21-610
Algebra I

Rohan Jain

Contents

Chapter Page 2

Chapter 1

1.1 1/17 - Group Actions

Definition 1.1.1: Action

With a group G and set X, an *action* of G on X is a HM from G to Σ_X (the group of permutations of X).

Definition 1.1.2: $g \cdot x$

If $\phi : G \to \Sigma_X$ is an action, then for $g \in G$ and $x \in X$, we write $g \cdot x$ for $\phi(g)(x)$.

Note:

People will eventually lose the $\cdot$. So, $g \cdot x$ will be written as gx.

Example 1.1.1 (actions)

- $1 \cdot x = x$ $(*)$
- $g \cdot (h \cdot x) = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))(x) = \phi(gh)(x) = (gh) \cdot x$ $(**)$

If $\cdot : G \times X \to X$ satisfies $(*)$ & $(**)$, then there's unique action $\phi : G \to \Sigma_X$ such that $g \cdot x = \phi(g)(x)$.

Proof. Define $\phi : G \to^X X$ by $\phi(g)(x) = g \cdot x$.
$\phi(g^{-1})$ is 2-sided inverse of $\phi(g)$, $\phi(g) \in \Sigma_X$. So ϕ is an HM by $(**)$. 😊

Definition 1.1.3: Orbit Equivalence Relation

Let G act on X. The *orbit equivalence relation* on X is induced by action: $x \sim y$ if $\exists g \in G$ such that $g \cdot x = y$.

Definition 1.1.4: Orbits

The equivalence classes of this relation are called *orbits*. They are defined as

$$O_x = \{y : x \sim y\} = \{y : \exists g, g \cdot x = y\}$$

Definition 1.1.5: Stabilizer

Let G act on X. The *stabilizer* of $x \in X$ is the subgroup of G defined as

$$G_x = \{g \in G : g \cdot x = x\}$$

Note that $G_x \leqslant G$.

Proof. We need to show that G_x is a subgroup of G.

- $1 \cdot x = x$, so $1 \in G_x$.
- $g \in G_x \implies g \cdot x = x \implies g^{-1} \cdot x = x \implies g^{-1} \in G_x$.
- $g, h \in G_x$. $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, so $gh \in G_x$.

😄

A calculation:

$$\begin{aligned} g_1 \cdot x = g_2 \cdot x &\iff g_2^{-1} \cdot (g_1 \cdot x) = x \\ &\iff (g_2^{-1} g_1) \cdot x = x \\ &\iff g_2^{-1} g_1 \in G_x \\ &\iff g_1 \in g_2 G_x \\ &\iff g_1 G_x = g_2 G_x \end{aligned}$$

This gives a bijection between O_x and set of left cosets of G_x. So, we have the orbit-stabilizer theorem:

Theorem 1.1.1 Orbit-Stabilizer Theorem

Let G act on X. Then for all $x \in X$, $|O_x| = [G : G_x]$.

Definition 1.1.6: Fixed Point

Let G act on X. A *fixed point* of the action is an $x \in X$ such that $g \cdot x = x$ for all $g \in G$. That is, $G_x = G$.

Definition 1.1.7: Fixed-Point Set

Let G act on X. Choose a $g \in G$. The *fixed-point set* of g is the set of all $x \in X$ such that $g \cdot x = x$ and is denoted X_g.

1.2 1/19 - Group Actions

Example 1.2.1 (Automorphism Groups)

$$\mathrm{Aut}(G) = \{f : G \to G : f \text{ is an isomorphism}\}$$

$\phi \in \Sigma_G$, $\phi(ab) = \phi(a)\phi(b)$. Recall conjugate of h by g is $h^g = ghg^{-1}$.
Fact 1: For any $g \in G$, $h \mapsto h^g$ is an automohism of G.
Fact 2: If $\phi : G \to \mathrm{Aut}(G)$, $\phi : g \mapsto (h \mapsto h^g)$, then ϕ is an HM for G to $\mathrm{Aut}(G)$.
G acts on G by automorphisms. $g \cdot h = h^g = ghg^{-1}$.
In this setting:

1. Orbit equivalence relation is conjugacy.
2. Orbits are conjugacy classes.
3. For $h \in G$, the stabilizer of h for conjugation action $= \{g : h^g = g\}$.

$$\begin{aligned} h^g = h &\iff ghg^{-1} = h \\ &\iff gh = hg \\ &\iff g \in C_G(h) \end{aligned}$$

Definition 1.2.1: Centralizer

Let G act on X. The *centralizer* of $x \in X$ is the subgroup of G defined as

$$C_G(x) = \{g \in G : g \cdot x = x \cdot g\}$$

Theorem 1.2.1 Orbit-Stablizer Equation for conjugation action

$$|\text{conj class of } h| = [G : C_G(h)]$$

$$|G| = \sum_{C \text{ conj. class}} |C|$$

So, if C = class of h, $|C| = [G : C_G(h)]$.

Recall the definition of a fixed-point. So, for G acting on G by conjugation, $X_g = C_G(g)$. That is,

$$h \text{ fixed point} \iff h^g = h \iff hg = gh \qquad \text{(for all } g\text{)}$$

Definition 1.2.2: Center

The *center* of G is $Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}$. In fact, $Z(G)$ is normal in G. That is, $Z(G) \triangleleft G$.

Theorem 1.2.2

Let p be prime. Let G be a group of order p^n. Then $Z(G) \neq 1$.

Proof. Let G act on G by conjugation. G is partitioned into orbits (i.e. conjugacy classes).

For any h, we know that the size of the class of h is $[G : C_G(h)] = \dfrac{p^n}{|C_G(h)|}$. Each orbit has size 1 or a power of p. So, $|C_G(h)|$ is a power of p.

Note in any action of G onto X, x being a fixed point implies $O_x = \{x\}$. So, $|O_x| = 1$.

So, $|G| = A + B$ where A is the number of orbits of size 1 and $B = \sum |C|$ where C is a conjugacy class of size p^n for $n > 0$.

So, $A = p^n - B$. So $p|A$. As $Z(G) \neq \emptyset$, $|Z(G)| > 0, p||Z(G)|$. So, $|Z(G)| \geqslant p$, which is at least 2, so $Z(G) \neq 1$. 😄

Theorem 1.2.3 Cauchy's Theorem

Let G be a finite group. If p is a prime dividing $|G|$, then G has an element or subgroup of order p.

Facts to remember from undergraduate group theory:

- Let $N \triangleleft G$. Then subgroups of G/N are in bijection with $\{H : N \leqslant H \leqslant G\}$. In fact $H \mapsto H/N$ is a bijection.
- Normal subgroups of G/N are uniquely of the form H/N where $H \triangleleft G$ and $N \leqslant H$.
- $H/N \triangleleft G/N$, $\frac{G/N}{H/N} \cong G/H$.

1.3 1/22 - Using Group Actions to Prove Theorems

Now we prove Cauchy's Theorem:

Proof. Let $X = \{(g_1, \ldots, g_p) \in G^p : g_1 \cdots g_p = 1\}$. Some remarks:

- $(g_1, \ldots, g_p) \in X \iff (g_1 \ldots g_{p-1})g_p = 1$. So, $g_p = (g_1 \ldots g_{p-1})^{-1}$ and $(g_p, g_1, \ldots, g_{p-1}) \in X$. So, $|X| = |G|^{p-1}$.
- $X \neq \emptyset$ as $(1, \ldots, 1) \in X$.

So now it's easy to define an action of C_p(cyclic group of order p) on X. Explicitly, if $C_p = \langle a \rangle >$, then $a \cdot (g_1, \ldots, g_p) = (g_2, \ldots, g_p, g_1)$.

Now we analyze the fixed-points. $(g_1, \ldots, g_p)$ if and only if all the g_i are equal. So, fixed points in the action of C_p on X are $(g, \ldots, g) \in X$ where $g^p = 1$.

As $p \mid |G|$, $p \mid |X| = |G|^{p-1}$. As p is prime, $|C_p| = p$. So all orbits have size 1 or p. X is partitioned into orbits, say

$$|X| = C + D_p$$

So $p|C$ where C is the number of fixed-points for this action. As $(1, \ldots, 1)$ is a fixed-point, $C > 0$, so $C \geqslant p > 1$. So, there is a fixed-point $(g, \ldots, g) \in X$ where $g^p = 1$. So, g has order p. 😊

Definition 1.3.1: $\mathrm{Syl}_p(G)$

$\mathrm{Syl}_p(G) = \{H : H \leqslant G, |H| = p^k \text{ for some } k \geqslant 1 \text{ for largest } k\}$

Note:

If $p \nmid |G|$, then $\mathrm{Syl}_p(G) = \{1\}$.

Theorem 1.3.1 Sylow's Theorem

Let G be a finite group. Let p be a prime dividing $|G|$.

1. If $H \leqslant G$ and $|H|$ is a power of p, there is $K \in \mathrm{Syl}_p(G)$ such that $H \leqslant K$.
2. If $K_1, K_2 \in \mathrm{Syl}_p(G)$, then K_1 and K_2 are conjugate.
3. $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$ and divides $|G|$.

Notes before proof:

- Let G be a group. $\alpha \in \mathrm{Aut}(G), H \leqslant G$. Then $\alpha[H] = \{\alpha(h) : h \in H\}$ is a subgroup of G and $\alpha[H] \cong H$. α is a bijection from H to $\alpha[H]$.
- In particular, for $g \in G$, if α is "conjugation by g", then $\alpha[H] = gHg^{-1}$ or H goes to H^g. We can check: G acts on $\{H : H \leqslant G\}$. $g \cdot H = H^g = gHg^{-1}$.
- H is a fixed point of this action if and only if $H^g = H$ for all $g \in G$. That is, $H \lhd G$.
- For any H, stabilizer of H for this action is $N_G(H) = \{g \in G : gHg^{-1} = H\}$.

Definition 1.3.2: Normalizer

Let $H \leqslant G$. The *normalizer* of H in G is $N_G(H) = \{g \in G : gHg^{-1} = H\}$.

- Let G act on X. Then we know that if $Y \subseteq X$, and $g \cdot y \in Y$ for all $g \in G$ and $y \in Y$, then Y is a union of orbits and we then get an action for G onto Y.
- Let G act on X. Let $H \leqslant G$, now easily H acts on X. Each G-orbit breaks up as a union of H-orbits.

1.4 1/26 - Using Group Actions to Prove Theorems

Now we finally prove Sylow's.

Proof. 😊

1.5 1/29 - Series in Groups

Definition 1.5.1: Subnormal Series

A *subnormal series* for a group G is a sequence (G_i) of subgroups

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

Definition 1.5.2: Normal Series

A subnormal series is a *normal series* if $G_i \triangleleft G$ for all i.

Definition 1.5.3: Characteristic Series

A *characteristic series* is a normal series (G_i) such that $G_i \text{char} G$ for all i.

Definition 1.5.4: Commutator

Let G be a group. The *commutator* of $g, h \in G$ is $[g, h] = ghg^{-1}h^{-1}$.

Note:

$[g, h] = 1$ if and only if $gh = hg$.

Definition 1.5.5: Commutator Subgroups

The *commutator subgroup* of G is $[G, G] = \langle [g, h] : g, h \in G \rangle$.

Note:

If $\alpha \in \text{Aut}(G)$, then $\alpha([g, h]) = [\alpha(g), \alpha(h)]$. So $\alpha([G, G]) = [G, G]$. So $[G, G] \triangleleft G$.

What does it mean for G/N to be abelian? We get:

$$\begin{aligned} &[aN, bN] = 1 \forall a, b \\ \iff &[a, b]N = 1 \\ \iff &[a, b] \in N \\ \iff &[G, G] \leqslant N \end{aligned}$$

So $[G, G]$ is the least normal subgroup of G such that G/N is abelian.

Definition 1.5.6: Solvable

A group G is *solvable* iff there is a subnormal series (G_i) in G such that G_{i+1}/G_i is abelian for all $i < n$.

Trivially, abelian groups are solvable. But there are non-abelian solvable groups. For example, S_3 is solvable. This is because $1 \triangleleft A_3 \triangleleft S_3$. $S_3/A_3 \cong C_2$ is abelian.

Theorem 1.5.1

If G is solvable and $H \leqslant G$, then H is solvable.

Proof. Let (G_i) be a subnormal series for G such that $[G_{i+1}, G_{i+1}] \leqslant G_i$ for all $i < n$. Then $(H \cap G_i)$ is a subnormal series for H such that $[H \cap G_{i+1}, H \cap G_{i+1}] \leqslant H \cap G_i$ for all $i < n$. 😄

Theorem 1.5.2

If G is solvable and $N \triangleleft G$, then G/N is solvable.

Proof. Note: If we have $N \triangleleft G$ and $H \leqslant G$ and $\phi_N : G \to G/N$ is the natural homomorphism, then $\phi_N(H) \leqslant= HN/N \leqslant G/N$.

Let (G_i) be a subnormal series for G such that $[G_{i+1}, G_{i+1}] \leqslant G_i$ for all $i < n$. Then (G_iN/N) is a subnormal series for G/N such that $[G_{i+1}N/N, G_{i+1}N/N] \leqslant G_iN/N$ for all $i < n$. 😄

1.6 1/31 -

Theorem 1.6.1

If $N \triangleleft G$ with N and G/N both solvable, then G is solvable.

Proof. Let (N_i) be a subnormal series for N such that $[N_{i+1}, N_{i+1}] \leqslant N_i$ for all $i < n$. Let (V_i) be a subnormal series for G/N such that $[V_{i+1}, V_{i+1}] \leqslant V_i$ for all $i < n$.

For each j, let G_j be the unique subgroup of G such that $N \leqslant G_j$ and $G_j/N = V_j$.

What we want is that $N_0, N_1, \ldots, N_m = N = G_0, G_1, \ldots, G_m = G$ is a subnormal series for G such that $[G_{i+1}, G_{i+1}] \leqslant G_i$ for all $i < n$.

Since $V_j \triangleleft V_{j+1}$, run time to check that $G_j \triangleleft G_{j+1}$. We know that N_{j+1}/N_j and V_{j+1}/V_j are abelian. So we have that $V_{j+1}/V_j = G_{j+1}/N/G_j/N \cong G_{j+1}/G_j$ is abelian. So G_{j+1}/G_j is abelian. So G is solvable. 😄

Definition 1.6.1: Derived Series

Let G be a group. Then the *derived series* of G is a sequence of subgroups of G defined as

$$G^{(0)} = G, G^{(1)} = [G, G], G^{(2)} = [G^{(1)}, G^{(1)}], \ldots, G^{(n+1)} = [G^{(n)}, G^{(n)}]$$

Note:

$G^{(n)}/G^{(n+1)}$ is abelian. In fact, $G^{(n+1)}$ is the best normal subgroup of $G^{(n)}$ such that $G^{(n)}/G^{(n+1)}$ is abelian.

Note:

$G^{(n)}$char$G$ for all n.

Proposition 1.6.1

If there is n with $G^{(n)} = 1$, then G is solvable.

Proof. $G^{(n)} = 1 \implies G^{(n-1)}$ is abelian. So $G^{(n-1)}/G^{(n)} = G^{(n-1)}$ is abelian. So G is solvable. 😄

Proposition 1.6.2

If G is solvable, then there is n with $G^{(n)} = 1$.

Proof. Let (G_i) be a subnormal series for G such that $[G_{i+1}, G_{i+1}] \leqslant G_i$ for all $i < n$. We show by induction on s that $G^{(s)} \leqslant G_{n-s}$ for $0 \leqslant s \leqslant n$.

If this works, then $G^{(n)} \leqslant G_0 = 1$. So $G^{(n)} = 1$.

Base Case: $s = 0$. $G^{(0)} = G \leqslant G_n = G$.

Now suppose $s < n$ and $G^{(s)} \leqslant G_{n-s}$. Then $G^{(s+1)} = [G^{(s)}, G^{(s)}] \leqslant [G_{n-s}, G_{n-s}] \leqslant G_{n-s-1}$.

So $G^{(n)} = 1$. 😊

Definition 1.6.2: Simple

G is *simple* if $G \neq 1$ and $N \triangleleft G$ implies $N = 1$ or $N = G$.

Corollary 1.6.1

If G is abelian and simple, then G is cyclic of prime order.

Theorem 1.6.2

For $n \geqslant 5$, A_n is simple.

Theorem 1.6.3

If G has a nonabelian simple subgroup, then G is not solvable.

Proof. (a) If K is simple and nonabelian, K is definitely not solvable.

(b) Subgroups of solvable groups are solvable.

😊

1.7 2/2 - (absent)

Definition 1.7.1: Nilpotence

A group G is *nilpotent* if there is a subnormal series (G_i) for G such that $G_{i+1} \triangleleft G_i/G_{i+1}$ for all i.

1.8 2/5 - Nilpotency

Definition 1.8.1: Central Series

A *central series* for a group G is a sequence (G_i) of subgroups

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

such that $G_i/G_{i-1} \leqslant Z(G/G_{i-1})$ for all i.

Note that G nilpotent $\iff$ G has a central series.

Definition 1.8.2: Descending Central Series

A *descending central series* for a group G is a sequence (G_i) of subgroups

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n \triangleright \cdots$$

where for each n, $G_{n+1} = [G_n, G]$. In other words, $L_1(G) = G$, $L_{n+1}(G) = [G, L_n(G)]$.

Note that G nilpotent $\iff$ G has a descending central series which has n such that $L_n(G) = 1$.

Definition 1.8.3: Ascending Central Series

An *ascending central series* for a group G is a sequence (G_i) of subgroups

$$1 = Z_0 \triangleleft Z_1 \triangleleft \cdots \triangleleft Z_n \triangleleft \cdots$$

where each successive group is defined by $Z_{n+1} = \{g \in G : \forall y \in G, [x, y] \leqslant Z_i\}$. In other words, $U_0(G) = 1$, $U_{n+1}(G)/U_n(G) = Z(G/U_n(G))$.

Note that G nilpotent $\iff$ G has an ascending central series which has n such that $U_n(G) = G$.

For G nilpotent:

The number of steps it takes the acs to reach G is the same number of steps the dcs takes to reach 1, which are both the least length of a central series.

Definition 1.8.4: Nilpotency Degree

If G nilpotent, G has *nilpotency degree* t if either series takes t steps.

Example 1.8.1 (Nilpotency Degrees)

- Degree 0: $G = 1$.
- Degree 1: G abelian, $G \neq 1$.

Fact ("normalizer property"):

- G nilpotent and $H < G \implies N_G(H) > H$.

Proof. We induct on nilpotence degree:

Base Case: $t = 0$ or $t = 1$. G abelian. $H < G$. $N_G(H) = G > H$.

Now suppose the nilpotenecy degree of $G = t + 1$ and we have the normalizer property for all groups of nilpotency degree $\leqslant t$. Let $H < G$. We proceed with case analysis involving the center. We know that $Z(G) \leqslant N_G(H)$, so:

- Case 1: If $Z(G) \not\leqslant H$, then $H \neq N_G(H)$, done.
- Case 2: If $Z(G) \leqslant H$, consider the acs. We have that $U_0 = 1, U_1 = Z(G)$. We take for granted that the nilpotency degree of $G/Z(G) = t$. So consider the acs of $G/Z(G)$, where $U_0 = Z(G)/Z(G) = 1$, $U_1 = G/Z(G)$. So, $Z(G) \leqslant H < G \implies H/Z(G) < G/Z(G)$ and $G/Z(G)$ has nilpotency degree t. So $N_{G/Z(G)}(H/Z(G)) > H/Z(G)$. So $N_G(H) > H$.

😊

Theorem 1.8.1

If G_1, G_2 are niltpotent, then $G_1 \times G_2$ is nilpotent.

Recall that if $M, N \triangleleft G$ and $M \cap N = 1$, then $mn = nm$ for all $m \in M$ and $n \in N$, then $MN \cong M \times N$ and $MN \triangleleft G$. This generalizes for more than 2 subgroups.

Also recall if G finite and $H \in \mathrm{Syl}_p(G)$, then $N_G(H) = N_G(N_G(H))$.

Proof. $H \triangleleft N_G(H)$, so H is the unique Sylow p-subgroup of $N_G(H)$. So now if $g \in N_G(N_G(H))$, then $N_G(H)^g = N_G(H)$, so H^g is the unique Sylow subgroup of $N_G(H)^g = H$, so $g \in N_G(H)$. ☺

Now let G be finite and nilpotent. Let $|G| = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$. We claim that for each i, G has a unique normal Sylow p_i-subgroup, P_i.

Proof. Let $P_i \in \mathrm{Syl}_{p_i}(G)$. Then $N_G(P_i) = N_G(N_G(P_i))$. By the normalizer property, $N_G(P_i) = G$. So $P_i \triangleleft G$ and P_i is the unique Sylow p_i-subgroup of G. ☺

Then by Lagrange, $P_i \cap P_j = 1$ for $i \neq j$. So $P_1 P_2 \dots P_k \triangleleft G$ and $P_1 \times P_2 \times \dots \times P_k \cong P_1 P_2 \dots P_k$. So $P_1 P_2 \dots P_k = G \cong P_1 \times P_2 \times \dots \times P_k$.

1.9 2/7 - Jordan Holder

Theorem 1.9.1 Jordan-Holder

Let G be a group. Let $(H_i)_{0 \leqslant i \leqslant n}$ and $(G_j)_{0 \leqslant j \leqslant m}$ be two composition series of G. Then $n = m$ and there is a permutation σ of $\{0, 1, \dots, n\}$ such that $H_i / H_{i-1} \cong G_{\sigma(i)} / G_{\sigma(i-1)}$ for all i.

Proof. If $G = 1$ or if G is simple, then the result is trivial. So assume G is not simple or trivial so that $m, n > 1$.

Let $H = H_{n-1}$, so $1 < H \triangleleft G$. G/H is simple and $(H_i)_{0 \leqslant i \leqslant n-1}$ is a composition series for H.

Let k be least k such taht $G_k \not\leqslant H$. Note that $0 < k < m$. ($G_0 = 1 \leqslant H, G_m = G \not\leqslant H$.) Form the subnormal series $(G_i H/H)_{0 \leqslant j \leqslant m} \in G/H$. As G/H is simple, this series is a series of H/H's followed by series of G/H's.

For $j < k$, $G_j \leqslant H, G_j H = H \Rightarrow G_j H/H = H/H = 1$.

So for $j \geqslant k$, $G_j H/H = G/H$, so $G = G_j H$.

For $j \geqslant k$, $G/H = G_j H/H \cong G_j/(G_j \cap H)$.

So (G/H simple), $G_j/(G_j \cap H)$ simple for $j \geqslant k$.

Recall $(H_i)_{0 \leqslant i \leqslant n-1}$ is for h with $n-1$ steps, so our IH applies to H.

Define subnormal series in H that is $(G_j \cap H)_{0 \leqslant j \leqslant m}$.

We want to argue two things:

(a) Deleting one repetition in $(G_j \cap H)_{0 \leqslant j \leqslant m}$, we obtain a composition series for H.

(b) By IH applied to H, $m - 1 = n - 1$ so $m = n$. Argue that we can find IM's between quotients of G_j and H_j.

Note that for $j < k, G_j \leqslant H$, so $G_j = G_j \cap H$.

Let $j > k$. $G_{j-1} \triangleleft G_j, G_j \cap H \triangleleft G_j$. Then we have that $G_{j_1}(G_j \cap H) = G_j$. This yields:

$$\frac{G_{j-1}(G_j \cap H)}{(G_j \cap H)} \triangleleft \frac{G_j}{G_j \cap H} \qquad \text{(this RHS is simple)}$$

So either $G_{j-1}(G_j \cap H) = G_j$ or $G_{j-1}(G_j \cap H) = G_j \cap H$. However, since $j > k$, we have that $G_{j-1} \not\leqslant H$, so $G_{j-1}(G_j \cap H) = G_j$. So:

$$\begin{aligned} \frac{G_j}{G_{j-1}} &= \frac{G_{j-1}(G_j \cap H)}{G_{j-1}} \\ \cong \frac{G_j \cap H}{(G_j \cap H) \cap G_{j-1}} &= \frac{G_j \cap H}{G_{j-1} \cap H} \end{aligned}$$

To finish, we have that $G_{k-1} = G_{k-1} \cap H = G_k \cap H$. We also want to show that $G/H \cong G_k/G_{k-1}$. From $G_{k-1} = G_k \cap H$, $G_k/G_{k-1} \cong G_k/(G_k \cap H) \cong G/H$, by fact already proved.

If G has a composition series with n steps, then a U composition series have n steps and "same quotients".

$G \neq 1$, G not simple. So $n \geqslant 2$. Fix a compostion series $(H_i)_{0 \leqslant i \leqslant n}$ so that $H = H_{n-1} \leqslant G$.

Get another composition series $(G_j)_{0 \leqslant j \leqslant m}$. Choose k such that $G_k \not\leqslant H$. Recall that $G_j \cap H = G_j$ for $j < k$ and that for $j > k$, $\frac{G_j \cap H}{G_{j-1} \cap H} \cong \frac{G_j}{G_{j-1}}$.

We are left to prove that $G_{k-1} = G_k \cap H$ and $\frac{G_k}{G_{k-1}} \cong \frac{G}{H}$.

Assessing this, $G_{k-1} \cap H = G_k \cap H$ and $\text{seq}(G_j \cap H : j \neq k, 0 \leqslant j \leqslant m)$ is a composition series for H with $m-1$ steps with quotients $\frac{G_j}{G_{j-1}}$ for $0 < j \leqslant m, j \neq k$.

We have 2 composition series for h with

$$(H_i)_{0 \leqslant i \leqslant n-1} \text{ and } (G_j \cap H)_{0 \leqslant j \leqslant m-1}$$

By the inductive hypothesis, $m-1 = n-1$, so $m = n$ and up to isomorphism, we can match the quotients of the two series. 😄

1.10 2/9 - Free Groups

Recall that G is cyclic if $G = \langle g \rangle$ for some $g \in G$. In this case, there is a unique HM $\phi : (\mathbb{Z}, +) \to G$ such that $\phi(1) = g$. Clearly ϕ is surjective, so $G \cong \mathbb{Z}/\ker\phi$. So G is abelian.

If $\ker(\phi) = 0 = 0\mathbb{Z}$, then $|G| = \infty$, ϕ is an isomorphism from $\mathbb{Z}$ to G. So there is a unique $n > 0$ such that $\ker(\phi) = n\mathbb{Z}$ and $|g| = n$. ϕ induces an IM from $\mathbb{Z}/n\mathbb{Z}$ to G.

Let's talk about groups that are generated by two elements $G = \langle a, b \rangle$.

1. Any symmetric group S_n for $n \geqslant 2$ is generated by two elements.

$$S_n = \langle (12), (1 \dots n) \rangle$$

2. Any dihedral group D_k for finite k.

Our goal is to find a group $F = \langle a, b \rangle$ such that for all G and all $g, h \in G$, there is a unique HM $\phi : F \to G$ such that $\phi(a) = g$ and $\phi(b) = h$.

We start by trying to construct F using words. Let $\Sigma = \{a, b\}$. A *word* in Σ is a finite sequence of elements of $\Sigma \times \mathbb{Z}$.

Example 1.10.1 (Words)

- Write $(a,3)(b,5)(a,2)(b,1)$ as $a^3b^5a^2b$.

A word is reduced if

- No pairs of form $(s, 0)$ for $s \in \Sigma$
- No successive pairs of form $(s,i)(s,j)$ for $s \in \Sigma$.

Definition 1.10.1: Reduction

Remove terms of the form s^0 and replace successive terms of the form $s^i s^j$ with s^{i+j}.

1.11 2/12 - More Alphabet Stuff

Let σ be a set of any symbols. Words are finite sequences of elements of $\sigma \times \mathbb{Z}$. A word is reduced if it has no terms of the form $(s, 0)$ and no successive terms of the form $(s,i)(s,j)$.

Let W be the set of all reduced words in σ^*. We want to associated to each $s \in \Sigma$, a permutation π_s of W. The idea is that $\pi_s(w)$ is a unique reduction of sw.

$\pi_s(w) = sw$ makes w start with a term s^i for some $i \in \mathbb{Z}$.

If $w = s^i \dots$ and $i \neq -1$, then $\pi_s(w) = s^{i+1} \dots$.

If $w = s^{-1} \dots$, then $\pi_s(w) = \dots$.

Define ρ_s, whose intuition is to reduce $s^{-1}w$.

$\rho_s(w) = s^{-1}w$ unless w starts with a power of s.

If $w = s^i \dots$ and $i \neq 1$, then $\rho_s(w) = s^{i-1} \dots$.

If $w = s\ldots$, then $\rho_s(w) = \ldots$.

One can check that $\pi_s \circ \rho_s = \rho_s \circ \pi_s = \mathrm{id}_W$. As such, π_s is a permutation and $\rho_s = \pi_s^{-1}$.

Let G be the subgroup of Σ_w (the group of permutations of w) generated by $\{\pi_s : s \in \Sigma\}$. If w is a word (not necessarily reduced), say $w = s_1^{i_1} s_2^{i_2} \ldots s_n^{i_n}$, then $\pi_w = \pi_{s_1}^{i_1} \pi_{s_2}^{i_2} \ldots \pi_{s_n}^{i_n} \in G$.

Key fact 1: If w' is obtained from w by a single reduction step, then $\pi_{w'} = \pi_w$.

Key fact 2: $G = \{\pi_w : w \in W\}$.

Proof. from key fact 1. 😄

Key fact 3: If $w \in W$, then $\pi_w(\epsilon) = w$.

So every $g \in G$ is of form π_w for unique reduced word w, where $w = g(\epsilon)$.

Key fact 4: For any words v, w, $\pi_v \circ \pi_w = \pi_{vw}$.

Key fact 5: if w is a word and reduced v is obtained from w by some reduction sequence, then $\pi_v(\epsilon) = \pi_w(\epsilon) = v \Rightarrow v$ is determined by w.

Key fact 6: If $v, w \in W$ and u is the unique redcuced word obatined by reducing vw, then $\pi_u = \pi_v \circ \pi_w$.

Conclusion: G is isomorphic to the group of whose underlying set is W and whose group operation is "concatenate and reduce".

Key point: G_Σ has the following "universal property": For any group H and any function $\phi : \Sigma \to H$, there is a unique HM $\Phi : G \to H$ such that $\Phi \circ \pi_s = \phi(s)$ for all $s \in \Sigma$.

Definition 1.11.1: Free Group

The *free group* on Σ is the group G_Σ with the universal property.

1.12 2/14 - Free Groups

Key property of $Free(\Sigma)$ is called the "universal property." Basically, for all groups H and functions $f : \sigma \to H$, there is unique HM $\alpha : Free(\Sigma) \to H$ such that $\alpha(s') = f(s)'$ for all $s \in \Sigma$.

Let's proceed with a proof of the universal property.

Proof.

1. If such an α exists, then it must be given by the formula

$$\alpha(s_1^{i_1} s_2^{i_2} \ldots s_n^{i_n}) = f(s_1)^{i_1} f(s_2)^{i_2} \ldots f(s_n)^{i_n}$$

for all reduced words $s_1^{i_1} s_2^{i_2} \ldots s_n^{i_n}$.

2. Need to verify that function α specified by (x) is a group HM.

Let $v = s_1^{i_1} s_2^{i_2} \ldots s_n^{i_n}$ and $w = t_1^{j_1} t_2^{j_2} \ldots t_m^{j_m}$ be reduced words. Then vw is a reduced word and $\alpha(vw) = \alpha(v)\alpha(w)$.

😄

1.13 2/19 - Rings

What do we mean when we say R is a ring? For now, they will be commutative rings with unity.

Definition 1.13.1: Ring Homomorphism

Let R and S be rings. Then $\phi : R \to S$ is a *ring homomorphism* iff:

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \\ \phi(ab) &= \phi(a)\phi(b) \\ \phi(1_R) &= 1_S \end{aligned}$$

for all $a, b \in R$.

Definition 1.13.2: Subring

Let $R \subseteq S$ be a subring. This means that the inclusion map $\iota : R \to S$ is a ring homomorphism.

Definition 1.13.3: Ideal

$I \subseteq R$ is an *ideal* iff $I \leqslant (R, +)$ and $tr \in I$ for all $t \in R$ and $r \in I$.

Note:

If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi) = \{r \in R : \phi(r) = 0\}$ is an ideal of R.
Also, if I is an ideal, then $I = R$ iff $1 \in I$.
$\{0\}$ and R are always ideals. 'zero ideal'

Definition 1.13.4: Quotient Ring

Let $I \lhd R$. Then $R/I = \{r + I : r \in R\}$ is the *quotient ring* of R by I.

Note:

$(s + I)(t + I) = st + I$. $\phi_I : R \to R/I$ is a quotient homormophism. $\phi_I(r) = r + I$. $\ker(\phi_I) = I$.

Definition 1.13.5: R-module

Let R be a ring. M is an *R-module* if M is equipped with operations $+ : M \times M \to M$ and scalar multiplication: $R \times M \to M$ with the following properties:

- $(M, +)$ is an abelian group.
- $r(m + n) = rm + rn$ for all $r \in R$ and $m, n \in M$.
- $(r + s)m = rm + sm$ for all $r, s \in R$ and $m \in M$.
- $(rs)m = r(sm)$ for all $r, s \in R$ and $m \in M$.
- $1m = m$ for all $m \in M$.
- $0m = 0$ for all $m \in M$.

Example 1.13.1

1. If R is a field, R-modules are just vector spaces over R.
2. Let $R = \mathbb{Z}$. We claim that $\mathbb{Z}$-modules are just abelian groups. Let G be a $\mathbb{Z}$-module. Just forget scalar multiplication to get an abelian group.

   Converse: Let $(G, +)$ be an abelian group. We have that $0g = 0$, $1g = g, (n + 1)g = ng + g$, and $(-n)g = 0 - (ng)$.
3. Let K be a field, $R = K[x]$. Let M be a $K[x]$-module.
   (a) K is a subring of $K[x]$. So M is a K-module that is a vector space over K.
   (b) Let $T : M \to M$ be given by $T(m) = xm$. Then T is a K-linear map. Note that we can recover $K[x]$-module structure from K-vector space structure and T. Namely, $(a_0 + a_1x + \ldots + a_nx^n)m = a_0m + a_1T(m) + \ldots + a_nT^n(m)$.
4. For any ring R, R is an R-module.
5. Let M, N be R-modules. $M \dotplus N = \{(m, n) : m \in M, n \in N\}$ is an R-module with coordinatewise operations.

6. Let M, N be R-modules. $Hom_R(M,N) = \{f : M \to N : f \text{ is an } R\text{-module HM}\}$ is an R-module that is R linear.

Definition 1.13.6: Submodule

If N is an R-module then $M \subseteq N$ is a *submodule* iff M is a subgroup of $(N,+)$ and $rm \in M$ for all $r \in R$ and $m \in M$.

Example 1.13.2

1. Submodules of vector spaces over R are just subspaces.
2. In abelian groups, submodules are just subgroups.
3. If R is a ringe viewed as an R-module, then submodules are just ideals.
4. If V is a vector space over K with $T : V \to V$ linear, view V as a $K[x]$-module. Then submodules of V are just T-invariant subspaces.

Definition 1.13.7: Quotient Module

If $M \leqslant N$, N/M is defined in the obvious way. $N/M = \{n + M : n \in N\}$.

$\phi_M : N \to N/M$ is a quotient homomorphism.
Also, if $T : M \to N$ is a linear homomorphism, then $\ker(T) = \{m \in M : T(m) = 0\}$. also, $im(T) \cong M/\ker(T)$.

Definition 1.13.8: Cokernel

The *cokernel* of T is $N/im(T)$.

1.14 Some Random Category Stuff

Definition 1.14.1: Finitely Generated

An R-module M is *finitely generated* if there is $X \subseteq M$ finite such that $M = \text{span}(X)$.

Definition 1.14.2: Noetherian

An R-module M is *Noetherian* if every submodule of M is finitely generated.

Definition 1.14.3: Noetherian Ring

A ring R is *Noetherian* iff R is Noetherian as an R-module.

Example 1.14.1

PID's are Noetherian rings.

Note:

For any ring R, R is the R-span of $\{1\}$. So R is finitely generated.

Example 1.14.2 (Non-Noetherian Ring)

Let $R = \mathbb{Z}[x_1, x_2, \ldots]$ be the ring of polynomials in infinitely many variables. Then R is not Noetherian. We have that $I = (x_0, x_1, \cdots)$, which is $p \in R$ such that the constant term of p is 0. Supposed by contradiction that I is finitely generated. Say that $I = R$-span of $(p_0, \cdots, p_{n-1})$. That is, $I = (\sum_{i=0}^{n-1} a_i p_i : a_i \in R)$. Then $x_n \in I$, so $x_n = \sum_{i=0}^{n-1} a_i p_i$ for some $a_i \in R$. Let R be so large that x_k does not appear in any p_j. $x_k \in I$, so $x_k = \sum_{i=0}^{n-1} a_i p_i$.
Consider assigning values to x like:

- $x_k \to 1$
- $x_i \to 0$ for $i \neq k$

This gives $1 = \sum_{i=1}^{n-1} a_i 0 = 0$, which is a contradiction.

Theorem 1.14.1

Let M be an R-module. Then the following are equivalent:

1. M is Noetherian.
2. Whenever (N_i) such that $N_i \leqslant N_{i+1}$ and $N_i \leqslant M$, N_i is eventually constant.
3. Any nonempty famiy of submodules of M has a maximal element.

Proof.

- $1 \implies 2$. Let (N_i) be a chain of submodules of M. Then $N = \bigcup_{i=1}^{\infty} N_i$ is a submodule of M. N is finitely generated, so fix $X \subseteq N$ where X is finite. $N = \text{span}(X)$, find i such that $X \subseteq N_i$. Now $N_i \subseteq N$, so $N = \text{span}(X) \subseteq N_i$. So $N_i = N_j = N$ for $j \geqslant i$.
- $\neg 1 \implies \neg 2$.

😊