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

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

Now $M/(f_1, \dots, f_n)$ has torsion, because if $g \in M, g \notin (f_1, \dots, f_n)$ 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, $M/(f_1, \dots, f_n)$ 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.

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

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 $\text{ann}_R M = (a)$, 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 $\text{ann}(M(p) \oplus M(q)) = p^k q^\ell$ 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 $\text{ann}\, M = (p^a)$. $M = \sum_{i=1}^n Rf_i$. 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 $\ell_i \le k_i$. 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 $p^{\ell_i} f_i = u p^{m_i} f_1$ for $u \in R$ coprime to p where we claim $m_i \ge \ell_i$, 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 $k_i - \ell_i \ge k_1 - m_i$. Finally, $m_i \ge k_1 - k_i + \ell_i$ and by definition of the first one, we had $k_1 \ge k_i$. Thus, we have $m_i \ge \ell_i$.

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 $p^b(up^{d-b}) = p^b g_1$. Surbtracting 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:

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

where $p_i^{a_{ij}} \mid p_i^{a_{ik}}$ for $j \le k$. 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 $[a_1, \dots, a_r]$.

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 $h, h' \in H$

$$gh = kh'$$
$$ghH = kh'H$$
$$gH = kH$$

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 $\text{Stab}_G(gH) = gHg^{-1}$.
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 $\text{Stab}_G(gP) = gPg^{-1}$. 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 $\text{Stab}_H(gP) = H \cap gPg^{-1}$ which means $|H(gP)| = |H|/|H \cap gPg^{-1}|$, which must only have a 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 $H \subset \text{Stab}_H(gP) = gPg^{-1}$. 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 $1 +$ 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.
The left and middle chains and the right and middle chains are equal up to permutation by induction. $G = H_1H_1'$ because $H_1H_1' \triangleright G$ 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.