

# Algebra I: Class Notes

Wilson Pan

February 20, 2026

## Contents

# 1 Lecture 1: Group Actions & The Orbit-Stabilizer Theorem (Jan 12)

## 1.1 Permutations and Automorphisms

**Definition 1.1** (Symmetric Group). Let  $X$  be a set. The set of all permutations (bijections) of  $X$  is denoted by  $\text{Sym}_X$  (or sometimes  $\Sigma_X$ ). Under function composition,  $\text{Sym}_X$  forms a group.

**Definition 1.2** (Automorphism Group). Let  $(G, \cdot)$  be a group. An automorphism of  $G$  is a bijection  $\phi : G \rightarrow G$  that is also a homomorphism, i.e.,

$$\phi(g_1 g_2) = \phi(g_1) \phi(g_2) \quad \forall g_1, g_2 \in G.$$

The set of all such automorphisms is denoted by  $\text{Aut}(G)$ . It forms a group under composition.

## 1.2 Group Actions

**Definition 1.3** (Group Action). Let  $G$  be a group and  $X$  be a set. An **action** of  $G$  on  $X$  is a homomorphism  $\phi : G \rightarrow \text{Sym}_X$ .

We typically write the action as  $g \cdot x := \phi(g)(x)$ . This notation satisfies two axioms (equivalent to the homomorphism property):

1. **Identity:**  $1 \cdot x = x$  for all  $x \in X$ .
2. **Compatibility:**  $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$  for all  $g_1, g_2 \in G, x \in X$ .

**Theorem 1.4** (Equivalence Relation on  $X$ ). Let  $G$  act on  $X$ . Define a relation  $\sim$  on  $X$  by:

$$x_1 \sim x_2 \iff \exists g \in G \text{ such that } g \cdot x_1 = x_2.$$

Then  $\sim$  is an equivalence relation.

*Proof.* We check the properties:

1. **Reflexive:**  $1 \cdot x = x \implies x \sim x$ .
2. **Symmetric:** If  $g \cdot x_1 = x_2$ , acting by  $g^{-1}$  gives  $g^{-1} \cdot (g \cdot x_1) = g^{-1} \cdot x_2 \implies (g^{-1}g) \cdot x_1 = g^{-1} \cdot x_2 \implies x_1 = g^{-1} \cdot x_2$ . Thus  $x_2 \sim x_1$ .
3. **Transitive:** If  $g \cdot x_1 = x_2$  and  $h \cdot x_2 = x_3$ , then  $h \cdot (g \cdot x_1) = x_3 \implies (hg) \cdot x_1 = x_3$ . Thus  $x_1 \sim x_3$ .

□

### 1.3 Orbits and Stabilizers

The equivalence classes under the relation  $\sim$  partition the set  $X$ . These classes are called **orbits**.

**Definition 1.5** (Orbit). *For  $x \in X$ , the orbit of  $x$  is the set of all places  $x$  can be moved to by  $G$ :*

$$\mathcal{O}_x = \text{Orb}(x) = \{g \cdot x : g \in G\}.$$

**Definition 1.6** (Stabilizer). *For  $x \in X$ , the stabilizer of  $x$  is the set of elements in  $G$  that fix  $x$ :*

$$G_x = \text{Stab}(x) = \{g \in G : g \cdot x = x\}.$$

*Note that  $G_x$  is a subgroup of  $G$  (denoted  $G_x \leq G$ ).*

**Theorem 1.7 (Orbit-Stabilizer Theorem).** *Let  $G$  act on  $X$ . For any  $x \in X$ , there is a bijection between the orbit  $\mathcal{O}_x$  and the set of left cosets  $G/G_x$ . Consequently:*

$$|\mathcal{O}_x| = [G : G_x].$$

*If  $G$  is finite,  $|G| = |\mathcal{O}_x| \cdot |G_x|$ .*

*Proof.* Define a map  $\psi : G/G_x \rightarrow \mathcal{O}_x$  by  $\psi(gG_x) = g \cdot x$ .

1. **Well-defined:** Suppose  $g_1G_x = g_2G_x$ . Then  $g_1^{-1}g_2 \in G_x$ , so  $(g_1^{-1}g_2) \cdot x = x$ , implying  $g_2 \cdot x = g_1 \cdot x$ .
2. **Injectivity:** If  $\psi(g_1G_x) = \psi(g_2G_x)$ , then  $g_1 \cdot x = g_2 \cdot x$ . Multiplying by  $g_1^{-1}$ , we get  $x = g_1^{-1}g_2 \cdot x$ , so  $g_1^{-1}g_2 \in G_x$ , implying  $g_1G_x = g_2G_x$ .
3. **Surjectivity:** By definition, any  $y \in \mathcal{O}_x$  is of the form  $g \cdot x$  for some  $g$ , which is exactly  $\psi(gG_x)$ .

Thus,  $\psi$  is a bijection. □

## 2 Lecture 2: Cauchy's Theorem & Conjugation (Jan 14)

### 2.1 Cauchy's Theorem

**Lemma 2.1.** *If  $X$  is a finite set and  $G$  is a  $p$ -group (a group of order  $p^k$ ) acting on  $X$ , then:*

$$|X| \equiv |X^G| \pmod{p},$$

where  $X^G = \{x \in X : g \cdot x = x, \forall g \in G\}$  is the set of fixed points.

**Theorem 2.2** (Cauchy's Theorem). *If  $G$  is a finite group and  $p$  is a prime dividing  $|G|$ , then  $G$  has an element of order  $p$ .*

*Proof (McKay's Proof).* Let  $X$  be the set of  $p$ -tuples of elements of  $G$  whose product is the identity:

$$X = \{(g_1, \dots, g_p) \in G^p : g_1 g_2 \cdots g_p = 1\}.$$

Notice that  $g_p$  is uniquely determined by the first  $p-1$  elements ( $g_p = (g_1 \cdots g_{p-1})^{-1}$ ), so  $|X| = |G|^{p-1}$ . Since  $p \mid |G|$ , we have  $p \mid |X|$ .

Let  $\mathbb{Z}_p$  (cyclic group of order  $p$ ) act on  $X$  by cyclic shift:

$$\sigma \cdot (g_1, g_2, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1).$$

This is a valid action because if  $g_1 \cdots g_p = 1$ , then  $g_1(g_2 \cdots g_p) = 1 \implies g_2 \cdots g_p = g_1^{-1}$ , so  $(g_2 \cdots g_p)g_1 = g_1^{-1}g_1 = 1$ .

By the Lemma,  $|X| \equiv |X^{\mathbb{Z}_p}| \pmod{p}$ . Fixed points are tuples  $(a, a, \dots, a)$  such that  $a^p = 1$ . Since  $(1, \dots, 1) \in X^{\mathbb{Z}_p}$ , the set of fixed points is non-empty. Since  $p$  divides  $|X|$  and  $p$  divides the congruence  $|X| - |X^{\mathbb{Z}_p}|$ ,  $p$  must divide  $|X^{\mathbb{Z}_p}|$ . Therefore, there are at least  $p$  fixed points. There must exist some  $a \neq 1$  such that  $a^p = 1$ .  $\square$

### 2.2 Conjugation

Conjugation is a specific action of  $G$  on itself.

**Definition 2.3.** *For  $g, h \in G$ , the **conjugate** of  $g$  by  $h$  is  $g^h := hgh^{-1}$ . The map  $\phi_h : G \rightarrow G$  defined by  $g \mapsto hgh^{-1}$  is an automorphism (an inner automorphism).*

**Definition 2.4** (Classes and Centralizers). *Let  $G$  act on itself by conjugation ( $h \cdot g = hgh^{-1}$ ).*

- The orbit of  $g$  is the **Conjugacy Class** of  $g$ :  $Cl(g) = \{hgh^{-1} : h \in G\}$ .
- The stabilizer of  $g$  is the **Centralizer** of  $g$ :  $C_G(g) = \{h \in G : hg = gh\}$ .

By Orbit-Stabilizer:  $|Cl(g)| = [G : C_G(g)]$ .

**Definition 2.5** (Center of  $G$ ). The **Center**,  $Z(G)$ , is the set of elements that commute with everything:

$$Z(G) = \{z \in G : zg = gz, \forall g \in G\} = \bigcap_{g \in G} C_G(g).$$

$Z(G)$  is the kernel of the conjugation homomorphism  $G \rightarrow \text{Aut}(G)$ . Thus  $Z(G) \trianglelefteq G$ .

**Definition 2.6** (Normalizer). Let  $H \leq G$ . The **Normalizer** of  $H$  in  $G$  is:

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

$N_G(H)$  is the largest subgroup of  $G$  in which  $H$  is normal.

## 3 Lecture 3: Sylow Preliminaries & Isomorphism Theorems (Jan 16)

### 3.1 Product of Subgroups

**Definition 3.1.** Let  $K, N \leq G$ . Define  $KN = \{kn : k \in K, n \in N\}$ .

- In general,  $KN$  is not a subgroup.
- If  $N \trianglelefteq G$  (or just  $N \subseteq N_G(K)$ ), then  $KN$  is a subgroup.
- Size formula:  $|KN| = \frac{|K||N|}{|K \cap N|}$ .

**Theorem 3.2** (Second Isomorphism Theorem). Let  $K \leq G$  and  $N \trianglelefteq G$ . Then  $K \cap N \trianglelefteq K$ , and

$$\frac{KN}{N} \cong \frac{K}{K \cap N}.$$

*Proof.* Consider the natural projection  $\pi : G \rightarrow G/N$ . Restrict it to  $K$ , i.e.,  $\phi = \pi|_K : K \rightarrow G/N$ . The image of  $\phi$  is  $\{kN : k \in K\} = KN/N$ . The kernel of  $\phi$  is  $\{k \in K : kN = N\} = \{k \in K : k \in N\} = K \cap N$ . By the First Isomorphism Theorem,  $K/\ker(\phi) \cong \text{Im}(\phi)$ .  $\square$

### 3.2 Sylow Definitions

**Definition 3.3** ( $p$ -group). Let  $p$  be a prime. A group  $G$  is a  $p$ -group if every element has order a power of  $p$ . For finite groups, this is equivalent to  $|G| = p^k$ .

**Definition 3.4** (Sylow  $p$ -subgroup). Let  $|G| = p^n m$  where  $p \nmid m$ . A subgroup  $P \leq G$  is called a **Sylow  $p$ -subgroup** if  $|P| = p^n$ .

$$\text{Syl}_p(G) = \{P \leq G : P \text{ is a Sylow } p\text{-subgroup}\}.$$

## 4 Lecture 4: The Sylow Theorems (Jan 21)

**Theorem 4.1 (The Sylow Theorems).** *Let  $G$  be a finite group of order  $p^n m$  where  $p \nmid m$ .*

1. **Existence:**  $\text{Syl}_p(G) \neq \emptyset$ . (There exists a subgroup of order  $p^n$ ).
2. **Conjugacy:** Any two Sylow  $p$ -subgroups are conjugate in  $G$ . That is, if  $P, Q \in \text{Syl}_p(G)$ ,  $\exists g \in G$  such that  $gPg^{-1} = Q$ .
3. **Number:** Let  $n_p = |\text{Syl}_p(G)|$ . Then:
  - $n_p \equiv 1 \pmod{p}$ .
  - $n_p \mid m$  (equivalently  $n_p \mid |G|$ ).

*Proof.* Let  $p$  be a prime such that  $p \mid |G|$ . Define the set of all  $p$ -subgroups:

$$\Sigma = \{H : H \leq G, |H| = p^n \text{ for some } n > 0\}.$$

Define  $\Omega$  as the set of maximal elements in  $\Sigma$  under inclusion:

$$\Omega = \{H : H \in \Sigma, \text{ there is no } K \in \Sigma \text{ such that } H \subsetneq K\}.$$

We let  $G$  act on the set of subgroups  $\{H : H \leq G\}$  by conjugation. Since conjugation is an isomorphism ( $H^g \simeq H$ ), it preserves the order of subgroups. Thus:

$$H \in \Sigma \iff H^g \in \Sigma \quad \text{and} \quad H \in \Omega \iff H^g \in \Omega.$$

Therefore,  $G$  acts on  $\Omega$  by  $g \cdot H = H^g$ .

**Claim 1:** Let  $H \in \Omega$ . Consider the action of  $H$  on  $\Omega$  by conjugation. Then  $H$  is the *unique* fixed point of this action.

*Proof of Claim:*

- **Existence:** It is trivial to see that  $H$  is a fixed point, as  $H^h = hHh^{-1} = H$  for any  $h \in H$ .
- **Uniqueness:** Let  $K \in \Omega$  be a fixed point of the action of  $H$ .

$$K \text{ is fixed by } H \iff K^h = K \quad \forall h \in H \iff H \leq N_G(K).$$

Since  $K \trianglelefteq N_G(K)$ , and  $H \leq N_G(K)$ , the product  $HK$  is a subgroup of  $N_G(K)$ , and thus  $HK \leq G$ . Using our counting lemma:

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Since  $H, K \in \Omega$ , their orders are powers of  $p$ . Thus  $|HK|$  is a power of  $p$ , meaning  $HK \in \Sigma$ .

We have  $H \leq HK$ . Since  $H$  is maximal in  $\Sigma$  (by definition of  $\Omega$ ) and  $HK \in \Sigma$ , it must be that  $H = HK$ . Similarly,  $K \leq HK$  implies  $K = HK$ . Therefore,  $H = K$ .

**Claim 2: Size of  $\Omega$  Modulo  $p$** **Statement:**  $|\Omega| \equiv 1 \pmod{p}$ .*Proof of Claim:* Let  $H \in \Omega$ . We decompose  $\Omega$  into disjoint orbits under the action of  $H$ .

$$\Omega = \{H\} \cup \bigcup_{K \neq H} \text{Orb}_H(K).$$

By Claim 1,  $H$  is the only fixed point (an orbit of size 1). For any  $K \in \Omega$  with  $K \neq H$ , the stabilizer of  $K$  in  $H$  is a proper subgroup, so by the Orbit-Stabilizer theorem for  $p$ -groups,  $|\text{Orb}_H(K)|$  is divisible by  $p$ .

$$|\Omega| = 1 + \sum (\text{multiples of } p) \implies |\Omega| \equiv 1 \pmod{p}.$$

**Claim 3: Transitivity (Conjugacy of Elements in  $\Omega$ )****Statement:** Any two elements of  $\Omega$  are conjugate.*Proof of Claim:* Suppose for contradiction that  $H, K \in \Omega$  are not conjugates. Let  $\theta_1 = \text{Orb}_G(H)$  and  $\theta_2 = \text{Orb}_G(K)$ . Since they are distinct orbits,  $\theta_1 \cap \theta_2 = \emptyset$ .Consider the action of  $H$  on these sets:

- On  $\theta_1$ :  $H \in \theta_1$ . By Claim 1,  $H$  is the unique fixed point of  $H$  in  $\Omega$ . Since  $\theta_1 \subseteq \Omega$ ,  $H$  is the unique fixed point in  $\theta_1$ . Thus,  $|\theta_1| \equiv 1 \pmod{p}$ .
- On  $\theta_2$ : Since  $H \in \theta_1$  and  $\theta_1 \cap \theta_2 = \emptyset$ , we have  $H \notin \theta_2$ . Therefore,  $\theta_2$  contains *no* fixed points under the action of  $H$  (because the only fixed point in all of  $\Omega$  is  $H$ ). Thus, every orbit of  $H$  inside  $\theta_2$  has size divisible by  $p$ . This implies  $|\theta_2| \equiv 0 \pmod{p}$ .

By symmetry, we can swap the roles of  $H$  and  $K$ . Running the same argument with  $K$  acting on the sets implies  $|\theta_2| \equiv 1 \pmod{p}$  and  $|\theta_1| \equiv 0 \pmod{p}$ .

This results in a contradiction (e.g.,  $|\theta_1| \equiv 1$  and  $|\theta_1| \equiv 0$ ). Thus,  $\theta_1 = \theta_2$ , so  $H$  and  $K$  are conjugate.

*Corollary:* Since there is only one orbit,  $\Omega = \theta_1$ . Thus  $|\Omega| = |\theta_1| \equiv 1 \pmod{p}$ .**Claim 4: Divisibility****Statement:**  $|\Omega| \mid |G|$ .*Proof of Claim:* Let  $H \in \Omega$ . Since  $\Omega$  is exactly the orbit of  $H$  under conjugation (from Claim 3), the size of the orbit is the index of the stabilizer:

$$|\Omega| = [G : \text{Stab}_G(H)] = [G : N_G(H)] = \frac{|G|}{|N_G(H)|}.$$

Thus  $|\Omega|$  divides  $|G|$ .**Claim 5: Identification with Sylow Subgroups****Statement:**  $\Omega = \text{Syl}_p(G)$ .*Proof of Claim:* We know  $\text{Syl}_p(G) \subseteq \Omega$  because Sylow subgroups are maximal  $p$ -subgroups by definition. We must show the reverse: every  $H \in \Omega$  is a Sylow  $p$ -subgroup.



Let  $H \in \Omega$ . Assume for contradiction that  $H \notin \text{Syl}_p(G)$ . Let  $|G| = p^s m$  where  $p \nmid m$ . Since  $H$  is a  $p$ -group but not Sylow,  $|H| = p^t$  with  $t < s$ .

Consider the normalizer  $N_G(H)$ . From Claim 2, we know  $|\Omega| = [G : N_G(H)] \equiv 1 \pmod{p}$ . Therefore,  $p$  does *not* divide  $[G : N_G(H)]$ . Since  $|G| = [G : N_G(H)] \cdot |N_G(H)|$ , all factors of  $p$  in  $|G|$  must reside in  $|N_G(H)|$ . Thus,  $|N_G(H)|$  is divisible by  $p^s$ .

Consequently, the index  $[N_G(H) : H] = \frac{|N_G(H)|}{|H|} = \frac{(\text{multiple of } p^s)}{p^t}$  is divisible by  $p$  (since  $s > t$ ).

By Cauchy's Theorem applied to the quotient group  $N_G(H)/H$ , there exists a subgroup of order  $p$ , say  $\bar{K} \leq N_G(H)/H$ . By the Correspondence Theorem, there exists a subgroup  $K$  such that  $H \leq K \leq N_G(H)$  with  $|K| = p \cdot |H| = p^{t+1}$ .

Since  $K$  is a  $p$ -group,  $K \in \Sigma$ . However,  $H \subsetneq K$ , which contradicts the definition of  $H$  as a maximal element in  $\Omega$ .

Therefore,  $H$  must already be of order  $p^s$ . Thus  $\Omega = \text{Syl}_p(G)$ . □

## 5 Lecture 5: Normal Series & Solvability (Jan 23)

### 5.1 Normal and Subnormal Series

**Definition 5.1.** A **subnormal series** of a group  $G$  is a chain of subgroups:

$$\{1\} = H_0 \leq H_1 \leq \cdots \leq H_k = G$$

such that  $H_i \trianglelefteq H_{i+1}$  for all  $i$ . The quotient groups  $H_{i+1}/H_i$  are called the **factors** of the series.

**Definition 5.2** (Composition Series). A subnormal series is a **composition series** if all factors  $H_{i+1}/H_i$  are **simple** groups (non-trivial groups with no normal subgroups other than  $\{1\}$  and themselves).

**Theorem 5.3** (Jordan-Hölder). Any two composition series of a finite group  $G$  are equivalent. That is, they have the same length, and their factors are isomorphic (up to reordering).

### 5.2 Solvable Groups

**Definition 5.4.** A group  $G$  is **solvable** if it has a subnormal series where all factors  $H_{i+1}/H_i$  are **abelian**.

**Definition 5.5** (Commutator). The commutator of  $g, h$  is  $[g, h] = ghg^{-1}h^{-1}$ . The **Derived Subgroup** (or Commutator Subgroup)  $G'$  or  $[G, G]$  is the subgroup generated by all commutators.

**Proposition 5.6.**  $G/N$  is abelian if and only if  $[G, G] \leq N$ . Thus,  $[G, G]$  is the smallest normal subgroup such that the quotient is abelian.

**Remark 5.7** (Derived Series). Define  $G^{(0)} = G$ ,  $G^{(1)} = [G, G]$ , and  $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ .  $G$  is solvable if and only if the derived series terminates at  $\{1\}$  (i.e.,  $G^{(n)} = \{1\}$  for some  $n$ ).

## 6 Lecture 6: Solvable and Derived Series (Jan 26)

**Lemma 6.1.** *Let  $\alpha \in \text{Aut}(G)$  then  $\alpha([g, h]) = [\alpha(g), \alpha(h)]$ .*

**Lemma 6.2.** *For  $N \trianglelefteq G$  then  $G/N$  is abelian iff  $[G, G] \leq N$ .*

**Theorem 6.3.** *If  $N \trianglelefteq G$ ,  $g, h \in G$  and  $[gN, hN] = [g, h]N$ . Additionally,  $gN$  and  $hN$  commutes iff  $[g, h]N = N$  iff  $[g, h] \subseteq N$ .*

**Definition 6.4.**  *$G$  is solvable iff there is a subnormal series  $\langle H_i : 0 \leq i \leq t \rangle$  such that  $[H_{i+1}, H_{i+1}] \leq H_i$  for all  $0 \leq i \leq t-1$ .*

**Theorem 6.5.** *The following are true*

1. *If  $G$  solvable and  $K \leq G$  then  $K$  is solvable*
2. *If  $G$  is solvable and  $N \trianglelefteq G$  then  $G/N$  is solvable.*
3. *For  $N \trianglelefteq G$ ,  $G$  solvable iff both  $N$  and  $G/N$  are solvable*

*Proof.* We prove the previous theorems

1. Let  $\langle H_i : 0 \leq i \leq t \rangle$  be a series in  $G$  such that  $[H_{i+1}, H_{i+1}] \leq H_i$  for all  $0 \leq i \leq t-1$ . We can let  $H'_i = K \cap H_i$  for  $0 \leq i \leq t$  and we need to verify  $\langle H'_i : 0 \leq i \leq t \rangle$  is a solvable series in  $K$ .
2. Let  $\langle H_i : 0 \leq i \leq t \rangle$  be a series in  $G$  such that  $[H_{i+1}, H_{i+1}] \leq H_i$  for all  $0 \leq i \leq t-1$ . Let  $H'_i = \phi_N[H_i] = H_i N / N$ . Verify it is solvable.
3. The forward direction is trivial by (1) and (2). For the reverse direction,  $N$  solvable and  $G/N$  solvable  $\langle N_i : 0 \leq i \leq s \rangle$  subnormal in  $N$  and  $N_{i+1}/N_i$  abelian and similar for  $\langle H_j N / N : 0 \leq j \leq t \rangle$  subnormal in  $G/N$  and  $(H_{j+1} N / N)_{j+1} / (H_j N / N)$  abelian. We know  $H_{j+1} \trianglelefteq H_j$  and  $[H_{j+1}, H_{j+1}] \leq H_j$  for all  $0 \leq j \leq t-1$ . So  $N_0 = 1 \trianglelefteq N_1 \cdots \trianglelefteq N_s = N = H_0 \trianglelefteq H_1 \cdots \trianglelefteq H_t = G$ .

□

**Definition 6.6.** *Given  $G$ , the derived series of  $G$  is given by  $G'_0 = G$  and  $G'_{i+1} = [G'_i, G'_i]$  for  $i \geq 0$ .*

**Theorem 6.7.**  *$G$  is solvable iff there is  $n$  such that  $G'_n = \{1\}$ .*

*Proof.* For the backwards direction, by construction  $G'_i / G'_{i+1}$  is abelian. Let  $H_j = G_{n-j}$ . For the forward direction, let  $\langle H_j : 0 \leq j \leq n \rangle$  be a subnormal series in  $G$ ,  $H_{j+1} / H_j$  abelian. Show by induction that  $G'_i \leq H_{n-i}$  for all  $i$ . □

**Theorem 6.8.** *Suppose  $G$  abelian and simple, let  $a \in G$  and  $a \neq 1$  then  $G = \langle a \rangle$  and  $|a|$  is prime.*

**Theorem 6.9.** *Let  $G$  be simple and let  $\langle H_i : 0 \leq i \leq t \rangle$  be subnormal series in  $G$ . Then there is  $n < t$  such that  $H_i = 1$  for  $0 \leq i \leq n$  and  $H_i = G$  for  $n < i \leq t$ .*

## 7 Lecture 7: Nilpotent Groups and Free Groups (Jan 28)

### 7.1 Nilpotent Groups

**Definition 7.1.** For  $H, K \leq G$ ,  $[H, K] = \langle [h, k] : h \in H, k \in K \rangle$

**Remark 7.2.**  $G'_i$  is characteristic in  $G$  for all  $i$ , in particular  $G'_i \trianglelefteq G$ .

**Lemma 7.3.** If  $N \trianglelefteq G, N \leq H \leq G$  then

$$\frac{H}{N} \leq Z\left(\frac{G}{N}\right) \iff [G, H] \leq N.$$

**Definition 7.4.** A normal series in  $G$ ,  $\langle H_i : 0 \leq i \leq t \rangle$  is a central series if  $\frac{H_{i+1}}{H_i} \leq Z\left(\frac{G}{H_i}\right)$  for all  $0 \leq i \leq t-1$ . Equivalently,  $[G, H_{i+1}] \leq H_i$  for all  $0 \leq i \leq t-1$ .

**Definition 7.5.**  $G$  is nilpotent iff  $G$  has a central series.

**Remark 7.6.** Nilpotent groups are solvable.

**Definition 7.7.** Let  $G$  be a group

1. The descending central series is the sequence of subgroup given by  $\gamma_1(G) = G$  and  $\gamma_{i+1}(G) = [G, \gamma_i(G)]$  for  $i \geq 1$ .
2. The ascending central series is the sequence of subgroup given by  $Z_0(G) = 1$  and

$$\frac{Z_{n+1}(G)}{Z_n(G)} = Z\left(\frac{G}{Z_n(G)}\right).$$

**Remark 7.8.** By induction,  $Z_n(G)$  and  $\gamma_n(G)$  are characteristic in  $G$ . and  $Z_n(G) \trianglelefteq G$  and  $\gamma_n(G) \trianglelefteq G$  for all  $n \geq 0$ .

**Remark 7.9.** For any  $G$  and  $N \trianglelefteq G$ ,  $[G, N] \leq N$  because for any  $g \in G, n \in N$  we have  $[g, n] = gng^{-1}n^{-1}$  and  $n^g \in N$  since  $N \trianglelefteq G$ . So  $[G, N] \leq N$ .

**Theorem 7.10.**  $G$  is nilpotent iff there is a  $N \geq 0$  such that  $Z_n(G) = G$  iff there is  $n \geq 0$  such that  $\gamma_{n+1}(G) = \{1\}$ . Moreover, the least  $n$  such that  $Z_n(G) = G$  is the least  $n$  such that  $\gamma_{n+1}(G) = \{1\}$ .

*Proof.* Take any central series then the decreasing and ascending central series will grow at least as fast as the arbitrary central series.  $\square$

## 7.2 Free Groups

**Example 7.11.** Consider  $\mathbb{Z} = (\mathbb{Z}, +)$ , 1 is a generator  $\mathbb{Z} = \langle 1 \rangle$ . The universal property of  $\mathbb{Z}$ , 1. For any group  $G$  and any  $g \in G$ , there is a unique homomorphism  $\phi : \mathbb{Z} \rightarrow G$  and  $\phi(1) = g$ .

*Proof.* If  $\phi$  exist let  $\phi(n) = g^n$  then  $\phi$  is a homomorphism.  $\square$

$g$  is free because whatever 1 is mapped to in the homomorphism it won't mess you up compared to a finite group.

**Definition 7.12.**  $F$  is a free group on 2 element if

1. There exist  $a, b \in F$ ,  $F = \langle a, b \rangle$
2. For all  $G$ , all  $g, h \in G$  there is a unique homomorphism  $\phi : F \rightarrow G$  such that  $\phi(a) = g$  and  $\phi(b) = h$ .

## 8 Lecture 8: Free Groups

**Theorem 8.1.** For any set  $X$ , there are a group  $F$  and an injective function  $i : X \rightarrow F$  such that

1. For any group  $G$  and any function  $f : X \rightarrow G$  there is a unique homomorphism  $\phi : F \rightarrow G$  such that  $\phi(i(x)) = f(x)$  for all  $x \in X$ .

$$\begin{array}{ccc} X & \xrightarrow{i} & F \\ & \searrow f & \downarrow \phi \\ & & G \end{array}$$

The diagram commutes:  $\phi \circ i = f$ . The homomorphism  $\phi$  is unique.

2.  $F$  is generated by  $i[X]$

*Proof.* A word (on alphabet  $X$ ) is a (possibly empty) finite sequence from  $X \times \mathbb{Z}$ . We will write  $x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$  for the word  $x_1, x_2, \dots, x_k$  for  $\langle (x_1, n_1), (x_2, n_2), \dots, (x_k, n_k) \rangle$ .

**Example 8.2.** Let  $X = \{x, y, z\}$  then  $w = x^0 x^{15} y^{-23} z^{27}$  is a word.

Let  $w$  be the set of words. Given a word, we can possibly perform a reduction step

1. If word contains an entry  $\langle x, 0 \rangle$ , remove it.
2. If the word contains successive entries  $\langle x, n \rangle$  and  $\langle x, m \rangle$  then replace them with  $\langle x, n + m \rangle$ .

**Example 8.3.**  $y^{15} x^3 x^{-2} x^{-1} y^2 z^5 \rightarrow y^{15} x^1 x^{-1} y^2 z^5 \rightarrow y^{15} x^0 y^2 z^5 \rightarrow y^{15} y^2 z^5 \rightarrow y^{17} z^5$ .

Let  $R$  be set of all reduced words, where no more reductions can be done.

For any word  $w$ , there is a unique reduced word  $w'$  such that  $w$  can be transformed into  $w'$  by a finite set of reductions.

We will not be able to show this property using group properties but instead we'll produce a group  $F$  with the property that every word is equivalent to a unique reduced word.

Given  $x \in X$ , I will replace  $f_x : F \rightarrow F$

1.  $w$  does not begin with some  $x^m$  then  $f_x(w) = xw$
2.  $w$  is of the form  $x^{-1}v$  then  $f_x(w) = v$
3.  $w$  is of the form  $x^n v$  for  $n \neq -1$  then  $f_x(w) = x^{n+1}v$

I also define  $g_x : R \rightarrow R$  by

1.  $w$  does not begin with some  $x^n$  then  $g_x(w) = x^{-1}w$
2.  $w$  is of the form  $x^1 v$  then  $g_x(w) = v$
3.  $w$  is of the form  $x^n v$  for  $n \neq 1$  then  $g_x(w) = x^{n-1}v$

We can observe that  $f_x \circ g_x = g_x \circ f_x = 1_R$ .

For each  $x \in X$ ,  $f_x \in \sum_R$  (the group of permutations of  $R$ ) and  $g_x = f_x^{-1}$ . Let  $F$  be the subgroup of  $\sum_R$  generated by  $\{f_x : x \in X\}$  or  $\{f_{x_1}^{n_1}, \dots, f_{x_t}^{n_t} : x_i \in X, n_i \in \mathbb{Z}\}$ .

Let  $i : X \rightarrow F$  with  $i(x) = f_x$ . For any word  $w = x_1^{n_1} x_2^{n_2} \dots x_t^{n_t}$ . Let  $f_w = f_{x_1}^{n_1} f_{x_2}^{n_2} \dots f_{x_t}^{n_t} \in F$ .

Key Facts:

1. If  $w$  is obtained from  $\bar{w}$  by a single reduction step,  $f_w = f_{\bar{w}}$ .
2. If  $w$  is obtained from  $\bar{w}$  by any sequence of reduction steps, then  $f_w = f_{\bar{w}}$ .
3. If  $w \in R$  then  $f_w(\langle \rangle) = w$
4. For any word  $w$ ,  $f_w(\langle \rangle)$  the unique reduced word to which  $w$  can be transformed by reduction step.
5. If  $w_1, w_2$  are reduced words then  $v =$  unique reduction of  $w_1 w_2$ ,  $f_v = f_{w_1} f_{w_2}$

Let  $F'$  be the group whose underlying set is  $R$  whose operation is "concatenate and reduce". Then  $F \simeq F'$  by  $f_v \mapsto v$ . To finish, let  $G$  be a group,  $h : X \rightarrow G$  function. We want to find there is a unique homomorphism  $\phi$  with  $F' \rightarrow G$  and  $\phi \circ i = h$ .

1. If  $\phi$  exists then

$$\begin{aligned} \phi(x_1^{n_1} x_2^{n_2} \dots x_t^{n_t}) &= \phi(i(x_1))^{n_1} \phi(i(x_2))^{n_2} \dots \phi(i(x_t))^{n_t} \\ &= h(x_1)^{n_1} h(x_2)^{n_2} \dots h(x_t)^{n_t} \end{aligned}$$

2. Verify  $\phi$  is a homomorphism.

□

**Example 8.4.** Let  $X = \langle x, y \rangle$ , let  $G$  be any group with 2 generators say  $G = \langle a, b \rangle$ . Let  $F$  be a free group on  $X$ . Let  $\phi : F \rightarrow G$  be unique homomorphism such that  $\phi(x) = a$  and  $\phi(y) = b$ .  $\phi$  is surjective because  $G$  is generated by  $a$  and  $b$ . Thus,  $G \simeq \frac{F}{\ker \phi}$ .



## 9 Lecture 9: Generators and Relations (Feb 2)

**Definition 9.1.** let  $X$  be a set, let  $F$  be a free group on  $X$ . Let  $A \subseteq F$  and  $N =$  least normal subgroup of  $F$  containing  $A$ .

**Theorem 9.2.** Let  $\bar{F} = F/N$  and  $j : X \rightarrow \bar{F}$  by  $j(x) = xN$ .

$$\begin{array}{ccc} F & \xrightarrow{\phi_N} & \bar{F} \\ \uparrow i & \nearrow j & \\ X & & \end{array}$$

The following are true:

1.  $\bar{F}$  is generated by  $\{j(x) : x \in X\}$ . Let  $\bar{x} = j(x)$
2. If  $a = x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t} \in A$  then  $a \in N$  and  $\bar{x}_1^{n_1} \bar{x}_2^{n_2} \cdots \bar{x}_t^{n_t} = \phi_N(a) = 1_{\bar{F}}$

"Universal Property of  $\bar{F}$ ": Let  $G$  be a group and let  $h : X \rightarrow G$  such that  $a = x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t} \in A$  and  $h(x_1)^{n_1} h(x_2)^{n_2} \cdots h(x_t)^{n_t} = 1_G$ . There is an unique homomorphism  $\mathcal{T} : \bar{F} \rightarrow G$  such that

$$\begin{array}{ccc} X & \xrightarrow{j} & \bar{F} \\ & \searrow h & \downarrow \mathcal{T} \\ & & G \end{array}$$

So  $h = \mathcal{T} \circ j$

*Proof.* Since  $\{\bar{x} : x \in X\}$  generates  $\bar{F}$  there is at most one  $\tau$ . By universal property of  $F$ , there is unique homomorphism  $\phi : F \rightarrow G$  such that

$$\phi(x^1) = h(x). \quad (\text{For all } x \in X)$$

Use property of  $F$

$$\begin{array}{ccc} X & \xrightarrow{i} & F \\ & \searrow h & \downarrow \phi \\ & & G \end{array}$$

Claim: By hypothesis on  $h$ ,  $A \subseteq \ker(\phi)$ .

Let  $a = x_1^{t_1} x_2^{t_2} \cdots x_k^{t_k} \in A$  then  $\phi(a) = \phi(x_1)^{t_1} \phi(x_2)^{t_2} \cdots \phi(x_k)^{t_k} = h(x_1)^{t_1} h(x_2)^{t_2} \cdots h(x_k)^{t_k} = 1_G$  since  $h(x_1)^{t_1} h(x_2)^{t_2} \cdots h(x_k)^{t_k} = 1_G$ . Thus,  $a \in \ker(\phi)$ .

By choice of  $N$ ,  $N \leq \ker(\phi)$ , we'll attempt to define  $\tau : \bar{F} \rightarrow G$  by  $\tau(wN) = \phi(w)$  for  $w \in F$ .

$\tau$  is well defined because  $w_1 N = w_2 N \implies w_1^{-1} w_2 \in N \implies w_1^{-1} w_2 \in \ker(\phi) \implies \phi(w_1)^{-1} \phi(w_2) = 1 \implies \phi(w_1) = \phi(w_2)$ . Showing  $\tau$  is a homomorphism is straightforward.

$$\begin{array}{ccc} X & \xrightarrow{i} & F \\ & \searrow h & \downarrow \phi_N \\ & & \overline{F} \end{array} \quad \begin{array}{ccc} & & \searrow \phi \\ & & G \\ & \dashrightarrow \mathcal{T} & \end{array}$$

□

## 10 Lecture 10: Presentation of Groups (Feb 4)

**Example 10.1.** *Dihedral Group:  $D_n$  = symmetry group of a regular  $n$ -gon.*

*Let  $D_n = \langle a, b \rangle$  where  $a$  = rotation by  $\frac{2\pi}{n}$  and  $b$  = reflection about the vertical axis. Then  $D_n$  is generated by  $a$  and  $b$  with the relations  $a^n = 1$  and  $b^2 = 1$ .*

*We have  $bab^{-1}a = 1$*

*Let  $X = \{x, y\}$  and  $F$  be free group and  $A = \{x^n, y^2, yxy^{-1}x\}$  and  $N =$  least normal subgroup  $\supseteq A$ . Let  $\bar{x} = xN$  and  $\bar{y} = yN$ . Then  $F/N = \langle \bar{x}, \bar{y} \rangle$  and*

$$\overline{yxy^{-1}x} = \bar{y}\bar{x}\bar{y}^{-1}\bar{x}^{-1} = 1_{\bar{F}}.$$

*There is a unique homomorphism  $\tau : F/N \rightarrow D_n$  such that  $\tau(\bar{x}) = a$  and  $\tau(\bar{y}) = b$  as  $D_n = \langle a, b \rangle$  so  $\tau$  is surjective. So  $|F/N| \geq 2n$ .*

*Claim:  $|F/N| \leq 2n$  (so  $\tau$  is isomorphism)*

*Proof: Using relations from before, we can simply write any expression in  $\bar{x}, \bar{y}$  down to  $\bar{x}^s \bar{y}^t$  for  $0 \leq s \leq n$  and  $0 \leq t \leq 2$ .*

# 11 Lecture 11: Category Theory (Feb 6)

## 11.1 Categories

**Example 11.1.**

1. Category of sets, if we have two sets  $A$  and  $B$  then  $A \rightarrow B$  is a function  $f : A \rightarrow B$
2. Category of groups, if we have two groups  $G$  and  $H$  then  $G \rightarrow H$  is a homomorphism  $\phi : G \rightarrow H$
3. Category of topological spaces, if we have two topological spaces  $X$  and  $Y$  then  $X \rightarrow Y$  is a continuous function  $f : X \rightarrow Y$

**Definition 11.2.** A category  $\mathcal{C}$  consists of the following data:

1. A collection of objects  $Ob(\mathcal{C})$
2. A collection of morphisms  $Mor(\mathcal{C})$
3. For each morphism  $f$ , there are objects  $dom(f)$  and  $cod(f)$  such that  $dom(f) \rightarrow cod(f)$  is a morphism in  $Mor(\mathcal{C})$
4. A composition operation  $Mor(\mathcal{C}) \times Mor(\mathcal{C}) \rightarrow Mor(\mathcal{C})$
5. An identity morphism  $1_A : A \rightarrow A$  for each object  $A \in Ob(\mathcal{C})$

**Lemma 11.3.** The following are true:

1. If  $a \xrightarrow{f} b$  then  $f1_a = f$  and  $1_b f = f$ .
2. If  $a \xrightarrow{f} b \xrightarrow{g} c \xrightarrow{h} d$  then  $h(gf) = (hg)f$

**Example 11.4.** Posets:  $\mathbb{P}$  is a poset with  $\leq$  binary relation such that

1.  $a \leq a$  for all  $a \in \mathbb{P}$
2.  $a \leq b$  and  $b \leq a \implies a = b$
3.  $a \leq b$  and  $b \leq c \implies a \leq c$

Given poset  $\mathbb{P}$ , make "poset category" with objects the elements of  $\mathbb{P}$ . There is only one morphism  $a \rightarrow b$  if  $a \leq b$  and no morphism if  $a \not\leq b$ .

**Definition 11.5.** Let  $\mathcal{C}$  be a category. An object is an initial if for all object  $b$  there is a exactly one arrow  $a \rightarrow b$ .

**Definition 11.6.** An arrow  $a \xrightarrow{f} b$  in  $\mathcal{C}$  is an isomorphism iff there is another  $b \xrightarrow{g} a$  such that  $gf = 1_b$  and  $fg = 1_a$ .

**Lemma 11.7.** *If  $a, b$  are initial objects in  $\mathcal{C}$  they are uniquely isomorphic.*

*Proof.* Let  $a \xrightarrow{f} b$  and  $b \xrightarrow{g} a$  be unique arrows from  $a$  to  $b$  and  $b$  to  $a$  respectively. Then we have  $a \xrightarrow{gf} a$  and  $b \xrightarrow{fg} b$  so  $gf = 1_a$  and  $fg = 1_b$ .  $\square$

**Definition 11.8.** *Object  $b$  is terminal iff for all  $a$  there is a unique  $a \rightarrow b$  iff  $b$  is initial in  $\mathcal{C}^{op}$*

**Lemma 11.9.** *Two terminal objects are uniquely isomorphic.*

**Definition 11.10.** *Let  $\mathcal{C}$  and  $\mathcal{D}$  be categories. A functor from  $\mathcal{C}$  to  $\mathcal{D}$  is  $\mathcal{C} \xrightarrow{F} \mathcal{D}$ . Assign to each object  $a$  of  $\mathcal{C}$  an object  $F(a)$  of  $\mathcal{D}$ . For each arrow  $a \xrightarrow{f} b$  there is an arrow  $F(a) \xrightarrow{F(f)} F(b)$  with  $f(1_a) = 1_{F(a)}$ . Additionally,  $F(gf) = F(g)F(f)$*

## 12 Lecture 12: Ring Theory (Feb 8)

**Definition 12.1.** A ring is a set  $R$  with two binary operations  $+$  and  $\times$  such that

1.  $(R, +)$  is an abelian group
2.  $(R, \times)$  is associative
3.  $a \times (b + c) = a \times b + a \times c$  and  $(b + c) \times a = b \times a + c \times a$  for all  $a, b, c \in R$

**Example 12.2.** The following are rings

1.  $\mathbb{Z}, 2\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
2.  $M_2(\mathbb{Z})$
3.  $\{f : \mathbb{R} \rightarrow \mathbb{R} \text{ continuous}\}$
4.  $\{f : \mathbb{R} \rightarrow \mathbb{R} \text{ differentiable}\}$

**Definition 12.3.**  $R$  is commutative iff  $rs = sr$  for all  $r, s \in R$

**Definition 12.4.**  $R$  is unital iff there exists  $1_R \in R$  such that  $1_R r = r 1_R = r$  for all  $r \in R$

**Definition 12.5.** Let  $R, S$  be rings. A ring homomorphism from  $R$  to  $S$  if  $\phi : R \rightarrow S$  satisfy:

1.  $\phi(r + s) = \phi(r) + \phi(s)$  for all  $r, s \in R$
2.  $\phi(rs) = \phi(r)\phi(s)$  for all  $r, s \in R$
3.  $\phi(1_R) = 1_S$

**Definition 12.6.** Let  $S$  be a subring of  $R$  if  $S$  is a ring and the inclusion map  $i : S \rightarrow R$  is a ring homomorphism.

**Definition 12.7.** Let  $\phi : R \rightarrow S$  be a ring homomorphism then

1.  $\ker(\phi) = \{r \in R : \phi(r) = 0\}$  is a subring of  $R$
2.  $\phi(R) = \{s \in S : \exists r \in R, \phi(r) = s\}$  is a subring of  $S$

**Remark 12.8.** In general, not the case that  $\ker(\phi)$  is a subring of  $R$ .

**Definition 12.9.** Let  $R$  be a ring. An ideal of  $R$  is a subring  $I$  of  $R$  such that

1.  $I \leq (R, +)$
2. For all  $a \in R$  and  $b \in I$ ,  $ab \in I$ .

**Definition 12.10.** *Let  $I$  be an ideal of  $R$  then we define  $r + I = \{r + i : i \in I\}$*

## 13 Lecture 13: Ideals and Quotient Rings (Feb 10)

**Theorem 13.1.** *First Isomorphism Theorem of Rings: Let  $R, S$  be rings and  $\phi : R \rightarrow S$  be a homomorphism with  $\ker(\phi)$  an ideal of  $R$  and  $\text{im}(\phi)$  a subring of  $S$ . Then we get isomorphism*

$$\tau : \frac{R}{\ker(\phi)} \xrightarrow{\cong} \text{im}(\phi) \text{ and } \tau : r + \ker(\phi) \mapsto \phi(r).$$

**Theorem 13.2.** *The following are true for any ideals  $I, J$  of  $R$ :*

1.  $I + J =$  smallest ideal containing  $I$  and  $J$
2.  $I \cap J =$  largest ideal contained in  $I$  and  $J$
3.  $IJ = \{\sum_{i=1}^n r_i s_i | n \in \mathbb{N}, r_i \in I, s_i \in J\} \subseteq I \cap J$
4. Ideals of  $R/I$  are in bijection with ideals of  $R$  that contain  $I$

**Definition 13.3.**  $R$  is a zero ring if  $R = \langle 0_R \rangle$

Note: If  $1_R = 0_R$  then  $r \cdot 1 = r \cdot 0 = 0$  and  $R$  is a zero ring.

**Definition 13.4.**  $R$  is an integral domain iff

1.  $1_R \neq 0_R$  ( $R$  is not a zero ring)
2. For all  $a, b \in R$ 

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

**Definition 13.5.**  $R$  is a field iff

1.  $1_R \neq 0_R$
2. Every element of  $R \setminus \{0_R\}$  has a multiplicative inverse

**Exercise 13.6.** If  $R$  is a field then  $R$  is an integral domain.

**Definition 13.7.** Let  $R$  be a ring. Then  $u \in R$  is a unit iff  $u$  has a multiplicative inverse.

We let

$$U(R) = \{u \in R : u \text{ is a unit}\}.$$

$U(R)$  is a group under multiplication.

**Definition 13.8.** An ideal  $I$  of  $R$  is principal iff  $I = aR$

**Lemma 13.9.** Let  $R$  be any ring then  $R$  is the largest ideal and  $\{0_R\}$  is the smallest ideal.



**Remark 13.10.** We have  $R/R = \{0_R\}$  and  $R/\{0_R\} \simeq R$

**Theorem 13.11.** Let  $R$  be a field and let  $I$  be an ideal then  $I = 0$  or  $I = R$

*Proof.* Assume  $I \neq 0$ , let  $a \in I$  and  $a \neq 0$ . There exist  $b \in R$  such that  $ab = 1 \in I$ . In any ring  $1 \in I$  iff  $I = R$ . □

**Theorem 13.12.** If  $R \neq 0$  are the only two ideals of  $R$  then  $R$  is a field.

*Proof.* Let  $a \in R, a \neq 0$  then  $(a) \neq 0$  as  $a \in (a)$  so  $(a) = R$  so  $1 \in (a)$  and  $1 = ab$  for some  $b$ . □

**Definition 13.13.** An ideal  $I$  of  $R$  is maximal iff

1.  $I \neq R$
2. For all ideals  $J \supseteq I$ ,  $J = I$  or  $J = R$

$I$  is maximal in poset  $\{J : J \text{ ideal}, J \neq R\}$  ordered by  $\subseteq$

**Lemma 13.14.** If  $I$  is an ideal of  $R$ ,

$$I \text{ maximal} \iff R/I \text{ is a field.}$$

*Proof.*  $R \neq I \iff 1_{R/I} \neq 0_{R/I}$ . By  $R$  maximal iff there are only two 2 ideals of  $R/I$  which are 0 and  $R/I$ . □

**Definition 13.15.** Ideal  $I$  is prime iff

1.  $I \neq R$
2. For all  $a, b \in R$ ,  $ab \in I \implies a \in I$  or  $b \in I$

**Lemma 13.16.**  $R/I$  is an integral domain iff  $I$  is a prime ideal.

**Definition 13.17.**  $\text{Spec}(R) = \{I : I \text{ is a prime ideal of } R\}$

**Theorem 13.18.** Let  $R$  be a ring.  $I$  is an ideal of  $R$ ,  $I \neq R$ . Then there is a maximal ideal  $J$  such that  $I \subseteq J$ .

## 14 Lecture 14: Zorn's Lemma and Modules (Feb 13)

**Lemma 14.1.** *Zorn's Lemma: If  $\mathbb{P}$  is a poset such that every chain in  $\mathbb{P}$  has an upper bound, then for every element  $p$  of  $\mathbb{P}$  there is a  $q \geq p$  with  $q$  maximal.*

**Example 14.2.** *Claim:  $\mathbb{Q}$  satisfies the hypothesis of Zorn's Lemma.*

*Proof.* Let  $(I_a : a \in A)$  be a chain in  $\mathbb{Q}$ . That is,  $I_a$  is ideal with  $I_a \neq R$  and for  $a, b \in A$ ,  $I_a \subseteq I_b$  or  $I_b \subseteq I_a$ . We need upper bound, let

$$J = \bigcup_{a \in A} I_a = \{r : \text{there is } a \in A, r \in I_a\}.$$

Verify  $J$  is an ideal and for  $r, s \in J$  then  $r \in I_a$  and  $s \in I_b$ . WLOG let  $I_a \subseteq I_b$  so  $r, s \in I_b$  so  $r + s \in I_b \subseteq J$ .

Verify  $J \neq R$ , easy as  $1 \notin I_a$  all  $a$  so  $1 \notin J$ . □

### 14.1 Modules

**Definition 14.3.** *Let  $R$  be a ring. A  $R$ -module is an abelian group  $(M, +)$  equipped with a function  $R \times M \rightarrow M$  by  $(r, m) \mapsto rm$  such that*

1.  $0_R m = 0_M, 1m = m$  for all  $m \in M$
2.  $(r_1 + r_2)m = r_1 m + r_2 m$  and  $m(r_1 + r_2) = m r_1 + m r_2$
3.  $r(sm) = (rs)m$  for  $r, s \in R$  and  $m \in M$

**Definition 14.4.** *If  $M$  is a  $R$ -module, we can form "linear combinations"*

$$\sum_{i=1}^n r_i m_i \text{ for } r_i \in R \text{ and } m_i \in M.$$

**Example 14.5.** *Let  $R = \mathbb{Z}$  and  $(G, +)$  be an abelian group. Then  $G$  is a  $\mathbb{Z}$ -module.*

**Definition 14.6.** *If  $M$  is a  $R$ -module, a submodule of  $M$  is  $N$  such that  $N \leq (M, +)$ ,  $rn \in N$  for  $r \in R$  and  $n \in N$ .*

**Remark 14.7.** *If  $R$  is a ring, we can view  $R$  as a  $R$ -module. The ideals of  $R$  are the submodules of  $R$  (viewed as a  $R$ -module).*

**Definition 14.8.** *Let  $M, N$  be  $R$ -modules. A  $R$ -module homomorphism is a function  $\phi : M \rightarrow N$  such that*

1.  $\phi$  is a group homomorphism for  $(M, +)$  to  $(N, +)$
2.  $\phi(rm) = r\phi(m)$  for  $r \in R$  and  $m \in M$

*Note: This is like linear transformation in linear algebra.*

## 15 Lecture 15: Modules (Feb 16)

**Definition 15.1.** Let  $M$  and  $N$  be  $R$ -modules then we say  $\phi : M \rightarrow N$  is  $R$ -linear if

$$\phi\left(\sum_{i=1}^n r_i m_i\right) = \sum_{i=1}^n r_i \phi(m_i) \text{ for } r_i \in R \text{ and } m_i \in M.$$

**Definition 15.2.** Let  $M \leq N$  ( $M$  is submodule of  $N$ ),  $N/M = \{n + M : n \in N\}$ . We define

$$1. n_1 + M + n_2 + M = (n_1 + n_2) + M$$

$$2. r(n + M) = (rn) + M$$

We can define the  $R$ -linear quotient map  $\phi_M : N \rightarrow N/M$  by  $\phi : n \mapsto n + M$  with  $\ker(\phi_M) = M$ .

**Theorem 15.3.** First Isomorphism Theorem for Modules: Let  $\phi : M_1 \rightarrow M_2$  linear, then

$$\text{im}(\phi) \simeq \frac{M_1}{\ker(\phi)}.$$

via  $m + \ker(\phi) \mapsto \phi(m)$

**Definition 15.4.** Given  $R$ -module  $M$  and set  $X \subseteq M$ , the least submodule containing  $X$  is

$$\text{Span}(X) = \left\{ \sum_{i=1}^n r_i x_i \mid n \in \mathbb{N}, r_i \in R, x_i \in X \right\}.$$

We specifically define  $\text{Span}(\emptyset) = \{0_M\}$

**Definition 15.5.** If  $R$  is a ring,  $X \subseteq R$  we write  $\langle X \rangle$  for the least ideal containing  $X$

$$\langle X \rangle = \left\{ \sum_{i=1}^n r_i x_i \mid n \in \mathbb{N}, r_i \in R, x_i \in X \right\}.$$

**Definition 15.6.** A ring  $R$  is a principal ideal ring iff all ideals of  $R$  are principal (a principal ideal is of form  $Ra$  for some  $a \in R$ ).

**Definition 15.7.**  $R$  is a principal ideal domain iff  $R$  is integral domain and principal ideal ring.

**Definition 15.8.** A ring  $R$  is noetherian iff every ideal of  $R$  is finitely generated. (An ideal is finitely generated if  $I = Ra_1 + \cdots + Ra_n$  for some  $a_1, \dots, a_n \in R$ .)

**Theorem 15.9.** *If  $I$  is an ideal of  $R$  the ideals  $R/I$  are in bijection with  $\{J : J \text{ ideal of } R, J \supseteq I\}$ .*

*Also prime ideals of  $R/I$  correspond to prime ideals of  $R$  that contain  $I$ .*

**Example 15.10.** *Common PID's*

1.  $\mathbb{Z}$
2.  $k[x]$  for  $k$  a field

**Definition 15.11.**  *$R$  is a Euclidean Domain iff*

1.  *$R$  is integral domain*
2. *There is a function  $\phi : R \setminus \{0\} \rightarrow \mathbb{N}$  such that for all  $a, b \in R$ , for  $b \neq 0$ , there exist  $q, r$  such that  $a = bq + r$  either  $r = 0$  or  $\phi(r) < \phi(b)$*

**Example 15.12.** *If  $R = \mathbb{Z}$  then  $\phi(n) = |n|$  is a Euclidean Domain.*

**Example 15.13.** *If  $R = k[x]$  for  $k$  a field then  $\phi(f) = \deg(f)$  is a Euclidean function.*

**Theorem 15.14.** *If  $R$  is a Euclidean Domain then  $R$  is a PID.*

*Proof.* Let  $R$  be euclidean domain and let  $I$  be the ideal of  $R$ . If  $I = 0$  then we're done. If  $I \neq 0$  consider  $\{\phi(r) | r \in I, r \neq 0\} \subseteq \mathbb{N}$ . Let  $n$  be the minimal element and let  $a \in I \setminus \{0\}$  such that  $\phi(a) = n$ . As  $a \in I, Ra \subseteq I$ . Let  $b \in I$ , find  $q, r$  such that  $b = aq + r$  either  $r = 0$  or  $\phi(r) < n$ . We have  $r = b - aq \in I$ . So  $r = 0$  and  $b \in Ra$ .  $\square$

**Lemma 15.15.** *Facts about Integral Domains: Let  $R$  be an integral domain.*

1. *If  $a \neq 0$  and  $ab = ac$  then  $a(b - c) = 0$*
2.  *$Ra = Rb$  iff  $a$  and  $b$  are associates*

**Lemma 15.16.** *Let  $R$  be any ring, the following are true about units*

1.  *$u$  unit iff  $u$  has a multiplicative inverse*
2. *Units of  $R$  form a group under multiplication*
3.  *$a, b \in R$  are called associates iff there is an unit  $u$  such that  $au = b$ .*

**Example 15.17.**  $\mathbb{Z}[x]$  is not a PID. Consider the ideal  $\langle 2, x \rangle = \{f : \text{constant term of } f \text{ is even}\}$ .

**Theorem 15.18.**  *$R$  Noetherian iff  $R[x]$  is Noetherian.*

## 16 Lecture 16: Integral Domains

**Definition 16.1.** Let  $p \in R$

1.  $p$  is prime if and only if  $p$  is a nonzero non-unit and for all  $r, s \in R$ ,  $p|rs$  implies  $p|r$  or  $p|s$ .
2.  $p$  is irreducible if and only if  $p$  is a nonzero non-unit and for all  $r, s \in R$  and  $p = rs$  then one of  $r$  or  $s$  is a unit.

**Lemma 16.2.** The following are true

1. As  $R$  is an ID, for any  $a \in R$ , a nonzero non-unit iff  $(a) \neq 0, R$
2. If  $p$  is prime, then  $(p)$  is a prime ideal
3.  $p$  prime implies  $p$  is irreducible.
4. If  $R$  PID then prime = irreducible.
5. In any ID,  $(0)$  is a prime ideal.

**Definition 16.3.**  $R$  is a unique factorization domain (UFD) iff

1.  $R$  is an integral domain
2. Every non-zero nonunit in  $R$  is a product  $u_1, \dots, u_n$ ,  $n > 0$ ,  $u_i$  irreducible.
3. If  $m, n > 0$  then  $u_1 \dots u_n = v_1 \dots v_m$  and  $u_i, v_j$  irreducible, then  $m = n$  and  $u_i$  are associates and permutations of  $v_j$

**Recall 16.4.** An  $R$ -module  $M$  is finitely generated (fg) if there are  $m_1, \dots, m_n \in M$  such that  $M = \text{Span}(m_1, \dots, m_n)$ .

**Definition 16.5.** An  $R$ -module  $N$  is Noetherian iff every submodule of  $N$  is finitely generated.

Equivalently, Ring  $R$  is Noetherian iff  $R$  is Noetherian as an  $R$ -module that is all ideals are finitely generated.

**Example 16.6.** Non-Noetherian Rings:

$$R = \bigcup_{n=1}^{\infty} \mathbb{Z}[x_1, \dots, x_n].$$

Consider the ideal

$$I = \langle x_1, x_2, \dots \rangle = \{f \in R : f \text{ has no constant term}\} = \{f : f(0, \dots) = 0\}.$$

*Proof.* If  $I$  is finitely generated there is  $h_1, \dots, h_n \in I$  such that

$$I = Rh_1 + \dots + Rh_n = (h_1) + \dots + (h_n).$$

Each  $h_i$  has finite  $x_j$ 's in it so find  $N$  so large that  $x_N$  does not appear in any  $h_i$ . As  $x_N \in I$  there are  $f_1, \dots, f_n \in R$  such that  $x_N = \sum_{i=1}^n f_i h_i$ . Substitute

$$x_j = \begin{cases} 0 & \text{if } j < N \\ 1 & \text{if } j \geq N \end{cases}.$$

Then we conclude  $1 = 0$  which is a contradiction.  $\square$

**Theorem 16.7.** *Let  $M$  be a  $R$ -module then the following are equivalent*

1.  $M$  is Noetherian
2. For any increasing chain of submodules  $N_0 \subseteq N_1 \subseteq N_2 \subseteq \dots$  of  $M$ , the chain is eventually constant.
3. For any nonempty set  $X$  of submodules of  $M$ , there is some  $N \in X$  which is maximal under inclusion.

*Proof.* (1)  $\implies$  (2): Consider  $N_\infty = \bigcup_{i=0}^\infty N_i = \{m : \exists i \in \mathbb{N}, m \in N_i\}$ .

Verify that  $N_\infty$  is a submodule of  $M$ , as  $M$  is noetherian,  $N_\infty$  is finitely generated say  $N_\infty = \text{Span}(X)$  with  $X \subseteq N_\infty$  finite. Find  $i$  such that  $X \subseteq N_i$  then  $N_\infty = \text{Span}(X) \subseteq N_i \subseteq N_j \subseteq N_\infty$  for  $j \geq i$ .

(2)  $\implies$  (1): AFSOC there is  $N \leq M$  with  $N$  not finitely generated. Take  $n_0 \in N$  and  $n_0 \neq 0$ . Choose  $n_1 \in N \setminus Rn_0$  and generally

$$n_k \in N \setminus \left( \sum_{i < k} Rn_i \right).$$

In the end, let  $N_i = \sum_{j < i} Rn_j$  then  $N_0 < N_1 < N_2 < \dots$ , a contradiction.  $\square$

## 17 Lecture 17: PID (Feb 19)

**Lemma 17.1.** *If  $R$  PID then*

1.  $R$  is Noetherian
2.  $0$  is a prime ideal and  $0$  is maximal iff  $R$  is a field
3. For  $a \neq 0$ ,  $(a)$  prime iff  $a$  prime iff  $(a)$  maximal iff  $a$  irreducible

**Theorem 17.2.** *If  $R$  is a PID then  $R$  UFD*

**Claim 17.3.** *Every nonzero non-unit  $a \in R$  is a product of irreducibles.*

*Proof.* If not, choose  $a$  that is not a finite product of irreducibles such that  $(a)$  is maximal under inclusion,  $a$  not finite product of irreducibles.  $a$  is not irreducible.

So  $a = bc$  where  $b, c$  not units. So  $(a) \subsetneq (b)$  and  $(a) \subsetneq (c)$  so  $b, c$  are finite products of irreducibles. Contradiction so  $a$  is a finite product of irreducibles.  $\square$

**Claim 17.4.** *If  $u_1 \dots u_n = v_1 \dots v_m$  with  $u_i, v_j$  irreducible then  $m = n$  and  $u_i, v_j$  are the same up to permutations and associates.*

*Proof.*  $u_1$  divides  $v_1 \dots v_m$ . As  $R$  PID,  $u_1$  is prime so  $u_1 | v_j$  for some  $j$ . As  $v_j$  is irreducible,  $u_1$  either unit or an associate of  $v_j$ . As  $u_1$  irreducible,  $u_1$  not a unit. So  $u_1$  and  $v_j$  are associates. Say  $u_1 = x \cdot v_j$  for  $x$  unit. Then

$$xu_2 \dots u_n = v_1 \dots v_{j-1} v_{j+1} \dots v_m.$$

Finish by induction.  $\square$

**Corollary 17.5.** *If  $k$  field,  $k[x]$  is a UFD.*

**Lemma 17.6.** *If  $R$  PID and  $p \in R$  irreducible then  $R/(p)$  is a field.*

**Theorem 17.7.** (Hilbert's Basissatz Theorem) *If  $R$  Noetherian ring then  $R[x]$  is Noetherian ring.*

*Proof.* Let  $I$  be ideal of  $R[x]$ . For each  $n$  let

$$J_n = \{r \in R : \exists c_0, \dots, c_{n-1} \in R, rx^n + \sum_{i=0}^{n-1} c_i x^i \in I\}.$$

$\square$