Contents

7 Basics

7.1 Introduction to rings

Definition: Ring $(R, +)$ is an abelian group, $\cdot$ is associative, left-and-right distributivity; can be commutative or not; can have identity or not (some always assume yes)

Properties: Ring

1. $0a = 0$ for all $a \in R$;
2. If $1 \in R$, its additive inverse is -1, and $-a = (-1)a$;

Definition: division ring A ring R with unity $1 \neq 0$ is a division ring if for each $a \in R \setminus \{0\}$, there is an element $b \in R$ such that $ab = ba = 1$ (i.e., $R \setminus \{0\}$ is a group under $\cdot$). If it's commutative, R is a field.

Examples: Rings

1. Trivial: all products are zero (can't contain identity)
2. Zero ring
3. Integers
4. Rationals, reals, complex
5. $\mathbb{Z}/n\mathbb{Z}$, but there's something to check here
6. $\mathrm{Mat}_{n\times n}(\mathbb{F})$
7. Quaternion ring $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ with $ij = k$, $jk = i$, $ki = j$, and minuses if you reverse
8. Rings of functions: $Y^X = \{f : X \to Y\}$. If Y is a ring, then define $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. $\boxed{\text{VII.i.1}}$ When is it unital? When is it commutative? $\boxed{\text{VII.i.2}}$ What if we require the functions to have property F?
9. Given a field F, $F[x_1, \ldots, x_n]$ polynomials, $F(x_1, \ldots, x_n)$ rational functions, $F[[x_1, ..., x_n]]$ formal power series, $F[x]/(x^m)$ in which x^m is set equal to zero, and others...
10. Weird one... perhaps: Let n be an integer, and F be a field. Let FQ denote the vector space defined on the basis elements t_{ij} where $1 \leq i \leq j \leq n$. Define multiplication of these elements via $t_{ij}t_{kl} = \begin{cases} t_{il} & \text{if j=k} \\ 0 & \text{otherwise} \end{cases}$ and extend this multiplication linearly. This is called the *path algebra* associated to the directed graph $1 \to 2 \to \ldots \to n$.
11. $R[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in R\}$ (suppose R is commutative) where d is some integer. We make sense of multiplication via $(a + b\sqrt{d})(a' + b'\sqrt{d}) = aa' + d(bb') + (ab' + ba')\sqrt{d}$ and dr is taken to mean $\underbrace{r + r + \ldots + r}_{d}$.

Definition: Zero divisor & Unit $a \in R \setminus \{0\}$ is a *zero divisor* if $\exists b \in R$ such that $ab = 0$ or $ba = 0$. a is *unit* if $\exists b \in R$ such that $ab = 1$. The set of units of R is denoted $R^\times$. (Note: it is a group!)

Exercise: zero divisors/units $\boxed{\text{VII.i.3}}$ Prove that if a is a unit, it is not a zero divisor, and that if a is a zero divisor, then it is not a unit. $\boxed{\text{VII.i.4}}$ Find an example of a ring R and an element a where a is neither a zero divisor nor a unit.

Exercise: units/zero divisors examples VII.i.5 Describe the units and zero divisors of $\mathbb{Z}$. VII.i.6 Describe the set of zero divisors of $\mathbb{Z}/n\mathbb{Z}$. VII.i.7 Describe the units in $\mathbb{Z}/n\mathbb{Z}$.

Exercise: quadratic number field VII.i.8 Show that $\mathbb{Q}[\sqrt{d}]$ has no zero divisors (and hence that $\mathbb{Z}[\sqrt{d}]$ has no zero divisors). VII.i.9 Show that $\mathbb{Q}[\sqrt{d}]$ is a field.

Definition: integral domain A *commutative ring* with no zero divisors is an integral domain.

Property: cancellation in integral domains VII.i.10 In an integral domain, $ab = 0$ implies $a = 0$ or $b = 0$, so $ab = ac$ with $a \neq 0$ implies $b = c$.

Exercise VII.i.11 A finite integral domain is a field!

Definition: subring A subring is a subgroup that is also closed under multiplication. It is assumed to have the same identity if it has one.

Exercises

- VII.i.12 The center of a ring is the set of all elements that commute with everything. Prove that the center is a subring. Prove that the center of a division ring is a field.
- VII.i.13 Suppose that F, G are two fields and $F \subset G$. Prove that G is a vector space over F (hence it makes sense to talk about its dimension over F).
- VII.i.14 Prove that if R is an integral domain, the equation $ax = b$ has at most one solution x for any pair $a, b \in R$ with a and b not both equal to zero.
- VII.i.15 Prove that if R is an integral domain, there are at most two solutions to the equation $ax^2 = b$ for any $a, b \in R$ with a and b not both equal to zero.
- VII.i.16 Let I be some indexing set, and R_i be a ring for each $i \in I$. Define $\prod_{i \in I} R_i$ to be the direct product ring (Cartesian product with componentwise addition and multiplication). Prove that this is commutative if and only if each R_i is, an integral domain if and only if each R_i is, and a ring with unity if and only if each R_i is.
- VII.i.17 Consider the subset $\bigoplus_{i \in I} R_i$ within $\prod_{i \in I} R_i$ of elements $(r_1, r_2, \ldots)$ in which all but finitely many of the r_i are equal to zero. Prove that this

subset is a ring. Explain further why this *direct sum* ring does not have an identity if I is infinite (even if each R_i does have an identity).

- $\boxed{\text{VII.i.18}}$ Let R be a commutative ring with identity, and $G = \{g_1, \ldots, g_n\}$ be a finite group with operation written as multiplication (no matter what it really is). Define RG to be the set of formal sums

$$a_1 g_1 + \ldots + a_n g_n$$

where $a_i \in R$ and $g_i \in G$. Define addition componentwise, and multiplication by $(ag_i)(bg_j) = (ab)(g_i g_j)$. Show that RG is a ring, which is commutative if and only if G is Abelian.

- $\boxed{\text{VII.i.19}}$ Prove that if in the group ring RG, any element $1g_i$ is a unit, but that if $G \neq \{e\}$, there are always zero divisors.
- $\boxed{\text{VII.i.20}}$ Prove that the real quaternion ring is a division ring.

7.3 Ring homomorphisms

Definition: homomorphism/isomorphism A ring homomorphism $\phi : R \to R'$ is a group homomorphism of the additive groups $(R, +), (R', +')$ satisfying $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$. An isomorphism is a bijective homomorphism.

Exercise: inverse homomorphism $\boxed{\text{VII.iii.1}}$ If $\phi : R \to S$ is a ring homomorphism that is bijective, then $\phi^{-1} : S \to R$ is also a ring homomorphism.

Definition: image and kernel The *kernel* of a ring hommormophism is the set $\{r \in R \mid \phi(r) = 0\}$.

Exercise: substructure of kernel and image $\boxed{\text{VII.iii.2}}$ The image of a ring homomorphism is a subring of the codomain. $\boxed{\text{VII.iii.3}}$ The kernel K of a ring homomorphism $\phi : R \to S$ is a subring of the domain with the additional property that $rk \in K$ for any $k \in K$ and $r \in R$.

Exercise: examples

- $\boxed{\text{VII.iii.4}}$ For any positive integer n define the map $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ via $\phi(m) = [m]_n$ (the congruence class of m modulo n.) Compute its kernel.
- $\boxed{\text{VII.iii.5}}$ Let F be a field, and $a \in F$ be a fixed element. Define $\text{ev}_a : F[x] \to F$ by the following assignment: $\text{ev}_a(p(x)) = p(a)$. Prove that ϕ is a ring homomorphism. Describe the kernel.
- $\boxed{\text{VII.iii.6}}$ Challenge: Consider the homomorphism from the above. Show that if $F = \mathbb{C}$, then $\ker(f) = \{p(x) \in \mathbb{C}[x] \mid p(x) = (x-a)q(x), \exists q(x) \in \mathbb{C}[x]\}$.

- VII.iii.7 Let m be an integer. Determine the values of m for which the function $\phi_m : \mathbb{Z} \to \mathbb{Z}$ given by $\phi_m(n) \mapsto m \cdot n$ is a homomorphism.

Definition: quotient rings So the kernel $\ker \phi$ is a homomorphism $\phi : R \to S$ is, at core, an additive subgroup of the R. From groups, we know that it is normal, and the first isomorphism theorem for groups tells us that $R/\ker \phi$ is isomorphic (as a group) to $\operatorname{image} \phi$ via $\tilde{\phi} : r + \ker \phi \mapsto \phi(r)$. VII.iii.8 Prove that $\tilde{\phi}$ is a ring homomorphism.

Exercise VII.iii.9 Let $\mathbb{Q}$ be the rational number field, and consider the ring $\mathbb{Q}[x]$. Define the function $\varphi : \mathbb{Q}[x] \to \mathbb{R}$ by $\varphi(f) = f(\sqrt{5})$.

1. Compute the kernel of φ.
2. Show that the image of φ is isomorphic to $\mathbb{Q}[\sqrt{5}]$.

Definition: ideals Motivated by the additional structure of the kernel of a homomorphism, define an ideal. Let I be a subgroup of $(R, +)$. Then I is a

- *left ideal* if $rx \in I$ for all pairs $r \in R$ and $x \in I$;
- *right ideal* if $xr \in I$ for all pairs $r \in R$ and $x \in I$.
- *two-sided ideal* if it is both a left and right ideal.

we can form the quotient ring of R by any two-sided ideal exactly as we did above.

Exercise Let $I \subset R$ be an ideal.

- VII.iii.10 If there is an invertible element $x \in I$ such that $x^{-1} \in I$, then $I = R$.
- VII.iii.11 If $a_1, \ldots, a_k \in I$ and $r_1, \ldots, r_k \in R$ and I is a left ideal, then $a_1 r_1 + \ldots + a_k r_k \in I$.
- VII.iii.12 Let $I \subset \mathbb{Q}[x]$ be the set of polynomials whose summands are of degree at least 2. Compute the dimension of $\mathbb{Q}[x]/I$ as a vector space over $\mathbb{Q}$. Find a complete set of representatives for the elements of $\mathbb{Q}[x]/I$.
- VII.iii.13 List the ideals of $\mathbb{Z}/n\mathbb{Z}$ for each integer n.
- VII.iii.14 Prove that a commutative ring R is a field if and only if it has no non-trivial ideals (i.e., its only ideals are R and $\{0\}$.

Exercise: examples

- VII.iii.15 Describe all ideals in $\mathbb{Z}$.

Exercise: reduction for Diophantine The greeks (and beyond) were interested deeply in Diophantine equations, that is, polynomial equations in multiple variables with integer coefficients. The goal is to find all integer solutions, but this can be hard (Fermat's Last Theorem anyone?) Reduction modulo an integer can help because there are now only finitely many possibilities. $\boxed{\text{VII.iii.16}}$ Consider the equation $x^2 + y^2 = 3z^2$. Show that the only integer solution to this equation is the trivial one ($x = y = z = 0$) by reducing modulo 4 and investigating the perfect squares in this ring.

Exercise: ideal algebra There are some nice algebraic steps that can be carried out with ideals. Let I and J be two-sided ideals:

- $\boxed{\text{VII.iii.17}}$ Show that the sum of I and J, defined by
$$I + J = \{a + b \mid a \in I,\ b \in J\}.$$
- $\boxed{\text{VII.iii.18}}$ Show that the product of I and J, defined as the set of all finite sums of elements ab where $a \in I$ and $b \in B$ is a two-sided ideal.
- $I^n := I^{n-1}I$ are the powers, defined inductively.
- $\boxed{\text{VII.iii.19}}$ Suppose that $\{I_j \mid j \in \Omega\}$ is a set of ideals in a ring I (where Ω is a not-necessarily-finite index set). Prove that $\bigcap_{j\in\Omega} I_j$ is an ideal.
- $\boxed{\text{VII.iii.20}}$ Suppose that $I_1 \subset I_2 \subset \dots$ is a set of ideals in a ring R that form a chain. Prove that $\bigcup_{n=1}^{\infty} I_n$ is an ideal.

Exercise: more ideal algebra Suppose that $m, n \in \mathbb{Z}$ and consider the ideals $m\mathbb{Z}$ and $n\mathbb{Z}$ in $\mathbb{Z}$. $\boxed{\text{VII.iii.21}}$ Express the ideal $m\mathbb{Z}+n\mathbb{Z}$ as an ideal of the form $d\mathbb{Z}$. I.e., what is d and why? $\boxed{\text{VII.iii.22}}$ Express the ideal $(m\mathbb{Z})(n\mathbb{Z})$ as an ideal of the form $d\mathbb{Z}$.

Exercise: the isomorphism theorems Throughout, R is a ring with identity.

1. $\boxed{\text{VII.iii.23}}$ Suppose that A is a subring of R and I is an ideal of R. The set $A + I$ is defined to be the set $\{a + y \mid a \in A,\ y \in I\}$. Prove that
$$(A + I)/I \cong A/(A \cap I).$$
2. $\boxed{\text{VII.iii.24}}$ Suppose that $I \subset J \subset R$ is a chain of ideals in R. Prove that $(R/I)/(J/I) \cong R/J$.
3. $\boxed{\text{VII.iii.25}}$ Prove that there is a bijection between the set of ideals in R containing I and ideals in R/I.

7.4 Properties of ideals

Definitions Let A be a subset of a ring R, a ring with identity.

1. We denote by (A) the smallest ideal of R containing A, called the *ideal generated by* A. [Note: this is the intersection of all ideals that contain A, so by above exercises, it is clearly an ideal.]
2. We have the following:

$$\begin{aligned} RA &= \{r_1a_1 + \ldots + r_na_n \mid r_i \in R,\ a_i \in A\} \\ AR &= \{a_1r_1 + \ldots + a_nr_n \mid r_i \in R,\ a_i \in A\} \\ RAR &= \{r_1a_1r_1' + \ldots + r_na_nr_n' \mid r_i, r_i' \in R,\ a_i \in A\}. \end{aligned}$$

3. An ideal that can be generated by a single element is a *principal ideal*;
4. An ideal that can be generated by a finite set of elements is called *finitely generated*.

Exercises

1. $\boxed{\text{VII.iv.1}}$ Prove that every ideal in $\mathbb{Z}$ is a principal ideal.$\star$
2. $\boxed{\text{VII.iv.2}}$ Show that the ideal $(2, x) \subset \mathbb{Z}[x]$ is *not* a principal ideal.
3. $\boxed{\text{VII.iv.3}}$ Suppose that R is a ring with identity and I is a two-sided ideal in R. Prove that $I = R$ if and only if I contains an invertible element.
4. $\boxed{\text{VII.iv.4}}$ Suppose that R is a commutative ring. Prove that R is a field if and only if its only ideals are R and 0. As a corollary, prove that if F is a field and $\varphi : F \to R'$ is a non-zero ring homomorphism, then φ is injective.
5. $\boxed{\text{VII.iv.5}}$ Suppose that I is a two-sided ideal in the matrix ring $M_n(\mathbb{C})$.

Remark If we're thinking about substructures within algebraic structures, it often makes sense to ask about the smallest among them and the largest. Of course, the smallest ideal in a ring R is $\{0\}$, and the largest is R. But perhaps we'd want to avoid those. It turns out that the large non-trivial ones are really interesting (but you're free to think about what the smallest might look like).

Definition: maximal A two-sided ideal $\mathfrak{m} \subsetneq R$ is called *maximal* if there are no ideals I with $\mathfrak{m} \subsetneq I \subsetneq R$.

Exercise: Using Zorn's Lemma $\boxed{\text{VII.iv.6}}$ Prove that every ring R with identity $1 \neq 0$ has at least one maximal ideal. The proof of existence of some maximal element is often achieved using Zorn's lemma, which you can find in the Appendix in Dummit and Foote.

Exercises

1. $\boxed{\text{VII.iv.7}}$ Suppose that R is a commutative ring with identity. Prove that an ideal $\mathfrak{m} \subsetneq R$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field. This exercise is vitally important for the study of Fields and Galois Theory. It says that if you can construct a commutative ring, R and a maximal ideal $\mathfrak{m}$ within, then $R/\mathfrak{m}$ is a field. As an example, see the next exercise.
2. $\boxed{\text{VII.iv.8}}$ Consider the ring $\mathbb{R}[x]$. Prove that the ideal (x^2+1) is a maximal ideal, then show that $\mathbb{R}[x]/(x^2+1)$ is isomorphic to a field that you're very familiar with.
3. $\boxed{\text{VII.iv.9}}$ Prove that $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is a prime number.

Remark Now let's think about generalizing some behavior within the integers. A positive integer $p > 1$ is *prime* if $ab = p$ implies $a = \pm 1$ or $b = \pm 1$. But the really nice property is that if ab is a multiple of p, then $p \mid a$ or $pmidb$. When we cast that into the ideal corresponding to p, (p), that means that if $ab \in (p)$, then $a \in (p)$ or $b \in (p)$. This inspires the following.

Definition: Primeness Let R be a commutative ring. An ideal $P \neq R$ is called *prime* if $ab \in P$ implies that $a \in P$ or $b \in P$.

Exercises

1. $\boxed{\text{VII.iv.10}}$ Let $R = \mathbb{Q}[x,y]$. Prove that the set of polynomials in R with 0 constant term is maximal, the ideal of all multiples of x is prime but not maximal, and the ideal of all multiples of xy is not prime and not maximal.
2. $\boxed{\text{VII.iv.11}}$ Suppose that R is a commutative ring. Prove that an ideal $P \subset R$ is prime if and only if R/P is an integral domain. As a corollary, show that all maximal ideals are prime ideals.
3. $\boxed{\text{VII.iv.12}}$ Prove that $(2, x)$ is a maximal ideal in $\mathbb{Z}[x]$.
4. $\boxed{\text{VII.iv.13}}$ Let's write $F_2 = \mathbb{Z}/2\mathbb{Z}$, the field with two elements. Consider the ideal I in $F_2[x]$ generated by (x^2+x+1). Prove that I is a maximal ideal, and determine the addition and multiplication table for the field $F_2[x]/(x^2+x+1)$. Congratulations! You've witnessed a field with 4 elements.

Concluding Remarks What is happening here? First, recall that we might start by being interested in integral solutions to equations of the form $p(x_1, x_2, \ldots, x_n) = 0$. For example, $x^2 + y^2 - 3z^2 = 0$. We witnessed a while back that if we were to reduce the coefficient set modulo 4 (i.e., reduce the polynomial via the ideal generated by 4) it could help us understand or restrict the possibilities. Think about the following progression:

1. When we only had the natural numbers, we had no solutions to the equations of the form $x+a=b$ when $b<a$. How frustrating! So let's introduce the integers. We now have additive inverses *and* multiplication.
2. We notice that we have this nice property that if $a \neq 0$, then $ax = ay$ if and only if $x = y$. So cancellation works.
3. But we also notice we don't *always* have solutions to equations of the form $ax = b$, though when we do, we only have one. Why is that... and how could we break it? So let's introduce division. Now we have the rational numbers.
4. Over the rationals, we can solve all equations of the form $ax = b$ when $a \neq 0$. Great!
5. What about polynomials? A polynomial of degree d with rational coefficients doesn't always have all of its roots rational, but in general there are at least d of these roots (counting multiplicity). Cool. What do we have to do to get the rest of these roots? It turns out going to the reals isn't enough, so we actually have to pass to the complex numbers. That leap is two steps. The first is using analysis to pass to the real numbers, then using ring theory to pass to the complex numbers.

7.5 Rings of fractions: localization

Let's focus on the step from the integers to the rational numbers. The idea is that the integers weren't robust enough to have solutions to all equations of the form $ax = b$ where $a, b \in \mathbb{Z}$ and a is non-zero (if $a = 0$, then b must be zero to admit any solutions, and we don't have a problem with that). So we introduce inverses.

Remark Fractions in the realm of integers goes like this: we consider the set of ordered pairs (a, b) where $b \neq 0$. The first component is the numerator, and the second component is the denominator. Now we want to declare (a, b) to be equivalent to (c, d) when $ax = b$ has the same solution as $cx = d$. This would imply that $axd = cxb$, or $(ad - bc)x = 0$. If we assume R is an integral domain, then this means $x = 0$ or $ad - bc = 0$. I.e., $ad = bc$. Look familiar? So we have a set of ordered pairs $\{(a, b) \mid a, b \in R,\ b \neq 0\}$ and an equivalence relation $(a, b) \sim (c, d)$ if $ad = bc$. Can we define arithmetic?

Theorem: Inversion Suppose that R is a commutative ring with identity and that $D \subset R$ is a *multiplicative set.* I.e., if $a, b \in D$, then $ab \in D$, and furthermore $1 \in D$. There is a ring $D^{-1}R$ with the following properties:

- There exists a homomorphism $\phi : R \to D^{-1}R$;
- If $d \in D$, then $\phi(d)$ is a unit in $D^{-1}R$;
- If there is any other ring T and ring homomorphism $f : R \to T$ such that $f(d) \in T^*$ for all $d \in D$, then there exists a unique ring homomorphism $\tilde{f} : D^{-1}R \to T$ such that $\tilde{f} \circ \phi = f$.

$D^{-1}R$ is referred to as the *localization* of R with respect to D, or the ring of fractions of D in R.

Exercises

1. $\boxed{\text{VII.v.1}}$ Consider the set $R \times D$ of ordered pairs and define a relation $\sim_D$ via $(r_1, d_1) \sim (r_2, d_2)$ if there exists an element $t \in D$ such that $t(r_1 d_2 - r_2 d_1) = 0$. Show that $\sim_D$ is an equivalence relation on $R \times D$.

2. $\boxed{\text{VII.v.2}}$ We define addition and multiplication on $R \times D$ in the way that we do on fractions:

$$(r_1, d_1) \cdot (r_2, d_2) = (r_1 r_2, d_1 d_2)$$
$$(r_1, d_1) + (r_2, d_2) = (r_1 d_2 + r_2 d_1, d_1 d_2)$$

Prove that these operations are well-defined on $R \times D/\sim_D$.

3. $\boxed{\text{VII.v.3}}$ Show that $R \times D/\sim_D$ is a ring with identity (d, d) for any $d \in D$. (If we hadn't assumed that R was a ring with identity, but had that D was non-empty, this would give us an identity in $D^{-1}R$.)

4. $\boxed{\text{VII.v.4}}$ Prove that the map $\phi : R \to D^{-1}R$ defined by $\phi(r) = (r, 1)$ is a ring homomorphism and that $\phi(d)$ is a unit in $D^{-1}R$.

5. $\boxed{\text{VII.v.5}}$ Prove that the above map is one-to-one if and only if D contains no zero-divisors. In particular, if R is an integral domain and $0 \notin D$, this is always the case.

6. $\boxed{\text{VII.v.6}}$ Lemma: Prove that if $f : R \to T$ is a ring homomorphism and that $f(1_R) \neq 1_T$ then image$(f) \subset \text{ZD}(T)$. In particular, $f(r) \notin T^*$ for all $a \in R$.

7. $\boxed{\text{VII.v.7}}$ Lemma: Prove that if $f : R \to T$ is a ring homomorphism with $f(1_R) = 1_T$ and $d \in R^*$ then $f(d^{-1}) = f(d)^{-1}$ (in particular, $f(d)$ is invertible).

8. $\boxed{\text{VII.v.8}}$ Prove the universal property of $D^{-1}R$: If T is any ring and $f : R \to T$ is a ring homomorphism such that $f(d) \in T^*$ for all $d \in D$, then there exists a unique ring homomorphism $\tilde{f} : D^{-1}R \to T$ such that $\tilde{f} \circ \phi = f$.

Remark The word *universal property* showed up above, and it might seem strange. This starts a light conversation about categories. Much more is to be said, but a universal property gives us a way to define the type of behaviour we want to see (like invertibility of the elements of D) and determine if there is a unique way to define this structure.

Remark If R is a field and $0 \notin D$, then $D^{-1}R \cong R$. If R is an integral domain and $D = R \setminus \{0\}$, then $D^{-1}R$ is a field... and this is what we wanted in the first place.

Exercise $\boxed{\text{VII.v.9}}$ Consider $\mathbb{Z}$ and the two subsets $D = 2\mathbb{Z}$ and $S = \{2^n \mid n \in \mathbb{Z}_{\geq 0}\}$. Describe $D^{-1}\mathbb{Z}$ and $S^{-1}\mathbb{Z}$. Are they isomorphic?

Exercise $\boxed{\text{VII.v.10}}$ If $d \in R$ is not zero and not a zero-divisor, then define $d^{\mathbb{Z}} = \{1, d, d^2, \dots, \}$. Then $(d^{\mathbb{Z}})^{-1}R$ is like the ring of polynomials in the variable $1/d$, which we write $R[1/d]$. (There's something to prove here: that the powers are really independent.)

Exercise $\boxed{\text{VII.v.11}}$ If R is an integral domain and F is a field containing R, then F contains $\mathcal{Q}R$ is isomorphic to a subfield of F.

Exercise $\boxed{\text{VII.v.12}}$ Let R be an integral domain and D be a multiplicative set. Then there is a bijection between prime ideals in $D^{-1}R$ and prime ideals in R not intersecting D.

Exercise $\boxed{\text{VII.v.13}}$ A commutative ring is called *local* if it has a unique maximal ideal $\mathfrak{m}$. Prove that $R - \mathfrak{m} = R^*$ if R is a local ring.

Exercise $\boxed{\text{VII.v.14}}$ Consider the commutative ring with identity R and a multiplicative set S. Prove that the localization φ furnishes a bijection between the set of prime ideals in R not intersecting S and the prime ideals in $S^{-1}R$.

Exercise $\boxed{\text{VII.v.15}}$ Let p be a prime integer, and consider S the multiplicative set of integers that are *not* multiples of p. (Note, this is precisely the complement of (p) in $\mathbb{Z}$.) The localization $S^{-1}\mathbb{Z}$ is often denoted $\mathbb{Z}_{(p)}$. Prove that $\mathbb{Z}_{(p)}$ is a local ring with maximal ideal $\{\frac{t}{q} \mid t \in (p), q \in S\}$. (You may refer to the previous exercise.)

7.6 Interlude: Categories

A *category* $\mathcal{C}$ is a pair with a class of objects, $\text{obj}(\mathcal{C})$ and a set $\text{mor}_{\mathcal{C}}(A, B)$ for all pairs of objects A, B in $\mathcal{C}$ such that for each triple of objects $A, B, C \in \text{obj}(\mathcal{C})$, there is a function $\circ : \text{mor}_{\mathcal{C}}(B, C) \times \text{mor}_{\mathcal{C}}(A, B) \to \text{mor}_{\mathcal{C}}(A, C)$ known as *composition* that is associative on 4-tuples of objects. We further insist that for every object $X \in \mathcal{C}$, there is an element $1_X \in \text{mor}_{\mathcal{C}}(X, X)$ such that $1_X \circ f = f$ and $g \circ 1_X = g$ for all $f \in \text{mor}_{\mathcal{C}}(Y, X)$ and $g \in \text{mor}_{\mathcal{C}}(X, Z)$.

Examples

1. Let $\mathcal{C}$ be the category whose objects are the positive integers, with $\text{mor}_{\mathcal{C}}(m, n) = \begin{cases} \{n/m\} & \text{if divisible} \\ \emptyset & \text{otherwise} \end{cases}$. So the *morphism* set from m to n is either a singleton if m doesn't divide n, and empty otherwise. We also need to furnish a *composition* of functions! What should $\circ : \text{mor}_{\mathcal{C}}(m, n) \times \text{mor}_{\mathcal{C}}(l, m) \to \text{mor}_{\mathcal{C}}(l, n)$ do? Let's assume that there *is* a divisibility, that $l \mid m$ and

$m \mid n$. Then $l \mid n$ and its morphism is n/l which is equal to $n/m \cdot m/l$. So let's say:

$$(n/m) \circ (m/l) = n/l$$

but if either set is empty, then the codomain is empty, so composition is just the trivial map from empty set to empty set.

This category already has an interesting object: an *initial* object, an object χ with the property that $\mathrm{mor}_{\mathcal{C}}(\chi, n) \neq \emptyset$ for all $n \in \mathrm{obj}(\mathcal{C})$. What is it? Is it unique? Why? Does it have a *dual* notion?

2. Let $\mathcal{A}\lfloor$ be the category whose objects are finite abelian groups, and whose morphism sets are the set of group homomorphisms, with composition being... composition. Notice that the kernel of such a homomorphism is still a finite abelian group and the cokernel is also. This is called an *abelian* category.

3. Let $\mathcal{S}et$ be the category whose objects are sets and whose morphisms are set functions. Composition is just composition. What is the *initial* object here? Can you realize intersection as an object with a universal property? What about union?

4. Vector spaces over a given field, with linear transformations.

5. Topological spaces with continuous maps.

6. Products are universal objects, that may or may not exist: $\boxed{\text{Definition:}}$ Let I be an indexing set, and let R_i be an object for each index $i \in I$. A *product* of R_i, denoted $\prod_{i\in I} R_i$ is an object with a morphism $p_j : \prod_{i\in I} R_i \to R_j$ for each $j \in I$ satisfying the following universal property: if T is any other object in $\mathcal{C}$ with morphisms $\varphi_j : T \to R_j$ for each $j \in J$, then there is a unique map $\Phi : \prod_{i\in I} R_i \to T$ such that $\varphi_j \circ \Phi = p_j$ for each $j \in J$.

7. You can check that the product of rings is such a universal object.

8.

7.7 Chinese remainder theorem

The defining structure of rings comes partly from the ring of integers, so let's spend a little bit of time on them. We've already seen that every ideal in $\mathbb{Z}$ is principal. In particular, every quotient of $\mathbb{Z}$ is of the form $\mathbb{Z}/n\mathbb{Z}$. But does this *decompose* further?

Definition Ideals A and B in a ring R are called *comaximal* if $A + B = R$.

Theorem: Chinese Remainder Theorem Let $A_1, \ldots, A_k$ be ideals in a commutative ring R with identity. Then the map

$$\begin{aligned} R &\to R/A_1 \times R/A_2 \times \ldots \times R/A_k \\ r &\mapsto (r + A_1, r + A_2, \ldots, r + A_k) \end{aligned}$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \ldots \cap A_i$. If for each pair i, j with $i \neq j$ we hav A_i and A_j are comaximal, then the map is surjective, and the kernel is $A_1 A_2 \cdots A_k$. Thus,

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \ldots \cap A_k) \cong R/A_1 \times \ldots \times R/A_k.$$

Note Note that if A_i are principal ideals generated by a_i, then $A_1 A_2 \cdots A_k = (a_1 a_2 \cdots a_k)$.

Proof Let's work with $k = 2$. Consider $\varphi : R \to R/A \times R/B$ with $\varphi(r) = (r + A, r + B)$. Ring homomorphism is easy, the kernel is those elements with $\varphi(r) = (0 + A, 0 + B)$ which means $r \in A$ and $r \in B$, so the intersection. Assuming A and B are comaximal, this means $1 = a + b$ for some $a \in A$ and $b \in B$. But then $\varphi(r_1 a + r_2 b) = (r_1 a + r_2(1 - a) + A, r_1(1 - b) + r_2 b + B)$, which is $(r_2 + A, r_1 + B)$, so φ is onto. Clearly $AB \subset A \cap B$ by the absorption property. Now suppose that $x \in A \cap B$. Then $x = x(a + b) = xa + xb$. $xa \in AB$ since $x \in B$, and $xb \in AB$ since $x \in A$. Thus, the result is proven.

Exercise: The case of the integers Consider the case of the integers. VII.vii.1 Prove that two ideals (n) and (m) are comaximal if and only if $\gcd(m, n) = 1$.

Exercise VII.vii.2 Describe the ideal $(n) \cap (m)$ in terms of number theory.

Exercise VII.vii.3 For each integer n, let us denote by $\varphi(n)$ the number units in $\mathbb{Z}/n\mathbb{Z}$. Find a formula for $\varphi(p^k)$ when p is prime and k is a positive integer.

Exercise VII.vii.4 Prove that if m and n are relatively prime, then $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$. You may want to consider how to relate the set of units in the ring $R \times S$ to the set of units in R and S separately.

Exercise: central idempotents Let R be a ring (not necessarily commutative) with identity $1 \neq 0$. An element $e \in R$ is called an *idempotent* if $e^2 = e$. VII.vii.5 Prove that $1 - e$ is also an idempotent, and that both e and $1 - e$ are non-trivial zero divisors when $e \neq 1$ and $e \neq 0$.

Exercise VII.vii.6 Prove that if e is an idempotent such that $re = er$ for each $r \in R$, then in the two-sided ideal Re, the element e is the identity.

Exercise VII.vii.7 Show that if $re = er$ for all $r \in R$, then $R \cong Re \times R(1 - e)$ by using the theorem above.

8 Special Classes of Domains

Many rings appearing in number theory have interesting structure that we should identify and study. We only take on commutative domains in this chapter.

8.1 Euclidean domains

Inspired by the Euclidean algorithm, we seek integral domains that have such an algorithm.

Definition: Norm A function $N : R \to \mathbb{Z}_{\geq 0}$ with $N(0) = 0$ is called a *norm* on R. If, in addition, $N(\alpha) > 0$ for all $\alpha R \setminus \{0\}$, then N is a positive norm.

Remark Very vague, not much there.

Definition: Euclidean domain A domain R is called a *Euclidean Domain* if it admits a norm N relative to which R has a division algorithm. That is, for any $a, b \in R$ with $b \neq 0$, there exist elements $q, r \in R$ such that

$$\begin{aligned} a &= qb + r \\ \text{such that} r &= 0 \\ \text{or } N(r) &< b \end{aligned}$$

q is called the *quotient* and r the *remainder*.

Examples Clearly $\mathbb{Z}$ is an example of a Euclidean domain, as is $F[x]$ for any field F.

Euclidean Algorithm The importance is that there is a Euclidean Algorithm:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

where in each case we have divided r_i by r_{i+1} to get to the next line. Since $N(r_1) > \ldots > N(r_n)$, is a decreasing sequence bounded below by zero, it must terminate, and it can only terminate if $r_{n+1} = 0$.

Why do we like it? What's nice now is that r_n can be expressed as an R combination of a and b (so, for example, if a and b are in an ideal, so must r_n be).

Exercise

1. $\boxed{\text{VIII.i.1}}$ Prove that if R is a Euclidean domain then r_n can be written as an R-linear combination of a and b.

2. VIII.i.2 Prove that r_n divides both a and b. This shows that the proceedure outlined above, the Euclidean Algorithm, produces a common divisor. Throughout, we should try to investigate the say in which it is the "greatest" divisor. Since we don't really have an order on R, the notion of largest doesn't yet make sense.
3. VIII.i.3 Suppose that I is a non-zero ideal in a Euclidean domain, and that $x \in I$ is an element of minimal norm among all non-zero elements of I. Prove that $I = (x)$.

Definition A *greatest common divisor* of a and b in a commutative ring R is a non-zero element such that

i. $d \mid a$ and $d \mid b$, and

ii. if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Exercise VIII.i.4 Rephrase the notion of a greatest common divisor in terms of ideals generated by the elements a, b, d.

Exercise VIII.i.5 Prove that r_n is a GCD of a and b.

Exercise VIII.i.6 Let R be an integral domain. Suppose that d and d' are elements in R such that $(d) = (d')$.[1] Prove that there exists a unit $\gamma \in R$ such that $d\gamma = d'$. (In some texts, they would call the pair d, d' *associates*.)

Theorem Let R be a Euclidean Domain, and $a, b \in R$. Let d be the final remainder r_n from the Euclidean Algorithm. Then $(a, b) = (d)$, and d is a GCD of a and b.

Exercise Consider the rings of the form $R = \mathbb{Z}[\sqrt{d}]$ where $d \in \mathbb{Z}$. Define $N : R \to \mathbb{Z}$ via $N(a+b\sqrt{d}) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2-b^2d$. VIII.i.7 Prove that this is a *multiplicative norm* when $d \leq 0$. (Multiplicative means $N(z \cdot z') = N(z) \cdot N(z')$ for any $z, z' \in R$.)

Exercise Consider the ring $R = \mathbb{Z}[i]$ and elements $\alpha = a + bi$ and $\beta = c + di$ with $\beta \neq 0$. In the field $\mathbb{Q}(i)$, $\frac{\alpha}{\beta} = r + si$ with $r, s \in \mathbb{Q}$ (by rationalizing the denominator). Round r, s to the nearest integer, call it $\overline{r}, \overline{s}$. Then $|r - \overline{r}| \leq 1/2$, and $|s - \overline{s}| \leq 1/2$. Define $\gamma = \beta\left[(r - \overline{r}) + (s - \overline{s})i\right]$. VIII.i.8 Prove that $\alpha = (p + qi)\beta + \gamma$, and that $\gamma \in \mathbb{Z}[i]$. VIII.i.9 Prove that $N(\gamma) \leq \frac{1}{2}N(\beta)$ (hint: use multiplicativity).

[1] Recall that (x) is the ideal generated by x in R.

8.2 Principle ideal domain

We saw in the last section that all ideals in a Euclidean domain are generated by a single element. This characteristic deserves its own name.

Definition A *principal ideal domain* (PID) is an integral domain in which every ideal is principal.

Exercise VIII.ii.1 Show that $\mathbb{Q}[x]$ a PID but $\mathbb{Z}[x]$ is not.

Remark The work of the previous section shows that the generator of an ideal can be computed by finding the mutual GCD of all its elements. One powerful notion about PIDs is their ideal structure.

Proposition VIII.ii.2 Prove that if R is a PID and P is a prime ideal in R, then P is also a maximal ideal.

Exercise VIII.ii.3 Suppose that R is a PID, and (p), (q) are two ideals that are comaximal[2]. Prove that 1 is a GCD of a and b.

8.3 Unique factorization domains

In looking at one final class of integral domains, we attempt to recognize another special property of the integers. Namely, we consider the way factorization works. An integer can, of course, be factored in many ways. $12 = 6 \cdot 2 = 4 \cdot 3 = 12 \cdot 1 = -4 \cdot -3$ and so on. (You might be surprized by the negative factors, but we're trying to replicate the behavior in other rings, and it's not clear what "negative" should mean in the case of an arbitrary ring.) To get some sort of uniqueness, we attempt to factor as far as possible, which leads to the idea of primes. The further factorization that is possible, namely peeling off a factor of 1 or -1 seem useless, so let's agree not to have these as possible factors.

But what is prime? We have two great definitions: it doesn't further factor... or is it that whenever it divides a product, it must divide one of the factors?

Definition Let R be an integral domain.

a. A non-zero, non-unit element $r \in R$ is called *irreducible* in R if $r = ab$ implies either a or b is a unit.

b. A non-zero element $p \in R$ is *prime* if the ideal generated by p is a prime ideal. I.e., if $p \mid ab$ then $p \mid a$ or $p \mid b$.

c. Two elements $a, b \in R$ with $a = ub$ for some unit u are *associates*.

Question Are irreducible elements prime? Are prime elements irreducible? Is this just special behavior in $\mathbb{Z}$?

[2] Recall, comaximal means that $(p) + (q) = R$.

Proposition $\boxed{\text{VIII.iii.1}}$ Prove that a prime element in an integral domain is irreducible.

Exercise Recall that on a quadratic integer ring, $R = \mathbb{Z}[\sqrt{d}]$, where d is negative, we have defined the norm $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d})$. We've also shown that it is a multiplicative norm. $\boxed{\text{VIII.iii.2}}$ Show that in the ring $R = \mathbb{Z}[\sqrt{-5}]$, the element 3 is irreducible, but is not prime (because 3 divides $(2 + \sqrt{-5})(2 - \sqrt{-5})$ but doesn't divide either).

Exercise That was the case of an interesting domain in which prime is not the same as irreducible. In PIDs, the two ideas do coincide. $\boxed{\text{VIII.iii.3}}$ Prove that if R is a PID and x is irreducible, then x is prime. (Hint: Show (x) is a maximal ideal by assuming there is another maximal ideal containing it.)

Definition A *unique factorization domain (UFD)* is an integral domain in which every non-zero non-unit has a factorization $r = p_1 p_2 \cdots p_n$ into irreducibles which is unique up to associates. (I.e., if $r = q_1 \cdots q_m$ is another factorization into irreducibles, then $n = m$, and with some reordering (if necessary), p_i and q_i are associates.

Example $\mathbb{Z}$ and $F[x]$ are examples.

Proposition $\boxed{\text{VIII.iii.4}}$ In a UFD, a non-zero element is prime if and only if it is irreducible. (From above, we only need to show irreducible implies prime. Assume p is irredubiel and $p \mid ab$, so $ab = pc$. UFT implies we can factor into irreducibles, so p divides one of the irreducibles (is associate to it) so it divides a or b.)

GCD $\boxed{\text{VIII.iii.5}}$ Prove that in a UFD, if

$$a = up_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$
$$b = vp_1^{f_1} \cdots$$

then $d = \prod p_i^{min(e_i, f_i)}$ is a GCD of a and b.

Theorem PIDs are UFDs (so EDs are UFDs).

Proof. Start factoring r. If r is irreducible, then we're done (irreducibles are prime). Otherwise, $r = r_1 r_2$. If they're irreducible, we're done. Else, keep going $r_1 = r_{11} r_{12}$ and so on. Suppose this does not terminate, so there is a sequence of non-units r_i with $r_i \mid r_{i-1}$ and $r_i \neq r_{i-1}$ for each i. Then we have a strictly ascending chain of ideals $(r) \subset (r_1) \subset \ldots \subset R$. Then $\bigcup_{i \geq 0} (r_i)$ is an ideal, and must be principal since R is a PID, suppose it is (a). a must be in (r_n) for some n, so $(r_n) \subset I$ and $I \subset (r_n)$. So the chain is stationary. Hence, the procedure must terminate.

Unique factorization is an exercise in induction. □

Example $\mathbb{Z}$ is a UFD, as is $\mathbb{F}[x]$.

8.4 Gaussian integers

We note first that if D is not a perfect square in $\mathbb{Q}$ (meaning $D \neq \frac{p^2}{q^2}$ for any $p, q \in \mathbb{Z}$, then $\mathbb{Q}(\sqrt{D} = \{a + b\sqrt{D}\}$ is a field (we can assume actually that D is a square-free integer. The quadratic integers in $\mathbb{Q}(\sqrt{D})$ are $\mathbb{Z}[\omega]$ where

$$\begin{cases} \sqrt{D} & D = 2, 3 \mod 4 \\ (1+\sqrt{D})/2 & D = 1 \mod 4 \end{cases}.$$

We seek to describe the irreducible elements in $\mathbb{Z}[i]$ and relate them to a theorem of Fermat.

Recall $N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}_{\geq 0}$ given by $N(a+b\sqrt{D}) = a^2 - b^2D$ is a multiplicative norm (when D is negative).

Exercise If $N(\alpha) = \pm 1$, then α is invertible.

Suppose α is an element with $N(\alpha)$ a prime integer. If α factors, then the norms of one of the factors must be ± 1, so it's a unit. **Thus $N(\alpha)$ is $\pm p$ (a prime integer) then α is irreducible.**

Suppose π is prime in $\mathcal{O}$. (π) the ideal generatd by π. Verify that $(\pi) \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.

Additionally, $N(\pi) \in (\pi)$, so $(\pi) \cap \mathbb{Z} = p\mathbb{Z}$ for some integer prime p. Since $p \in (\pi)$, π is a divisor of p, so to describe the primes in $\mathcal{O}$, we need only see how primes in $\mathbb{Z}$ factor in the larger ring $\mathcal{O}$.

If π divides p in $\mathcal{O}$, $p = \pi\pi'$. By norm computation, either π is an associate of p, or $N(\pi) = N(\pi') = \pm p$. So π' is also irreducible, so p factors into the product of two irreducibles.

In case we are studying $\mathbb{Z}[i]$, we already know the units, $\pm 1, \pm i$.

$\mathbb{Z}[i]$ is a Euclidean (hence PID and UF) domain. So prime and irreducible are the same. So we need only try to factor into prime elements in $\mathbb{Z}[i]$.

Suppose that $\alpha = a+bi$. $N(\alpha) = a^2+b^2$. Hence, p factors into irreducibles precisely when $p = a^2 + b^2$, and the factors are $(a \pm bi)$.

2 fits this bill. $(1 + i)$ and $(1 - i)$ are associates;

Now we think about the expression $p = a^2+b^2$. Modulo 4, a^2 and b^2 are congruent to 1 or 0. An odd prime must be congruent to 1 mod 4, so one must be congruent to 1 mod 4, and the other 0. Hence, if $p \cong 3 \mod 4$, it is not the sum of two squares, so it is irreducible in $\mathbb{Z}[i]$.

If p is a prime in $\mathbb{Z}$ with $p \cong 1 \mod 4$, we will show that p can't be irreducible.

8.5 Non-commutative rings

There are three examples of non-commutative rings worth considering before we dive into module theory: group rings, matrix rings, and diagram algebras (known as path algebras).

8.5.1 Group rings

Definition Let G be a group, and F be a field. Define by FG the *group ring*. As a F-vector space, FG has a basis given by formal symbols $\{x_g \mid g \in G\}$, one basis element for each group element. The addition is given by collecting like terms, and the multiplication is described by $x_g x_{g'} = x_{gg'}$ for $g, g' \in G$ (importantly, keep in mind that gg' is the group operation). Its identity element is x_e where e is the identity element of G. Associativity and all other important properties follow naturally from the group structure.

Exercise VIII.v.1 The group ring of $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are different. Describe each, and show there is no isomorphism between the two. Then show why neither one is an integral domain.

Exercise VIII.v.2 Prove that FG is commutative if and only if G is abelian.

8.5.2 Matrix rings

A *matrix ring* M is a subring of $\mathrm{Mat}_{n\times n}(R)$ where R is any ring. Examples include upper triangular matrices, diagonal matrices, and many others.

Exercise VIII.v.3 Prove that if I is a two-sided ideal in $\mathrm{Mat}_{n\times n}(F)$ where F is a field, then $I = \{0\}$ or $I = \mathrm{Mat}_{n\times n}(F)$. (This is like a non-commutative analogue of a field, but it is very much not a field since there are many non-invertible elements.)

Exercise VIII.v.4 Since any left ideal of $\mathrm{Mat}_{n\times n}(F)$ is also a vector space, we can compute its dimension. Compute the dimension of the left ideal generated by

$$\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$$

where I_r is the $r \times r$ identity matrix.

8.5.3 Path algebras

Definition A *quiver* is a set of vertices Q_0, and arrows Q_1. Each arrow $a \in Q_1$ has a starting vertex $t(a)$ and an ending vertex $h(a)$ known as the head and tail. A *directed path* on Q is a sequence of arrows $a_n a_{n-1} \cdots a_0$ such that $h(a_i) = t(a_{i-1})$. (The convention is that a path is written as a sequence of arrows that connect when read from right-to-left.) Finally, each vertex x has an associated *lazy* path e_x of length zero, with $h(e_x) = t(e_x) = x$.

Definition The *path algebra* of a quiver (Q_0, Q_1) is denoted FQ (where F is some pre-determined field). It is the vector space with basis $\{x_p \mid p \text{ is a directed path on Q}\}$. The multiplication of basis elements is given by

$$x_p x_q = \begin{cases} x_{pq} & \text{if } h(q) = t(p) \\ 0 & \text{otherwise} \end{cases}.$$

Example $1 \xrightarrow{a} 2$ has paths e_1, a, e_2. Hence, FQ is a three dimensional vector space. An arbitrary element takes the form

$$\Gamma = \gamma_1 x_{e_1} + \gamma_2 x_a + \gamma_3 x_{e_2}.$$

If we have another element $\Gamma' = \gamma_1' x_{e_1} + \gamma_2' x_a + \gamma_3' x_{e_2}$ then their product

$$\begin{aligned}\Gamma \cdot \Gamma' &= (\gamma_1 x_{e_1} + \gamma_2 x_a + \gamma_3 x_{e_2})(\gamma_1' x_{e_1} + \gamma_2' x_a + \gamma_3' x_{e_2}) \\ &= \gamma_1\gamma_1' x_{e_1} x_{e_1} + \gamma_1\gamma_2' x_{e_1} x_a + \gamma_1\gamma_3' x_{e_1} x_{e_2} \\ &\quad + \gamma_2\gamma_1' x_a x_{e_1} + \gamma_2\gamma_2' x_a x_a + \gamma_2\gamma_3' x_a x_{e_2} \\ &\quad + \gamma_3\gamma_1' x_{e_2} x_{e_1} + \gamma_3\gamma_2' x_{e_2} x_a + \gamma_3\gamma_3' x_{e_2} x_{e_2}\end{aligned}$$

Now note that $h(e_1) = e_1, h(a) = e_2, h(e_2) = e_2$, and $t(e_1) = e_1, t(a) = e_1, t(e_2) = e_2$. Using our "concatenation" product, this yields

$$\begin{aligned}\Gamma \cdot \Gamma' = \gamma_1\gamma_1' x_{e_1} \\ &+ (\gamma_2\gamma_1' + \gamma_3\gamma_2') x_a \\ &+ \gamma_3\gamma_3' x_{e_2}\end{aligned}$$

Conveniently, we could store this multiplication in a $|P| \times |P|$ matrix where P is the set of directed paths on Q. We simply assign to the p_i, p_j entry the path $p_i p_j$ if it exists, or 0 otherwise. Calling this matrix M, the product $\Gamma \cdot \Gamma'$ can be obtained by computing $(\Gamma')^T \cdot M \cdot \Gamma$ where in this case Γ and Γ''s coefficients have been put in a vector in the same order as the matrix.

Exercise $\boxed{\text{VIII.v.5}}$ Write the identity element of FQ as a linear combination of the basis elements.

8.6 Polynomial rings I

9 Modules

Analogies existed when I took the SAT. Here's one: Field is to vector space as ring is to module. That is, you can think of a module as being the natural extension of a vector space but that the algebraic object over which you're working is a ring and not necessarily a field.

In all that comes, we'll assume R has an identity $1 \neq 0$ unless otherwise stated.

9.1 Basic definitions

Definition Let A be an abelian group. We denote by $\mathrm{End}_{gp}(A)$ the set of group homomorphisms $\varphi : A \to A$.

Example $\boxed{\text{IX.i.1}}$ Describe $\mathrm{End}_{gp}(\mathbb{Z})$.

Remark On $\mathrm{End}_{gp}(A)$, we can impose two binary operations: $+$ and $\circ$. If φ and φ' are two endomorphisms on A, then $\varphi+\varphi'$ is an endomorphism with $(\varphi+\varphi')(a) = \varphi(a)+\varphi'(a)$. The second operation is composition of functions. You'll recognize each operation produces a new endomorphism.

Exercise $\boxed{\text{IX.i.2}}$ Verify that $\mathrm{End}_{gp}(A)$ is a ring with identity having operations $+$ and $\circ$.

Exercise $\boxed{\text{IX.i.3}}$ Describe $\mathrm{End}_{gp}(\mathbb{Z}/n\mathbb{Z})$

Definition Let R be a ring. A *left R-module* is an abelian group M together with a ring homomorphism $\varphi : R \to \mathrm{End}_{gp}(M)$ such that $\varphi(1_R) = id_M$.

Definition A *right R-module* is an abelian group M with a ring homomorphism $\varphi : R \to \mathrm{End}_{gp}(M)^{op}$ where the binary operation in $\mathrm{End}_{gp}(M)^{op}$ is $f \star g = g \circ f$.

Remark Generally we think about a module by analogy with group actions. A group action on a set is a function $G \times M \to M$ so that if you give me an element of M and a group element g, g sends m to a new element $g.m$ in M. So the elements of g permute the elements of M. A ring action is what we've defined above. Thus, it is typical to suppress the ring homomorphism φ and simply write rm.

Example Consider the ring $R = \mathbb{Z}$, and the abelian group $M = \mathbb{Z}/2\mathbb{Z}$. We'll take $\varphi : R \to \mathrm{End}_{ab}(M)$ so that $\varphi(k)$ is the endomorphism given by $\varphi(k) : [n]_2 \mapsto [kn]_2$. It would be more typical to write this as $n \cdot [s] = [ns]$

Example Let's suppose that the ring R is a field, and let V be our abelian group. So we have that for each $\lambda \in R$ and $v \in V$, we define $\lambda \cdot v$ to be another element of V. We also have to satisfy the axioms

- $(\lambda + \mu)v = \lambda v + \mu v$
- $\lambda(v + w) = \lambda v + \lambda w$
- $(\lambda\mu)(v) = \lambda(\mu v)$
- $1v = v$

but altogether, that just means that V is a vector space. So vector spaces are modules over fields.

Extended example Consider the ring $R = F[t]$ where F is a field. What does it mean to have a module V? For each polynomial $p(t) \in F[t]$ and $v \in V$, we need to describe $p(t) \cdot v$. Let's investigate four pieces:

- Since $F \subset R$ is a subring, we can also see that it acts on V ($F \subset R \xrightarrow[\varphi]{\text{End}}{}_{gp}(V)$ is still a group homomorphism), so V must also be a **vector space.**
- Now $\varphi(t)$ must be a group endomorphism of V... but additionally

$$\begin{aligned}\varphi(t)(\lambda v) &= \varphi(t)\varphi(\lambda)v \\ &= \varphi(t\lambda)v \\ &= \varphi(\lambda t)v \\ &= \varphi(\lambda)\varphi(t)(v)\end{aligned}$$

  for all $\lambda \in F$, and

$$\varphi(t)(v+w) = \varphi(t)v + \varphi(t)w$$

  by definition. Hence, $\varphi(t)$ must be a vector space endomorphism.
- $\varphi(t^n) = \varphi(t)^n = \varphi(t) \circ \varphi(t) \circ \ldots \circ \varphi(t)$, so if we know what $\varphi(t)$ is, $\varphi(t^n)$ is just the n-th power of that vector space endomorphism
- Finally, $\varphi(\sum_{i=1}^n a_i x^i) = \sum_{i=1}^n a_i \varphi(x)^i$.

Putting this all together, the data of a module over $F[t]$ is *entirely* captured by a vector space V, and a linear endomorphism T.

Extension of previous example What about $F[t]/(t^n)$, in which $t^n = 0$? In this case, T is still an endomorphism, but we insist that $T^n = 0$. So a module is a vector space together with a nilpotent endomorphism.

Definition A *submodule* of an R module M is a subgroup N of M such that $\varphi(r)N \subset N$ for all $r \in R$.

Obvious submodules The 0 subset is a submodule, as is M. Others are more interesting.

Example $\boxed{\text{IX.i.4}}$ Suppose that R is a ring. Prove that R is a left R module with action given by $\varphi(r) \cdot r' = rr'$.

$\boxed{\text{IX.i.5}}$ Describe the submodules of R in the above exercises.

$\boxed{\text{IX.i.6}}$ Let R be a ring, and consider $\prod_{n \in \mathbb{N}} R$, the countable product of the ring with itself. Prove that this is a module with action given by $\varphi(r) \cdot (x_1, x_2, \ldots,) = (rx_1, rx_2, \ldots,)$

$\boxed{\text{IX.i.7}}$ What is a $\mathbb{Z}$ module?

IX.i.8 Suppose that M is a left R module and I is an ideal in R such that $\varphi(r) \equiv 0_M$ for all $r \in I$. Prove that M is also a left R/I module in a natural way.

IX.i.9 What are the submodules of a $F[t]$ module V?

Example Suppose that G is a group, and that V is a vector space over a field F. A *group representation* on V is a group homomorphism $\rho : G \to \mathrm{GL}_F(V)$. (In finite dimensions, if we've chosen a basis for V, then this is a choice of a matrix for each group element.) IX.i.10 Prove that a group representation is given by the same data as a module over FG.

IX.i.11 Suppose that $f : R \to R'$ is a ring homomorphism. Show that R' is a module over R via $r \cdot r' := f(r)r'$.

IX.i.12 More generally, suppose that $f : R \to R'$ is a non-trivial homomorphism with $f(1_R) = 1_{R'}$, and suppose that M is an R' module. Show that M is also an R module.

IX.i.13 Prove that the intersection of submodules is a submodule, and that the sum of submodules is a submodule (sum taken in the abelian group sense).

Denote by $\mathrm{Tor}(M)$ the set of so-called *torsion* elements in M. That is,

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some } r \in R \setminus \{0\}\}.$$

IX.i.14 Prove that if R is an integral domain, $\mathrm{Tor}(M)$ is a submodule of M. (b) If R is not an integral domain, show that $\mathrm{Tor}(R)$ is not even a submodule of R.

9.2 Module homomorphisms

Homomorphisms Let R be a ring and M, N two R modules.

- A group homomorhpism $\varphi : M \to N$ is a module homomorphism if

$$\varphi(rm) = r\varphi(m)$$

  for all $r \in R$, and $m \in M$.
- The *kernel* of a ring homomorphism is the set $\{m \in M \mid \varphi(m) = 0\}$
- The *image* of a ring homomorphism is the set $\varphi(M) = \{\varphi(m) \mid m \in M\}$.
- $\mathrm{Hom}_R(M, N)$ is the set of all R-module homomorphisms from M to N, which is itself an abelian group (and more: an R-module if R is commutative)

IX.ii.1 Prove that kernels and images of ring homomorphisms are submodules. The relationship between kernels and one-to-one-ness also exists. Namely, if $y \in N$ such that there exists an element $x \in M$ with $\varphi(x) = y$, then $\varphi(x+k) = y$ for all $k \in \ker\varphi$, so one-to-oneness is equivalent to $\ker\varphi = \{0\}$.

IX.ii.2 Prove that if N is an R-submodule of M, then M/N is also an R-module in a natural way.

Exercise IX.ii.3 Prove that $\mathrm{Hom}_R(M, N)$ is an abelian group (here, I'm asking you to define the group operation yourself), and that it is an R-module if R is commutative. What goes wrong if R is not commutative?

Isomorphism theorems Fortunately, the isomorphism theorems are still valid for modules.

Definition An R-module M is called *simple* or *irreducible* if its only R-submodules are 0 and M. It is called *semi-simple* if it is (isomorphic to) a direct sum of simple submodules. Furthermore, the ring R is called simple (resp. semi-simple) if it is simple as a module over itself.

Exercise IX.ii.4 Prove that if R is commutative, then R is simple if and only if R is a field.

Exercise IX.ii.5 Find an example of a non-commutative ring R which is simple but is *not* a field (nor even a division ring).

Exercise IX.ii.6 Which of the $\mathbb{Z}$-modules of the form $\mathbb{Z}/n\mathbb{Z}$ are simple?

9.3 Generation of modules, direct sums, and free modules

We now turn to how we can understand modules from small amounts of data. One piece of inspiration should be vector spaces, where all we really need to have is a basis. Once a basis is in hand, we can easily (and uniquely) describe every element from the vector space. We can't quite say the same for modules, but we want to get close.

Module operations Let M be an R-module, $N_1, \dots, N_k$ submodules.

Sum The set of finite sums of elements from N_i is a submodule

Generation Submodule generated by a set of elements in a natural way.

Finite generation A submodule is finitely generated if there is some finite set that generates it

Cyclic A submodule is cyclic if it is generated by a single element

Proposition Suppose that M is a cyclic module over R, and that M is generated by m. I.e., $M = \{rm \mid r \in R\}$. Then $M \cong R/\operatorname{Ann}_R(m)$. (Here $\operatorname{Ann}_R(m) = \{r \in R \mid rm = 0\}$).

Exercise $\boxed{\text{IX.iii.1}}$ Prove the above statement.

Exercise $\boxed{\text{IX.iii.2}}$ Suppose that M is an R-module, and that I is an ideal such that $I \subset \operatorname{Ann}_R(M)$.[3] Prove that M is an R/I-module in a natural way.

Exercise $\boxed{\text{IX.iii.3}}$ Suppose that M is a cyclic R-module, and that $f : M \to N$ is a *surjective* module homomorphism. Prove that N is also cyclic.

Question: What is a PID in terms of modules?

Scary remark Submodules of finitely generated modules needen't be finitely generated (so the analogy from vector spaces breaks down). For example, $F[x_1, x_2, x_3, ...]$ the polynomial ring in infinitely many variables is generated by 1 over itself, but the module generated by $\{x_1, x_2, x_3, \dots\}$ is not.

Proposition $\boxed{\text{IX.iii.4}}$ Suppose that M is a finitely-generated module over R, generated by elements $\{m_1, \dots, m_n\}$. Then M is a quotient of $R^{\oplus n}$.

Definition For this reason, the notion of a *free* module arises. A module M over R is *free* if it has a basis, meaning a generating set $\{m_1, m_2, \dots\}$ that is R-linearly independent. (I.e., if $\sum_{finite} r_i m_i = 0$ then all $r_i = 0$.

Free modules In particular, the modules $R^{\oplus n}$ and $\coprod\limits_{\alpha \in A}$ are free.

Proposition If M is a free module as generated by $\{m_1, m_2, \dots\}$, and $x \in M$, then there exists a unique finite subset $I \subset \mathbb{Z}$ and coefficients $r_i \in R$ for $i \in I$ such that

$$x = \sum_{i \in I} r_i m_i.$$

Construction Given any set A, we can construct a free module of *rank* $|A|$ by simply taking $F(A) = \coprod_{\alpha \in A} R$. There is an obvious set map $\iota : A \to F(A)$ taking the elementary coordinate vector. The universal property satisfied is:

$$\begin{tikzcd}
A \arrow[r, "\iota"] \arrow[dr, "g"'] & F(A) \arrow[d, dotted, "\tilde{g}"] \\
& M
\end{tikzcd}$$

$\boxed{\text{IX.iii.5}}$ Decode what this means!

Decomposition We're often interested in decomposing modules into their smallest pieces... whatever that means. Here we define that.

[3] $\operatorname{Ann}_R(M) = \{r \in R \mid rm = 0 \forall m \in M\}$.

Definition If M and N are two R-modules, we define $M \oplus N$ to be the *external direct sum*. That is, the set $\{(m, n) \mid m \in M, n \in N\}$ with addition and R-action defined componentwise.

Exercise IX.iii.6 Show that if M and N are both finitely generated, then so is $M \oplus N$.

Internal decomposition We next want to ask whether a module M has submodules N and L so that M is isomorphic to $N \oplus L$. Naturally, if $(n, l) \in N \oplus L$, we could probably define an element $\varphi(n, l) \in M$ via $n + l$. If we want this to be an isomorphism, φ should be one-to-one and onto.

Definition IX.iii.7 Write the appropriate definition of an *internal direct sum*. That is, if M is an R-module with submodules N, L, then $N \oplus L \cong M$ if...

Exercise IX.iii.8 Consider the ring $R = \mathbb{Z}$, and $\mathbb{Z}$ as a module over itself. Prove that $\mathbb{Z}$ is *not* a direct sum of any of its submodules.

Definition An R-module M is called *decomposable* if $M \cong N \oplus L$ for some nontrivial R modules N, L. It is called *indecomposable* otherwise. (The definition can be written in a way similar to that of simple modules: M is *indecomposable* if $M \cong N \oplus L$ implies that $N = 0$ or $N = M$.)

Exercise IX.iii.9 Which of the $\mathbb{Z}$-modules of the form $\mathbb{Z}/n\mathbb{Z}$ are indecomposable?

Direct sum decomposition So *when* is it the case that a module decomposes? We have something similar to the story for rings themselves.

Proposition Let $N_1, \ldots, N_k$ be submodules of the R-module M. The following are equivalent:

- The map $\pi : N_1 \oplus \ldots \oplus N_k \to N_1 + N_2 + \ldots + N_k$ defined by
$$\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \ldots + a_k$$
is an isomorphism of R-modules.
- $N_j \cap (N_1 + N_2 + \ldots + \hat{N_j} + \ldots + N_k) = 0$ for all j.
- Every $x \in N_1 + \ldots + N_k$ can be written uniquely in the form $a_1 + a_2 + \ldots + a_k$ with $a_i \in N_i$.

Example Consider the $\mathbb{C}[t]$-module corresponding to the pair $M = \left(\mathbb{C}^2, \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}\right)$. Let N_i be the subset $\operatorname{span}(e_i)$ (check that it's a submodule). Note that indeed $N_1 \cap N_2 = 0$. So $M \cong N_1 \oplus N_2$. Now notice that N_1 is isomorphic to $(\mathbb{C}^1, [2])$ and N_2 is isomorphic to $(\mathbb{C}^1, [3])$. Note that these are both indecomposable $\mathbb{C}[t]$ modules.

Example The module $\mathbb{Z}/6\mathbb{Z}$ has $\mathbb{Z}$ submodules $N_1 = \{0, 2, 4\}$ and $N_2 = \{0, 3\}$. Note that $N_1 \cap N_2 = \{0\}$, so $N_1 \oplus N_2 \cong N_1 + N_2$, and $N_1 + N_2 = \mathbb{Z}/6\mathbb{Z}$, so $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Note that these are both indecomposable $\mathbb{Z}$ modules, so we cannot further "factor" this.

Exercise IX.iii.10 Suppose that M and N can be generated by m and n-element subsets, respectively. Prove that $M \oplus N$ is can be generated by $m+n$ elements.

Exercise IX.iii.11 Suppose that M is a finitely generated R-module. Prove that M/L is finitely generated.

Exercise IX.iii.12 Suppose that L and M/L are finitely generated. Then M is finitely generated. This exercise forms a jumping-off point for us, in a way. We will often try to under stand modules by understanding their sub- and quotient modules.

Exercise IX.iii.13 Suppose that M is an R-module, $M \neq 0$. Prove that M is irreducible if and only if M is cyclic and can be generated by any of its non-zero elements.

Exercise IX.iii.14 Suppose that R is commutative. Show that M is irreducible if and only if $M \cong R/I$.

9.4 Tensor products of modules

Let's work on a few analogies between vector spaces and modules:

Vector space over F	Modules over R
linear transformation	module homomorphism
vector subspace	submodule
quotient space	quotient module
dimension	rank (of a free module)
direct sums of vector spaces	direct sums of modules
dimension of direct sum is sum of dimensions	rank of the direct sum is sum of the ranks
tensor product of vector spaces	tensor products of modules
dimension of tensor product is product of dimensions	rank of tensor product is tensor product of ranks

Here's a "categorification" way to think about tensor products:

- Zero dimensional vector spaces exist, it's just the singleton 0 vector.
- There is a vector space of dimension equal to each positive integer n, F^n.
- Given a vector space V and a subspace W, we can construct a vector space of dimension $\dim V - \dim W$.
- Given two vector spaces V and W, we can construct a vector space of dimension $\dim V + \dim W$

- What about a vector space of dimension $\dim V \cdot \dim W$?

Idea Suppose that V and W are vector spaces over F with bases $\{e_i\}$ and $\{f_j\}$. Build a new space $V \otimes_F W$ as the free vector space with basis $\{e_i \otimes f_j \mid i \in I, j \in J\}$. Then, for any $v \in V, w \in W$, define $v \otimes w$ to be the linear combination $\sum_{i,j} c_{ij} e_i \otimes f_j$ where $c_{ij} = [v]_i \cdot [w]_j$ (the entries of the column vector of v and w written in their corresponding bases).

Example $\mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{R}^3$ is 6D. We can show that the expression of an element is *independent of basis chosen.* So $v \otimes w$ means something that has nothing to do with *how* v and w are represented[4]

Notes We *should* be able to do the same thing for a module... but it's not clear how unless we have a basis...

Notes It does seem that we want some conditions to hold: linearity in the *first* component and *second* component separately.

Definition Let M and N be R modules. A *bilinear map* $B : M \times N \to P$ is a function which is linear in each component. Note that $B(-, n)$ and $B(m, -)$ are linear (homomorphisms) for each $m \in M$, $n \in N$.

Examples

1. $B(v, w) = v \cdot w$ where $v, w \in \mathbb{R}^n$ is bilinear;
2. Matrix multiplication $B(X, Y) = XY$ is bilinear from $\mathrm{Mat}_{m\times n}(R) \times \mathrm{Mat}_{n\times l}(R)$ whenever R is commutative.
3. The cross-product is bilinear
4. The determinant is multilinear: $\det : \underbrace{F^n \times F^n \times \ldots \times F^n}_{n} \to F$
5. the module action $B : R \times M \to M$ is bilinear
6. Multiplication $R \times R \to R$ is bilinear
7. If $M^\vee = \mathrm{Hom}_R(M, R)$, then the *dual pairing* $(\varphi, m) \mapsto \varphi(m)$ is bilinear
8. If $\varphi \in M^\vee, \psi \in N^\vee$, then the function $M \times N \to R$ given by $\varphi(m)\psi(n)$ is bilinear
9. If $M \times N \to P$ is bilinear, and $P \to Q$ is linear, then the composition is bilinear.
10. *We would like the function* $M \times N \to M \otimes_R N$ with $(m, n) \mapsto m \otimes n$ to be bilinear.

Note Kernel is not a submodule (don't even know what the module structure on $M \times N$ is (but it's definitely not the normal one) and the image is not necessarily a submodule.

[4] Contrast with the dot product of two vectors, which is highly basis dependent.

Important example Consider the map $B : R^n \times R^n \to M_n(R)$ known as the *outer product*. It gives $B(v, w) = vw^T$ where v and w are column vectors. Note that $B(e_1, e_1) + B(e_2, e_2) = I_2$ but the identity matrix is not equal to $B(v, w)$ for any vectors v, w (since the outer product has rank 1, as all columns are multiples of v).

Construction Now that we have our wishlist: that (1) $M \otimes_R N$ should be a module, (2) it should admit a bilinear map from $M \times N$ to itself and (3) should be "as small as possible". Hence, we get the universal property

$$\begin{tikzcd}
M \times N \arrow[r, "\otimes"] \arrow[dr, "B\text{-bilinear}"'] & M \otimes_R N \arrow[d, dotted, "\exists!"] \\
 & P
\end{tikzcd}$$

Proposition The tensor product, if it exists, is unique because of the universal property.

Proposition The tensor product exists.

Proof. Let $F_R(M \times N)$ be the MASSIVE free module with basis $e_{m,n}$ for every pair $(m, n) \in M \times N$. This is not just the set of ordered pairs: it is the set with a basis element for each ordered pair. It has *rank* equal to $|M \times N|$. [Example:] If $M = \mathbb{Z}/2\mathbb{Z}$ and $N = \mathbb{Z}/3\mathbb{Z}$, then the corresponding $\mathbb{Z}$ module $F(M \times N)$ has rank 6. Its elements look like

$$a_{00}([0], [0]) + a_{10}(1, 0) + a_{01}(0, 1) + a_{11}(1, 1) + a_{02}(0, 2) + a_{12}(1, 2).$$

We take I to be the submodule of $F(M \times N)$ spanned by the elements of the form:

$$\begin{aligned}
e_{m+m',n} - e_{m,n} - e_{m',n} \\
e_{m,n+n'} - e_{m,n} - e_{m,n'} \\
e_{\lambda m,n} - \lambda e_{m,n} \\
e_{m,\lambda n} - \lambda e_{m,n}.
\end{aligned}$$

Then $M \otimes_R N = F(M \times N)/I$. □

Remark It's instructive to consider the difference between $M \oplus N$ and $M \otimes N$. For example, consider $R[x] \oplus R[y]$. This is the set of ordered pairs $(f(x), g(y))$ where f is a polynomial in x, and g is a polynomial in y. We further consider them as sums, so that $(f(x), g(y)) = (f(x), 0) + (0, g(y))$. However, $R[x] \otimes R[y]$ has elements which are *linear combinations* of pairs of polynomials. For example,

$$\sum_{i,j} c_{ij} x^i y^j \in R[x] \otimes R[y],$$

so $R[x] \otimes R[y]$ can be identified with $R[x, y]$.

Example $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = 0$. Indeed, $(r \otimes k) = (r/n)n \otimes [k] = r/n \otimes [nk] = r/n \otimes 0 = 0$.

Example What does it mean if $m \otimes n = 0$? It means that *every* bilinear map from $M \times N$ to any module P has $B(m, n) = 0$.

Example What does it mean if $M \otimes N = 0$? It means that every bilinear map from $M \times N$ to any other module is the zero map.

Example $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\gcd(n, m)\mathbb{Z}$

Proof. Suppose we have an element

$$\sum_i a_i \otimes b_i.$$

Then by using linearity, this is $(\sum_i a_i b_i)(1 \otimes 1)$, so $(1 \otimes 1)$ spans the tensor product. Note that $n(1 \otimes 1) = n \otimes 1 = 0$ and similarly with m, so the order or $(1 \otimes 1)$ divides m and n. Hence, the cardinality of the tensor product is bounded by $\gcd(m, n)$. In the other direction, let's actually create a bilinear map. $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ given by $(a, b) \mapsto [ab]_d$. It can be show that this is bilinear, so there is a unique map from the tensor product to $\mathbb{Z}/d\mathbb{Z}$. Further, $f(a, 1) = [a \cdot 1]_d$, so f is onto. □

Example $R/I \otimes R/J \cong R/(I + J)$ (use the map $(x, y) \mapsto xy$.

Example $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} A \cong A/n\mathbb{Z}$ for any abelian group A.

Example $\mathrm{Hom}_R(M, N) \cong M^{\vee} \otimes N$ when M is finitely-generated and free. (At least, think about the generalization).

Example $R \otimes_R M \cong M$

Example $F \otimes_R F'$ is free when F and F' are (and the basis works nicely too).

Example $F \otimes_R M$ has elements with unique representation as $\sum_{i \in I} m_i \otimes e_i$ where all but finitely many of the summands are zero.

Example (Excellent example to know) Extension of scalars: Suppose that $S \subset R$ is a subring. Hence, every module over R is a module over S. But, we can go the other way around. R is an S-module. Assume M is also an S module. Then $R \otimes_S M$ is now an R-module (since R can act on the first component).

9.5 Exact sequences and special modules

Buoyed by a few of the theorems from the section on modules (where understanding a submodule and quotient module can let us understand the module itself.

Sequence of morphisms A *sequence of morphisms*

$$\to X_1 \xrightarrow{f_1} X_2 \xrightarrow{f_2} X_3 \xrightarrow{f_3} X_4 \to \dots$$

is *exact at* X_n if $\ker f_n = \operatorname{image} f_{n-1}$.

Example As an example, $0 \to X \xrightarrow{f} Y$ is exact at X if and only if $\ker f = \operatorname{image} 0 = 0$, so if and only if f is one-to-one.

Example Similarly, $Y \xrightarrow{g} Z \xrightarrow{h} 0$ is exact at Z if and only if $Z = \ker h = \operatorname{image} g$, so if and only if g is onto.

Example The sequence

$$\mathbb{Z}/4\mathbb{Z} \xrightarrow{3 \cdot n} \mathbb{Z}/6\mathbb{Z} \xrightarrow{\text{reduce mod 3}} \mathbb{Z}/3\mathbb{Z}$$

is exact at $\mathbb{Z}/6\mathbb{Z}$. The kernel of reduction mod 3 is $\{0, 3\}$, which is the image of the first morphism.

Definition A sequence

$$0 \to X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \to 0$$

is called a *short exact sequence* of it is exact at X, Y, and Z.

Example If we work with arbitrary groups, the sequence

$$0 \to \mathbb{Z}/3\mathbb{Z} \xrightarrow{\overline{1} \mapsto (123)} S_3 \xrightarrow{sgn} \mathbb{Z}/2\mathbb{Z} \to 0.$$

Example

$$0 \to X \to X \oplus Z \to Z \to 0$$

Example Here's one that may look interesting:

$$0 \to \mathbb{Z} \xrightarrow{n \cdot} \mathbb{Z} \xrightarrow{[-]_n} \mathbb{Z}/n\mathbb{Z} \to 0$$

It seems like the middle should be "bigger" than the outer pieces, but that's not true.

Example Also, end terms don't uniquely determine the inner term:

$$0 \to \langle r^2 \rangle \to D_4 \to D_4/\langle r^2 \rangle \to 0$$
$$0 \to \{\pm 1\} \to Q_8 \to Q_8/\{\pm 1\} \to 0$$

Example There's a canonical short exact sequence associated with any homomorphism $f : M \to N$, namely:

$$0 \to \ker f \to N \to \text{image}(f) \to 0$$

Example Let M be a finitely-generated R-module, generated by $\{m_1, m_2, \ldots, m_t\}$. Let R^t be the free R-module of rank t. Then we have the homomorphism $\varphi : R^t \to M$ with $\varphi(e_i) = m_i$, which is onto. The *kernel* is referred to as the module of relations:

$$0 \to K \to R^t \to M \to 0.$$

Specific example Consider the ring $R = \mathbb{C}[x, y]$, and the ideal $I = (x, y)$. There is an onto map from R^2 to I sending e_1 to x and e_2 to y. Notice that

$$\begin{aligned} \ker \pi &= \{fe_1 + ge_2 \mid \pi(fe_1 + ge_2) = 0\} \\ &= \{fe_1 + ge_2 \mid fx + gy = 0\} \\ &= \{fe_1 + ge_2 \mid fx = -gy\} \\ &= \{\chi(y, -x) \mid \chi \in R\}. \end{aligned}$$

Then we have the exact sequence:

$$0 \to R \xrightarrow{e_1 \mapsto (y,-x)} R^2 \xrightarrow{\substack{e_1 \mapsto x \\ e_2 \mapsto y}} I \to 0.$$

Example $R = \mathbb{C}[t]$, $M = \mathbb{C}$ the module with $t.a = 0$, and N the module $\mathbb{C}^2$ with $t.e_1 = 0$ and $t.e_2 = e_1$. Then

$$0 \to M \xrightarrow{\begin{bmatrix} 0 \\ 1 \end{bmatrix}} N \xrightarrow{\begin{bmatrix} 1 & 0 \end{bmatrix}} M \to 0$$

Example A type A_2 example. In particular,

$$0 \to (0, \mathbb{C}, 0) \to (\mathbb{C}, \mathbb{C}, 1) \to (\mathbb{C}, 0, 0) \to 0$$

Splitting A short exact sequence is called *split* if $Y \cong X \oplus Z$.

Criterion for splitting: sections and retractions Suppose that

$$\eta = 0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0$$

is a short exact sequence, and that there exists a homomorphism $g' : Z \to Y$ such that $g \circ g' = id_Z$. Then η is a split exact sequence.

Proof. Given the above conditions, consider the submodules $x = \text{image}(f)$ and $z = \text{image}(g')$ in Y. Since f and g' are injective, $X \cong x$ and $z \cong Z$. Furthermore, $x \cap z = \{y \in Y \mid y = f(x) = g'(z)\}$, but if this is the case, then

$$g(f(x)) = g(g'(z))$$
$$0 = z$$

so $z = 0$, hence, $x = 0$ and $y = 0$. Thus, $x \cap z = 0$. Furthermore, if $y \in Y$, we claim $y = x + z$ for some $x \in f(X)$, and $z \in g'(Z)$. Indeed, let $z = g' \circ g(y) \in Z$. Then $g(z - y) = gg'g(z) - g(y) = g(y) - g(y) = 0$, so $z - y = x$ for some $x \in F(X)$. Hence, $y = z - x$. Thus, $X \oplus Z \cong f(X) + g'(Z) \cong Y$. □

Retractions Dually, a retraction is a homomorphism $f' : Y \to X$ such that $f' \circ f = id_X$. The dual proposition is that if there exists a retraction, then η splits.

Example If

$$\eta = 0 \to X \xrightarrow{f} Y \xrightarrow{g} Z \to 0$$

is a short exact sequence with Z free, then η splits.

Proof. By the discussion on sections, we can simply show that there exists a section. Suppose that Z is free with basis $\{z_\alpha \mid \alpha \in A\}$. Then, since g is a surjection, there exist elements $y_\alpha \in Y$ such that $g(y_\alpha) = z_\alpha$ for each α. Define the map g' with $g'(z_\alpha) = y_\alpha$. From the universal property of free modules, this extends to a homomorphism, and clearly $gg'(z_\alpha) = g(y_\alpha) = z_\alpha$ for each α. □

So what this says is that any short exact sequence with free right end splits. Are there other modules with this property?

Definition An R-module P is called *projective* if every short exact sequence

$$0 \to X \to Y \to P \to 0$$

splits. (Equivalently, every onto map $Y \to P$ has a section.)

Example Free modules are projective (see corollary above)

Example Consider the ring $R = \mathbb{C}[t]/(t^n)$. Then the only indecomposable (finite-dimensional) non-zero projective R-module is itself.

Example Consider the path algebra of $1 \to 2$. Its indecomposable projective modules are $F \xrightarrow{[1]} F$ and $0 \to F$.

Convenience It's convenient to think about the Hom$(-, -)$ functor.

Proposition TFAE for an R-module P

1. P is projective

2. There exists a module Q such that $P \oplus Q$ is free.
3. If $\pi : M \to N$ is surjective and $\varphi : P \to N$ is a homomorphism, then there exists a homomorphism $\Phi : P \to M$ such that $\varphi = \pi \circ \Phi$
4. If $\pi : M \to N$ is a surjection, the natural map $\operatorname{Hom}(P, M) \to \operatorname{Hom}(P, N)$ is surjective.

Definition $\operatorname{Hom}_R(P, -)$ is a *functor* from $\text{mod}\ (R)$ to $\mathcal{A}\lfloor$. That is, an assignment of an abelian group $\operatorname{Hom}_R(P, M)$ to each module M in $\text{mod}\ (R)$ and a morphism $\operatorname{Hom}_R(P, f) : \operatorname{Hom}_R(P, M) \to \operatorname{Hom}_R(P, N)$ for each morphism $f : M \to N$. (This is called *covariant*.)

Proposition $\operatorname{Hom}_R(P, -)$ is *left-exact*, meaning that if $f : M \to N$ is injective, so is $\operatorname{Hom}_R(P, f)$. It is not necessarily right-exact. Indeed, consider $M = \mathbb{Z}/4\mathbb{Z}$, $N = \mathbb{Z}/2\mathbb{Z}$ and the projection, and $P = \mathbb{Z}/2\mathbb{Z}$. Then $\operatorname{Hom}_R(P, M) = \{[2x]_4, [0]_0\}$ and $\operatorname{Hom}_R(P, N) = \{[x]_2, [0]_2\}$. However, $f = [x]_2$, so any composition of it with something in $\operatorname{Hom}_R(P, M)$ is zero.

Proof. Suppose that $f : M \to N$ is injective. We have the map $\operatorname{Hom}_R(P, M) \xrightarrow{f \circ -} \operatorname{Hom}_R(P, N)$ defined by composition, so suppose $f \circ \varphi_1 = f \circ \varphi_2$ for some morphisms $\varphi_i \in \operatorname{Hom}_R(P, M)$. Then $f(\varphi_1(x)) = f(\varphi_2(x))$ for all $x \in P$. But f is injective, so $\varphi_1(x) = \varphi_2(x)$ for all $x \in P$. Hence, $\varphi_1 = \varphi_2$. □

10 Algebraic geometry

The origins of algebraic geometry lie in the solutions to systems of polynomial equations. You've already seen a subset of this topic in linear algebra, which originates as the study of the solutions to systems of linear equations. The "geometric" part there was that solutions to systems of linear equations were (affine) vector spaces, which could be obtained by finding one particular solution and the family of homogeneous solutions. We then showed that every solution is a sum of your particular solution and a homogeneous solution. We further saw what happened if we wanted to "intersect" these spaces: you get another (affine) vector space, and the dimension of the intersection can be understood as bounded by certain dimensions.

Now suppose that we have a system of polynomial equations:

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &= 1 \\ ab + cd &= 0 \\ ac + bd &= 0 \\ ad + bc &= 0. \end{aligned}$$

(This actually came up on a homework problem.) You'll quickly find there are subcases based on whether one element is 0 or not and how they relate to the others. It is, generally, a pain.

Reframing Let $R = \mathbb{Q}[x_1, \ldots, x_n]$ be the polynomial ring in n variables. Let $F = \{f_1, \ldots, f_m\} \subset R$ be a collection of polynomials. We seek to compute (or at least understand in some way)

$$V(F) := \{(a_1, \ldots, a_n) \mid f_i(a_1, \ldots, a_n) = 0 \forall i\}$$

called the *vanishing set of* F.

Example Let $F = \{x^2 + y^2 + z^2 - 1, x + y + z\}$, then $V(F)$ is the cross-section of the sphere of radius 1 with the plane $x + y + z = 0$. What does this look like?

Note Suppose that $\underline{a}$ is a solution to each f_i. Then it is also a solution to

$$\sum c_i f_i$$

for all choices of functions $c_i \in R$. In particular, this shows that $V(F) = V(RF)$ where RF is the ideal generated by F.

Definition A set $Z \in \mathbb{A}^n$ is called *algebraic* if $Z = V(J)$ for some ideal $J \subset R$.

Other direction Now given a set of points $Z \subset \mathbb{A}^n$, we could ask "which functions vanish at all of them?" This is called the *ideal* of Z, denoted $I(Z)$.

Example $I(\{(1, 1)\}) = (x - 1, y - 1)$

Bouncing What happens when we bounce back-and-forth? Well, $V(I(Z))$ is not necessarily equal to Z, but it certainly contains Z. It is exactly Z precisely when Z is an algebraic set. Furthermore, $I(V(J))$ is not necessarily J, but it contains J. The reason that $I(V(J)) \neq J$ is given by the following example.

Example $J = (x^2 - 2xy + y^2)$. $V(J) = \{(a, b) \mid a^2 - 2ab + b^2 = 0\}$ but this is the same as saying $(a - b)^2 = 0$, so $a = b$. Thus, $V(J) = \{(a, a) \mid a \in F\}$. It's not hard to show that $I(V(J)) = (x - y)$. You see, $f = (x - y)^2$, so $f(a, b) = 0$ if and only if $(x - y) = 0$.

Definition An ideal $J \subset R$ is called *radical* if $f^n \in I$ for some $n > 0$ implies $f \in J$. So J is closed under taking n-th roots for any n.

Theorem: Hilbert Nullstellensatz $I(V(J)) = \sqrt{J}$, where $\sqrt{J}$ is the set $\{r \in R \mid r^n \in J \exists n > 0\}$.

What? So really, the study of algebraic sets is equivalent to the study of radical ideals. Sets X such that $X = V(J)$ for J a radical ideal are called *algebraic varieties.*

Algebra/Geometry Here's a question: when can you break your set into pieces?

Definition Z is called *irreducible* if $Z = Z_1 \cup Z_2$ implies $Z = Z_1$ or $Z = Z_2$. (Hence, Z cannot be written as a union of strictly smaller varieties.)

Theorem The variety V is irreducible if and only if $I(V)$ is prime.

Proof. If V is irreducible, let $I(V)$ be its ideal. If $fg \in I$ but $f, g \notin I$, then define $V_1 = V(I + \langle f \rangle) \subsetneq V(I)$ and $V_2 = V(I + \langle g \rangle) \subsetneq V(I)$. But $x \in V$ is either in V_1 or V_2, so $V = V_1 \cup V_2$. On the other hand, if I is prime, and $V(I)$ is reducible, then $V = V_1 \cup V_2$ with $V_i \subsetneq V$. So we can find $f \in I(V_1) \setminus I(V_2)$ and $g \in I(V_2) \setminus I(V_1)$. Note $fg \in I$ since fg kills anything in V_1 or V_2; but I is prime. □

Dimension So now let's think about dimension. Things are different in algebraic geometry than Euclidean. In particular, suppose that we have irreducible varieties such that $Z_1 \supsetneq Z_2 \supsetneq \ldots$. This means that we have a sequence of prime ideals $I(Z_1) \subsetneq I(Z_2) \subsetneq \ldots$ all in R. However, the famous "Hilbert Basis Theorem" says that $\mathbb{C}[x_1, \ldots, x_n]$ is a so-called *Noetherian ring*, which means that the ideals stabilize. Hence, there are no infinitely descending chains of irreducible subvarieties of $\mathbb{A}^n$ (compare to the scenario with balls of radius r for any r). Furthermore, the analytic dimension (Euclidean) of Z_i is decreasing (again, compare to the Euclidean case).

Example In $\mathbb{C}[x, y]$, we have the unit circle $C = \{(a, b) \mid a^2 + b^2 - 1 = 0\}$. I.e., $C = V(x^2 + y^2 - 1)$. The ideal generated by $x^2 + y^2 - 1$ is prime. If we intersect this set with $x = 0$ and take one of the two pieces, we have $V(x, y - 1)$, which is a point, and $(x, y - 1)$ is a maximal ideal, so there are no larger ideals other than R. So we have: *circ* $\supset$ *point* $\supset \emptyset$ given by $(x^2 + y^2 - 1) \subset (x, y - 1) \subset R$.

11 Multilinear algebra

Let's think about the way the determinant works: it is a function on the columns (let's say) of a matrix, which returns an element of the ground field. If $\dim V = n$ then

$$\det : \underbrace{V \times V \times \ldots \times V}_{n} \to F$$

is the map defined by

$$\det(v_1, \ldots, v_n) = \det \begin{bmatrix} | & | & \ldots & | \\ v_1 & v_2 & \ldots & v_2 \\ | & | & \ldots & | \end{bmatrix}.$$

We've already seen that it's multilinear, so really it is a homomorphism from $V^{\otimes n}$ to F. (If we want to be really fancy, $\mathrm{Hom}_F(V^{\otimes n}, F) \cong (V^{\otimes n})^* \otimes_F F \cong (V^*)^{\otimes n}$, so the determinant is nothing but an element of this big tensor product.

But more than that, we have an extra relation held by the determinant. Namely $\det(v_{(1,2,\ldots,v_n)}) = (-1)^{\operatorname{sign}\sigma} \det(v_{\sigma(1,2,\ldots,n)})$. It is a so-called *alternating* function (this is equivalent to the fact that if two of the vectors are equal, the element is equal. We have another relationship: alternating, let's make a universal property.

Definition Let V be a free F-module, and k an integer. $\bigwedge^k V$, the k-th exterior power of V, is the module with the following properties:

- There is a multilinear, alternating map $\wedge : \underbrace{V \times \ldots \times V}_{k} \to \bigwedge^k V$ and
- For any multilinear, alternating function $M : \underbrace{V \times \ldots \times V}_{k} \to P$, there is a unique homomorphism $\Psi : \bigwedge^k V \to P$ such that $\Psi \circ \wedge = M$.

Remark The construction of $\bigwedge^k V$ is easy once you have the tensor product: simply take $V^{\otimes k}/I$ where I is the ideal generated by all sums of the form $v_1 \otimes \ldots \otimes v_k + v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(k)}$. The equivalence class of $v_1 \otimes \ldots \otimes v_k$ in $\bigwedge^k V$ is denoted $v_1 \wedge \ldots \wedge v_k$.

Example Consider the element $(5e_1+2e_2)\wedge(e_1+3e_2)$ in $\bigwedge^2(F^2)$. Using the relations, we have

$$\begin{aligned}(5e_1 + 2e_2) \wedge (e_1 + 3e_2) &= 5 \cdot 1e_1 \wedge e_1 + 2 \cdot 1e_2 \wedge e_1 \\ &\quad 5 \cdot 3e_1 \wedge e_2 + 2 \cdot 3e_2 \wedge e_2 \\ &= (5 \cdot 3 - 2 \cdot 1)e_1 \wedge e_2.\end{aligned}$$

Look familiar? Indeed, we can consider the determinant function $\det : F^2 \times F^2 \to F$. Because of the universal property, there is a unique function $\Psi : \bigwedge^2(F^2) \to F$ with $\Psi(v \wedge w) = \det(v, w)$. It's clearly the function which takes $v \wedge w$ to $\det(v, w)$.

Example Consider the function $M : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ given by the following: $M(v, w) = \langle v_2w_3 - v_3w_2, -(v_1w_3 - v_3w_1), v_1w_2 - v_2w_1\rangle$. (Note that M is the usual cross-product from multivariable calculus.) This gives us a linear function $\Psi : \bigwedge^2(\mathbb{R}^3) \to \mathbb{R}^3$ with $\Psi(v \wedge w) = v \times w$. This is used heavily in differential geometry.

Utility