# Tilings

D. Zack Garza

February 6, 2020

## Contents

**1 Wednesday January 8** **1**

**2 Monday January 13** **3**
2.1 Logistics . . . 3
2.2 Rings of Functions . . . 4
2.3 Rings . . . 5

**3 Wednesday January 15th** **5**
3.1 Ideals and Quotients . . . 7

**4 Friday January 17th** **7**

**5 Wednesday January 22nd** **8**
5.1 Pushing / Pulling . . . 10

**6 Friday January 24th** **11**
6.1 Ideals and Products . . . 11
6.2 Modules . . . 14

**7 Monday January 27th** **14**
7.1 Localization . . . 14
7.2 Modules . . . 15

**8 Friday January 31st** **16**
8.1 Tensor and Hom . . . 16
8.2 Free Torsion Modules . . . 17

# 1 Wednesday January 8

Course text: `http://math.uga.edu/~pete/integral2015.pdf`

Summary: The study of commutative rings, ideals, and modules over them.

The chapters we'll cover:

- 1 (Intro),

- 2 (Modules, partial),
- 3 (Ideals, CRT),
- 7 (Localization),
- 8 (Noetherian Rings),
- 11 (Nullstellensatz),
- 12 (Hilbert-Jacobson rings),
- 13 (Spectrum),
- 14 (Integral extensions),
- 17 (Valuation rings),
- 18 (Normalization),
- 19 (Picard groups),
- 20 (Dedekind domains),
- 22 (1-dim Noetherian domains)

In number theory, arises in the study of $\mathbb{Z}_k$, the ring of integers over a number field $k$, along with *localizations* and *orders* (both preserve the fraction field?).

In algebraic geometry, consider $R = k[t_1, \cdots, t_n]/I$ where $k$ is a field and $I$ is an ideal.

Some preliminary results:

1. In $\mathbb{Z}_k$, ideals factor uniquely into primes (i.e. it is a Dedekind domain).
2. $\mathbb{Z}_k$ has an integral basis (i.e. as a $\mathbb{Z}$-modules, $\mathbb{Z}_k \cong \mathbb{Z}^{[k:\mathbb{Q}]}$).
3. The Nullstellansatz: there is a bijective correspondence

$$\left\{\text{Irreducible Zariski closed subsets of } \mathbb{C}^n\right\} \iff \left\{\text{Prime ideals in } \mathbb{C}[t_1,\cdots,t_n]\right\}.$$

4. Noether normalization (a structure theorem for rings of the form $R$ above).

All of these results concern particularly "nice" rings, e.g. $\mathbb{Z}_k, \mathbb{C}[t_1, \cdots, t_n]$. These rings are

- Domains
- Noetherian
- Finitely generated over other rings
- Finite Krull dimension (supremum of length of chains of prime ideals)
  - In particular, $\dim \mathbb{Z}_k = 1$ since nonzero prime ideals are maximal in a Dedekind domain
- Regular (nonsingularity condition, can be interpreted in scheme-theoretic language)

> Note: schemes will have "local charts" given by commutative rings, analogous to building a manifold from Euclidean $n$-space. General philosophy (Grothendieck): Every commutative ring is the ring of functions on some space, so we should study the category of commutative rings as a whole (i.e. let the rings be arbitrary). This does not hold for non-commutative rings! I.e. we can't necessarily associate a geometric space to every non-commutative ring. A common interesting example: $k[G]$, the group ring of an arbitrary group. Good references: Lam, 'Lectures on Modules and Rings'.

*Example:* Let $X$ be a topological space and $C(X)$ be the continuous functions $f : X \to \mathbb{R}$. This is a ring under pointwise addition/multiplication. (This generally holds for the hom set into any commutative ring.)

*Example:* Take $X = [0, 1]$ and $C(X)$ as a ring.

**Exercise:**

1. Show that $C(X)$ is a not a domain.

> Hint: find two nonzero functions whose product is identically zero, e.g. bump functions. Note that they are not analytic/holomorphic.

2. Show that it is not Noetherian (i.e. there is an ideal that is *not* finitely generated).
3. Fix a point $x \in [0,1]$ and show that the ideal $\mathfrak{m}_x = \left\{ f \;\middle|\; f(x) = 0 \right\}$ is maximal.
4. Are all maximal ideals of this form?

> Hint: See textbook chapter 5, or Gilman and Jerison 'Rings of Continuous Functions'.

**Theorem of Swan:** A theorem about topological vector bundles over $C([0,1])$, see textbook. There is a categorical equivalence between vector bundles on a compact space and f.g. projective modules over this ring.

> So commutative algebra has something to say about other branches of Mathematics!

**Definition:** A topological space is called *boolean* (or a *Stone space*) iff it is compact, hausdorff, and totally disconnected.

*Example:* A projective variety over $p$-adics with $\mathbb{Q}_p$ points plugged in.

**Definition:** A ring is boolean if every element is idempotent, i.e. $x \in R \implies x^2 = x$.

**Exercise:** If $R$ is a boolean domain, then it is isomorphic to the field with 2 elements.

**Lemma:** There is a categorical equivalence between Boolean spaces, Boolean rings, and so-called "Boolean algebras".

# 2 Monday January 13

## 2.1 Logistics

Some topics for final projects

- The cardinal Krull dimension of $\mathrm{Hol}(X)$.
- Galois connections
- Ordinal filtrations
- Lam-Reyes prime ideal principal
- $C(X)$
- $\mathrm{Hol}(X)$
- Semigroup rings
- Swan's Theorem
  - Vector bundles on a compact space
- Boolean rings and Stone duality
- More Nullstellansatz
  - Beyond Hilbert's usual one
- Hochster's Theorem
  - Characterizes $\mathrm{Spec}R$ as a topological space, i.e. when is a topological space homeomorphic to the spectrum of some commutative ring.
- Invariant theory (quotients of rings under finite group actions, i.e. $R^G$ for $|G| < \infty$)

  - For $R = k$ a field, this is Galois theory
  - Easy case of geometric invariant theory, when $G$ is infinite
- UFDs
  - What conditions does a ring need to have to ensure unique factorization?
- Euclidean rings
- Claborn (Leedham-Green-Clark): Every commutative group is (up to isomorphism) the class group of some Dedekind domain.
  - A type of inverse problem, class group measures deviation from being a UFD
  - Uses ordinal filtrations, transfinite induction
  - See proof in elliptic curves course

## 2.2 Rings of Functions

Let $k$ be a field, $X$ a set of cardinality $|X| \geq 2$, and define $k^X \coloneqq \text{Maps}(X.k) = \{f : X \to K\}$ is a ring under pointwise addition and multiplication. As a ring, this is a (big!) cartesian product.

*Some facts:*

- $k^X$ is not a domain (**exercise**), and there are nontrivial idempotents ($e^2 = e$)

  > Note: it could be worse and have nilpotents.

- $k^X$ is *reduced*, i.e. it has no nonzero nilpotents, where $z \in R$ is nilpotent iff $\exists n \geq 1$ such that $z^n = 0$.
  - Note: domains are reduced, cartesian products of reduced rings are reduced.
- Every subring of $k^X$ is reduced.

  > Moral: should be viewing every ring as functions on some space, but this can't literally be true because of the above restrictions. Nilpotent elements are "hard to view as functions".

- For $X$ a topological space, $C(X)$ the ring of continuous functionals to $\mathbb{R}$, then $C(X) \subset \mathbb{R}^X$.

**Exercise:** When is $C(X)$ a domain? (Note that we can have products of nonzero functions being identically zero.)

*Example:* Let $R$ be the ring of holomorphic functions $\mathbb{C}\circlearrowleft$, i.e. $\text{Hol}(\mathbb{C}, \mathbb{C}) \coloneqq \left\{ f : \mathbb{C} \to \mathbb{C} \;\middle|\; f \text{ is holomorphic} \right\}$.

The set of zeros of such an $f$ must be discrete, the example of bump functions doesn't go through holomorphically.

This is a domain, not Noetherian, not a PID, but every f.g. ideal is principal (thus this is a Bezout domain, a non-Noetherian analog of a PID).

It has infinite Krull dimension: recall that ideals are prime iff $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ iff $R/\mathfrak{p}$ is a domain, and the Krull dimension is the supremum $S$ of lengths of chains of prime ideals (only when $S$ is finite).

If $C \subset (X, \leq)$ is a finite-length chain in a totally ordered set, then the length $\ell(C) = |C| - 1$ (1 less than the number of elements appearing). The *cardinal Krull dimension* of a ring $R$ is the actual supremum.

> Note: in Noetherian rings, there can still be finite but unbounded length chains.

Letting $X$ be a complex manifold (i.e. covered by subsets of $\mathbb{C}^n$ with holomorphic transition functions) and let $\mathrm{Hol}(X)$ be the holomorphic functionals $f : X \to \mathbb{C}$. Then $\mathrm{Hol}(X)$ is a domain iff $X$ is connected.

> Note that if $X$ is disconnected, we can take a function that is constant on one component and zero on another, then switch, then multiply to get a zero function.

If $X$ is a compact connected projective variety, then $\mathrm{Hol}(X)$ is just constant functions by the open mapping functions. So $\mathrm{Hol}(X) = \mathbb{C}$, and $\mathrm{carddim}\mathbb{C} = 0$ because for any field there are only two ideals, and here (0) is prime. Moreover, $\mathrm{carddimHol}(\mathbb{C}) \geq \alpha_0$.

> Note that for complex manifolds, $X$ is either compact or supports many holomorphic functions.

**Theorem:** If $X$ is a connected complex manifold which has a nontrivial holomorphic function, i.e. $\mathrm{Hol}(X) \supset \mathbb{C}$, then there exists a chain of prime ideals in $\mathrm{Hol}(X)$ of length $|\mathbb{R}| > \aleph_0$, i.e. it has at least the cardinality of the continuum.

> Note: the cardinality could be even bigger!

> Maximals are prime: equivalent to fields are integral domains.

### 2.3 Rings

Take all rings to be unital, i.e. containing 1. A ring without identity is referred to as an *rng*. In this course, all rings are commutative.

*Example:* This is a fairly special restriction. Take $(A, +)$ a commutative group and define $\mathrm{End}(A) = \{f : A \to A\}$ the ring of group homomorphisms under pointwise addition and composition. This is generally not commutative, i.e. $\mathrm{End}(\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)) = M_2(\mathbb{Z}/(2))$ the ring of matrices with $\mathbb{Z}/(2)$ entries, which is not commutative.

**Exercise:** Given $(A, +)$, show that $\mathrm{End}(\bigoplus^n A) = M_n(\mathrm{End}(A))$.

Generally, if $R$ is a ring and $M$ is as $R$-module, then $\mathrm{End}_R(M) = \{f : M \to M\}$ of $R$-module homomorphisms is always a ring under pointwise addition and composition, and is (probably) non-commutative.

## 3 Wednesday January 15th

**Cayley's theorem:** For $G$ a group, then there is a canonical injective group homomorphism $\Phi : G \hookrightarrow \mathrm{Sym}(G) \cong S_n$ for $n = |G|$. The map is given by $g \mapsto g\,\cdot$, i.e. multiplying on the left.

Is there an analog for rings?

Take a similar map:

$$\begin{aligned} R &\to \mathrm{End}_{\mathbb{Z}}(R, +) \\ r &\mapsto (x \mapsto rx). \end{aligned}$$

Unfortunately there is no specialization for commutative groups/rings – $\mathrm{Sym}(G)$ for example is noncommutative when $|G| \geq 2$. Similarly, even if $R$ is commutative, $\mathrm{End}(R, +)$ is probably not.

As per the Grothendieck philosophy, we find that all rings are a ring of functions on something – namely themselves, since this map is injective.

All rings are commutative here, so take $R^\times = \left\{ x \in R \;\middle|\; \exists y \text{s.t.} xy = 1 \right\}$. For $R$ a group, $R^\times$ is a commutative group, so this is an interesting invariant.

Another interesting invariant: the class group.

*Notation:* Let $R^\bullet = R \setminus 0$. An element $x \in R$ is a zero divisor iff there exists $y \in R^\bullet$ such that $xy = 0$. For $x, y \in R$ we write $x \;\middle|\; y$ iff $\exists z \in R$ such that $xz = y$.

$R$ is a domain iff 0 is the only zero divisors, i.e. $xy = 0 \implies x = 0$ or $y = 0$. $(R^\bullet, \cdot)$ is a commutative monoid (group without inverses) iff $R$ is a domain. Observe that $R$ is a field iff $R^\bullet = R^\times$.

For rings $R, S$ we have the usual definition of ring homomorphism, additionally requiring $f(1) = 1$. Note that $f(0) = 0$ follows from $f(x+y) = f(x) + f(y)$, but $f(1) = 1$ does not. Rings have products $R_1 \times R_2$ which is again a ring under coordinate-wise operations. Note that there are canonical projections $\pi_i R_1 \times R_2 \to R_i$. There is a dual inclusion $\iota_1 : R_1 \to R_1 \times R_2$ given by $x \mapsto (x, 0)$, but these are not ring homomorphisms (although everything is a group homomorphism). This is because $\iota_1(1) = (1, 0) \neq (1, 1)$, the identity of $R_1 \times R_2$. Note that 1 always has to map to an idempotent element, i.e. $e^2 = e$, and idempotents are always zero divisors. Also note that the map $x \mapsto 0$ is not a ring homomorphism unless $S = 0$.

**Definition:** A ring homomorphism is a map $f : R \to S$ is an isomorphism iff it has a two-sided inverse, i.e. there exists a morphism $g : S \to R$ with $g \circ f = \mathrm{id}_R$ and $f \circ g = \mathrm{id}_S$.

**Exercise:** Check that this is equivalent to $f$ being a bijection.

**Exercise:** Check that the zero ring is the final object in the category of rings. Show that $\mathbb{Z}$ is the initial object in this category?

$R$ is a subring of $S$ iff $R \subset S$ and the inclusion $R \hookrightarrow S$ is a morphism.

Adjoining elements: Suppose $R \leq S$ is a subring and $X \subset S$ is just a subset. Then there exists a ring $R[X]$ such that

- Top-down description: $R[X] \leq S$ is a subring containing $R$ and $X$, and is minimal with respect to this property (obtained by intersecting all such subrings)
- Bottom-up description: things resembling $\sum r_i x_i$

**Exercise 1.6:** Take $R = \mathbb{Z}, S = \mathbb{Q}$, $P$ a arbitrary set of prime numbers. Let $\mathbb{Z}_\mathcal{P} = \mathbb{Z}[\left\{ \frac{1}{p} \;\middle|\; p \in P \right\}]$.

a. When do we have $\mathbb{Z}_{\mathcal{P}_1} \cong \mathbb{Z}_{\mathcal{P}_2}$?

Hint: take $P_1 = \{3, 7, 11\}, P_2 = \{5\}$. Need $P_1 = P_2$!

b. Show that every subring $T$ such that $\mathbb{Z} \leq T \leq \mathbb{Q}$ is of the form $\mathbb{Z}_\mathcal{P}$ for some unique set of primes $P$.

Note that if $T$ is any intermediate ring between $R$ and $S$, then $R[T] = T$.

### 3.1 Ideals and Quotients

For $f : R \to S$ a ring homomorphism, define $I = \ker f = f^{-1}(\{0\})$. Then $I$ is a subgroup of $(R, +)$, and for all $i \in I$ and all $r \in R$ we have $ri \in I$, since $f(ri) = f(r)f(i) = f(r)0 = 0$. In other words, $RI \subseteq I$.

By definition, an ideal $I$ of $R$ is an additive subgroup of $R$ that satisfies these properties. Is every ideal the kernel of a ring homomorphism? The answer is yes, namely the quotient $\pi : R \to R/I$.

**Theorem:** Let $I \subset (R, +)$, then TFAE:

a. $I$ is an ideal of $R$, written $I \trianglelefteq R$.
b. There exists a ring structure on the quotient group $R/I$ such that the projection $r \mapsto r + I$ is a ring morphism.

When these conditions hold, the ring structure on $R/I$ is *unique* and we refer to this as the *quotient ring.*

## 4 Friday January 17th

For a $R \subset T$ a subring of a ring, the set of intermediate rings is a large/interesting class of rings. Recall: uncountably many rings between $\mathbb{Z}$ and $\mathbb{Q}$! Taking $R$ a PID and $T$ its fraction field, a similar result will hold.

Define $I \trianglelefteq R$ as the kernel of a ring morphism. This implies that $I \subset (R, +)$ with the absorption property $RI \subset I$. Conversely, any $I$ satisfying these two properties is the kernel of a ring morphism: namely $R \to R/I$. This makes sense as a group morphism.

**Exercise:** Define $xy+I = (x+I)(y+I)$, need to check well-definedness. Write out $(x+i_1)(y+i_2) = \cdots$, need to check that $i_1y + i_2x + i_1i_2 \in I$, but the absorption property does precisely this.

Note that if we were in a non-commutative setting, this would define a left ideal. These don't have to coincide with right ideals – there are rings where the former satisfy properties that the latter does not.

*Example:* The subrings of $R = \mathbb{Z}$ are of the form $n\mathbb{Z}$ for $n \geq 0$, with the usual quotient.

**Definition:** An ideal $I \trianglelefteq R$ is *proper* iff $I \subsetneq R$.

**Exercise:** An ideal $I$ is not proper iff $I$ contains a unit.

**Exercise:** $R$ is a field iff the only ideals are $0, R$.

**Definition:** Let $\mathcal{I}(R)$ be the set of all ideals in $R$. What structure does it have? It is partially ordered under inclusion. It is a complete lattice, i.e. every element has an infimum (GLB) and a supremum (LUB). Namely, for a family of ideals $\{I_j\}$, the infimum is the intersection and supremum is defined as $\left\langle I_j \;\middle|\; j \in J \right\rangle$, the smallest ideal containing all of the $I_j$, i.e. $\langle y \rangle = \left\{ \sum^{n} r_i y_i \;\middle|\; n \in \mathbb{N}_{>0},\ r_i \in R,\ y_i \in y \right\}$.

**Exercise:** For $I_1, I_2 \trianglelefteq R$, it is the case that $I_1 + I_2 \coloneqq \{i_1 + i_2\} = \langle I_1, I_2 \rangle$.

**Theorem:** Let $I \trianglelefteq R$ and $\phi : R \to R/I$, and define $\ell(I) = \{I \subset J \trianglelefteq R\}$. Then we can define maps

$$\Phi : \ell(R) \to \ell(R/I)$$
$$J \mapsto \frac{I+J}{J},$$

and

$$\Psi : \ell(R/I) \to \ell(R)$$
$$J \trianglelefteq R/I \mapsto \phi^{-1}(J).$$

We can check that $\Psi \circ \Phi)(J) = I + J$, and $\Phi \circ \Psi(J) = J$ $(= J/I?)$ So $\Psi$ has a left inverse and is thus injective. Its image is the collection of ideals that contain $J$, and $\Psi : \ell(R/I) \to \ell_I(R)$ is a bijection and is in fact a lattice isomorphism with $\ell_I(R) \subset \ell(R)$.

Note that this gives us everything above (?) an ideal in the ideal lattice; the dual notion will come from localization.

*Remarks:* The ideal lattice $\ell(R)$ is

- A complete lattice under subset inclusion,
- A commutative monoid under addition
- A commutative monoid under *multiplication*, which we'll define.

**Definition:** For $I, J \trianglelefteq R$, we define $IJ = \left\langle ij \;\middle|\; i \in I,\ j \in J \right\rangle$. Note that we have to take the ideal generated by products here.

For $\langle x \rangle = (x)$ a principal ideal and $\langle y \rangle$ principal, we do have $(x)(y) = (xy)$. Note that $IJ \subset I \bigcap J$, whereas the sum was larger than $I, J$.

**Exercise:** Note that $(\ell(R), \cdot)$ has an absorbing element, namely $(0)I = (0)$. For $(M, +)$ a commutative monoid and $M \hookrightarrow G$ a group, then multiplication by $x$ is injective and so for all $y \in M$, $xz = yz \implies x = y$, so $M$ is cancellative.

Question: what if we consider $\mathcal{I}^\bullet(R)$ the set of nonzero ideals of $R$. Does this help? We will see next time.

## 5 Wednesday January 22nd

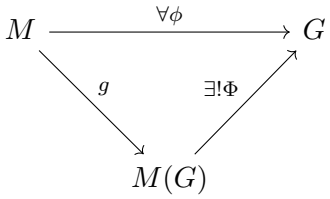
Let $R$ be a ring and let $\mathcal{I}(R)$ be the set of ideals $I \trianglelefteq R$. This algebraic structure is

- Partially ordered under inclusion
- Forms a complete lattice with sup the ideal generated by a family and inf the intersection.
- Forms a commutative monoid under $I + J$
- Forms a commutative monoid under $IJ$

For any commutative monoid $(M, +)$, there exists a group completion $G(M)$ such that

- $G(M)$ is a commutative group
- $g : M \to G(M)$ is a monoid homomorphism

- For any map $\phi : (M, +) \to (G, +)$ into a commutative group, we have the following diagram




So $\phi$ factors through $M(G)$.

If this exists, it is unique up to unique isomorphism (as are all objects defined by universal properties). It remains to construct it.

**Exercise:** For $(M, +)$ a commutative monoid, show that TFAE

1. There exists an injective $\iota : M \hookrightarrow G$ monoid homomorphism for $G$ some commutative group.
2. The map $g : M \to G(M)$ is an injection.
3. $M$ is cancellative, i.e. $\forall x, y, z \in M$ we have $x+z = y+z \implies x = y$, i.e. the map $p_z(x) = x+z$ is injective.

The content here is in $3 \implies 1$.

A commutative monoid is *reduced* iff $M^\times = (0)$, i.e. if "$\forall m \in M \exists n$ such that $m + n = 0$" $\implies m = 0$

*Example:* $(\mathbb{N}, +)$ and $(\mathbb{Z}^+, \cdot)$ are cancellative and reduced.

**Definition**: $z \in M$ is a zero element iff $z + x = z$ for all $x \in M$.

*Remark:* If $M$ has a zero element, then $G(M) = \{0\}$.

$(0)$ is a zero element of $(\mathcal{I}(R), \cdot)$, so this is not cancellative. If we take $\mathcal{I}^\bullet$ the set of nonzero ideals with multiplication, then this is a submonoid of $\mathcal{I}(R)$ iff $R$ is a domain.

For $R$ a domain, let $\mathcal{I}_1(R)$ be the set of nonzero principal ideals of $R$, then $\mathcal{I}_1(R) = R^\bullet/R^\times$, so this is reduced and cancellative.

What is the group completion? In this case, it will consist of fractional ideals.

If $R$ is a PID, then $\mathcal{I}_1^\bullet(R) = \mathcal{I}^\bullet(R)$ is reduced and cancellative.

*Example:* $\mathcal{I}^\bullet \cong (\mathbb{Z}^+, \cdot)$.

**Warning:** If $R$ is not a PID, then $\mathcal{I}^\bullet(R)$ need not be cancellative.

**Exercise:** Take $R = \mathbb{Z}[\sqrt{-3}]$ and $p_2 \coloneqq \left\langle 1 + \sqrt{-3}, 1 - \sqrt{-3} \right\rangle$. Show that $|R/p_2| = 2$, $|R/(2)| = 4$, and $p_2^2 = p_2(2)$ and $\left|R/p_2^2\right| = 8$. Conclude that $\mathcal{I}^\bullet(R)$ is not cancellative.

What went wrong here? Take $K = \mathbb{Q}[\sqrt{-3}]$, then $\mathbb{Z}_k[\frac{1+\sqrt{-3}}{2}]$ is the integral closure of $\mathbb{Z}$ in $K$. $\mathbb{Z}_k$ is a Dedekind domain, and there are inclusions

$$\mathbb{Z} \subset \mathbb{Z}[\sqrt{-3}] \subsetneq \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] \subseteq K.$$

Here the problem is that $\mathbb{Z}[\sqrt{-3}]$ is not a Dedekind domain. If $R$ is a Dedekind domain, then $\mathcal{I}^\bullet(R)$ is cancellative.

**Exercise:** Does the converse hold?

> Things that are too small to be the full rings of integers, and things tend to wrong.

## 5.1 Pushing / Pulling

Let $f : R \to S$ be a ring homomorphism.

We can define a pushforward on the set of ideals $\mathcal{I}(R)$:

$$\begin{aligned} f_* : \mathcal{I}_R &\to \mathcal{I}(S) \\ I &\mapsto \langle f(I) \rangle . \end{aligned}$$

and a pullback

$$\begin{aligned} f^* : \mathcal{I}(S) &\to \mathcal{I}(R) \\ J &\mapsto f^{-1}(J). \end{aligned}$$

**Exercise:** Show that $f^{-1}(J) \trianglelefteq R$.

For $I \trianglelefteq R$ and $J \trianglelefteq S$, then

$$\begin{aligned} f^* f_*(I) &\supseteq I \\ f_* f^*(J) &\subseteq J. \end{aligned}$$

**Exercise:** These are not equal in general, and give examples where equality does and does not hold.

If $f$ is surjective, $f_* f^* J = J$.

> Will also hold for localization, which is dual to taking a quotient.

Define $\overline{I} \coloneqq f^* f_*(I)$ and $J^\circ \coloneqq f_* f^*(J)$, the closure and interior respectively. Show that these operations are idempotent.

**Definition:** An ideal $\mathfrak{p}$ is *prime* iff $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

**Exercise:** $I$ is prime iff $R/I$ is a domain.

**Definition:** $\operatorname{Spec}(R) = \{\mathfrak{p} \trianglelefteq R\}$ the collection of prime ideals is the spectrum.

**Exercise:** Show that for $I \trianglelefteq R$, if we define

$$V(I) \coloneqq \left\{ \mathfrak{p} \in \operatorname{Spec}(R) \;\middle|\; p \supseteq I \right\} \subseteq \operatorname{Spec}(R),$$

then $\left\{V(I) \;\middle|\; I \in \mathcal{I}(R)\right\}$ are the closed sets for a topology on $\mathrm{Spec}(R)$ (the Zariski topology).

**Exercise:** If $f : R \to S$ and $J \in \mathrm{Spec}(S)$ then $f^*(J) \in \mathrm{Spec}(R)$. Show that $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is a continuous map. Conclude that $\mathrm{Spec}(\,\cdot\,)$ is a functor.

**Definition:** $I \trianglelefteq R$ is maximal iff $I$ is proper and is not contained in any other proper ideal.

**Exercise:** $I$ is maximal iff $R/I$ is a field.

**Exercise:** Show that maximal ideals are prime.

**Definition:** Let $\mathrm{Spec}_{\max}(R)$ be the set of maximal ideals and define $V(I) = \left\{\mathfrak{m} \in \mathrm{Spec}_{\max}(R) \;\middle|\; \mathfrak{m} \supseteq I\right\}$.

**Exercise:** Show that these form the closed sets for a topology, and that this is the subspace topology for the Zariski topology.

**Exercise:** Show that if $f : R \to S$ and $\mathfrak{m} \in \mathrm{Spec}_{\max}(S)$ that $f^*(\mathfrak{m})$ is prime but need not be maximal.

**Exercise:** Show that if $f$ is an integral extension, then maximals do pull back to maximals.

# 6 Friday January 24th

## 6.1 Ideals and Products

Recall: Prime and maximal ideals.

***Fact:*** If $I \trianglelefteq R$ then there exists a maximal ideal $I \subset \mathfrak{m} \trianglelefteq R$.

*Proof:* Use Zorn's lemma.

**Corollary:** $\mathrm{maxSpec}\ R \neq \emptyset \iff R \neq 0$.

Later: Multiplicative avoidance, if $S \subset R$ is nonempty with $SS \subset S$, let $I \trianglelefteq R$ with $I \bigcap S = \emptyset$, then

a. There exists an ideal $J \supseteq I$ with $J \bigcap S = \emptyset$ which is maximal with respect to being disjoint from $S$.

b. Any such ideal $J$ is prime.

Taking $S = \{1\}$ recovers the previous fact.

**Exercise:** Let $f : R \to S$ be a ring homomorphism and $\mathfrak{p} \in \mathrm{Spec}(R)$. Show that $f_*(\mathfrak{p})$ need not be prime in $S$.

We can consider products of rings, and correspondingly $\mathcal{I}(R_1 \times R_2)$.

**Exercise:** Show that if $\phi$ is surjective, $\phi(I)$ is an ideal.

**Proposition:** Let $I \in \mathcal{I}(R_1 \times R_2)$. Take $\pi_i \to R_i$ the projections, and let $I_i$ be the corresponding images of $I$. Then $I = I_1 \times I_2$.

Note: a suspiciously strong result! Not every group is the cartesian product of some subgroups.

It's clear that $I \subset I_1 \times I_2$.

*Proof:* Showing $I_1 \times I_2 \trianglelefteq R_1 \times R_2$ is an ideal, since it equals $\langle I_1 \times \{0\}, \{0\} \times I_2 \rangle$.

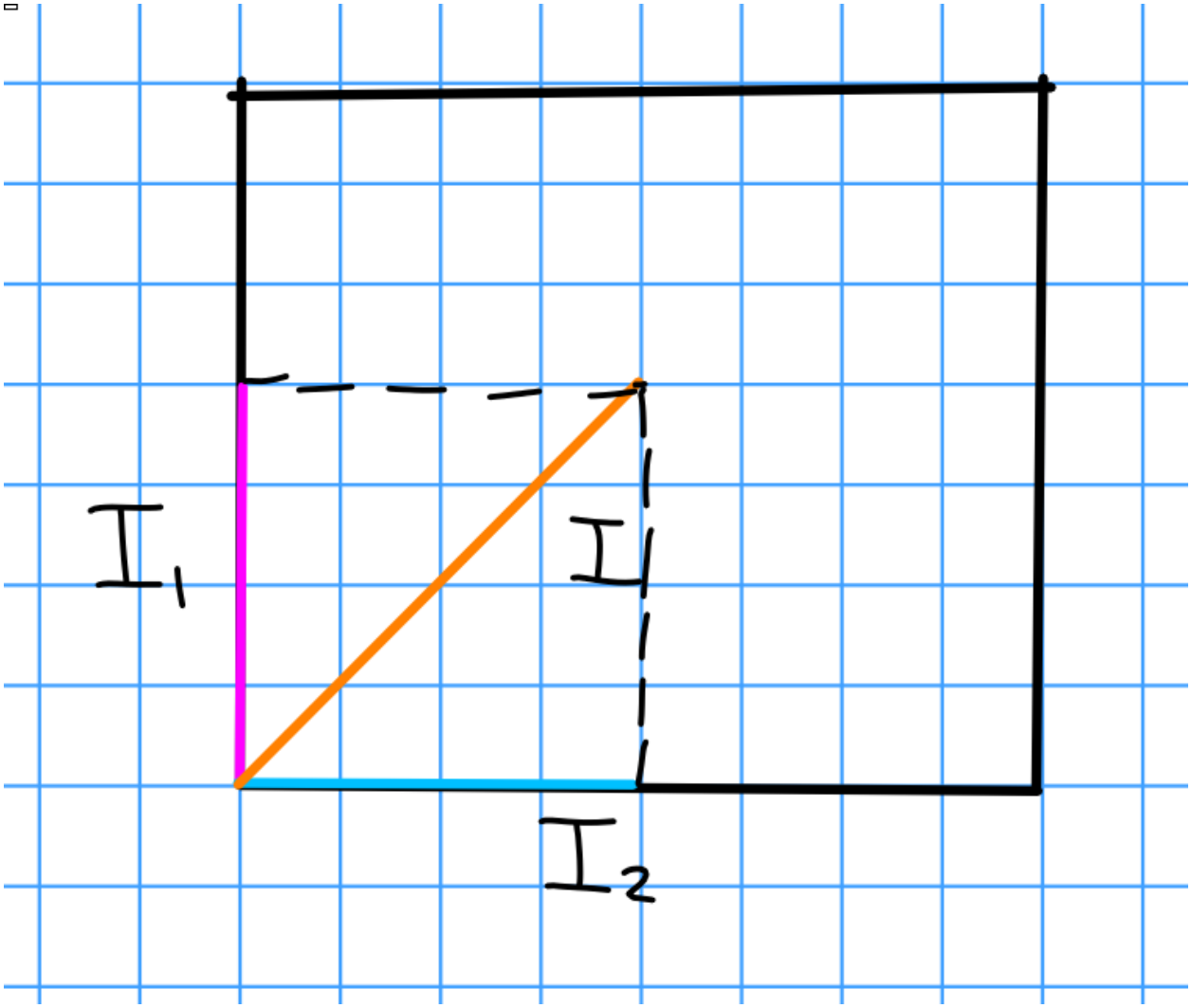



Figure 1: Image

To show $I_1 \times I_2 \subseteq I$, show that $I_1 \times 0, 0 \times I_2 \subseteq I$. E.g. $I_1 \times 0 \subseteq I$: take $(x,0) \in I_1 \times 0$ such that there exists a $y \in R_2$ with $(x,y) \in I$. Then $(x,y)\cdot(1,0) = (x,0) \in I$, then similarly $0 \times I_s \subseteq I$.

■

**Exercise:** Use $\mathcal{I}(R_1 \times R_2) = \mathcal{I}(R_1) \times \mathcal{I}(R_2)$ to describe $\mathrm{Spec}(R_1 \times R_2)$ in terms of $\mathrm{Spec}(R_1)$ and $\mathrm{Spec}(R_2)$.

Question: For a ring $R$, when is $R \cong R_1 \times R_2$ for some nonzero $R_1, R_2$?

**Exercise**: Show that comaximal ideals correspond with coprime ideals when $R = \mathbb{Z}$.

**Theorem (Chinese Remainder):** If $I_1, I_2$ are comaximal, so $I_1 + I_2 = R$, then the map

$$\begin{aligned} \Phi : R &\to R/I_1 \times R/I_2 \\ x &\mapsto (x + I_1, x + I_2). \end{aligned}$$

Then $\ker \Phi = I_1 \bigcap I_2 \overset{\text{CRT}}{=} I_1 I_2$ and $\Phi$ is surjective, and

$$R/(I_1 \bigcap I_2) = R/I_1 I_2 \cong R/I_1 \times R/I_2.$$

Case 1: Let $I_1 + I_2 = R$ and $I_1 \bigcap I_2 = 0$ (equivalently $I_1 I_2 = (0)$), then $R \cong R/I_1 \times R/I_2$.

Conversely, let $R = R_1 \times R_2$ with $R_1, R_2$ nonzero. Let $e_1 = (1,0)$ and $e_2 = (0,1)$. Then $e_1 e_2 = 0$ and $e_2 = (1 - e_1)$, so $0 = e_1(1-e_1) = e_1 - e_1^2$ and $e_1$ is idempotent. So $e_1, e_2$ are complementary nontrivial idempotents. Then $I_1 I_2 = e_1 e_2 = (0)$, $I_1 + I_2 = \langle e_1, e_2 \rangle = R$, and thus $R = R/e_2 R \times R/e_1 R$. Note that $e_2 R = 0 \times R_2$ and $e_1 R = R_1 \times 0$, thus

$$\begin{aligned} R/e_2 R &= \frac{R_1 \times R_2}{0 \times R_2} = R_1 \\ R/e_1 R &= \frac{R_1 \times R_2}{R_1 \times 0} = R_2. \end{aligned}$$

■

We thus have a correspondence

$$\left\{\text{Nontrivial product decompositions } R{=}R_1{\times}R_2\right\} \iff \left\{I_1{,}I_2 \trianglelefteq R \text{ such that } I_1 I_2{=}0 \text{ and } I_1{+}I_2{=}R\right\} \iff \left\{\text{Idempotents } e{\neq}0{,}1\right\}.$$

Thus a ring can be decomposed as a product iff it contains nontrivial idempotents.

**Definition:** $R$ is connected iff there do not exists nonzero $R_1, R_2$ such that $R \cong R_1 \times R_2$ iff $R$ does not contain an idempotents $e \neq 0, 1$.

*Exercise:* Show that $R$ is connected iff $\mathrm{Spec}(R)$ is connected as a topological space.

Note: Not every ring is a finite product of connected rings.

## 6.2 Modules

For $(M, +)$ a commutative group, we want an action $R \curvearrowright M$ for $R$ a ring. Recall that $\mathrm{End}(M)$ for a group is a (potentially noncommutative) ring. An $R$-module structure is a ring homomorphism $R \to \mathrm{End}(M)$. Equivalently, it is a function $R \times M \to M$ with $rs(x) = r(sx)$, $r(x+y) = rx + ry$, and $1 \cdot x = x$ for all $x \in M$.

> Note that this defines a left $R$-module, but right/left modules coincide for commutative rings.

*Exercise:* Let $M$ be an $R$-module and for $m \in M$ define $\mathrm{Ann}(m) = \left\{ r \in R \;\middle|\; xm = 0 \right\} \trianglelefteq R$; show this is in fact an ideal.

> Note: skipped chapter on Galois connections, i.e. some binary relation on a pair of sets. This is an instance of such a connection, where $x \sim m \iff xm = 0$.

For any subset $S \subset M$, define $\mathrm{Ann}(S) \coloneqq \left\{ x \in R \;\middle|\; xm = 0 \; \forall m \in S \right\}$. Show that $\mathrm{Ann}(S) = \bigcap_{m \in S} \mathrm{Ann}(m)$ and $\mathrm{Ann}(M) = \left\{ x \in R \;\middle|\; xM = 0 \right\} = \ker(R \to \mathrm{End}(M))$.

**Definition:** $M$ is faithful iff $\mathrm{Ann}(M) = 0$ iff $R \hookrightarrow \mathrm{End}(M)$ is an injection.

*Exercise:* Any $M$ is naturally a faithful $R/\mathrm{Ann}(M)$-module.

# 7 Monday January 27th

## 7.1 Localization

Consider rings $T$ such that $\mathbb{Z} \subseteq T \subseteq \mathbb{Q}$, and let $P$ be a set of prime numbers. We've shown that if $P, Q$ are two sets of prime numbers, then $\mathbb{Z}_p = \mathbb{Z}_q \iff \mathbb{Z}_p \cong \mathbb{Z}_q \iff P = Q$.

Let $R$ be a domain with fraction field $K$. Let $P$ be a set of mutually nonassociate prime elements. Note that $p \in R$ is a prime element iff $(p)$ is a prime ideal. We say $x, y$ are associates iff there exists a $u \in R^\times$ such that $y = ux$. Since we're in a domain, (exercise) this is equivalent to $(x) = (y)$.

**Fact:** We can then consider $R_P \coloneqq R[\left\{ \frac{1}{p} \;\middle|\; p \in P \right\}]$, and the fact is that the previous statement still holds.

But if $R = \mathbb{Z}$, we also have (exercise) if $Z \subset T \subset \mathbb{Q}$ then $T = \mathbb{Z}_p$ for a unique $P$.

**Exercise:** How do we find such a $P$? This comes down to looking at $\frac{a}{b} \in T$ with $\gcd(a, b) = 1$, then $\frac{1}{b} \in T$.

> Hint: In a PID, $\gcd(a, b)$ exists and is a $\mathbb{Z}$-linear combination of $a$ and $b$. The solution should work for an arbitrary PID.

Let $R$ be a domain and $S$ multiplicatively closed (so $(S, \cdot) \leq (R, \cdot)$ is a submonoid). Then $S$ is *primal* if $S$ is generated as a monoid by its prime elements. Suppose that $S$ is *saturated*, i.e. if $s \in S$ and $r \in R$ with $r \mid s$, then $r \in S$.

> Can always add in all divisors.

We can then define the localization of $R$ at $S$,

$$R_s \coloneqq \left\{ \frac{a}{s} \;\middle|\; a \in R, s \in S \right\}.$$

This satisfies $R \subset R_S \subset K$, and is a multiplicative partial group completion. If we took nonzero elements, this would yield exactly the fraction field.

**Theorem (Negata):** Let $R$ be a Noetherian domain with $S \subset R$ primal as above. If $R_S$ is a UFD, then $R$ is a UFD.

**Exercise:** Show that the converse holds.

> Fraction fields are always UFDs? Localizing makes it easier for irreducibles to be prime. This helps prove that some interesting rings are UFDs.

## 7.2 Modules

If $M$ is an $R$-module, then an $R$-submodule $N \leq M$ is a subgroup of $(M, +)$ such that $R \curvearrowright N \subset N$.

Every ring $R$ is an $R$-module over itself, and the $R$-submodules of $R$ are precisely the ideals of $R$.

> Can express certain concepts about rings/commutative algebra in the language of modules.

A morphism of $R$-modules $f : M \to N$ is a homomorphism $(M, +) \to (N, +)$ such that $f(r \curvearrowright m) = r \curvearrowright f(m)$.

**Exercise:** Any module morphism that is a bijection is an isomorphism. (Usually true in algebraic settings.)

We can form quotient modules $\dfrac{M}{N}$ which is an $R$-module with $r \curvearrowright (m + N) = (r \curvearrowright m) + N$, and $M \to \dfrac{M}{N}$ is a surjective morphism.

If $I \trianglelefteq R$ is an $R$-submodule of $R$, then $R/I$ is an $R$-module. We have $\operatorname{Ann}(R/I) = I$.

**Fact:** Every ideal in $R$ is the annihilator of some $R$-module.

**Fact:** Suppose $R$ is a ring such that every every nonzero $R$-module is faithful, then $R$ is a field. The converse also holds.

> General idea: we study rings by looking at modules over them.

For an $R$-module $M$ and $S \subset M$, then we can consider $\langle S \rangle$ the $R$-submodule generated by $S$. We can write this as

$$\bigcap_{N \text{ s.t. } S \subset N \subseteq RM} N = \left\{ \sum_{i=1^n} r_i s_i \;\middle|\; r_i \in R, s_i \in S \right\}.$$

We say $R$ is finitely generated iff there exists a finite generating set $S \subset M$. We say $M$ is cyclic iff it is generated by a single element, i.e. $M = \langle s \rangle$.

Let $\{M_i\}_{i\in I}$ be a family of $R$-modules. Let $\prod_{i\in I} M_i$ be the cartesian product with a coordinate-wise $R$-action be the direct product. Let

$$\bigoplus_{i\in I} M_i = \left\{(x_i) \in \prod M_i \;\middle|\; x_i \neq 0 \text{ for finitely many } i\right\},$$

which is a submodule of $\prod M_i$. When $I$ is finite, these are equal.

Recall: If $R$ is a PID and $M$ is a finitely generated $R$-module, then there exist finitely many cyclic $R$- modules $\{C_1, \cdots, C_n\}$, then $M \cong \bigoplus C_i$.

**Exercise:** Let $R$ be a ring and $C$ a cyclic $R$-module, then show that $C \cong R/\mathrm{Ann}(C)$ as $R$-modules.

We'll later see that the class of rings $R$ such that every $R$-module is free are exactly fields.

*Remark:* Let $I \trianglelefteq R$, then $I$ is cyclic as an $R$-module iff $I$ is principal.

**Exercise:**

a. Let $I \trianglelefteq R$ for $R$ a domain, then $I$ is indecomposable, i.e. $I \neq M_1 \oplus M_2$ for any nonzero $M_1, M_2$ $R$-modules.

b. If $R$ is additionally Noetherian and not a PID, then there exists an $I \trianglelefteq R$ where $I$ is finitely generated, not principal, and so $I$ is not a cyclic $R$-module.

Converse to structure theorem! Mild assumptions negate cyclic direct sum decomposition.

# 8 Friday January 31st

## 8.1 Tensor and Hom

Let $M, N$ be $R$-modules, then we define

$$\hom_R(M,N) \coloneqq \left\{f : M \to N \;\middle|\; f \text{ is an } R\text{-module map}\right\}.$$

Recall that $R$-module maps satisfy

- $f : (M,+) \to (N,+)$ a morphism of abelian groups
- For all $r \in R$, for all $m \in M$, $f(rm) = rf(m)$.

Note that $\hom_R$ is a commutative group, and is in fact an $R$-module with structure given by $(r \cdot f) \cdot m \mapsto rf(m) = f(rm)$.

Note that the proof of this fact uses commutativity in a key way.

Facts:

$$\begin{aligned}
\hom_R(R,N) &= N \\
\hom_R\left(\bigoplus_{s\in S} R_s, N\right) &= N^S \\
\hom_R(M,R) &\coloneqq M^\vee.
\end{aligned}$$

Note: Infinite dimensional vector spaces over fields are never isomorphic to its dual.

**Exercise:** Think about $M^\vee$ and $(M^\vee)^\vee$.

Recall the map

$$\begin{aligned} \iota : M &\to (M^\vee)^\vee = \hom_R(\hom_R(M,R),R) \\ x &\mapsto (\ell : M \to R \mapsto \ell(x) \in R). \end{aligned}$$

**Exercise:** If $R = k$ is a field, then show that $\iota$ is injective iff $\dim M$ is finite.

Is this always injective? No! Counterexample: Take $R = \mathbb{Z}$ and $M = \mathbb{Z}/p\mathbb{Z}$, then $M^\vee = \hom_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}) = 0$.

It can also fail to be surjective in the infinite dimensional case – the space $M^\vee$ is strictly larger than $M$.

**Definition:** $M$ is *reflexive* if $\iota : M \xrightarrow{\sim} (M^\vee)^\vee$ is an isomorphism.

**Exercise:** Show the following:

- If $M$ is free and finitely generated, then $M$ is reflexive.
- If $R = k$ is a field, then $M$ is reflexive iff $M$ is finitely generated.
- There exists a ring $R$ and a reflexive $R$-module $M$ that is not finitely generated.

## 8.2 Free Torsion Modules

Let $R$ be a domain, and for all $a \in R^\bullet$ the map $[a] : R \to R$ is injective, and $[a] \in \hom_R(R,R) = R$.

**Definition:** $M[\text{tors}] \coloneqq \left\{ m \in M \;\middle|\; \operatorname{Ann}(m) \neq (0) \right\} \leq M$ is the torsion submodule of $M$.

**Definition:** $M$ is *torsion* iff $M = M[\text{tors}]$, and $M$ is *torsion-free* iff $M[\text{tors}] = (0)$.

**Exercise:** Show that if $0 \to A \to B \to C \to 0$, then

- Show that if $B$ is torsion then $A, C$ are torsion.
- If $A, C$ are torsion, must $B$ be torsion?
- Show that if $B$ is torsion-free then $A$ is torsion-free but $C$ need not be torsion-free.
- If $A, C$ are torsion-free, must $B$ be torsion-free?

Note: $0 \to \mathbb{Z}/2 \to \mathbb{Z}/4 \to \mathbb{Z}/2 \to 0$ is an extension that isn't a semidirect product!

**Fact:** Free modules are torsion-free.

Note that we need to be in a domain to even talk about torsion.

**Proposition:** Let $R$ be a domain and $M$ an $R$-module. Then

a. $M/M[\text{tors}]$ is torsion-free.
b. If $M$ is finitely generated, then $M$ is torsion free iff $M$ is isomorphic to a submodule of a finitely-generated free module.

**Proposition:** Free $\implies$ projective $\implies$ flat $\implies_{R \text{ a domain}}$ torsion-free.

*Proof of a:* Let $x \in M/M[\text{tors}]$ such that $\exists r \in R^\bullet$ such that $rx = 0$. Lift $x$ to $\tilde{x} \in M$, then $r\tilde{x} \in M[\text{tors}]$. Then $\exists r' \in R^\bullet$ such that $0 = r'(r\tilde{x}) = (r'r)\tilde{x} \coloneqq r_2\tilde{x}$ for some $r_2 \neq 0$. But then $\tilde{x} \in M[\text{tors}]$, and so $x = 0$ in $M/M[\text{tors}]$.

*Proof of b:* Let $M = \langle x_1, \cdots, x_r \rangle$ with $r \geq 1$ and $x_i \neq 0$. After reordering, there exists some $s$ with $1 \leq s \leq r$ such that $x_1, \cdots, x_s$ are $R$-linearly independent, and for all $i > s$, $\{x_j\}_{j \leq s} \bigcup x_i$ is linearly *dependent*. Then define $F \coloneqq \langle x_1, \cdots, x_s \rangle$; this is a finitely generated free module. If $r = s$, we done.

Otherwise, $r < s$, then $\forall i > r$ there exists an $a_i \in R^\bullet$ such that $a_i x_i \in F$. So we can take $a \coloneqq a_{s+1} \cdots a_r \neq 0$; then $aM \subset F$. Since $M$ is torsion-free, the multiplication maps are injective, so $[a] : M \xrightarrow{\cong} M \subset F$, so $M \hookrightarrow F$ embeds $M$ into a free module.

■

Does this work with $M$ not finitely generated? No, we can't take an infinite product for $a$. Is every torsion-free module a submodule of a free module? No.

*Remark:* This fails without finite generation, see Theorem 3.56 on ordinal filtration. If $R$ is a PID and $F$ is a free $R$-module and $M \leq F$ as an $R$-submodule, then $M$ is free.

Thus if $R$ is a PID, "subfree" $\iff$ free. Does torsion-free imply free? No, take $R = \mathbb{Z}$ and $M = (\mathbb{Q}, +)$, this is not finitely generated and torsion-free but not a free $\mathbb{Z}$-module.

**Definition:** For $R$ a domain, $M$ is *divisible* if $\forall a \in M^\bullet$ iff $[a] : M \twoheadrightarrow M$ is a surjection. $M$ is *uniquely divisible* if for all $a \in M^\bullet$, $[a] : M \xrightarrow{\cong} M$ is an isomorphism, i.e. $M$ is torsion-free and divisible.

**Exercise:** Show that $(\mathbb{Q}, +)$ is a uniquely divisible $\mathbb{Z}$-module.

**Exercise:** Let $R$ be a domain with fraction field $K$, with $R \neq K$. Show that a nonzero free $R$-module is not divisible but $(K, +)$ is a divisible torsion-free $R$-module. Thus $(K, +)$ is a torsion-free module $R$-module that is not free.

Remark: Finitely generated torsion free modules are embedded in free modules. Note that in the spectrum of properties earlier (projective, free, etc), the two extremes are equal for f.g. PIDs.

**Exercise:** Let $R$ be a Noetherian domain which is not a PID. Then an ideal $I \trianglelefteq R$ with $I$ f.g., not principal, and a torsion-free $R$-module. Show that since $I$ is not principal, $I$ is not free as an $R$-module.

> So ideals can't contain linearly independent elements, so they have to be free of rank 1 and thus principal. So f.g. torsion-free is strictly weaker then free in this setting.