, \ldots, a_m\}$, then it is natural set $\mathcal{O}(U_S) = [x][\frac{1}{x-a_1}, \ldots, \frac{1}{x-a_m}] = [x][\frac{1}{f}]$ where $f = (x - a_1) \cdots (x - a_n)$.

What is the stalk? of $\mathcal{O}$ at $a \in \operatorname{Spec}(R)$? We have $\mathcal{O}_a = \varinjlim_{U \subseteq \operatorname{Spec}(R), a \in U} \mathcal{O}(U) = \{\frac{q(x)}{p(x)} \mid q(x), p(x) \in [x] \text{ and } p(a) \neq 0\}$. For the generic point, $\mathcal{O}_*$ is the inverse limit of every open sets which are non-empty which will yield the fraction field. □

Exercise 251. In the following setting: If L/K is Galois, with $G = \operatorname{Gal}(L/K)$ and

$$\begin{tikzcd}
\mathcal{O}_L \arrow[r, hook] & L \\
\mathcal{O}_K \arrow[r, hook] \arrow[u] & K \arrow[u]
\end{tikzcd}$$

$\mathfrak{p} \lhd \mathcal{O}_K \subset K$, and $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Show that G acts transitively on the set of primes in the decomposition.

Proof. Assume not, then after reordering, we can assume that $\mathfrak{p}_1 \neq \sigma\mathfrak{p}_2$ for all $\sigma \in G$. Therefore $\{\sigma\mathfrak{p}_2\}_{\sigma \in G}$ is a finite collection of distinct primes not containing $\mathfrak{p}$. Using the CRT, we can find $a \in \mathcal{O}_L$ such that $a \in \mathfrak{p}_1$ and $a \equiv 1 \pmod{\sigma\mathfrak{p}_2}$ for all $\sigma \in G$. □

Exercise 252. Let $V = M_{m \times n}(k)$, then $M_m(k)$ acts naturally on V by left multiplication. Then, $\mathcal{Z}_{\operatorname{End}_k(V)}(M_m(k) = M_n(k)$

Proof. $M_n(k)$ also acts on V by right multiplication but less naturally, i.e.: it sends A to the map $(M \mapsto MA^t)$. This clearly commutes with $M_m(k)$ and then we just have to check dimensionality (using double centralizer). □

Exercise 253. Suppose that V is a finite dimensional vector space of dimension N and $A \subseteq \operatorname{End}_k(V)$ and $A \cong M_n(k)$. Then, $n \mid N$ and $B = \mathcal{Z}_{\operatorname{End}_k(V)}(A) \cong M_{N/n}(k)$.

Proof. The double centralizer implies B is simple and B is central over k. We claim there is a natural map $A \otimes B \to \operatorname{End}_k(V) = a \otimes b \mapsto a \cdot b$. Since A and B are CSA over k, then $A \otimes_k B$ is also a CSA and then by dimension count and simplicity, we find it is an isomorphism. We conclude with the Brauer equivalence and the fact that $\operatorname{End}_k(V) = M_{(mn)^2}(k)$. □