# Algebra Notes

May Piatt

February 2024

## Contents



# 0 Lecture 0

## 0.1 Direct Sums

The construction that's going to be the most useful for us is direct sums. Let $R$ be a ring and $M_i$ for $i \in I$ be modules. Recall that the direct product

$$\prod_{i\in I} M_i = \{m : I \to \bigcup_{i\in I} M_i : \ m(i) \in M \forall i \in I\}$$

We know that

$$\mathrm{Hom}_R(N, \prod_{i\in I} M_i) = \prod_{i\in I} \mathrm{Hom}_R(N, M_i)$$

and we have the direct sum of the $M_i$

$$\bigoplus_{i\in I} M_i = \{m \in \prod_{i\in I} : \ m(i) = 0 \text{ for all but finitely many } i\}$$

and the direct sum is equal to the direct product when $I$ is finite. We have not had to deal with infinite products very much, but we may as well talk about them lol. for each $j \in I$, we take $\sigma_j : M_j \to \prod_{i\in I} M$ for the map taking $m \in M_j$ to the element of the product given by

$$\sigma_j(m)(i) = \begin{cases} m & i = j \\ 0 & \text{else} \end{cases}$$

**0.1.1 Proposition.**

- $\sigma_j : M_j \to \prod_{i\in I} M_i$ is an injective $R$-module homomorphism with $\sigma_j(M_j) \subseteq \bigoplus_{i\in I} M_i$
- Denote the projection map $p_j : \prod_{i\in I} M_i \to M_j$, then we have that $p_j \circ \sigma_k = \begin{cases} \mathrm{id}_{m_j} & j = k \\ 0 & \text{else} \end{cases}$

**0.1.2 Theorem.** Suppose $N$ is an $R$-module. Then there is a bijection

$$\mathrm{Hom}_R\left(\bigoplus_{i\in I} M_i, N\right) \to \prod_{i\in I} \mathrm{Hom}(M_i, n)$$

given by $f \mapsto (f \circ \sigma_i)_{i\in I}$. ie. giving an $R$-module homomorphism $f_i \oplus M_i \to N$ is the same as giving an $R$-moduls homomorphism $f_i : M_i \to N$ for each $i \in I$.

*Proof.* Suppose we have $R$-module homs $f_i : M_i \to N$ and let $m : I \to \bigcup_{i\in I} M_i$ be an element of $\bigoplus_{i\in I} M_i$. Let's set

$$f(m) = \sum_{i\in I} f_i(m(i))$$

Since $m \in \bigoplus M_i$, all but finitely many of the terms are $0$, so the sum makes sense. We need to check the following:

$$f : \bigoplus_{i\in I} M_i \to N$$

is an $R$-module hom, and that

$$f \circ \sigma_j = f_j$$

where $\sigma_j$ is inclusion of the $j$-th term $M_j$ into $\bigoplus_{i\in I} M_i$, and that the maps in the theorem actually is a bijection.

## 0.2 Freedom and Cofreedom

We will first talk about cofreedom, which is not as interesting as freedom. We will suppose that all our modules are *left* $R$-modules

We know that $R$ itself is an $R$-module!

Suppose $I$ is a set, and we let $M_i = R$ as an $R$-module for all $i \in I$. Let's set $R^I = \prod_{i\in I} M_i$, which is the set of all maps $x : I \to R$, where $R$ acts on $R^I$ pointwise. This might be the "cofree module" but no one cares. What's more important is the *free module*

**0.2.1 Definition.** We write $R^{(I)} = \bigoplus_{i \in I} M_i$. This is called the *free* $R$-module on $I$, or the free $R$-module *generated by* $I$

For each $j \in I$ let $\sigma_j : R \to \bigoplus_{i \in I} M_i$ and we set $e_j = \sigma_j(1)$. We know that $x \in R^{(I)}$ are officially maps $x : I \to R$ such that $x(i) = 0$ for all but finitely many $i$, and we therefore know that $e_j(i) = \delta^i_j$.

**0.2.2 Lemma.** for any $x \in R^{(I)}$, we have that

$$x = \sum_{i \in I} x(i) e_i$$

with only finitely many terms in the sum nonzero. Then we have that $M = \langle E \rangle$, where $E = \{e_i : i \in I\}$

**0.2.3 Remark.** Recall the definition of a module generated by a set: If $M$ is an $R$-module and $S \subseteq R$ is a set, then $\langle S \rangle$ is going to be given by

$$\langle S \rangle = \bigcap \{N \subset M : \ S \subseteq N, \ N \text{ is an } R\text{-submodule of } M \ \}$$

**0.2.4 Theorem.** Suppose $N$ is an $R$-module. Then the map $\mathrm{Hom}_R(R^{(I)}, N) \to \mathrm{Hom}_{\mathsf{Set}}(I, N)$ given by $f \mapsto (i \mapsto f(e_i))$ is a bijection of sets. That is, to give an $R$-module homomorphism from $R^{(I)} \to N$ is the same thing as giving a map of sets from $I \to N$ and sending the basis element $e_i$ to $f(i)$. NOTE THAT $N$ DOES NOT HAVE TO BE FREE.

*Proof.* This follows directly from the universal property of coproducts once you check that $\mathrm{Hom}_R(R, N)$ is sort of the same as $N$, but this does also have a direct explanation. Suppose $g : I \to N$ is a map of sets and that $x \ in R^{(I)}$. Then we have that $x = \sum x(i)e_i$, and it looks not necessarily finite, but all but finitely many of the terms are 0, so it's finite. Then we let $f(x) = \sum_{i \in I} x(i)g(i)$, and we easily prove that this is a bijection.

## 0.3 Exact Sequences

Suppose we have a sequence

$$\ldots \to G_a \to G_{a-1} \to G_{a-2} \to \ldots \to G_{b+1} \to G_b \to G_{b-1} \to \ldots$$

Where $f_b : G_b \to G_{b-1}$. then we say that the sequence is *exact at* $b$ if $\mathrm{Ker}(f_b) = \mathrm{Im}(f_{b+1})$.

**0.3.1 Example.** A *short exact sequence* is a sequence with exactly 3 nonzero terms.

# 1 Lecture 1

## 1.1 Some module stuff

**1.1.1 Definition.** Suppose $M$ is an $R$-module and $S \subseteq M$. We write $f : R^{(S)} \to M$for $R$-module hom coming from $*$. Then we say $S$ is *independent if* $f$ is $1 - 1$. We say that $S$ is a basis if $f$ is an isomorphism, and we say that $M$ is free if $M$ has at least one basis.

**1.1.2 Proposition.** $M$ is free if and only if $M \equiv R^{(i)}$ for some set $I$.

There are not many things to check for that proposition, so we will skip the proof. Maybe I'll fill it in later.

## 1.2 Duality

Suppose that $R$ is a ring and let $R^{op}$ be the opposite ring to $R$. Let $M$ be a left $R$-module. Then we get the *dual* of $M$, denoted $M^* = \text{Hom}_{R\text{-mod}}(M, R)$. We will use the notation $R$-Mod for the category of left $R$-modules and Mod-$R$ for the category of right $R$-modules.

Suppose $r \in R$ and $\lambda \in D(M)$. Define $(\lambda r)(m) = \lambda(m)r$. Then we have that $\lambda r \in D(m)$ and the map $D(m) \times R \to D(m)$ given by $(\lambda, r) \mapsto \lambda r$ makes $D(M)$ into a right $R$-module

remember that we showed that $R$-modules was enriched over $Z(R)$-mod. It is clear that $\lambda r : M \to M$ is a group homomorphism. We just have to show that it commutes with the action of $R$ on $M$. But this will come from the basic fact that left and right actions commute. eg. all we have to do is check that $\lambda r$ is in $D(M)$, which can be done by showing that if $m \in M, s \in R$, then $\lambda r(sm) = s(\lambda r)(m)$. But we just compute

$$\lambda r(sm) = \lambda(sm)r = s(\lambda(m)r) = s(\lambda r)(m)$$

So we get a map

$$D : R\text{-Mod} \to \text{Mod-}R$$

by

$$M \mapsto D(M)$$

or equivalently, we have that $D$ is a functor from $(R - \text{Mod})^{op} \to R^{op}$-Mod

**1.2.1 Proposition.** $D : R$-Mod $\to$ Mod-$R$ is a contravariant functor between the two categories.

Recall the definition of a contravariant functor: For two categories $C$ and $D$, then a (covariant) functor $F : C \to D$ is a pair of maps Obj$(F)$ : Obj$(C) \to$ Obj$(D)$, and for each $X, Y$ in Obj$(C)$, then we get that the map $F : \text{Hom}_C(X, Y) \to \text{Hom}_D(F(X), F(Y))$ where we have that composition of maps is preserved. A contravariant functor is a covariant functor from $C^{op} \to D$. Then we can reason about whatever else. You essentially can take a "functor" from $C$ to $D$, but flip the arrows in the information preservation part.

Anyways, we can talk about the proof of the theorem. Suppose that $\alpha : M \to N$ is a map of $R$-modules. Then we get a map $F(\alpha) : D(N) \to D(M) = \text{Hom}_R(N, R) \to \text{Hom}_R(M, R)$ given by $f \mapsto f \circ \alpha$. Then all we have to do is check that the map $\alpha^*$ is a morphism in $R^{op}$-Mod. Checking this is just a bunch of "moving parentheses around", which we will not do in class but I might fill in the details later.

We know what $D$ does on $R$, we know that $D(R) \equiv R$ as a right $R$-module. In fact, the map $D(R) = \text{Hom}_{R\text{-Mod}}(R, R)$ by $\lambda \mapsto \lambda(1)$ is an isomorphism of right $R$-Modules. For instance, we can tell you what the inverse is. We can define $\phi_R : R \to R$ by $\phi_R(s) = sr$, and it's easy to check that $\phi_s \in D(R)$, and that $ev(\phi_s) = s, \phi(ev(\lambda)) = \lambda$.

**1.2.2 Corollary.** $D(R^{(S)}) \equiv R^S$ as a right $R$-Module. In particular, if $S$ is finite, then $D(R^{(S)}) \equiv R^{(S)}$.

This is apparent from thm. 0.1.2. The fact that this map is also a map of $R$-Modules is just moving parentheses around.

## 1.3 Two Theorems

We are going to prove two theorems that are related to each other, but seem unrelated at first.

**1.3.1 Theorem (classification of finitely generated modules over a PID).** Suppose $M$ is a finitely generated $R$-Module over a PID $R$. Then there exists a sequence

$$d_1|d_2|\dots|d_r$$

non-unit elements of $R$ such that

$$M \equiv \bigoplus_{i\in 1\dots r} \frac{R}{d_i R}$$

Furthermore, this sequence is unique up to unit.

**1.3.2 Theorem.** If $R$ is a UFD, then so is $R[x]$.

These two theorems have the "same" proof. The weird problem on the homework about the generalization of the gcd is related to these two theorems. The second theorem is also called "Gauss's Lemma". He only proved it for the integers, but what he wrote happened to be the proof of this theorem.

You can reduce this to an algorithm to reducing a matrix to a diagonal matrix that has certain properties. The proof is essentially equivalent is to make matrices into JCF. But matrices of polynomials are really hard to do without making mistakes. Computers can do this pretty easily, though, you should do this in sagemath.

# 2 Lecture 2

## 2.1 Some Facts of Life

We want to prove the two theorems from earlier. To start, let's consider $R$ an integral domain, and $S$ a subset of $R$, then we want to define the GCD and LCM for any subset of $R$.

set

$$CD(S) = \{x \in R : \forall s \in S\ x|s\}$$

. Then set

$$CM(S) = \{x \in R : \forall s \in S\ s|x\}$$

Then we take

$$\text{GCD}(S) = CD(S) \cap CM(CD(S))$$

and

$$LCM(S) = CM(S) \cap CD(CM(S))$$

We know that if GCD$(S)$ is not empty, it consists of one equivalence class of associates. The same is true for LCM. We also know that if $a, b \in R \setminus \{0\}$, then $gcd(a, b) \in$ GCD$(\{a, b\})$. Furthermore, if $R$ is a UFD, then the GCD and LCM sets are nonempty for any subset $S \subseteq R$. Also, if $d \in$ GCD$(S)$, and $R$ is a UFD, then $dR$ contains $\sum_{x \in S} Rx$, with equality holding if and only if $R$ is a PID.

Note that by "associates" we just mean multiplication by a unit, or the equivalence class of the relation $a \sim b \leftrightarrow ua = b$ for $u$ a unit.

If $R$ is a UFD, and $d \in LCM(S)$, then $dR = \bigcap_{s \in S} Rs$.

We will prove all of these things on the homework. Note that the GCD of $\varnothing$ is just $\{0\}$, and you can verify this pretty easily by understanding that the $CD$ of the empty set is $R$, and the common multiple set of $R$ is just $\{0\}$.

**2.1.1 Lemma.** Suppose that $S \subseteq R$ and $R$ is an integral domain. Then

$$CD(S) = CD\left(\sum_{s \in S} Rs\right)$$

The proof is "obvious" but I will verify this later.

## 2.2 Primitivity and Content

Suppose $R$ is an integral domain.

**2.2.1 Definition.** IF $S \subseteq R$, then we say that $S$ is *primitive* if for every principal prime ideal $P = pR$ in $R$, there exists some $s \in S \setminus P$

If you have this definition, but replace *principal prime* with *prime*, then you get that this is an equivalent condition to "$S$ generates $R$".

**2.2.2 Proposition.** Suppose $R$ is a UFD. Then $S \subseteq R$ is primitive $\iff 1 \in$ GCD$(S)$.

*Proof.* Pick a set $\Sigma \subseteq R$ of representatives of the irreducibles in $R$. That is, every element irreducible element of $R$ is an associate of exactly one element of $\Sigma$. If $1 \in$ GCD$(S)$, then for every $q \in \Sigma$, there has to be some $s \in S$ such that $q \not| s$, (otherwise, $q$ would divide all the $s's$, but $1$ is not a multiple of $q$, so we know that $1$ would not be in the GCD). Since $q$ is irreducible, $qR$ is a principal prime ideal (as $R$ is a UFD), this shows that $S$ is primitive if $q \in$ GCD$(S)$.

On the other hand, suppose $S$ is primitive. then we just reverse the steps that we did before. Let $q \in \Sigma$, then there exists some $s \notin qR$. So $q \not| s$. So if $d \in$ GCD$(S)$, and $q \not| d$. Therefore the elements of the GCD$(S)$ are not divisible by any irreducibles, so (as $R$ is a UFD), they have to be units.

**2.2.3 Definition.** Suppose $R$ is an integral domain and $F$ is a free $R$-module. Suppose $x \in F$. We say that $x$ is *primitive* if for every primcipal prime ideal $P = pR$, there exists a $\lambda \in F^*$ such that $x \notin P$.

The content ideal of $x$, denoted $C_F(x) = \{\lambda(x) : \lambda \in F^*\}$

Note that we didn't choose a basis for this definition, nor did it depend on a choice of irreducibles.

Note that in this definition, we are saying that the content ideal is a subset of $R$, since we are taking a set of $\lambda(x)$, which pair to get a guy in $R$.

**2.2.4 Proposition.** Suppose $F = R^{(I)}$ is free and $x = \sum_i x_i e_i$ is in $F$. Then

- $C_F(s) = \sum_{i \in I} x_i R$.
- $x$ is primitive if and only if $\{x_i\}$ is primitive.
- $1 \in \text{GCD}(C_F(x))$ implies that $x$ is primitive.

# 3 New Lecture

Suppose $R$ is a ring and $S$ is a subset of $R$. Then we are going to define the equivalence relation on $S^{-1}R$ just formally, and then mod out by the equivalence relation that you would expect for fractions.

**3.0.1 Definition.** Suppose $A$ is an integral domain, and $S = A \setminus \{0\}$. Then $S^{-1}A$ is a field, called the *field of fractions* of $A$. It is the smallest field that $A$ can go into.

*Proof.* It works for the same reason that the elementary school teachers say it does. We denote frac$A$ denote the field of fractions.

**3.0.2 Example.** Take $R = \mathbb{Z}$ and let $S = \{n \in \mathbb{Z} : p \not| n\}$. Then $S^{-1}\mathbb{Z} = \mathbb{Z}_{(p)} \subseteq \mathbb{Q}$.

I really don't feel like fixing this stuff right now. Just go read about the fractions

# 4 Generalizing the notion of fraction fields and content

Let $R = \mathbb{C}[x, y]$. We will see that $R$ is a UFD. Take $E = R^2$. Then $c_E((x, y)) = \gcd(x, y) = 1$. Note that in a PID, $\gcd(a, b)R = aR + bR$, but in general for a UFD, this is not true, since $\gcd(x, y)R = R \supsetneq xR + yR$ There are *many* more UFD's than PID's.

**4.0.1 Lemma.** Suppose $R$ is a UFD, with $S \subseteq R$. Then

- $\gcd(aS) = c(a) \gcd(S)$, where $c(a) = c_R(a)$
- if $F$ is free, say $F = R^{(a)}$, then $c_F(ax) = c(a)c_F(x)$

*Proof.* we showed a while ago, that $GCD(aS) = aGCD(S)$, and the first item follows. Then, the second item follows from the first item.

**4.0.2 Lemma.** Suppose $S \subseteq k = \text{Frac}(R)$, and , and $a, b \in R \setminus \{0\}$, are two elements such that $aS + bS \subseteq R$. Then $c(b)\gcd(aS) = c(a)\gcd(bS)$. Consequently,

$$\frac{\gcd(aS)}{c(a)} = \frac{\gcd(bS)}{c(b)}$$

Because by the first item in the previous lemma, we have $c(b)\gcd(aS) = \gcd(abS)$ etc.

**4.0.3 Definition.** If $S \subseteq k$ is a subset, such that there exists some $a \in R \setminus \{0\}$, such that $aS \subseteq R$, then we say that $S$ has 1*bounded denominator*. We set $\gcd(S) = \frac{\gcd(aS)}{c(a)}$, and this definition is independent of $a$ by the previous lemma.

**4.0.4 Example.** We have that $\gcd(\frac{1}{5}, \frac{1}{7}) = \frac{1}{35}$. These guys are hte minimum of the $\nu_p$ of the guys in the set. eg. $\gcd(a, b) = \prod_{p \in \Sigma} p^{\min_{s \in S}(\nu_p s)}$.

SEt $F = R^{(I)} \subseteq L = k^{(I)}$. Then if $x \in L$, then we can always find soime $a \in R \setminus \{0\}$ such that $ax \in F$. Then set $c(x) = c_F(ax)/c(a)$ Then you can check that this doesn't depend on $a$ for the same reason as the last time we checked that the definition didn't depend on $a$. Take $F = \mathbb{Z}^2 \subseteq L = k^2$, and $x = (\frac{1}{5}, \frac{1}{7}) \in L$, then we have $c_F(x) = \frac{1}{35}c_F(7, 5) = \frac{1}{35} \cdot 1 = \frac{1}{35}$.

Suppose $x \in L \setminus \{0\}$. Then $x = c(x)x_{\text{prim}}$, where $x_{\text{prim}}$ is a primitive element of $F$, moreover, this decomposition is unique; if $x = uy$ for some $u \in k_\Sigma$, and we have $y$ primitive iff $u = c(x)$ and $y = x_{\text{prim}}$.

*Proof.* Find $a \in R \setminus \{0\}$ such that $ax \in F$. Then by multiplying $a$ by a unit, we can assume $a \in R_\Sigma$. Therefore, $c(a) = a$. Assuming this, set $x_{\text{prim}} = c_F(ax)^{-1}ax$. We know that since $x \neq 0$ then $c_F(ax)$ is invertible. Then $c(ax)$ is the gcd of the coefficients of $ax$, so $c(ax)^{-1}ax \in F$. Moreover, $c_F(c_F(ax)^{-1}ax) = c(c_F(ax)^{-1})c_F(ax) = 1$. Therefore, $c_F(ax)^{-1}$ is primitive. So $x_{\text{prim}}$ is primitive. The rest will be done next time.