Contents

1 Lecture 1

1.1 Rings

Recall that an abelian group is set equipped with an operation that works like addition: you can add and subtract, it's commutative, associative and monoidal.

Definition 1.1
A set R is a ring if it is an abelian group equipped with an associative "multiplication" operation which has a unit 1, where $1a = a$ and this multiplication distributes over addition.

The smallest ring is the zero ring, where $1 = 0$ (and the only element is 0). Other examples of rings are $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, quaternions. Less obvious are the polynomial rings, e.g. $\mathbb{C}[x_1, \ldots, x_n]$ or $M_n(\mathbb{R})$ (the $n \times n$ matrices over $\mathbb{R}$) or $\mathbb{Z}[G]$ (linear combinations of elements of a group G). Even fancier is derivative ring $\mathbb{C}[x_1, \ldots, x_n, \partial_1, \ldots, \partial_n]$, where x_i commutes with x_j and ∂_i commutes with ∂_j and ∂_i commutes with x_j for $i \neq j$, but $\partial_i x_i - x_i \partial_i = 1$ (this is a re-arrangement of the product rule).

Definition 1.2
Consider a commutative ring R. $I \subseteq R$ is an ideal if I is a subgroup of R (over the operation of addition) and it's closed under multiplication, e.g. for $r \in R$ and $i \in I$, $ri \in I$.

Ideals are generated by coprime elements; if they share a factor, some reduction can occur a la gcd and Bezout's. R is going to stand for a commutative ring from henceforth.

Definition 1.3
Consider a commutative ring R. R is a domain (or integral domain or entire ring) if $ab = 0 \implies a = 0$ or $b = 0$.

Definition 1.4
Consider a commutative ring R. R is a principal ideal ring (or principal ring) if every ideal is generated by 1 element.

A principal ideal domain is both a principal ring and a domain. We work towards the following result.

Theorem 1.5
Every finitely-generated module over a principal ideal domain is a direct sum of cyclic modules.

What do all of these words mean?

Definition 1.6
A module (or representation) over a ring R (or R-module) is an abelian group M combined with the operation of scalar multiplication by elements of R that distributes over addition. So for $r, s \in R, m, n \in M$, then $(r + s)(m + n) = rm + rn + sm + sn \in M$.

All vector spaces are modules over their field. The integers mod 12 is a $\mathbb{Z}$-module with integer multiplication as the scalar multiplication. Also $\mathbb{C}[x] \oplus \mathbb{C}[x]$ where $p(a, b) = (pa, pb)$. Furthermore,

A product of rings R_i, $\prod_i R_i$ is a funny object.

Definition 1.7
The product of rings $\prod_i R_i$ is the unique ring such that it has projection maps $\pi_j : \prod_i R_i \to R_j$ for any ring S with maps $f_j : S \to R_j$ there exists a unique map $f : S \to \prod_i R_i$ such that $f_j = \pi_j \circ f$.

The above property is called the universal property. The direct product of rings is just a ring where you just tuple together the ring elements to make a ring element.

The direct sum is similar, but with all the maps reversed. That is why it is sometimes called the coproduct.

Definition 1.8
An R-module A is the direct sum of R-modules M_i, $i \in I$ if there are maps $\phi_i : M_i \to A$ (reverse projections) and given a module B with maps $g_i : M_i \to B$, there exists a unique map $g : A \to B$ such that $g_i = g \circ \phi_i$.

The claim is that A is also a set of tuples, but $A = \{m \in \prod_i M_i \mid m_i = 0 \text{ for all but finitely many } i\}$

Definition 1.9
A module is cyclic if it is generated by one element. This element is called the generator. It is typically denoted as:

$$Rm = (m) = \{rm \mid r \in R\}$$

Definition 1.10
Consider an R-module M. If $m \in M$, then $\operatorname{ann}_R(m) = \{r \in R \mid rm = 0\}$.

The claim is that $Rm \cong R/\operatorname{ann}_R(m)$. Example $\mathbb{C}[x]/(x^{12} - 1)$.

Definition 1.11
A free R-module is a direct sum of copies of R as a module over R. We will denote this as $R^n = R \oplus \cdots \oplus R$.

So to classify finitely-generated modules, let's split them into free parts. Consider R as a PID and M as an R-module, then define

$$M_{\text{tors}} = \{m \in M \mid am = 0 \text{ for some } a \neq 0 \in R\}$$

to be the torsion submodule of M. One can easily check this is a submodule.

The following is an exact sequence, meaning that the image of each map is the kernel of the one after it.

$$0 \to M_{\text{tors}} \to M \to M/M_{\text{tors}} \to 0$$

We claim that M/M_{tors} is a free module. Consider $\overline{m} \in M/M_{\text{tors}}$. Then, $r\overline{m} = rm + M_{\text{tors}} \in M/M_{\text{tors}}$, which after addition shows the claim.

2 Lecture 2

2.1 Unique Factorization Domains

We wish to show today that all principal ideal domains are **Unique Factorization Domains**. For this lecture, we will assume R denotes a principal ideal domain. We wish to show that for $r \in R$, r admits a unique factorization in terms of irreducible elements.

Definition 2.1
An irreducible element $i \in R$ is an element that has no divisors except $\pm$ itself and ± 1 and units.

Definition 2.2
An element $p \in R$ is prime if $rs \in (p) \implies r \in (p)$ or $s \in (p)$.

Theorem 2.3
Every prime element is irreducible.

Proof
Suppose p is prime and you could factor it as $p = ab$. By primality, a or b is divisible by p, without loss of generality this is a. Then $a = kp$ for some k, so $p = kbp$ or $(kb - 1)p = 0$. Thus $kb - 1 = 0$ and $kb = 1$, so b and k must be units. Thus, p is irreducible.

The algorithm for creating this factorization is simple, if you have an irreducible element, just leave it. Otherwise it must be reducible; take that factor out and continue. Thus, to prove the claim, it's sufficient to show that this algorithm terminates. In other words, any chain of ideals has a largest element:

$$(r_1) \subset (r_2) \subset (r_3) \subset \cdots \subset (r)$$

If we have such a chain, note that it's finite by the following idea. Consider the union $\bigcup_i (r_i)$. Since this is an ideal and this is a PID, $\bigcup_i (r_i) = (r)$ for some $r \in R$. Furthermore, r must exist in one such ideal; that ideal must include (r), so it must be exactly (r). This property of all such chains of ideals being finite is called the *Noetherian* property. These kind of *Noetherian* rings are typically those that are finitely generated.

Theorem 2.4
Every irreducible element of a PID are prime.

Proof
Suppose $rs \in (p)$ for some $r,s \in R$. Suppose $p \in R$ is irreducible. Suppose $r \notin (p)$. But this means that $(r, p) \supsetneq (p)$. Since R is a PID, this means $(r, p) = (a)$ for some $a \in R$. Thus, $p = au$ for some $u \in R$ Thus, a is a unit, so $(a) = (1) = (r, p)$. That means for some x, y, we can write $1 = rx + py$. Multiplying by s, then $s = rxs + pys = (rs)x + pys$, so $s \in (p)$. Thus p is prime.

Now to proceed with the proof of factorization. By this algorithm, we know we can write $0 \neq r = \prod_{i=1}^{m} p_i^{a_i}$ as a product of primes (which are the same as irreducibles). Suppose there was another factorization $r = \prod_{i=1}^{n} q_i^{b_i}$. We claim that $\{p_i\}$ and $\{q_i\}$ (and associated exponents) are just the up to permutation and units. The proof is induction on $\sum_i a_i$: just take one of the primes on the left; it must divide one of the factors on the right by the definition of prime. Thus, divide on both sides and you reduce the a_is by 1 (perhaps you get some units as left-overs, we can ignore these).

2.2 Classification of Finitely-Generated Modules (Cont'd)

Recall the theorem we attempted to show last time.

Theorem 2.5
Suppose M is a finitely-generated module over a PID. then $M \cong \bigoplus_i M_i$, where each M_i is cyclic (generated by one element).

Multiplication by an element of a ring becomes a homomorphism on modules; in general this is a representation: which turns group elements into transformations. Recall we started the proof with the following construction. Take the torsion submodule

$$M_{\text{tors}} = \{m \in M \mid \exists r \neq 0 \in R, rm = 0\}$$

The claim is that $(M/M_{\text{tors}})_{\text{tors}} = \{0\}$, i.e. M_{tors} is torsion-free. Consider $\overline{m} \in M/M_{\text{tors}}$ such that $r\overline{m} = 0$ for some $r \neq 0$. This means that $rm \in M_{\text{tors}}$, so there exists $s \in R$ which is nonzero such that $srm = 0$. Since $m \in M_{\text{tors}}$, we're done. Consider the canonical homomorphism $M \to M/M_{\text{tors}}$. Why don't we just pick one representative from each coset? Usually this doesn't create a submodule, but it does here because the module is free.

Theorem 2.6
Any torsion-free finitely-generated module over a PID R is free (which means $\cong R^{\oplus n} = R^n$).

We first need the following lemma.

Lemma 1 *If $M \subset R^n$ is a submodule of the free module of rank n, then M is free of rank $\leq n$.* □

Definition 2.7
If $p \in R$ is prime, then $R/(p)$ is a field. Thus for any free R-module M, M/pM is a module over $R/(p)$ (in other words, a vector space). The rank of M is the rank of this vector space. Rank is well-defined for free modules. Equivalently, we can say that the rank is the maximal set of linearly independent elements that generate the module.

Clearly rank $R^n = \dim_{R/(p)} R^n/pR^n = (R/(p))^n$. Now let's prove our lemma by induction on n. If $n = 1$, then we have $M \subset R$. This means it's a principal ideal $(a) \subset R$ (as rings), but as R-modules, $(a)_{\text{module}} = aR \cong R^1$. Then for the inductive step, we know We know that $R^{n-1} \subset R^n$, so we have the exact sequence

$$0 \to R^{n-1} \to R^n \to_{\phi} R \to 0$$

we can rewrite this exact sequence for some $a \in R$:

$$0 \to M \cap R^{n-1} \to M \to (a) \to 0$$

Call $R^n = \bigoplus_{i=1}^n Rf_i$. Then we can decompose $m \in M$ as

$$m = \sum_{i=1}^{n} r_i f_i = \sum_{i=1}^{n-1} r_i f_i + r_n f_n$$

This means $\phi(m) = r_n$. This means $M = M \cap R^{n-1} \oplus aRf_n$. The first one is a subset of R^{n-1}, so it is a module of rank at most $n-1$ (by induction, free) and the second one is just R (so, free). Thus we get rank n.

Lemma 2 *If R is a PID and M is finitely generated over R and $M' \subset M$, then M' is finitely generated.*

Proof
There exists a surjective homomorphism $\phi : R^n \to M$ for some n, by the definition of direct sum. Call $M' \subset M$

and call $F = \phi^{-1}(M')$. By lemma, F is a free module of rank at most n and we have a surjective homomorphism from it to M'. Thus, it is generated by at most n elements.

Now we can prove the theorem. Suppose M is torsion-free that is finitely generated. Let's take a maximal set of linearly independent elements from M (note that this is always finite; if we have an increasing chain of inclusions, the module is finitely generated so there exists a finite set that contains every submodule). Call this set

$$f_1, \ldots, f_n \text{ where if } \sum_n r_n f_n = 0, r_n \in R \implies \text{all } r_n = 0$$

Now $M/(f_1, \ldots, f_n)$ has torsion, because if $g \in M, g \notin (f_1, \ldots, f_n)$ then there exists r_i's and r such that $\sum_i r_i f_i + rg = 0$ where not all the coefficients are 0 (and r cannot be either). So $r \cdot \overline{g} = 0$. Thus, $M/(f_1, \ldots, f_n)$ has all elements torsional.

Now consider all such g which are generators. This shows that if we take their r's and multiply them together to make $s \neq 0$, we can annihilate these generators and thus $sM \subset \sum_i R_i f_i \cong R^n$. But $M \cong sM$. So M is free. We claim this means that

$$M \cong M_{\text{tors}} \oplus M/M_{\text{tors}}$$

Clearly these are free modules–we just need to show that the canonical homomorphism is a splitting map, meaning it truly creates a direct sum.

Proof
Suppose $M/M_{\text{tors}} = \bigoplus_{i=1}^n R\overline{f}_i$ for some $f_i \in M$. Consider $\bigoplus Rf_i \subset M$, where f_i are some representatives of the barred versions. By our theorem, $\bigoplus Rf_i$ is free and $\bigoplus Rf_i \cap M_{\text{tors}} = 0$. Also, we can write $m \in M$ as $m' + m''$ with $m' \in M/M_{\text{tors}}$ and $m'' \in M_{\text{tors}}$, by the definition of quotient. Thus, the direct sum is indeed valid.

Theorem 2.8
If M has torsion and finitely generated, then M naturally splits as $M \cong \bigoplus_{\text{primes } p} M(p)$ where $M(p) = \{m \in M \mid p^k m = 0 \text{ for some } k \geq 0\}$.

Proof
There exists a nonzero element $r \neq 0 \in R$ such that $rM = 0$. In fact $M = \bigoplus_{p|r} M(p)$.

3 Lecture 3

3.1 Classification of Finitely-Generated Modules

Recall that for a PID R and a finitely generated R-module M we showed that $M/M_{\text{tors}} = F = R^n$ is a free module. Suppose we have the exact sequence:

$$\cdots \to M \to_{\phi} N \to 0$$

this means $M \cong N \oplus \ker\phi$. We claim this is true if and only if there exists $N' \subseteq M$ such that $\phi\Big|_{N'} : N' \to N$ is an isomorphism.

Note that if $M \cong N \oplus \ker\phi$, it's clear that there exists an isomorphism that identifies a part of M and N. To show that $M \equiv N' \oplus \ker\phi$ we need to show $N' \cap \ker\phi = \{0\}$ and $N' + \ker\phi = M$. The first statement follows because $N' \cap \ker\phi = \ker\phi\Big|_{N'} = \{0\}$ since it's an isomorphism. Furthermore, for some $m \in M$, take $\sigma = \phi|_{N'}^{-1}$ (the **section** or right-inverse of ϕ) and $\sigma \circ \phi(m) = m' \in N'$. Then $\phi(m' - m) = \phi(m) - \phi(m) = 0$. Thus, $m' - m \in \ker\phi$, so $m = m' - k$ and we are done.

Going back to M, we can pick a basis to write $R^n = \bigoplus_{i=1}^n Rf_i$

$$\phi : M \to R^n, f_i' \mapsto f_i$$

$\phi(f_i') = f_i$, then $\bigoplus_{i=1}^n Rf_i' \cong R^n$ because the f_i' are linearly independent. Thus $M \cong M_{\text{tors}} \oplus R^n$.

Now, assume M is a finitely generated torsion module over R PID. Recall we defined

$$M(p) = \{m \in M \mid p^k m = 0 \text{ for some } k\}$$

Theorem 3.1
We can write such a module as a direct sum.

$$M = \bigoplus_{p \text{ prime in } R, (p) \supset \operatorname{ann}_R(M)} M(p)$$

Proof
Look at $M(p) \cap \bigoplus_{(q)\neq(p)} M(q)$. If $m \in M(p) \cap \bigoplus_{(q)\neq(p)} M(q)$, then $p^k m = 0$ and $m = \sum_{i=1}^s m_i$ where $q_i^{k_i} m_i = 0$. Then m is annihilated by $Q := \prod_{i=1}^s q_i^{k_i}$. Note that $Q \notin (p)$ because none of the $q_i \in (q_i)$. Thus $(p^k, Q) = (1)$. So we can write $1 = ap^k + bQ$ and $m = ap^k m + bQm = 0$. Thus, the disjointness condition is met.
Note that $\operatorname{ann}_R M = (a)$, since if we multiply two annihilators, then we get another annihilator (and thus end up with an ideal). Furthermore, it's not just 0, because there are the annihilators of the f_i, which we can multiply together to get an annihilator (an infinite counter-example is $M = \oplus_{i=1}^\infty \mathbb{Z}/(2^i)$) Let's factorize $a = \prod p_i^{k_i}$.
Now consider a small case of two ideals $M = M(p) \oplus M(q)$. Then $\operatorname{ann}(M(p) \oplus M(q)) = p^k q^\ell$ for some k, ℓ. Note that $p^k M \subseteq M(q)$ and $q^\ell M \subseteq M(p)$. Also, we can write $1 = bp^k + cq^\ell$, meaning $m = bp^k m + cq^\ell m \in M(q) \oplus M(p)$.
To do it in general, write $a = p^k \cdot Q$ where p and Q are coprime. Then $1 = p^k b + Qc$ and $m = bp^k m + cQm$. Note $bp^k m \in M(Q)$ and $Qcm \in M(p)$, so $m \in M(Q) \oplus M(p)$. By induction on the number of prime factors of a, we get the claim.

Finally, suppose M is a module with $\operatorname{ann} M = (p^a)$. $M = \sum_{i=1}^n Rf_i$. This means there exist some j such that $p^a f_j = 0$ but e.g. $p^{a-1} f_j \neq 0$. Call this f_j f_1.

Note that we cannot just always take a submodule and say it's a summand. For example, $\mathbb{Z}/4\mathbb{Z} f_1 \oplus \mathbb{Z}/2\mathbb{Z} f_2$ has a summand which is $\mathbb{Z}/2\mathbb{Z}$, but also $(2f_1, f_2) \cong \mathbb{Z}/2\mathbb{Z}$ is is a submodule; one can show however that this one is not a summand.

We will proceed by induction on the number of generators of M. Note $R/(p^a) \cong Rf_1$ by the annihilation properties. Let's rewrite $M = R/p^a + \sum_{i=2}^n Rf_i = R/p^a + \bigoplus_{i=1}^m Rg_i$ by the inductive hypothesis.

$$R/p^a \subset M \to_\phi M/Rf_1 \cong \bigoplus_{i=2}^n Rg_i$$

By the result at the beginning of lecture, we need that there exists σ such that $\phi\sigma = \mathrm{id}_{M/Rf_1}$.

Choose representatives $f_i \in M$ such that $g_i = \phi(f_i)$. To any choice of f_i, we can add any multiple of f_1, which would still be a representative. Note that two cyclic modules are isomorphic if they have the same annihilator (at least in a PID). Thus, $\operatorname{ann} g_i = \operatorname{ann}(b_i f_1 + f_i)$ if and only if $Rg_i \cong R(f_i + b_i f_1)$. Then the map $g_i \mapsto f_i + b_i f_1$ is exactly a right inverse of ϕ. (Note that $g_i \mapsto f_i$ is not even a homomorphism).

If $R/(p^a)$ has an ideal I, then $I = (p^c)/(p^a)$. So all these annhililators will purely be powers of p. Suppose $\operatorname{ann} f_i = (p^{k_i})$ and $\operatorname{ann} g_i = (p^{\ell_i})$. Furthermore, since ϕ is a homomorphism, if $a \in \operatorname{ann} f_i$, then $a \in \operatorname{ann} g_i$. So $\ell_i \leq k_i$. We want to choose b_i such that $\operatorname{ann}(b_i f_1 + f_i) = \operatorname{ann} g_i = (p^{\ell_i})$. To do this:

$$p^{\ell_i}(b_i f_1 + f_i) = b_i p^{\ell_i} f_1 + p^{\ell_i} f_i$$

But $\phi(p^{\ell_i} f_i) = p^{\ell_i}\phi(f_i) = p^{\ell_i} g_i = 0 \pmod{Rf_1}$, i.e. $p^{\ell_i} f_i \in Rf_1$. Thus $p^{\ell_i} f_i = up^{m_i} f_1$ for $u \in R$ coprime to p where we claim $m_i \geq \ell_i$, so picking $b_i = p^{m_i - \ell_i}$ is sufficient (the above expression evaluates to multiple of f_1). To see why this inequality is true, note an annihilator of $p^{\ell_i} f_i$ is $p^{k_i - \ell_i}$. Furthermore, the smallest annihilator of $p^{m_i} f_1$ is $k_1 - m_i$. Thus $k_i - \ell_i \geq k_1 - m_i$. Finally, $m_i \geq k_1 - k_i + \ell_i$ and by definition of the first one, we had $k_1 \geq k_i$. Thus, we have $m_i \geq \ell_i$.

4 Lecture 4

4.1 Uniqueness of the Structure Theorem

Let's recap last time. Suppose M is a torsion finitely-generated module over a PID R; we wish to show $M \cong \bigoplus_a R/(a)$ for some a. We saw last time that

$$M \cong \bigoplus_{p \text{prime}} M(p)$$

where $M(p) = \{m \in M \mid p^n m = 0 \text{some } n\}$. Thus, without loss of generality, we can just take $M = M(p)$ and decompose it. We will show that we can write

$$M = \bigoplus_{i=1}^{m} R/(p^{a_i})$$

Suppose we have 2 generators and $\operatorname{ann}_R M = (p^a)$. That means there exists some element g_0 such that $\operatorname{ann}_R g_0 = p^a$. Without loss of generality, this is a generator; if both generators had a smaller annihilator, then so would g_0. We wish to look at $Rg_0 \subset M \to R/(p^b \overline{g}_1)$. Note that for the other generator, $\operatorname{ann}_R \overline{g_1} = (p^b)$ for some $b \le a$. Note that if there exists h wherein $\phi(h) = g_1$ (under the canonical homomorphism) such that $p^b h = 0$, then Rg_0 and Rh form that direct sum. Currently, we only have $\phi(p^b g_1) = 0$, so $up^d g_0 = p^b g_1$ for some d. We claim that $d \ge b$, if not then g_1 is a multiple of g_0, which would contradict linear independence. This means that $p^b(up^{d-b}) = p^b g_1$. Subrtracting these two, we define $h := g_1 - up^{d-b} g_0$ and we want $p^b h = 0$. It's clear that $\phi(h) = g_1$. Now, let's induct on n.

Proof
Let $p^a = \operatorname{ann}_R M$ and let g_0 be a generator such that $p^a = \operatorname{ann}_R g_0$. Then consider the exact sequence.

$$0 \to Rg_0 \to M \xrightarrow{\phi} \overline{M} \to 0$$

Then similarly under ϕ, $h_i := g_i - p^{d_i} u_i g_0 \mapsto \overline{g_n}$. In addition, by the same argument, there exists $b_i \le d_i$ such that $p^{b_i}(h_i)$. Our claim is then the splitting is

$$M = Rg_0 \oplus \bigoplus_{i=1}^{n-1} R(g_i - p^{d_i} u_i g_0)$$

First we shall show that

$$M = Rg_0 + \sum_{i=1}^{n-1} R(g_i - p^{d_i} u_i g_0)$$

This is true just because Then, we want to show that

$$\bigoplus_{i=1}^{n-1} R(g_i - p^{d_i} u_i g_0) \cong \overline{M}$$

We claim that ϕ is a valid map. Clearly it's surjective since we can produce the $\overline{g}_i$'s. It's also an injection because we preserve orders, so the kernel can only be trivial. Finally, we show that

$$Rg_0 \cup \bigoplus_{i=1}^{n-1} R(g_i - p^{d_i} u_i g_0)$$

But if this weren't the case, then ϕ has a nontrivial kernel (the elements of Rg_0 is the kernel)

We could also carry out the proof with the splitting lemma.

Theorem 4.1
Suppose we have exact sequence $M \xrightarrow{\phi} M' \to 0$ So having a submodule $M'' \subset M$, which is isomorphic to M', then the inverse of the isomorphism is σ a splitting. So both of these conditions are equivalent.

We can refine this result further. We propose if $(q_1, q_2) = (1)$, then $R/q_1 \oplus R/q_2 \cong R/q_1q_2$.

Proof
Two generators we could pick are $(1, 0)$ and $(0, 1)$. We claim that $(1, 1)$ generates M. Since

$$\begin{aligned} 1 &= r_1q_1 + r_2q_2 \\ (1,1) &= (r_1q_1 + r_2q_2)(1,1) \\ (1,1) &= r_1q_1(0,1) + r_2q_2(1,0) \end{aligned}$$

Furthermore, by the above, $r_1q_1(1, 1) = r_1^2q_1^2(0, 1)$. But $r_1q_1(0, 1) = (0, 1)$, so we can make it; we can make $(1, 0)$ by symmetry. We can see that we can generate any element. If the annihilator of $(1, 1) = (a)$, then $a \mid q_1q_2$. Furthermore a annihilates each one separately, so $q_1 \mid a$ and $q_2 \mid a$. Thus we must have $a = uq_1q_2$ for some unit u, we know that $R/(uq_1q_2) \cong R/(q_1q_2)$, so we're done.

Now for a torsion module M, we can decompose it into

$$M = M(p_1) \oplus \cdots \oplus M(p_k)$$

where:

$$\begin{array}{llll} M(p_1) & = R/p_1^{a_{11}} & \oplus R/p_1^{a_{12}} & \oplus \dots \\ \vdots & \vdots & \vdots & \dots \\ M(p_k) & = R/p_k^{a_{k1}} & \oplus R/p_k^{a_{k2}} & \oplus \dots \end{array}$$

where $p_i^{a_{ij}} \mid p_i^{a_{ik}}$ for $j \leq k$. We can instead sum the columns now

$$M \cong R/p_1^{a_{11}} \dots p_k^{a_{k1}} \oplus R/p_1^{a_{12}} \dots p_k^{a_{k2}} \oplus \dots$$

The torsion free part is free, so we can just use $R/(0)$ for those (if you like 0 to be prime).

Theorem 4.2
If we order the denominators in increasing order

$$M \cong M/q_1 \oplus R/q_2 \oplus \dots$$

with $q_1 \mid q_2 \mid \dots$, this decomposition is unique.

For M/p_1M for some prime p, we know it's isomorphic to a vector space R/p^{n_1} with dimension n_1. But under the theorem, then:

$$M/p_1M = R/(q_1, p_1) \oplus R/(q_2, p_1) \oplus \dots$$

When $(q_i, p_1) = (1)$, we get the 0 module, otherwise we get a non-trivial module. Thus, n_1 is just the number of q_i divisible by p_1. This means noting that $p_1R/q_i \cong R/(q_i/p_1)$.

$$p_1M = \bigoplus_{p_1 \mid q_i} p_1R/q_i$$

we make inductive progress because the sum of the powers of the prime factorizations of q goes down. Thus, the number of q's divisible by a certain prime is unique (due to the rank of the vector space).

4.2 Applications to Linear Algebra

Suppose we have a linear map $A : V \to V$ which is an endomorphism on finite-dimensional vector space V over field k. Now, defining $R = k[x]$, we can define an R-module structure on V by extending with $x \cdot v = Av$. This is a principal ideal domain, (it's Euclidean by polynomial division). In this ring, prime elements are just irreducible polynomials. By the structure theorem

$$V \cong \bigoplus_{f_i \text{irreducible}} \frac{k[x]}{f_i(x)}^{a_i}$$

Let's analyze the factor module $k[x]/f(x)$ where $f = x^d + a_1 x^{d-1} + \cdots + a_d$ has degree d. Then a basis for this module is $1, x, x^2, \ldots, x^{d-1}$. What does the matrix look like when using this basis?

$$\tilde{A} = \begin{pmatrix} 0 & 0 & \ldots & -a_d \\ 1 & 0 & \ldots & -a_{d-1} \\ 0 & 1 & \ldots & -a_{d-2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & \ldots & -a_1 \end{pmatrix}$$

Now suppose $V \cong k[x]/f^2$. Then we can take a basis that looks like $1, x, \ldots, x^{d-1}, f, xf, \ldots, x^{d-1}f$. Now what does the matrix look like?

$$\tilde{B} = \begin{pmatrix} \tilde{A} & \mathbf{0} \\ \mathbf{0}' & \tilde{A} \end{pmatrix}$$

where the $\mathbf{0}'$ has a 1 in the top right. Note that $\det(A - tI_d)$ is a polynomial in t which annihilates this whole thing.

5 Lecture 5

5.1 Modules over Arbitrary Rings

For a ring R, a left-module is an abelian group M with a pairing $R \times M \to M$ which we will apply as multiplication. This action is associative and distributive, as usual.

Theorem 5.1
If $0 \to M' \to M \xrightarrow{b} M'' \to 0$ is a short exact sequence and a map from a free module $c : F \to M''$, then there exists a map $d : F \to M$ that makes the diagram commute.

Proof
Write $F \cong \bigoplus_i Re_i$. Then, $c(e_i) = m_i$ for some m_i. Since the map b is onto, there exists n_i such that $b(n_i) = m_i$. Thus, define d as the map sending $e_i \to n_i$ and extending by linearity.

As a special case, if $0 \to M' \to M \xrightarrow{b} F \to 0$ is exact, then we can take $c = \mathrm{id}_F$, so there exists $d : F \to M$ where the composition of b and d yields identity; this is a section. So $M \cong F \oplus M'$.

Definition 5.2
P is projective if given $b : M \twoheadrightarrow M''$ and a map $c : P \to M''$, there exists $d : P \to M$ such that $bd = c$.

Example 5.3
Consider the following polynomial ring:

$$R = \frac{k[x_1, x_2, x_3, y_1, y_2, y_2]}{(\sum_{(y_1,y_2,y_3)} x_i y_i = 1)}$$

gives us exact sequence $0 \to R \to R^3 \to P \to 0$.

The nice thing about looking at things categorically is that we can turn around the arrows involved.

If R is an **injective** R-module when considering $0 \to E \to M \to M'' \to 0$, the property from before holds with all the arrows reversed.

For example we showed that for a PID R, if M is a torsion module and $p \in R$ is a prime such that $p^a M = 0$, which is equivalent to M is an R/p^a-module. We showed that then, $R' := R/p^a$ is a summand of M.

5.2 Groups

Definition 5.4
A **group** is a set with one operation $G \times G \to G : (a, b) \mapsto b$. This operation is associative, has a unit, and has inverses.

There's a school of thought that thinks this definition is not very good. How do they define a group?

Definition 5.5
A **group** is a set of permutations (bijections) of a given set S. This set should be closed under composition and inverses.

To see that these notions are equivalent, we can take $S = G$; then group multiplication is a group action of G on itself. Since these actions have inverses (multiplication by g^{-1}), all of them are permutations.

Every permutation can be written as a product of unique disjoint cycles (up to order of factors). To see this, consider the following greedy algorithm:

1. Take some element $a \in S$. See where it maps to in finite compositions of the permutation.
2. Whatever it doesn't ever lead to, create a new cycle starting with it.
3. Repeat this until you run out of elements.

We will denote a cycle as $[a_1, \ldots, a_r]$.

Definition 5.6
A G-set S is a set with action $A : G \times S \to S$ (a homomorphism from $G \to \mathrm{Perm}(S)$ where $(gh)(s) = g(h(s))$), where $(g, s) \to g(s)$ where the submap $s \to g(s)$ is a permutation.

Definition 5.7
The action of G on its G-set is **transitive** (or the set itself) if for any $s \in S$, we have $Gs = S$.

Not all actions are transitive. For example, take $G = \mathbb{Z}/2$ and act on the set $\{1, 2, 3\}$, which we denote as $\mathbb{Z}/2 \hookrightarrow \{1, 2, 3\}$. Consider the action sending $0 \to \mathrm{id}$ and $1 \to [1, 2]$.

Theorem 5.8
Every G-set is the disjoint union of transitive G-sets.

To see this, just decompose S into its orbits, for example, the orbit of 1 and 2 are $\{1, 2\}$ and the orbit of 3 is $\{3\}$.

Definition 5.9
Consider S is a G-set and $s \in S$. Then the **orbit** of s is $Gs = \{gs \mid g \in G\}$.

Consider G acting on S transitively. What elements of G have an element $s \in S$ as a fixed point?

Definition 5.10
The **Stabilizer** of an element s as

$$\mathrm{Stab}_G(s) = G_s = \{g \in G \mid gs = s\}$$

This is a subgroup of G.

It turns out, once you figure out what the stabilizer is for one element for a transitive action, you have uniquely determined the action.

Definition 5.11
A **subgroup** $H \leq G$ for group G is a subset of G which is itself a group. For strict containment, we have $H < G$.

Definition 5.12
A coset of $H \leq G$ is a $gH \subseteq G$, e.g. $gH = \{gh \mid h \in H\}$. The set of cosets is denoted as G/H.

Two cosets gH and kH for $g, k \in G$ are either equal or disjoint. If $gH \cap kH \neq \emptyset$, then for $h, h' \in H$

$$\begin{aligned} gh &= kh' \\ ghH &= kh'H \\ gH &= kH \end{aligned}$$

As a corollary, we get that

Theorem 5.13
If for finite G, $H \leq G$, then $|H| \mid |G|$.

Proof
$G = \bigcup_{g \in G} gH$, some set of which are disjoint, and all of the cosets are the same size.

Finally, it turns out we can identify these two things.

Theorem 5.14
The set of cosets of $H \leq G$ is a G-set with action $g(g'H) = (gg')H$. If $G \hookrightarrow S$ is transitive and $G_s = H$, then there is a bijection from S to the set of cosets of H which preserves the action of G.

Proof
Note that $\text{Stab}_G H \in G/H$ is exactly H. $(g, s) \to gH$ is clearly a surjection, because the action is transitive. Furthermore, $gs = g's$, then $g'^{-1}gs = s$, so $g'^{-1}gH = H$, meaning that $gH = g'H$, so we get the same coset. So the map is an injection too. We can also multiply elements of S by arbitrary group elements and get the exact same structure, proving the theorem.

6 Lecture 6

Definition 6.1
The symmetric group on a set S, Σ_S is the set of all permutations of S.

If we have G acting on a set S, then there should be a homomorphism identifying $G \to \Sigma_S$. One would think that the stabilizer of some element would then be the kernel of this homomorphism. However, stabilizer group that we had before need not be normal.

Theorem 6.2
A subgroup $N \leq G$ is **normal** if $gN = Ng$ for all $g \in G$.

Theorem 6.3
If $\varphi : G \to H$ is a map between groups, then $\ker \varphi$ is a normal subgroup of G.

Proof

$$h \in \ker \varphi \implies \varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = 1\varphi(g)\varphi(g^{-1}) = 1$$

Theorem 6.4
If N is normal, then the map $G \to G/N$ can be made a map of groups, with $gN \cdot g'N = gg'NN = gg'N$.

Theorem 6.5
Given any map of groups $G \xrightarrow{\varphi} H$ sending $N \to 1$ then there exists unique factor map f such that $\varphi = f \circ \sigma$, where σ is the canonical homomorphism $G \xrightarrow{\sigma} G/N$.

Now consider G acting on S transitively. Suppose for some $s \in S$, $H = \text{Stab}(s)$. We said last time that $S \cong G/H$. Then we wish to identify the kernel of the map $G \xrightarrow{\tau} \Sigma_{G/H}$. But now consider the stabilizer of $g'H$, e.g. $G_{g'H}$. Suppose $g \in G_{g'H}$. This means $g(g'H) = g'H$ so for all $h \in H$, $gg'h = g'h'$. But rearranging, this means that $g'^{-1}gg' \in H$. Thus $g \in g'Hg'^{-1}$,

Thus, we have that $\ker \tau = \bigcap_{g' \in G} G_{g'H} = \bigcap_{g' \in G} g'Hg'^{-1}$. This is the biggest normal subgroup of H.

Theorem 6.6
Consider $H < G$. $g \in G$ normalizes H if $gHg^{-1} = H$. The normalizer $N_G(H)$ is the set of all g that normalize H.

Notice that the act of conjugation by some element $g \in G$ is an automorphism from G to itself, which induces a map $G \to \text{Aut}G$.

Theorem 6.7
Let $H, K < G$. $K \subseteq N_G(H) \implies KH = HK$ and furthermore, $KH < G$ (i.e. it's a group).

Theorem 6.8
In this setting, H is a normal subgroup of HK and $K \cap H$ is normal in K, so $HK/H \cong K/(K \cap H)$.

Proof
We have that $(HK)H = H(KH) = H(HK)$, which is what we needed to show. Furthermore, we need $(H \cap K)K = K(H \cap K)$. But $KK = KK$ and $HK = KH$, so this is also true. Finally, to see the isomorphism, use the map $\varphi : k(H \cap K) \mapsto kH$ for some $k \in K$. Note that if $k \in H \cap K$, then $k \in H$ so this maps $H \cap K$ to H. If not, then we get some other subgroup. One can easily check that multiplication is preserved. Finally, note that φ is surjective, since all $k \in K$ end up multiplying H. Now, $\ker \varphi$ is precisely $\{H \cap K\}$, meaning we're done.

Definition 6.9
The **centralizer** of $H < G$ is $Z_G(H) = \{g \in G \mid gh = hg \; \forall h \in H\}$. The **center** of $Z(G)$ is the centralizer of G.

Let's learn about a new group.

Definition 6.10
$GL_n(F)$ over a field F is the general linear group, composed of all invertible $n \times n$ matrices.

How can we find $|GL_n(\mathbb{F}_p)|$? If I fix a basis $\mathbb{F}_p^n = \bigoplus_{i=1}^n F_p e_i$, how can we send the basis vectors? e_1 has $p^n - 1$ choices (excluding 0), e_2 has $p^n - p$ choices, e_3 has $p^n - p^2$ choices and so on. Thus

$$|GL_n(\mathbb{F}_p)| = \prod_{i=1}^{n} p^n - p^{i-1}$$

What are the subgroups of this group? The upper triangular matrices with all 1s on the diagonal, called the group of unipotent matrices U, forms a group. It also forms a $\mathbb{F}_p$-vector space. Namely, there are p choices for each upper entry, giving

$$|U| = p^{\sum_{i=1}^n i-1} = p^{\binom{n}{2}}$$

Note that this is the biggest power of p that divides the group order. It turns out this is enough to show that every group has a subgroup of this kind.

Theorem 6.11
Let G be a finite group.

1. Every p-subgroup (i.e. a subgroup with order a power of p) is contained in a Sylow p-subgroup (i.e. a subgroup with order the largest power of p).
2. Any 2 Sylow p-subgroups are conjugate, i.e. the conjugation action acts transitively on the set of Sylow p-subgroups.
3. The number of Sylow p-subgroups is congruent to $1 \pmod p$.

7 Lecture 7

Recall that in the past we proved the following facts.

1. If $H \leq G$ and $K \leq N_G H$ then $H \triangleleft KH \leq G$. In addition, $KH/H \cong K/(K \cap H)$. The isomorphism is taking an element from K and mapping it to $k \cdot 1 \pmod H$.
2. If $H \leq G$ then G acts on the set of cosets of H, G/H (who divide up the space). The disjoint union $\bigcup_g gH = G$ and $|G| = |H| \cdot \#$ of cosets of H. Then $\mathrm{Stab}_G(gH) = gHg^{-1}$.
3. Every G-set is a disjoint union of transitive G-sets. Each transitive G-set is isomorphic to G/H where H is the stabilizer of some element in each transitive class.
4. A Sylow p-subgroup is a subgroup of order a power of p where the power of p is maximal.
5. Recall $GL_n(\mathbb{F}_p)$ is the general linear group (group of invertible matrices) with elements in $\mathbb{F}_p$ for p prime. Every finite group can be embedded in this group, i.e. there exist a homomorphism from $G \to GL_{|G|}(\mathbb{F}_p)$. To see this, take $\mathbb{F}_p[G] = \bigoplus_{g\in G} \mathbb{F}_p\, g$. This is a G where multiplication by the element g just acts on each component separately; this is an action on g. But, this is also representable by an invertible matrix (it's a linear transformation), so $G \subset GL(\mathbb{F}_p[G]) \cong GL_n(\mathbb{F}_p)$ (as vector spaces).
6. Recall the unipotent subgroup of $GL_n(\mathbb{F})$, as
$$U = \left\{ \begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & \dots & * \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \right\}$$
We showed last time through direct computation of the orders that $\mathbb{F}_p$ is a Sylow p-subgroup.
7. The action of a a group on a set S has orbits which sum to the set. But each orbit also divides the size of the group.

We will use this to prove Sylow's theorems.

Lemma 3 *If $H < G$ and G has a Sylow p-subgroup then so does H.*

Proof
Let P be a Sylow p-subgroup of G. Note that $p \nmid G/P$. Then $\mathrm{Stab}_G(gP) = gPg^{-1}$. Now let H act on the set of cosets of P in G. Some coset gP has an H-orbit that has order coprime to p, because the number of cosets has no factors of p. But then $\mathrm{Stab}_H(gP) = H \cap gPg^{-1}$ which means $|H(gP)| = |H|/|H \cap gPg^{-1}|$, which must not have any factor of p. So the $H \cap gPg^{-1}$ is a Sylow p-subgroup of H.

Theorem 7.1
Every p-subgroup of a finite group G is contained in a Sylow p-subgroup.

Proof
Let $H \leq G$ be a p-subgroup and $P \leq G$ is a Sylow-p subgroup. Then $[G : P]$ is coprime to p. But then consider H acting on G/P by conjugation. Since H is a p-group, every orbit has size p^m for $m \geq 0$. But $|G/P|$ is coprime to p, so there must exist an orbit of size p^0 with element gP. So $H \subset \mathrm{Stab}_H(gP) = gPg^{-1}$. But this is also a Sylow p-subgroup, since conjugacy does not change the number of elements.

As a corollary, we immediately get that any two Sylow p-subgroups are conjugate. This is the second of Sylow's theorems:

Theorem 7.2
Let G be a finite group.

1. For all prime p there exists $P < G$ which is a Sylow p-subgroup.
2. Any two Sylow p-subgroups are conjugate.
3. The number of Sylow p-subgroups is congruent to 1 mod p.

Let's prove 3. We know G acts transitively on the set of Sylow p-subgroups by conjugation (call this set $\mathcal{P}$). This means the number of such subgroups is taking one of the subgroups P, $|G|/|\text{Stab}_G P| = |G|/|N_G(P)|$. But $P < N_G(P)$, which means that the number of such subgroups is coprime with p. Imagine acting P on $\mathcal{P}$. Clearly $P^{-1}PP = P$, so this orbit has size 1. Do any other orbits have size 1? This would mean $P^{-1}P'P = P'$ for $P' \neq P$ meaning that $P \leq N_G(P')$. By our previous theorem, this would mean PP' is a group, but also a p-subgroup with order strictly larger than P, which is a contradiction. But this means that the size of $\mathcal{P}$ must be $1 + \text{positive power of } p \equiv 1 \pmod p$.

7.1 Jordan-Holder Theorem

Theorem 7.3
If $G = H_0 \triangleright H_1 \triangleright H_2 \cdots \triangleright H_n \triangleright 1$ and $G = H'_0 \triangleright H'_1 \triangleright H'_2 \cdots \triangleright H_m \triangleright 1$ are both maximal chains of normal subgroups (there exist no refinements, e.g. each quotient H_i/H_{i+1} is simple), then $m = n$ and $H_i/H_{i+1} \cong H'_{\sigma(i)}/H'_{\sigma(i)+1}$ for some permutation σ.

Proof
Suppose n is minimal among all such chains. We will induct on n. $n = 1$ is just a simple group, which is trivial. Suppose the theorem is true for $n - 1$. We provide a picture. TODO: Add picture The left and middle chains and the right and middle chains are equal up to permutation by induction. $G = H_1 H'_1$ because $H_1 H'_1 \triangleright G$ and each of them are maximal (and different, lest the case is trivial), so they must be the whole group. By the isomorphism theorem, $G/H'_1 \cong H_1/H'_1 \cap H_1$. The parallelogram congruent shows that the corresponding factor groups are isomorphic, giving us the permutation.

8 Lecture 8

8.1 Semi-direct Product

Theorem 8.1
If $N \triangleright G$ and $H \leq G$ such that $H \cap N = \{1\}$ and $HN = G$, then G is the semi-direct product, i.e. $G = N \times H$ as a set, and we have the multiplication $(n, h)(n', h') = (nhn'h^{-1}, hh')$. This is isomorphic to the direct product.

8.2 Simplicity of A_n

Definition 8.2
The alternating group is the kernel of the map $\mu : \Sigma_n \to \{\pm 1\}$ which maps

$$\mu : \sigma \mapsto \frac{\prod_{i<j}(x_i - x_j)}{\prod_{i<j}(x_{\sigma_i} - x_{\sigma_j})}$$

also known as the "even" permutations.

Since Σ_n is generated by transpositions, A_n's are made up of even amounts of transpositions. Every product of odd cycles is in A_n, e.g. because $(123) = (12)(23)$. In fact, A_n

Theorem 8.3
If $n \geq 5$, then A_n is a simple group.

Proof
We will induct on n. First, for $n = 5$, note that $|A_5| = \frac{5!}{2} = 60$. We proceed by contradiction. Consider a Sylow 5-subgroup of Σ_5, call it S_5. Note that $|S_5| = 5$, and $S_5 \cong \mathbb{Z}/5$. Note that this is exactly a proper cycle of length 5. $[A_5 : \Sigma_5] = 2$, so if $S_5 \not\subset [A_5 \cap S_5 : S_5] = 2$,
Take $N \triangleleft A_5$. The first possibility is that $5 \mid |N|$, then N would be the unique Sylow 5-subgroup, which is a contradiction.

9 Lecture 9

9.1 Category Theory

Definition 9.1
A **category** is a collection of objects C with the following data

- For all $X, Y \in C$ there exists a set $\mathrm{Hom}(X, Y)$ of morphisms from X to Y.
- There are composition maps that let you compose morphisms, e.g. $\mu : \mathrm{Hom}(Y, Z) \times \mathrm{Hom}(X, Y) \to \mathrm{Hom}(X, Z)$.

These data satisfy:

- **Compositional Identity.** There exists $\mathrm{id}_X \in \mathrm{id}(X, X)$ such that for any morphisms f, g with the right domain/codomain, $f \cdot \mathrm{id}_X = f$ and $\mathrm{id}_X \cdot g = g$ (which is necessarily unique).
- **Associativity of Composition.**

Some examples of categories:

- The category Set consisting of sets as the objects and maps as morphisms.
- The category $R - \mathrm{Mod}$ consisting of R-modules as the objects and the maps as module homomorphisms.
- The category Ring consisting of rings as the objects and the maps as ring homomorphisms.
- Take a group G. Then call the category BG the category with one object O and morphisms that go $O \to O$ that are in one-to-one correspondence with the elements of G, where composition is just group multiplication. Then by the group axioms, the category axioms follow automatically.
- Let X be a space (say with a topology). Then there is a category $\mathrm{open}(X)$ whose objects are open subsets of X and the morphisms are inclusions.

Definition 9.2
A **functor** is a map between categories. That is, $F : C \to D$ is

- a map from objects of C to objects of D.
- For all $X, Y \in C$ there is a map $F_{X,Y} : \mathrm{Hom}_C(X, Y) \to \mathrm{Hom}_D(F(X), F(Y))$.

which has compatibility with id and composition.

Some examples of functors:

- Forgetful functors. There exists a functor $R - \mathrm{Mod} \to \mathrm{Set}$ where we can just "forget" the structure and just view all module homomorphisms as maps between sets.
- Representable functors: If C is a category and $X \in C$, we get a functor $\mathrm{Hom}(X, -) : C \to \mathrm{Set}$. (Note that if there's map $m \in \mathrm{Hom}(Y, Y')$, then there's a map $\mathrm{Hom}(X, Y) \to \mathrm{Hom}(X, Y')$).
- Presheaves. We make a functor $\mathrm{Open}(X)^{op} \to \mathrm{Set}$ where $U \mapsto$ functions on U and $U \subset V \mapsto$ restriction to U. We have to think of the opposite category (with the morphisms reversed) to the one above because a restriction of a function can only map from a function with a wider domain to one with a narrower domain.

Definition 9.3
An isomorphism between two objects $X, Y \in C$ is a morphism $f : X \to Y$ such that there exists another morphism $f^{-1} : Y \to X$ such that $ff^{-1} = \mathrm{id}_Y$, $f^{-1}f = \mathrm{id}_X$.

Definition 9.4
Let X_i for $i \in I$ be a collection of objects in a category C. The **product** of these objects (if it exists) is the unique object $\prod X_i$ with maps $\prod X_i \to X_i$ such that for any $Y \in C$, $\mathrm{Hom}(Y, \prod X_i) \to \prod \mathrm{Hom}(Y, X_i)$ is an isomorphism in the category of sets (where a product in the category of sets is the usual Cartesian product).

The main idea is that giving a map into $\prod X_i$ is equivalent to giving a collection of maps into each X_i'. Recall that in the category of R-modules and vector spaces, $\prod X_i$ is the set of tuples $(x_i)_{x_i \in X_i}$ where we could allow infinitely many $x_i \neq 0$. If we instead used the category of finitely generated R-modules, then the product might not exist; we can't take an infinite product and stay in the category.

Definition 9.5
The **sum** of objects X_i (if it exists) is the unique object $\bigoplus X_i$ with maps $X_i \to \bigoplus X_i$ such that for any $Y \in C$, $\mathrm{Hom}(\bigoplus X_i, Y) \to \prod \mathrm{Hom}(X_i, Y)$ is an isomorphism.

Now, in the category of R-modules, $\bigoplus X_i$ is the set of tuples $(x_i)_{x_i \in X_i}$ where for only finitely many i, $x_i \neq 0$.

Definition 9.6
Given $X, Y, Z \in C$ and maps $Z \to X$, $Z \to Y$, then the **coproduct** (if it exists) is the unique object $Y \coprod_Z X$ such that it makes the square in the following diagram commute and if there exists maps $Y \to W$ and $X \to W$ that all solid lines commute, then there exists unique $\mu : Y \coprod_Z X \to W$.

$$\begin{tikzcd}
Z \arrow[r] \arrow[d] & X \arrow[d] \arrow[ddr, bend left] & \\
Y \arrow[r] \arrow[drr, bend right] & Y \coprod_Z X \arrow[dr, dashed, "\mu"] & \\
 & & W
\end{tikzcd}$$

For example, let $C = \mathrm{Group}$. Consider the diagram:

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\times 3"] \arrow[d, "\times 2"'] & \mathbb{Z} \arrow[d] \\
\mathbb{Z} \arrow[r] & \mathbb{Z} \coprod_{\mathbb{Z}} \mathbb{Z}
\end{tikzcd}$$

$$G = \langle a, b \mid a^2 = b^3 \rangle$$

Let's understand some simple properties. We can show G is non-abelian by showing that there is a surjection from G to S_3. Define the map from the top, $1 \mapsto (123)$ and from the bottom $1 \mapsto (12)$. One can see this respects the diagram.

In addition, we can also see that G is infinite. Construct the following maps.

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\times 3"] \arrow[d, "\times 2"'] & \mathbb{Z} \arrow[d] \arrow[ddr, bend left, "\times 2"] & \\
\mathbb{Z} \arrow[r] \arrow[drr, bend right, "\times 3"'] & \mathbb{Z} \coprod_{\mathbb{Z}} \mathbb{Z} \arrow[dr, "\phi"] & \\
 & & \mathbb{Z}
\end{tikzcd}$$

We will show is ϕ is surjective. It's clear that 2 and 3 are in the image, and together they generate $\mathbb{Z}$.

10 Lecture 10

10.1 More Category Theory

Recall the definition of a category and functor from the previous lecture.

Definition 10.1
Consider two functors F, G that map objects in a category C to a category D. A **natural transformation** $\eta : F \to G$ is a set of arrows, $\eta_O : F(O) \to G(O)$ one for each object in $O \in C$, such that for every arrow $h : A \to A'$, the following diagram commutes:

$$\begin{tikzcd} F(A) \arrow[r, "\eta_A"] \arrow[d, "F(h)"'] & G(A) \arrow[d, "G(h)"] \\ F(A') \arrow[r, "\eta_{A'}"'] & G(A') \end{tikzcd}$$

We have to be careful if we say two categories are isomorphic–their collections of objects may not even form a set (they may be "too big"). Instead, we discuss categories being equivalent.

Definition 10.2
Two categories C and D are **equivalent** if there exist two functors $F : C \to D$ and $G : D \to C$ such that $F \circ G \cong \mathrm{id}_D$ (i.e. there exists a nautral transformation between) and $G \circ F \cong \mathrm{id}_C$.

Recall the definitions of product and coproduct from the previous lecture. Note that if $A = \prod_i A_i$, then $(-, A) = \prod_i (-, A_i)$ (and vice-versa, because each map from something to A is made up of maps to each A_i). Recall that $(-,A) : C \to \text{Set}$ is a contravariant functor, because it takes a morphism between say two objects B, B' called f and can give you a morphism from (B', A) to one from (B, A) made by precomposing by f. Similarly, if $B = \coprod B_i$, then we could say that for another object B', that $(B, B') = \prod_i (B_i, B')$, so $(B, -) = \prod (B_i, -)$. This one is a covariant (usual) functor.

Definition 10.3
A morphism $h : A \to A'$ is a **monomorphism** if for all morphisms f,$g : B \to A$ if $hf = hg \implies f = g$.

In the category of sets, this is an injection.

Definition 10.4
A morphism $h : A' \to A$ is a **epimorphism** if it is a monomorphism in the opposite category. That is, for all morphisms $f, g : A \to B$, that $fh = gh \implies f = g$.

In the category of sets this is a surjection.

Definition 10.5
Consider the following diagram.

$$\begin{tikzcd} A' \arrow[r, "h"] & A \arrow[r, bend left, "f"] \arrow[r, bend right, "g"'] & B \end{tikzcd}$$

h called the **equalizer** of morphisms f and g if it is thier "difference kernel" (in R modules it's exactly $h = \ker(f - g)$ as an inclusion). Specifically,

1. h is a monomorphism.

2. $fh = gh$

(Something about fiber products)

Definition 10.6
A **zero** object (if it exists) is an object 0 such that $\forall A \in \text{Obj}(C)$, there exists a unique map $(0, A)$ and a unique map $(A, 0)$. It is always unique.

Definition 10.7
Consider a map $f \in (A, B)$, then the composition of the maps $(A, 0)$ and $(0, A)$, ϕ. Then the difference kernel of f and ϕ is the **kernel** of f.

10.2 Tensor Products

Definition 10.8
Consider $C = \text{Vect}/k$, the set of vector spaces over k. Then $V \otimes_k W$ is called the **tensor product** of two such vector spaces and it is another vector space over k (it is universal). Its morphisms are exactly the set of bilinear maps from $V \times W \to U$. That is, $\phi(\alpha v + s, w) = \alpha\phi(v, w) + \phi(s, w)$ and the same for the other coordinate. If one fixes a factor, then it's a homomorphism.

For example, let us show $k^2 \otimes k^3 \cong k^6$. Let e_1, e_2 be a basis for the first vector space and f_1, f_2, f_3 be a basis for the vector space. We want $\phi(e_i, f_j)$ to map to a new basis element $g_{ij} = e_i \otimes f_j$. It's easy to check this map is bilinear and an isomorphism.

Theorem 10.9
Consider three vector spaces U, V, W. $(V \otimes W, U) \cong (V, (W, U))$

Proof
The left side is a bilinear map from $v, w \mapsto u$. But if one fixes v, then this is just a linear map from W to U, and it depends linearly in v. The other direction is obvious by currying. Thus, the two sides are equivalent.

10.3 Adjoint Functor

Note that there is a forgetful functor F : Group $\to$ Set where we destroy the structure. Similarly, we can use H : Set $\to$ Group where we turn a set into a free groups. But note the morphisms $(H(S), G) \cong (S, F(G))$. We call such functors an **adjoint pair**.

11 Lecture 11

I missed this lecture. Some stuff I know was discussed:

Definition 11.1
An **Abelian category** is a category C where

-

12 Lecture 12

12.1 Limits and Colimits

Suppose we have a diagram with lots of arrows. Then its limit M is the universal object where this diagram commutes.

$$\underset{\longleftarrow}{\lim} \begin{tikzcd} & B \arrow[dr] & \\ A \arrow[ur] \arrow[dr] & & H \\ C \arrow[r] & D & \end{tikzcd} = \begin{tikzcd} & & B \arrow[dr] & \\ M \arrow[urr] \arrow[r] \arrow[urrr, bend left] \arrow[dr] \arrow[drr] & A \arrow[ur] \arrow[dr] & & H \\ & C \arrow[r] & D & \end{tikzcd}$$

Definition 12.1
The **limit** of a diagram (set of maps) is a set of maps from some other object M to all the objects such that the new and old maps together commute such that M is universal; e.g. if there is a another object N satisfying this, then there is a map $N \to M$ making all the maps commute.

For example, if I have the diagram:

$$\begin{tikzcd} A \arrow[r, bend left] \arrow[r, bend right] & B \end{tikzcd}$$

Then its limit is exactly the equalizer.

Suppose we work in the category of commutative rings. Let (R, m) be a local ring, e.g. m is the only maximal ideal. Then if we take a limit of the diagram $\cdots \to R/m^2 \to R/m$, we call $\hat{R}_m$ the **completion** of the rings. If we use $\mathbb{Z} \supset (p)$, then if we have $\cdots \to \mathbb{Z}/p^2 \to \mathbb{Z}/p$, the limit of this diagram is $\hat{Z}_p$, the p-adic numbers.

If we have a diagram with no arrows, the limit is just the product. Similarly, if we have a diagram with arrows, the limit is just the co-product.

Definition 12.2
Consider two categories $\mathcal{C}, \mathcal{D}$. Then $F : \mathcal{C} \to \mathcal{D}$ is left-adjoint to $G : \mathcal{D} \to \mathcal{C}$ (or G is right adjoint to F) if $(F(-), -) \cong_\eta (-, G)$, where we mean these two objects are naturally equivalent in the sense that if there exists a map $\phi : B \to C$, then the following diagram commutes:

$$\begin{tikzcd} (FA, B) \arrow[r, "\eta_{AB}"] \arrow[d, "(FA,\phi)"] & (A, GB) \arrow[d, "(A,G\phi)"] \\ (FA, C) \arrow[r, "\eta_{AC}"] & (A, GC) \end{tikzcd}$$

AND if there exists a map $\psi : D \to A$, then the following diagram commutes:

$$\begin{tikzcd} (FA, B) \arrow[r, "\eta_{AB}"] \arrow[d, "(F\psi,B)"] & (A, GB) \arrow[d, "(\psi,GB)"] \\ (FD, B) \arrow[r, "\eta_{DB}"] & (A, GB) \end{tikzcd}$$

with all the η's being isomorphisms.

Theorem 12.3
If $F : \mathcal{C} \to \mathcal{D}$ is left-adjoint to $G : \mathcal{D} \to \mathcal{C}$ and $\mathcal{A} \subset \mathcal{C}$. If $\operatorname{colim} \mathcal{A}$ exists, then $F(\operatorname{colim} \mathcal{A}) = \operatorname{colim} F(\mathcal{A})$.

Proof
We note the following. By definition, $(\operatorname{colim} \mathcal{A}, B) = (\mathcal{A}, B)$ and

$$(F(\operatorname{colim} \mathcal{A}), B) = (\operatorname{colim} \mathcal{A}, GB) = \lim(\mathcal{A}, GB) = (F(\mathcal{A}), B) = (\operatorname{colim} F(\mathcal{A}), B)$$

12.2 (Covariant) Yoneda Lemma

Theorem 12.4
Consider a functor $F : \mathcal{C} \to \text{Set}$ and let $P \in \mathcal{C}$. $((P, -), F(-)) \cong F(P)$ e.g. the natural transformations from $(P, -)$ to F are naturally equivalent to $F(P)$.

Proof
Let $\gamma_P : ((P, -), F(-)) \to F(P)$ be the map we want one way and $\eta_P : F(P) \to ((P, -), F)$. Let $\alpha \in ((P, -), F(-))$ a natural transformation, where we write $\alpha_Q : (P, Q) \to F(Q)$. Then, define $\gamma(\alpha) = \alpha_P(\mathrm{id}_P) \in F(P)$. Now for $x \in F(P)$, $\eta(x)$ should give us back a map $(P, Q) \to F(Q)$ for each Q. So, define $\eta(x)_Q(\phi) = F(\phi)(x)$ (since $F(\phi) \in (F(P), F(Q))$). We will first show this is an isomorphism of sets. We want to show that $\gamma(\eta(x)) = x$. By definition:

$$\begin{aligned} \gamma(\eta(x)) &= (\eta(x))_P(1_P) \\ &= F(1_P)(x) = 1_{F(P)}(x) = x \end{aligned}$$

We also have to show the other way around $\eta(\gamma(\alpha)) = \alpha$. It's suffices to prove that for any Q and map $\phi : (P, Q) \to F(Q)$, $\eta(\gamma(\alpha))_Q(\phi) = \alpha_Q(\phi)$. Then:

$$\begin{aligned} \eta(\gamma(\alpha))_Q(\phi) &= \eta(\alpha_P(1_P))_Q(\phi) \\ &= F(\phi)(\alpha_P(1_P)) \end{aligned}$$

But now we can use naturality. Note that the following diagram commutes.

$$\begin{tikzcd} (P,P) \arrow[r, "\alpha_P"] \arrow[d, "{(P,\phi)}"] & F(P) \arrow[d, "F(\phi)"'] \\ (P,Q) \arrow[r, "\alpha_Q"'] & F(Q) \end{tikzcd}$$

This means that $F\phi\alpha_P = \alpha_Q(P, \phi)$ and $\alpha_Q(P, \phi)1_P = \alpha_Q(\phi)$, so we're done.

Consider a category with a single element, which is a ring R, where the hom set $(R, R) = R$, then there is a functor $\text{Ab} = FR = M$ acting on itself something about (TODO)

12.3 Sheaves and Pre-sheaves

Definition 12.5
Let X be a topological space. Then Cat X can be viewed as a category whose objects which are open subsets of X and an arrow between U and V if $U \subset V$. A presheaf of X is a contravariant functor $\text{Cat}\, X \to \mathcal{D}$. For any covering $U_i \subset U$. Let f be a presheaf. Then $f(U_i) \to f(U_j)$ whenever $U_j \subset U_i$. f is a sheaf if $f(U) = \lim f(U_i)$.

13 Lecture 13

13.1 Polynomials

Theorem 13.1
If k is a field, then $k[X]$ is a principal ideal domain (and hence a unique factorization domain).

This statement is clear with division with remainder making $k[X]$ a Euclidean domain.

Theorem 13.2
If $f, g \in R[X]$ such that the leading coefficient of g is a unit, then there exist $q, r \in R[x]$ such that $f = qg + r$ where $\deg r < \deg g$.

We now wish to prove the following theorem.

Theorem 13.3
If R is a unique factorization domain, then $R[X]$ is also a unique factorization domain.

Definition 13.4
Let R be a UFD, and k is the field of fractions of R. Then the **content** of a polynomial $f \in k[X]$, calling its coefficients a_i

$$\operatorname{cont}(f) = \prod_{\text{primes } p \in R} p^{\min_i \operatorname{order}_p(a_i)}$$

This is defined up to a unit. If R is a PID, then this is just the gcd of the coefficients of f.

Example 13.5

- Pick $R = k[u, v]$. Note that this is NOT a PID, but it is a UFD. Then take $f = uX + v \in R[X]$. We would define $\operatorname{cont}(f) = 1$, since there is no prime that divides everything.
- Let $R = \mathbb{Z}$, so $k = \mathbb{Q}$. Then let's compute $\operatorname{cont}\left(6x^2 + \frac{15}{4}x + \frac{12}{5}\right)$. Then $\operatorname{order}_2(6) = 1$, $\operatorname{order}_2\left(\frac{15}{4}\right) = -2$, $\operatorname{order}_2(\frac{12}{5}) = 2$, so the minimum is -2. Likewise all the coefficients have order 1 of three and the last one has order -1 of 5. No other primes are relevant here. Thus, $\operatorname{cont}\left(6x^2 + \frac{15}{4}x + \frac{12}{5}\right) = \frac{1}{4} \cdot 3 \cdot \frac{1}{5}$.

The key lemma is Gauss' lemma.

Theorem 13.6 (Gauss' Lemma)
Let R be a UFD and $f, g \in k[X]$ where $k = \operatorname{Frac} R$. Then $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$.

Proof
If $c \in k$, then it's clear $\operatorname{cont}(cf) = c \operatorname{cont}(f)$ (you would bump up all the orders based on the primes within c). Thus, it suffices to consider the case when $\operatorname{cont}(f) = \operatorname{cont}(g) = 1$ (these are called primitive polynomials, and necessarily $f, g, fg \in R[X]$). Consider arbitrary prime $p \in R$. Let $f = \sum a_i X^i$ and $g = \sum b_i X^i$. Let a_r be the smallest coefficient of f that p does not divide (this must exist because if p divided everything, the content wouldn't be 1). Define b_s similarly for g. Now, let's look at the X^{r+s} coefficient in fg.

$$c_{r+s} = \cdots + a_{r+1}b_{s-1} + a_r b_s + a_{r-1}b_{s+1} + \ldots$$

Every term except $a_r b_s$ is divisible by p, since there's only one that p doesn't divide, it doesn't divide the sum. This means there's no prime that divides every single coefficient in fg, so $\operatorname{cont}(fg) = 1$.

We have a nice corollary. If for a UFD R, $f \in R[X]$ is monic and $f = gh$ where $g, h \in k[X]$ and also monic, then actually $g, h \in R[X]$. To see this with Gauss' lemma just note that $\operatorname{cont}(f) = 1 = \operatorname{cont}(g)\operatorname{cont}(h)$. Since g, h are monic, $\operatorname{cont}(g) \notin (1), \operatorname{cont}(h) \notin (1)$. Thus, $\operatorname{cont}(g), \operatorname{cont}(h)$ are units.

A common trick that's useful is if $f \in R[X]$ and $f = gh$ for $g, h \in k[X]$, then we can rescale $f = \operatorname{cont} f \frac{g}{\operatorname{cont} g} \frac{h}{\operatorname{cont} h}$. But $\frac{g}{\operatorname{cont} g} \in R[X]$ and same for h. This means any reducible R polynomials over $\operatorname{Frac} R[X]$ are actually reducible over R. In other words, a polynomial irreducible over R if and only if it is irreducible over $\operatorname{Frac} R$.

Theorem 13.7
If R is a UFD, then $R[X]$ is a UFD.

Proof
Existence of a Factorization
Let $f \in R[X]$ and let $k = \operatorname{Frac} R$. Since $k[X]$ is a UFD, we know we can factor $f = p_1 \ldots p_r$ where $p_i \in k[X]$. But by the above, we can instead use polynomials in $R[X]$. The p_i are still irreducible in $k[X]$, so dividing by their content is will be irreducible in $R[X]$; the only threat is an R factor coming out. But any R factor shared between the coefficients would've already been removed by dividing by the content.
Uniqueness of Factorization
Suppose $f = \operatorname{cont}(f)p_1 \ldots p_r = \operatorname{cont}(f)q_1 \ldots q_s$ are two prime factorizations in $R[X]$. Recall all the primes are either constant polynomials which are prime in R, or content-1 higher degree polynomials. We do not need to worry about the constant polynomials and the constant in front, as R is a UFD and this can already be factored uniquely. Thus, we can assume $\operatorname{cont} p_i = \operatorname{cont} q_i = 1$. We know that $k[X]$ being a UFD, so we can factor f in the field to show that $r = s$ and after recordering that $p_i = cq_i$ for $c \in k^*$. But c must be a unit in R because $1 = \operatorname{cont} p_i = c \operatorname{cont} q_i = c$.

13.2 Integrally-Closed Domains

Definition 13.8
A domain R is called **integrally closed** if for any $\alpha \in k = \operatorname{Frac} R$ that is a root of a monic polynomial $f \in R[X]$ actually $\alpha \in R$.

We see that this is also a common phenomenon–we often can see that roots of polynomials in $R[X]$ in the rationals were really integer roots all alone.

Theorem 13.9
If R is a UFD, then R is integrally closed.

Proof
Suppose $f(\alpha) = 0$. Then we can factor $f = (X - \alpha)q + r$ for $q, r \in k[X]$. But $r \in K$ and plugging in $X = \alpha$ implies that $r = 0$. Thus $f = (X - \alpha)q$, where both factors are monic. But note that $\operatorname{cont} f = 1$ by it being monic and $\frac{1}{\operatorname{cont}(X-\alpha)} \in R$ and same thing for q. But by Gauss' lemma, $1 = \frac{1}{\operatorname{cont}(X-\alpha)} \cdot \frac{1}{\operatorname{cont} q}$, which means both things are units. This means $X - \alpha$ has unit content, so $\alpha \in R$.

Example 13.10
Here are some non-examples:

- $R = \mathbb{Z}[\sqrt{-3}]$. Note that $X^2 + X + 1$ has a root $\omega = \frac{1+\sqrt{-3}}{2} \in \mathbb{Q}[\sqrt{-3}]$ but $\omega \notin R$. This is thus not a UFD:
$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$
- $R = k[u,v]/(u^2 = v^3)$. Look at $X^2 - v \in R[X]$. Then it has a root at $\frac{u}{v} \in k$ but it's not in R. To see this, $\left(\frac{u}{v}\right)^2 - v = \frac{v^3}{v^2} - v = 0$.

14 Lecture 14

14.1 Eisenstein's Criterion

Theorem 14.1 (Eisentein)
Let R be a UFD. Let $f = \sum_{k=0}^{n} a_k X^k \in R[X]$. If there exists $p \in R$ prime such that $p \mid a_0, a_1, \ldots a_{n-1}$, but $p \nmid a_n$ and $p^2 \nmid a_0$, then f is irreducible.

Proof
Suppose that $f = gh$ where $g = \sum_{k=0}^{m} b_k X^m$ and $h = \sum_{k=0}^{\ell} c_k X^k$. Since p is prime and $p \mid a_0 = b_0 c_0$, but $p^2 \nmid b_0 c_0$, exactly one of them is divisible by p (say $p \mid b_0, p \nmid c_0$). Let b_r be the lowest coefficient of g such that $p \nmid b_r$ (this exists because p does not divide $a_n = b_m c_\ell$). Then, $a_r = b_r c_0 + b_{r-1} c_1 + \ldots$. But a_r is divisible by p and all the lowest b coefficients is divisible by p, so $p \mid b_r$, which is a contradiction.

This result is also true for the fraction field. To recall why this is true, suppose $f = gh$ where $g, h \in k[x]$. Then we could write $f = \mathrm{cont}(f) \frac{g}{\mathrm{cont}(g)} \frac{h}{\mathrm{cont}(h)}$, where $\mathrm{cont}(f) \in R$ and $\frac{g}{\mathrm{cont}(g)}, \frac{h}{\mathrm{cont}(h)} \in R$ by being content-1.

Example 14.2
Consider $f(X) = X^{p-1} + X^{p-2} + \cdots + 1$. We claim that f is irreducible. We change variables $Y = X - 1$. Then

$$\begin{aligned} f &= \frac{X^p - 1}{X - 1} \\ &= \frac{(Y+1)^p - 1}{Y} \\ &= \frac{Y^p + \binom{p}{p-1} Y^{p-1} + \cdots + \binom{p}{1} Y}{Y} \\ &= Y^{p-1} + \binom{p}{1} Y^{p-2} + \cdots + \binom{p}{1} \end{aligned}$$

Since $p \mid \binom{p}{i}$ for $0 < i < p$ and $p^2 \nmid \binom{p}{1} = p$, then Eisenstein's criterion applies.

14.2 Noetherian Rings and Hilbert's Theorem

Theorem 14.3
Let R be a commutative ring. Then the following are equivalent.

1. Every ideal is finitely-generated.
2. Every ascending chain $I_1 \subset I_2 \subset \ldots$ eventually terminates (eventually $I_N = I_{N+1} = \ldots$).

Proof
(1) $\Longrightarrow$ (2) Let $I_1 \subset I_2 \subset \ldots$. Consider their union $I = \bigcup I_i$; this is still an ideal. By assumption, $I = (a_1, \ldots, a_n)$ for some $a_i \in R$. Then each a_i is contained in some finite I_{n_i}. Then, just take $N = \max_i n_i$, then $I_N \supset I_{n_i} \ni a_i$, so $I \subset I_N$ and thus the ideals must terminate after that.
(2) $\Longrightarrow$ (1) Assume that there isn't an ideal which isn't finitely generated. Then there exist an infinite set of elements $\{a_i\}_{i=1}^{\infty}$ such that defininig $I_{i-1} = (a_1, a_2, \ldots, a_{i-1})$, $a_i \notin (a_1, a_2, \ldots, a_{i-1})$, so $I_1 \subset I_2 \subset \ldots$ doesn't terminate.

Definition 14.4
A ring is called **Noetherian** if either of the above is true.

Example 14.5
Consider a non-example, the polynomial ring on infinitely many variables $k[X_1, X_2, \dots]$. Note that $(X_1, X_2, \dots)$ is not f.g. so it fails the first item and $(X_1) \subset (X_1, X_2) \subset \dots$ doesn't terminate.

Theorem 14.6 (Hilbert)
If R is a Noetherian ring, then $R[X]$ is also Noetherian.

Proof
Let $I \subset R[X]$ and let $I_i = (a_i \mid \exists a_0 + \cdots + a_i X^i \in I) \subset R$ (we are only capturing the leading coefficient in the the generator builder notation). Then $I_0 \subset I_1 \subset \dots$ is an ascending chain of ideals, because if $a_i \in I_i$ then $p_i(X) = a_0 + \cdots + a_i X^i \in I$, so $Xp_i(X) = a_0 X + \cdots + a_i X^{i+1} \in I$, so then $a_i \in I_{i+1}$. Since R is Noetherian, there exists $I_r = I_{r+1} = \dots$, a termination ideal. Let $S_i \subset I$ be a finite set of degree i polynomials whose X^i coefficient generate I_i (this exists because R is Noetherian). Calling $I_i = (a_i^1, a_i^2, \dots)$ (where the superscripts are indices), we would have $S_i = \{a_0^1 + \cdots + a_i^1 X^i, a_0^2 + \cdots + a_i^1 X^i\}$. By iteratively subtracting off the leading term, any polynomial in I is generated by $S_1 \cup \cdots \cup S_r$. That is, if $f = b_0 + \cdots + b_n X^n \in I$, then if $n \leq r$, we can subtract them out by an appropriate element of I_n to knock down the power by 1. If $n > r$, $S_r = S_{r+1} = \dots$, so we can just take the relevant generator from S_r and multiply by X^{n-r} to reduce the power by 1. So $I = (S_1, \dots, S_r)$ is finitely generated.

If $R = k$ is a field, then $k[X]$ is a PID and thus Noetherian. If $R = k[Y]$ so $R[X] = k[X, Y]$; there are arbitrarily large ideals, but each one is finitely-ginerated. To see the first part, $(X^n, X^{n-1}Y, X^{n-2}Y^2, \dots, Y^n)$ cannot be generated by n elements.

Example 14.7
Here is an example of the proof in action. Let $R = \mathbb{Z}[Y]$ and $I = (2, 1 + YX, Y + X^3) \subset R[X]$. Then I_0 has all the coefficients of degree 0 polynomials, so $I_0 = (2)$. Furthermore, I_1 has all the coefficients of degree 1 polynomials, wherein we have YX and $2X$, so $I_1 = (2, Y)$. Similarly for quadratics $I_2 = (2, Y)$. Now for cubics, we can make 1, so $(1) = R = I_3 = I_4 = \dots$. Then, we construct $S_0 = \{2\}, S_1 = \{2X, 1 + YX\}, S_2 = \{2X^2, X + YX^2\}, S_3 = \{Y + X^3\}$. Let $f = (3 + Y) + (3 + 2Y)X + YX^2 + X^3 + X^4 \in I$. Then we can subtract off:

$$\begin{aligned} f &= (3 + Y) + (3 + 2Y)X + YX^2 + X^3 + X^4 \\ f - X(Y + X^3) &= (3 + Y) + (3 + Y)X + YX^2 + X^3 \\ f - X(Y + X^3) - (Y + X^3) &= 3 + (3 + Y)X + YX^2 \\ f - X(Y + X^3) - (Y + X^3) - (X + YX^2) &= 3 + (2 + Y)X \\ f - X(Y + X^3) - (Y + X^3) - (X + YX^2) - (2X + 1 + YX) &= 2 \\ f - X(Y + X^3) - (Y + X^3) - (X + YX^2) - (2X + 1 + YX) - (2) &= 0 \end{aligned}$$

A corollary is that every finitely-generated ring over a Noetherian ring is Noetherian.

Definition 14.8
A ring S is finitely generated over R if $S = R[X_1, \dots, X_n]/I$. for some ideal I.

Let G as an action on $\mathbb{C}^n$, a representation of a finite group. We can extend this to an action G on $\mathbb{C}[X_1, \dots, X_n]$.

Theorem 14.9
$\mathbb{C}[X_1, \ldots, X_n]^G$ is a finitely generated ring.

For example, let $G = \{\pm 1\}$ acting on $\mathbb{C}[X_1, X_2$ where $-1 \cdot X_1 = -X_1$ and $-1 \cdot X_2 = -X_2$. Then $\mathbb{C}[X_1, X_2]^G = \mathbb{C}[X_1^2, X_1 X_2, X_2^2] = \mathbb{C}[u, v, w]/(uw = v^2)$.

15 Lecture 15

15.1 Invariant Polynomials

Let $G \curvearrowright \mathbb{C}^n$ be a representation of a finite group, i.e. it acts linearly on $\mathbb{C}^n$ as some automorphism group. This induces a natural action $G \curvearrowright \mathbb{C}[x_1, \ldots, x_n]$, which is the identity on constants.

Definition 15.1
$\mathbb{C}[x_1, \ldots, x_n]^G$ is the subring of $\mathbb{C}[x_1, \ldots, x_n]$ which contains the polynomials f such that $gf = f$ for all $g \in G$.

As a simple example, if $G = \{\pm 1\}$ which acts on $\mathbb{C}[x, y]$ by simple multiplication, for instance $-1 \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and $1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ this means

$$\mathbb{C}[x, y]^G = \mathbb{C}[x^2, xy, y^2] = \mathbb{C}[u, v, w]/(uw = v^2)$$

Theorem 15.2 (Hilbert)
With these conditions, $\mathbb{C}[x_1, \ldots, x_n]^G$ is a finitely-generated ring over $\mathbb{C}$.

Definition 15.3
A ring R is generated over a subring k (not necessarily a field) by elements $f_1, \ldots, f_n \in R$ if any subring of R containing k and $f_1, \ldots, f_n$ is all of R.

In other words, we can make any element of R as polynomials in k and $f_1, \ldots, f_n$. This is equivalent to last time, where $R = k[f_1, \ldots, f_n]/I$, because it's equivalent to saying that there's a surjective map $k[f_1, \ldots, f_n] \to R$ (I is the kernel).

Also, one should note that a subring of a finitely-generated ring need not be finitely generated.

Example 15.4
Consider $\mathbb{C}[x, xy, xy^2, \ldots] \subset \mathbb{C}[x, y]$. The second ring is clearly finitely generated by the two generators x and y. But suppose you had a finite basis for the first ring, where the term with power 1 of x and largest power of y was xy^p. We cannot make xy^{p+1}.

With this in hand, let's prove the other Hilbert's theorem.

Proof
Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ be the ideal generated by all non-constant homogenous (all terms of the same degree) G-invariant polynomials (call such polynomials HNCGI polynomials). By Hilbert's theorem, the ring is Noetherian, so $I = (g_1, \ldots, g_r)$ is finitely generated (as an ideal over the ring $\mathbb{C}[x_1, \ldots, x_n]$). We claim that we can take these WLOG to be HNCGI. To see this, by definition, $g_i = r_1^{(i)} f_1^{(i)} + \cdots + r_{k(i)}^{(i)} f_{k(i)}^{(i)}$ so we can just replace $I = (f_1, \ldots, f_s)$ where all the f's are HNCGI. We will claim by induction on the degree that any HNCGI f is a polynomial in $f_1, \ldots, f_s$.

We can write $f = r_1 f_1 + \cdots + r_s f_s$ for $r_i \in \mathbb{C}[x_1, \ldots, x_n]$. We will apply the averaging operator which applies $Af = \frac{1}{|G|} \sum_{g \in G} g(f)$. This operator has three useful properties:

1. $\mathrm{im} A \subset \mathbb{C}[x_1, \ldots, x_n]^G$ because applying any group element will just permute the order of the sum, which doesn't change anything.
2. For $f \in \mathbb{C}[x_1, \ldots, x_n]$ we have $Af = f$, since every term gives f.

3. We have for each product term:

$$A(r_1 f_1) = \frac{1}{|G|} g(r_1 f_1) = \frac{1}{|G|} \sum g(r_1) g(f_1) = \frac{1}{|G|} \Big(\sum g(r_1) \Big) f_1$$

   Since f_1 is invariant.

Thus, applying the average of both sides yields

$$f = A(r_1) f_1 + \cdots + A(r_s) f_s$$

By induction on degree, since $A(r_1), \ldots, A(r_s)$ are G-invariant and have smaller degree than f (since f_i are homogenous and nonconstant). They may constants, but that's fine for our claim. If not, they might not be homogenous, but it's definitely a finite sum of homogenous things, which can each be written by induction as polynomials in $f_1, \ldots, f_s$. Which means f can be written as a $\mathbb{C}$-polynomial in $f_1, \ldots, f_s$, so the ideal is finitely-generated (as a ring).

15.2 Symmetric Polynomials

Example 15.5
Let $S_n \curvearrowright \mathbb{C}[x_1, \ldots, x_n]$ by $\sigma : x_i \mapsto x_{\sigma(i)}$. Then $\mathbb{C}[x_1, \ldots, x_n]^{S_n}$ is called the set of **symmetric polynomials**. Consider

$$(X + x_1)(X + x_2) \ldots (X + x_n) = e_0 X^n + e_1 X^{n-1} + \cdots + e_n$$

Then

$$\begin{aligned} e_0 &= 1 \\ e_1 &= x_1 + x_2 + \cdots + x_n \\ e_2 &= x_1 x_2 + x_1 x_3 + \ldots \\ &\vdots \\ e_n &= x_1 \ldots x_n \end{aligned}$$

where all the e's are symmetric polynomials. A symmetric polynomial is not necessarily one these, like $x_1^2 + x_2^2 + x_3^2$. But actually, any symmetric polynomial can be written in terms of these "elementary symmetric polynomials."

Theorem 15.6
$\mathbb{C}[x_1, \ldots, x_n]^{S_n} = \mathbb{C}[e_1, \ldots, e_n]$ **Proof.** By induction on degree on highest lexicographic monomial, $f - a e_1^{r_1 - r_2} e_2^{r_2 - r_3} \ldots e_n^{r_{n-1} - r_n}$ can cancel out an $a x_1^{r_1} \ldots x_n^{r_n}$ term.

Also the e_i are algebraically independent, where there are no relations between the generators.

Theorem 15.7
$R = \mathbb{C}[x_1, \ldots, x_n]$ is a free R^{S_n}-module of rank $n!$.

Proof
Consider the case of $n = 3$. $S_3 = \langle s_1, s_2 \mid s_1^2 = s_2^2 = 1, s_1 s_2 s_1 = s_2 s_1 s_2 \rangle$ where $s_1 = (12)$ and $s_2 = (23)$.
The amount of simple reflections needed to generate a permutation we will call its length.
We start with discriminant $\frac{1}{6}(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ and apply operators $\partial_1 f = \frac{f - s_1 f}{x_1 - x_2}$ and $\partial_2 f = \frac{f - s_2 f}{x_2 - x_3}$.
Here are some figures: TODO

16 Lecture 16

Recall that if R is Noetherian then $R[X]$ is Noetherian.

Theorem 16.1
If M is a finitely-generated module over R, Noetherian and if $N \subset M$ is a submodule, then N is finitely-generated.

Proof
We will use a trick called idealization, which converts statements about ideals of R into ones about R-modules. Consider $S = R \oplus M$, made into a ring R extended by M by stating that $M^2 = 0$. I.e.,

$$(r, m)(r', m') = (rr', rm' + r'm)$$

Then, any $N \subset M \subset S$ means N is an ideal of S. The only thing to check is that $SN \subset N$, which can be seen by considering cases of the direct sum. If $m_1, \ldots, m_g$ generate M as a module, then consider the map $R[x_1, \ldots, x_g] \to S$ such that $x_i \mapsto 0_R + m_i$, which is clearly surjective. Since $R[x_1, \ldots, x_g]$, this means that S is Noetherian (to see this, note that if there's any ascending chain of ideals in $R[x_1, \ldots, x_g]$, this maps to a chain of subideals in S). Thus, N is finitely generated.

16.1 Tensor Products

Let R be a commutative ring and M, N be R-modules. The defining property of a tensor product is that "maps from $M \otimes_R N$ are the same as R-bilinear maps from $M \times N$." That is,

1. There exists a bilinear map $M \times N \xrightarrow{\pi} M \otimes_R N$, $(m, n) \mapsto m \otimes n$.
2. Such a map is universal, that is if $M \times N \xrightarrow{\varphi} P$ is any R-bilinear map, then there exists a unique map such that $M \otimes N \xrightarrow{\alpha} P$ such that $\varphi = \alpha\pi$.

But how do we know that such a map exists? The construction is to make the "free-est" possible module we can with these properties.

1. Take $\tilde{M}$ as the free R-module with basis $= \{m \mid m \neq 0, m \in M\}$ and define $\tilde{N}$ the same.
2. Consider $M \otimes N = \frac{\tilde{M} \times \tilde{N}}{Q}$ where the submodule Q is the relations,

$$Q = ((m, n) + (m', n) - (m + m', n), (m, n) + (m, n') - (m, n + n'), (rm, n) - r(m, n), (m, rn) - r(m, n))$$

Example 16.2

- What is $M \otimes R$? Well, if $\phi : M \times R \to N$ is bilinear, so you need a module homomorphism from M to N and a linear map from R to N, which just involves sending $r \mapsto 1_N$. But $rm \otimes 1 = m \otimes r$ (TODO: Why?). So the unique module homomorphism from M to N characterizes all the data, so $M \otimes R = M$.
- $M \otimes N = N \otimes M$ because $m \otimes n \mapsto n \otimes m$ is a bilinear isomorphism (it's clear all the generators look like this).
- $M \otimes (N \otimes P) = (M \otimes N) \otimes P$. To see this, note that $\mathrm{Hom}_R(M \otimes N, P)$ is naturally isomorphic to $\mathrm{Hom}_R(M, \mathrm{Hom}(N, P))$. In particular, the maps $\phi : m \otimes n \mapsto \psi(m)(n)$ and $\psi :\mapsto (n \mapsto \phi(m \otimes n))$ correspond with each other. The tensor product preserve co-limits, because $- \otimes N$ is left adjoint to $\mathrm{Hom}(N, P)$. Recall the notion of a limit. Consider a category $\mathcal{C}$ and let $D = \{D_i, \varphi_\alpha\}$ be a diagram $\mathcal{C}$. We say $\operatorname{colim} D = B$ if there exist a bunch of maps $\psi_i : D_i \to B$ such that all maps with the existing

diagram commute. So, for example, the tensor product preserves direct sums.

Theorem 16.3
The tensor product commutes with all co-limits.

Proof
Call D a diagram in the category R-module. Call $M \otimes D$ the following diagram:

1. For object N, we have a new object $M \otimes N$.
2. For $\varphi : N \to N'$ $M \otimes \varphi : M \otimes N \xrightarrow{1\otimes\varphi} M \otimes N'$.

Suppose $D \xrightarrow{\varphi} B = \operatorname{colim} D$. Then, for some object C,

$$\operatorname{Hom}(M \otimes D, C) \cong \operatorname{Hom}(D, \operatorname{Hom}(M, C)) \cong \operatorname{Hom}(B, \operatorname{Hom}(M, C)) \cong \operatorname{Hom}(M \otimes B, C)$$

So $M \otimes B$ is the colimit of the diagram.

Example 16.4

- We can now extend our previous claim.
$$R^{\oplus n} \otimes_R M = (R \otimes M)^{\oplus n} = M^{\oplus n}$$
Furthermore, if we choose a basis for $R^{\oplus n} = \bigoplus_{i=1}^n Re_i$, every element of $R^n \otimes M$ can be written uniquely as $\sum_{i=1}^n e_i \otimes m_i$.
- If $P \to Q$ is a surjection, then $M \otimes P \to M \otimes Q$ is a surjection.
- If $N = \operatorname{coker}\varphi$ where $R^n \xrightarrow{\varphi} R^p \to N \to 0$, then $M \otimes N$ is cokernel of $M \otimes R^n \to M \otimes R^p \to M \otimes N \to 0$.
- Let $I \subset R$ be an ideal. Then consider $M \otimes (R/I)$. Let
$$0 \to I \to R \to R/I \to 0$$
be exact then
$$I \otimes M \xrightarrow{\phi} M \to R/I \otimes M \to 0$$
is also exact. But for $\phi : a \otimes m \mapsto am$ Thus, $R/I \otimes M = M/IM$

Call $M = \mathbb{Z}/4$ and $R = \mathbb{Z}/4$ as a ring. Then $(2) \subset \mathbb{Z}/4$ where $R/2 \to R$ has $1 \mapsto 2$. Thus, $R/2 \otimes_R R/2 = R/2$ and $R \otimes_R R/2 = R/2$. So, $R/2 \otimes R/2 \xrightarrow{0} R \otimes R/2$, which makes a non-monomorphism.

Consider R and $S \subset R$ be a multiplicatively closed set. We define

$$R[S^{-1}] = \left\{\frac{r}{s} \mid r \in R, s \in S\right\} / \approx$$

such that $\frac{r}{s} \approx \frac{r'}{s}$ if there exists $t \in S \setminus \{0\}$ such that $t(rs' - r's) = 0$. One can check that $R[S^{-1}]$ is a commutative ring. Then $R \to R[S^{-1}]$ is a universal map to a ring where elements of S become units. This is called the **localization** of R to S. One can define the same thing for modules, where the $\frac{m}{s} \approx \frac{m'}{s}$ if there exists $t \in S$ such that $t(ms' - sm')$.

Theorem 16.5
We have that $R[S^{-1}] \otimes_R M \cong M[S^{-1}]$.

Proof
Consider the map $\frac{r}{s} \otimes m \to \frac{rm}{s}$. The localization map $M \to M[S^{-1}]$ is universal for maps of M into an $R[S^{-1}]$-module. So then there's easy maps from $R \otimes M$ to $R[S^{-1}] \otimes M$ and to $M[S^{-1}]$.

If $0 \to A \to B \to C$ is a short exact sequence, then $0 \to A[S^{-1}] \to B[S^{-1}] \to C[S^{-1}] \to 0$. Then, if $\frac{a}{s} \mapsto \frac{\varphi(a)}{s} = 0$, then this means $t\phi(a) \approx 0$ for some $t \in S$. This means that $ta = 0$, meaning $\frac{a}{s} \approx 0$ to begin with. This is a property of modules called **flatness**.