Abstract Algebra Lecture Notes

Simon Xiang

Lecture notes for the Fall 2020 graduate section of Abstract Algebra (Math 380C) at UT Austin, taught by Dr. Ciperiani. I'm currently auditing this course due to the fact that I'm not officially enrolled in it. These notes were taken live in class (and so they may contain many errors). You can view the source code here: `https://git.simonxiang.xyz/math_notes/file/freshman_year/abstract_algebra/master_notes.tex.html`.

Contents

1 August 26, 2020 **3**
1.1 Oops . . . 3

2 August 28, 2020 **3**
2.1 Subgroups and Normal Subgroups . . . 3
2.2 Product and Quotient Groups . . . 3
2.3 Left and Right Cosets . . . 4
2.4 Lagrange's Theorem . . . 4

3 August 31, 2020 **5**
3.1 The Dihedral Group . . . 5
3.2 Group Homomorphisms, Isomorphisms, and Automorphisms . . . 5
3.3 The First Homomorphism Theorem . . . 5

4 September 2, 2020 **7**
4.1 The Symmetric Group Rises from the Automorphism Group . . . 7
4.2 On the Symmetric Group . . . 7
4.3 Transpositions and Cycles . . . 7

5 September 4, 2020 **9**
5.1 Group Actions . . . 9
5.2 Orbits and Stabilizers . . . 9
5.3 Quotient Group of Orbits . . . 11

6 September 9, 2020 **12**
6.1 Transitive and Faithful Actions . . . 12

6.2 Normal Subgroups from Group Actions 12
6.3 The Class Equation 13

7 September 11, 2020 **14**
7.1 Cauchy's Lemma 14
7.2 p-groups 14
7.3 Sylow Theorems 15

8 September 14, 2020 **16**
8.1 Class Introductions (not math) 16
8.2 Sylow Theory 16

9 September 16, 2020 **18**
9.1 Proving the Sylow Theorems 18
9.2 Applications to Simple Groups 18
9.3 Groups of Order 12 Are Not Simple 19

10 September 18, 2020 **20**
10.1 Representation Theory 20
10.2 Linear Actions 20
10.3 Regular Representations 21

§1 August 26, 2020

§1.1 Oops

Unfortunately, I couldn't attend Lecture 1.

§2 August 28, 2020

§2.1 Subgroups and Normal Subgroups

Lemma 2.1. *Let $H \subseteq G$, $\langle G, \cdot \rangle$ a group and $H \neq \emptyset$. Then H is a subgroup of G if and only if $h_1 h_2 \in H \implies h_1 h_2^{-1} \in H$.*

Proof. For all $h_2 \in H$, $h_2^{-1} \in H$ since H is a group. H is closed under multiplication implies $h_1 h_2^{-1} \in H$ for all $h_1, h_2 \in H$. Conversely, assume that $h_1 h_2 \in H \implies h_1 h_2^{-1} \in H$. Then for $h \in H$, $hh^{-1} \in H$ so $1 \in H$. Now that we know $1 \in H$, then for $h \in H$ we have $1 \cdot h \in H \implies h^{-1} \cdot 1 \in H$, so H is closed under inverses. Finally, associativity follows from the fact that $H \subseteq G \implies \forall h \in H, h \in G$ where G is a group, and we are done. $\boxtimes$

Definition 2.1 (Normal Subgroup). A *subgroup* H of G is normal if $gHg^{-1} = H$ for all $g \in G$.

Example 2.1. Let G be abelian: then every subgroup is normal since $ghg^{-1} = gg^{-1}h = h$ for all $g \in G, h \in H$.

Example 2.2. Take $G = S_3$. Then the subgroup $\langle (123) \rangle$ is normal. However, the subgroup $\langle (1, 2) \rangle$ is not normal, since $(13)(12)(13)^{-1} = (23) \notin \langle (12) \rangle$.

Example 2.3. Take $\mathrm{SL}_n\mathbb{R} \subseteq \mathrm{GL}_n\mathbb{R}$, where $\mathrm{SL}_n\mathbb{R}$ is the set of matrices with $\det(A) = 1$ for $A \in \mathrm{SL}_n\mathbb{R}$. We know $\mathrm{SL}_n\mathbb{R}$ forms a subgroup. Question: is $\mathrm{SL}_n\mathbb{R}$ normal? Answer: yes.

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(A)\det(A)^{-1}\det(B) = \det(B).$$

Proposition 2.1. Let H, K be subgroups of G, then $H \cap K$ is a subgroup of G. You can verify this in your free time.

Note: is $H \cup K$ a subgroup? No!

§2.2 Product and Quotient Groups

Definition 2.2 (Product Groups). Let G, H be groups. We define the *direct product* $G \times H$ with the group operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$. The identity is just $(1_G, 1_H)$ where 1_G and 1_H denotes the respective identities for G and H. Finally, the inverse is similarly defined as (g_1^{-1}, h_1^{-1}) where g_1^{-1} and h_1^{-1} are the respective inverses for $g_1 \in G$, $h_1 \in H$.

Some examples of product groups include $\mathbb{Z} \times \mathbb{Z}$ ($\mathbb{Z}$ denotes $\langle \mathbb{Z}, + \rangle$), and $\mathbb{Z} \times \langle \mathbb{R} \setminus \{0\}, \cdot \rangle$

Example 2.4 (Quotient Groups)**.** Let $n \in \mathbb{Z}$, for example $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$, equivalence relations: modulo n. $a, b \in \mathbb{Z}, a \equiv b \mod n \iff n \mid (a - b)$. Equivalence classes: $a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$. Notation: $\bar{a} = a + n\mathbb{Z} = [a]$. Our set $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{a + n\mathbb{Z} \mid a = 0, ..., n-1\}$. $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$, so this is a group operation. In this case, the identity is just $0 + n\mathbb{Z} = n\mathbb{Z}$. We have the inverse of $(a + n\mathbb{Z})$ equal to $(a + n\mathbb{Z})^{-1} = -a + n\mathbb{Z}$.

Remark: $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ is a quotient of the group $\langle \mathbb{Z}, + \rangle$ by the subgroup $\langle n\mathbb{Z}, + \rangle$. $\langle 1 \rangle = \mathbb{Z}, \langle 1 + n\mathbb{Z} \rangle = \langle \mathbb{Z}/n\mathbb{Z} \rangle$.

Quotient groups in general: G a group, H a **normal** subgroup.

§2.3 Left and Right Cosets

Definition 2.3 (Cosets)**.** Left cosets: $gH = \{gh \mid h \in H\}$. Right cosets: $Hg = \{hg \mid h \in H\}$. G/H - set of left cosets. $H \setminus G$ - set of right cosets.

Observe: Left and right cosets are in bijection with one another. $gH \mapsto Hg$, $gh \mapsto g^{-1}(gh)g = hg$. You can verify that this is a bijection. Let $g_1, g_2 \in G$, what map maps $g_1H \to g_2H$? $g_1h \mapsto (g_2g_1^{-1})g_1h = g_2h$.

Note. We have

$$\bigcup_{g \in G} gH = G.$$

Also: $g_1H \cap g_2H$ is either $\emptyset$ or they are equal. (Equivalence relation).

§2.4 Lagrange's Theorem

Proposition 2.2. If G is finite and H a subgroup of G, then $|H| \mid |G|$.

Proof. By the statement above,

$$G = \bigcup_{i=1}^{n} g_iH$$

since G is finite for $n \in \mathbb{N}$. Note that this is a disjoint union. So

$$|G| = \sum_{i=1}^{n} |g_iH| = n \cdot |H| \implies |H| \mid |G|.$$

⊠

Quotient group: G a group, H a normal subgroup, $G/H = \{gH \mid g \in G\}$. The multiplication is defined as $g_1H \cdot g_2H = g_1g_2H$. You can verify this operation is well defined (given that H is normal).

§3 August 31, 2020

§3.1 The Dihedral Group

Example 3.1 (Dihedral Group). Consider the free group $G = \langle g, \tau \rangle$ and the normal subgroup H_n of G generated by

$$g^n, \tau^2, \tau g \tau^{-1} g.$$

The dihedral group $D_{2n} = G/H_n$ (sometimes denoted D_n), is it automatically normal? What about conjugating by powers of g?

Observe that $\langle g \rangle \simeq \langle gH_n \rangle \subseteq D_{2n}$. $\langle g \rangle$ has order n and is normal (convince yourselves of this). τ has order 2 and so does $\langle \tau g^i \rangle$ for any i. Are these subgroups normal? (Yes sometimes, no some other times).

Consider the following: $2\mathbb{Z} \trianglelefteq \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} = \{2\mathbb{Z}, 1+2Z\}$, $\langle (123) \rangle \trianglelefteq S_3 = {}^{S_3}/_{\langle (123) \rangle} = \{1_{S_3}, (\bar{12})\}$, $\mathbb{R}^+ \setminus \{0\} \trianglelefteq \mathbb{R} \setminus \{0\} \to {}^{\mathbb{R}\setminus\{0\}}/_{\mathbb{R}^+\setminus\{0\}} = \{\bar{1}, \bar{-1}\}$. What distinguishes these groups (they all have order two)?

§3.2 Group Homomorphisms, Isomorphisms, and Automorphisms

Definition 3.1 (Homomorphisms). Let G, H be two groups. A map $\phi \colon G \to H$ is a homomorphism if

$$\phi(g_1 g_2) = \phi(g_1) \cdot \phi(g_2).$$

Definition 3.2 (Isomorphism). A map ϕ is an isomorphism is ϕ if a homomorphism and a bijection. If $\phi \colon G \to H$ is an isomorphism then we write $G \simeq H$.

Definition 3.3 (Automorphism). We have ϕ an automorphism if ϕ is an isomorphism from G onto itself, that is, $G = H$.

§3.3 The First Homomorphism Theorem

Remark 3.1. Let $\phi \colon G \to H$ be a group homomorphism. Then

1. $\phi(1_G) = 1_H$ and $\phi(g^{-1}) = \phi(g)^{-1}$,
2. $\phi(G) = \operatorname{im} \phi$ is a subgroup of H,
3. $\ker \phi = \{g \in G \mid \phi(g) = 1H\}$ is a normal subgroup of G,
4. ϕ is injective $\iff$ $\ker \phi = \{1_G\}$,
5. If G is finite then $|G| = |\ker \phi| \cdot |\operatorname{im} \phi|$.

Theorem 3.1. *Let $\phi \colon G \to H$ be a group homomorphism. Then $\bar{\phi} \colon G/\ker \phi \to \operatorname{im} \phi$ is an isomorphism.*

Proof. Left as an exercise to the reader (verify that $\bar{\phi}$ is well-defined, injective, surjective, and a homomorphism). $\boxtimes$

Example 3.2. Recall the groups ${}^{\mathbb{Z}}/_{2\mathbb{Z}} = \langle 1 + 2\mathbb{Z} \rangle$, ${}^{S_3}/_{\langle(123)\rangle} = \langle (12)\langle(123)\rangle \rangle$, ${}^{\mathbb{R}\setminus\{0\}}/_{\mathbb{R}^+\setminus\{0\}} = \langle (-1)\mathbb{R}^+ \setminus \{0\} \rangle$. Then we have isomorphisms onto all of them, so they are the same.

Remark 3.2. Product of groups $\iff$ quotient groups. H, K be groups. $G = H \times K$, $H \simeq H \times \{1_K\} \trianglelefteq G$. ??? $H, K \trianglelefteq G$, $H \cap K = \{1_G\}, HK = G \implies G \simeq H \times K$ (prove this). ${}^{G}/_{H} \simeq K$ and ${}^{G}/_{K} = H$: relax any of the implications, and the isomorphisms will fail.

§4 September 2, 2020

Last time: Homomorphisms, Isormorphisms, Automorphisms, trivial maps.

§4.1 The Symmetric Group Rises from the Automorphism Group

Example 4.1 (Group of Automorphisms)**.** Let X be a finite set. Let

$$S_x := \{f : X \to X \mid f \text{ is bijective}\}$$

Bijections on X preserve X: think of this set as the *group of automorphisms* on X, defined as $\mathrm{Aut}(X)$. The group operation is simply function composition. Then the identity element is the identity map, and the inverse of any $f \in S_x$ is $f^{-1} \in S_x$.

Assume that $g : X \to Y$ is a bijection. Then g gives rise to a homomorphism $\phi_g : S_y \to S_x$, $f \mapsto g^{-1}fg$. Verify that this map is well defined and a group homomorphism. Is ϕ_g an isomorphism? If $\phi_g^{-1} : S_x \to S_y$ were well-defined, then ϕ_g is a bijection. Consider $S_y(\phi_g) \to S_x(\phi_g^{-1}) \to S_y$, $f \mapsto g^{-1}fg \mapsto g(g^{-1}fg)g^{-1} = (gg^{-1})f(gg^{-1}) = f$. So $\phi_{g^{-1}} : S_x \to S_y$, $h \mapsto (g^{-1})^{-1}fg^{-1} = gfg^{-1}$.

Conclusion. Two finite sets X, Y have the same cardinality if there exists a bijection $g : X \to Y$. This bijection gives rise to the map $\phi_g : S_y \to S_x$ an isomorphism, so the group of automorphisms S_x depends only on the size of the group (when X is a finite set). Let $|X| = n$, then $S_x \simeq S_n$.

§4.2 On the Symmetric Group

A cycle in S_n: $(\alpha_x, ..., \alpha_k)$ is a k-cycle. $\alpha_1, ..., \alpha_k \in \{1, ..., n\}$, $a_i \neq a_j\ \forall i \neq j$. We have

$$(\alpha_1, ..., \alpha_k)(m) = \begin{cases} m & \text{if } m \neq \alpha_i\ \forall i = 1, ..., k \\ \alpha_{i+1} & \text{if } m = \alpha_i,\ i \in \{1, ..., k-1\} \\ \alpha_1 & \text{if } m = \alpha_k. \end{cases}$$

§4.3 Transpositions and Cycles

Definition 4.1 (Transpositions)**.** A *transposition* is a 2-cycle in S_n, denoted

$$(\alpha_1 \alpha_2),$$

where $\alpha_1 \neq \alpha_2$.

Definition 4.2. Two cycles $(\alpha_1, ..., \alpha_k)(\beta_1, ..., \beta_m)$ are *disjoint* if $\alpha_i \neq \beta_j$ for all $i \in \{1, ..., k\}$, $j \in \{1, ..., m\}$. Disjoint cycles commute, that is,

$$(\alpha_1, ..., \alpha_k)(\beta_1, ..., \beta_m) = (\beta_1, ..., \beta_m)(\alpha_1, ..., \alpha_k)$$

Lemma 4.1. *Every element $s \in S_n$ can be written uniquely (up to reordering) as a product of disjoint cycles.*

Proof. **Step 1**: Let $s \in S_n$. If $s = \mathrm{id}_{\{1,\dots,n\}}$, then $s = 1_{S_n}$. We have $s \neq 1_{S_n} \implies I_0(\neq \emptyset) := \{1 \leq k \leq n,\ s(k) \neq k\}$. Define $k_1 := \min I_0$. Then

$$\iota_1 := (k_1\, s(k_1)\, s^2(k_1)\, ...)$$

is an e_1-cycle where

$$\begin{cases} s^{e_1}(k_1) = k_1 \\ e_1 = \min\{d \in \mathbb{N} \mid s^d(k_1) = k_1\}. \end{cases}$$

Step 2: Now

$$I_1 = I_0 \setminus \{k_1, ..., s^{e_1}(k_1)\}.$$

If $I_1 = \emptyset$, we are done: $s = c$. If $I_1 \neq \emptyset$: $k_2 = \min I_1$. Set $\iota_2 = (k_2\, s(k_2)\, ...)$ an e_2-cycle where $s^{e_2}(k_2) = k_2)$, $e_2 = \min\{d \in \mathbb{N} \mid s^d(k_2) = k_2\}$.

Note. c_1, c_2 are disjoint cycles.

Step 3: $I_2 = i_1 \setminus \{k_2, s(k_2), ..., s^{e_2-1}(k_2)\}$. If $I_2 = \emptyset$ then we are done, verify $s = c_1c_2$. If $I_2 \neq \emptyset$ then $k_3 = \min I_2$. Repeat the steps until $I_j = \emptyset \implies s = c_1...c_j$ disjoint cycles by construction. Verify the uniqueness in your free time. ⊠

Note. $s \in S_n \implies s = \prod_{i=1}^{n} c_i$, where the c_i are *disjoint* cycles.

Claim. The order of s defined as

$$\mathrm{ord}\, s := \min\{k \in \mathbb{N} \mid s^k = 1_{S_n}\}$$

is equal to

$$\mathrm{lcm}\{\mathrm{ord}\, c_i \mid i = 1, \cdots, j\},$$

where each $\mathrm{ord}\, c_i$ is the length of each cycle c_i.

Verify that this claim holds in your free time.

Note. We will show next time that every finite group is a subgroup of S_n for some $n \in \mathbb{N}$ (Cayley's Theorem). This shows the importants of permutation groups: they contain all the information you need to know about groups.

§5 September 4, 2020

§5.1 Group Actions

Definition 5.1 (Group Action)**.** An *action* of a group G on a set X is a map

$$a\colon G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

such that

1. $(1_G, x) \mapsto x$,
2. $g_1(g_2 \cdot x) = (g_1 g_2) \cdot x$

for all $x \in X$, $g_1, g_2 \in G$. Notation: $G \hookrightarrow X$, G acts on X.

Proposition 5.1. Let G be a group and X a set. Actions of G on X ($a\colon G \times X \to X$) are in bijection with homomorphisms $\phi\colon G \to S_X$.

Proof. Given an action $a\colon G \times X \to X$, define $\phi_a\colon G \to S_X$, $g \mapsto (x \mapsto a(g, x))$, $a(g, x) \in X$. Verify that

1. $x \mapsto a(g, x)$ is a bijection on X ($\iff$ $[x \mapsto a(g, x)] \in S_x$),
2. ϕ_a is a homomorphism.

$\boxtimes$

Given $\phi\colon G \to S_X$ a homomorphism, define $a_\phi\colon G \times X \to X$, $(g, x) \mapsto \phi(g)(x) \in X$. We have to verify that

1. a_ϕ is a group action, i.e., a_ϕ is a well-defined map.
2. $a_\phi(1_G, x) = x$. $\phi(1_G)(x) = 1_{S_X}(x) = \mathrm{id}_X(x) = x$.
3. $a_\phi(g_1, a_\phi(??)$

Finally, we must verify that

$$a \mapsto \phi_a \mapsto a_{\phi_a} = a$$

and

$$\phi \mapsto a_\phi \mapsto \phi_{a_\phi} = \phi.$$

§5.2 Orbits and Stabilizers

Given an action $a\colon G \times X \to X$ and an element $x \in X$, we can talk about the *orbit* of this action under x.

Definition 5.2 (Orbits)**.** We define an *orbit* of x as

$$G \cdot x = \{g \cdot x \mid g \in G\}.$$

Definition 5.3 (Stabilizer)**.** We define the *stabilizer* of x as

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

Remark 5.1. We have $1_G \in G_x$ for all $x \in X$.

Claim. G_x is a subgroup of G. To show this, note that

1. $1_G \in G_x \impliedby (1_G, x) = x$,
2. $g \in G_x \implies g^{-1} \in G_x$. To see this, note that $g^{-1}(gx) = g^{-1}x$ (since g is in the stabilizer subgroup) and $(g^{-1}g)x = 1_G x = x$, which implies $g^{-1}x = x$, so $g^{-1} \in G_x$.
3. $g_1, g_2 \in G_x \implies g_1 g_2 \in G_x$. $(g_1 g_2)x = g_1(g_2 x) = g_1(x)$ since g_2 stabilizes x, which implies $g_1 x = x$ since g_1 also stabilizes x, and we are done.

Definition 5.4 (Transitive Action)**.** An action is *transitive* if

$$Gx = X$$

for some $x \in X$. Prove that if you have this property *for some* $x \in X$, then this is the same as *every* $x \in X$ having this property.

Lemma 5.1. *If $x, y \in X$ lie in the same orbit (there exists a $g \in G$ such that $gx = y$), then $G_x = g^{-1}G_y g$.*

Proof. We have

$$\begin{aligned} h \in G_y &\iff hy = y \\ &\implies hgx = gx \\ &\implies g^{-1}hgx = g^{-1}(gx) = (g^{-1}g)x = x. \end{aligned}$$

So $g^{-1}hg \in G_x$, which implies $g^{-1}G_y g \subseteq G_x$. To prove the reverse inclusion, let $h \in G_x$. Then

$$\begin{aligned} h \in G_x &\iff hx = x \\ &\implies hg^{-1}y = g^{-1}y \\ &\implies ghg^{-1}y = g(g^{-1}y) = (gg^{-1})y = y. \end{aligned}$$

So $ghg^{-1} \in G_y \implies gG_x g^{-1} \subseteq G_y \implies G_x \in g^{-1}G_y g$, and we are done. ⊠

Lemma 5.2. *Let $G \hookrightarrow X$. Then two orbits are either equal or disjoint.*

Proof. $G_x \cap G_y \neq \emptyset \implies G_x = G_y$. Let $z \in G_x \cap G_y \implies G_x = G_z = G_y$. ⊠

General idea of group actions: for every element of the set, you have its stabilizer, and you can look at its orbits (are the same or are they disjoint?).

§5.3 Quotient Group of Orbits

Let $G \hookrightarrow X$, $x \in X$. Consider the map

$$G/G_x \to G_x, \quad gG_x \mapsto g \cdot x.$$

Notice this is well defined because $gh \mapsto gh \cdot x = g(hx) = gx$ since $h \in G_x$.

Claim. The map $G/G_x \mapsto G_x$ is a bijection.

Surjectivity follows from the definition of an orbit, and injectivity ... is up to you to prove. (Not hard, think about the definitions). But what does this mean?

Proposition 5.2. If G is finite, then the size of each orbit divides the size of G.

Proof. $x \in X, G_x \leftrightarrow G/G_x \implies |G_x| = |G/G_x| \mid |G|$. ⊠

Example 5.1. Every group acts on itself in three different ways, that is, $G \hookrightarrow X$, $X = G$.

1. Left multiplication: $g \cdot x = gx$,
2. Conjugation: $g \cdot x = gxg^{-1}$,
3. Right multiplication: $g \cdot x = xg^{-1}$ (if we define it as xg some properties of group actions will not hold). Why? $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$.

Orbits and Stabilizers WRT the above actions:

1. $Gx = X = G$ for all $x \in X$, $G_x = 1_G$,
2. $Gx =$ conjugacy class of x, $G_x =$centralizer of $x = \{g \in G \mid gx = xg\}$,
3. $Gx = X = G$ for all $x \in X$, $G_x = 1_G$.

Proposition 5.3. Let G be a group of order n, then $G \simeq$ subgroup of S_n.

⇓⇓⇓ This is scratch work for some old Putnam problem about binary operations I was working out ⇓⇓⇓

Let $a, b \in H$. Then we WTS $a * b \in H$. Let $x \in S$, then $a * b * s = a * s * b$ (since $b \in H$) $= s * a * b$ since $a \in H$ and we are done.

Let $a, b \in H$. We WTS $a * b \in H$. We have $(a * b) * (a * b) = a * (b * a) * b$ since $*$ is associative $= a * (a * b) * b$ since $*$ is commutative $= (a * a) * (b * b)$ since $*$ is associative $= a * b$ since $a, b \in H$, and we are done.

Try $a * (b * c) * (b * c)$

Let $a, b, c \in S$. First, we want to show $(a * b) * c = a * (b * c)$. We have $(a * b) * c = (a * (b * b)) * c = ((b * b) * c) * a = ((b * c) * b) * a = (b * a) * (b * c) = ($

$((a * a) * (b * b)) * c = ((a * (b * b)) * a) * c$

Let $a, b \in S$. Then $a * b = (a * a) * b = (a * a) * (b * b) = (a * (b * b)) * a = ((b * b) * a) * a$

Proof. Let $a, b \in S$. Then $a * b = (a * b) * (a * b) = (b * (a * b)) * a = ((a * b) * a) * b = ((b * a) * a) * b = ((a * a) * b) * b = (b * b) * (a * a) = b * a$. Associativity follows, $(a * b) * c = (b * c) * a = a * (b * c)$ by our newly established commutativity. ⊠

§6 September 9, 2020

§6.1 Transitive and Faithful Actions

Group actions are connected to Representation Theory, a step forward from group actions (eg a group acting on a vector space). Then you can understand your "random group" through Linear Algebra.

Proposition 6.1. Let G be a group of order n, then G is isomorphic to a subgroup of S_n.

Proof. Consider $G \hookrightarrow G$, $g \mapsto [x \mapsto gx]$, with the corresponding homomorphism $\varphi\colon G \to S_G \simeq S_n$. $\operatorname{Ker}\varphi = ?$ $g \in \operatorname{Ker}\varphi \iff \varphi(g) = 1_G$, since $x \mapsto gx$, $x = gx \implies g = 1_G$. φ is an injective homomorphism implies that $\varphi\colon G \to \operatorname{im}\varphi \trianglelefteq S_n$ is an isomorphism. ⊠

Definition 6.1 (Faithful Group Actions)**.** Let $G \hookrightarrow X$. Then the group action is faithful if

$$\bigcap_{x\in X} G_x = \{1_G\}.$$

(Recall that the G_x are the stabilizing sets of x).

Example 6.1. Let G be a group, H some subgroup of G. Consider $X = G/H$ to be the set of left cosets. Then $G \hookrightarrow X$, $g \cdot (xH) = gxH$.

Orbits: $O_{xH} = G/H$, since $(yx^{-1})xH = yH$ for all $x, y \in G$. This is an example of a *transitive* group action.

Stabilizers: $G_{xH} = \{y \in G \mid yxH = xH\}$. $yxH = xH \iff x^{-1}yxH = H \iff x^{-1}yx \in H \iff y \in xHx^{-1}$. So $G_{xH} = xHx^{-1}$.

Example 6.2. Let $G \hookrightarrow X$, $X = \{xHx^{-1} \mid x \in G\}, H \trianglelefteq G$. Then the action is given by

$$g \cdot xHx^{-1} = gxHx^{-1}g^{-1},$$

which works because $gxH(gx)^{-1} \in X$. Then $O_{xHx^{-1}} = X$ for all $x \in G$ (so the action is transitive). What is the stabilizer of an element? Let $x = 1_G$, then $G_H = \{g \in G \mid gHg^{-1} = H\} =: N_G(H)$ ($N_G(H)$ denotes the normalizer of H in G). Verify that $G_{xHx^{-1}} = xN_G(H)x^{-1}$.

§6.2 Normal Subgroups from Group Actions

Theorem 6.1. *Let $H \leq G$ be a subgroup of index n. Then there exists an $N \trianglelefteq G$ such that $N \leq H$, $|G/N| \mid n!$.*

Proof. Consider $G \hookrightarrow G/H$, $g \cdot xH = gxH$. Observe that $|G/H| = n$. Then

$$\varphi\colon G \to S_{G/H} \simeq S_n.$$

Let $N = \operatorname{Ker}\varphi = \bigcap_{x\in G} G_{xH}$. $x = 1_G \implies G_H = H, gH = H$. Since N is the kernel of a group homomorphism, it is automatically a normal subgroup of G. $\operatorname{Ker}\varphi = N \implies$

$\varphi : G/N \hookrightarrow S_n$. $G/N \simeq \operatorname{im}\varphi \leq S_n$ which implies $|G/N| = |\operatorname{im}\varphi| \, |S_n| = n! \implies |G/N| \mid n!$.

$\boxtimes$

Corollary 6.1. *If G has a group of finite index, then G has a normal subgroup of finite index.*

Corollary 6.2. *Let G be a finite group and p be the smallest prime that divides $|G|$. Then every subgroup of index p is normal.*

Proof. We have $H \leq G$ such that $[G : H] = p$. Then by our theorem, there exists some normal subgroup $N \trianglelefteq H$ such that $N \leq H$, $|G/N \mid p!$. $p! = p \cdot (p-1)!$, which is only divisible by primes smaller than p. But $|G|$ is not divisible by any primes smaller than p, or any of the $(p-1)!$, so $\gcd(|G/N, (p-1)!) = 1$, which implies $|G/N| = p \implies N = H$, so H is normal. $\boxtimes$

§6.3 The Class Equation

Let $G \hookrightarrow X$ ($Z(G)$ denotes the center of the group). Then

1. $G/G_x \longleftrightarrow G_x$ a bijection $\implies [G : G_x] = |G_x|$. This is a bijection because $gG_x = \{gh \mid h \in G_x\} \mapsto ghx = gx$.
2. X is a disjoint union of the distinct orbits. $1_G x = x \to x \in G_x$ and two orbits are equal or disjoint. So $|x| =$ number of orbits of size $1 + \sum$ sizes of other larger distinct orbits. If $Gx = \{x\}, x$ is a fixed point of the action, so the number of orbits of size 1 are the fixed points of the action. $G \hookrightarrow G$ by conjugation, $g \cdot x = gxg^{-1} \implies |G| = |Z(G)| + \sum$ larger distinct conjugacy classes. This is known as *the class equation*. Formally,

$$|G| = |Z(G)| + \sum [G : C_G(g)]\,, C_G(g) = G_g.$$

   The conjugacy class of $x \in G = Gx = [G : G_x]$.

What can we tell from the class equation? If $|G| = p^n$ for p a prime, then $x \notin Z(G) \implies [G : C_G(x)]$ is divisible by p. $p^n = |Z(G)| + p \cdot m$ for $m \in \mathbb{Z}$. In addition, $Z(G) \ni 1_G \implies p \mid |Z(G)|$. Non trivial by the way.

§7 September 11, 2020

Last time: we had a proposition that said let p be a prime, G a group of order p^n for some $n \in \mathbb{N}$. Then G has a non-trivial center, more precisely, $|Z(G)| = p^m$ for some $m \geq 1$.

§7.1 Cauchy's Lemma

Dr. Ciperiani assumes we already know the Sylow theorems... why UNT.

Lemma 7.1 (Cauchy's Lemma)**.** *Let p be a prime such that $p \mid |G|$. Then G has an element of order p.*

Proof. Consider $X = \{(a_1 \cdots a_p)\}$ such that $a_i \in G$, $a_1 \cdots a_p = 1_G$. Observe $|X| = |G|^{p-1}$ (p is uniquely determined by varying the values of $a_1 \cdots a_{p-1}$ and letting p equal the inverse of such elements). The group $\mathbb{Z}/p\mathbb{Z}$ acts on X as such: $\overline{1}(a_1 \cdots a_p) := (a_2 \cdots a_p a_1)$, $\overline{n}(a_1 \cdots a_p) := (a_{1+n}, \cdots a_p, a_1, \cdots a_n)$. Verify that this is a group action. Since $|\mathbb{Z}/p\mathbb{Z}| = p$, we have $|O_{(a_1 \cdots a_p)}| = 1$ or p. $|O_{(a_1 \cdots a_p)}| = 1 \iff O_{(a_1 \cdots a_p)} = \{(a_1 \cdots a_p)\} \iff a_1 = a_2 = ... = a_p = a$. $(a \cdots a) \in X \implies a^{p=1}$, so $(1_G \cdots 1_G) \in X$. $O_x = \{x\} \iff x \in X^G$. So $X = X^G \cup (\cup \text{distinct orbits with more than 1 element})$, and all of these are disjoint unions. This implies $|X| = |X^G| + \sum$ sizes of nontrivial distinct orbits, which are all equal to p. So $|G|^{p-1} = |X|^G + pk$, where k is the number of distinct non-trivial orbits. This implies $|X^G| = |G|^{p-1} - pk$ which is divisible by $p \implies p \mid |X^G|$, furthermore $(1_G \cdots 1_G) \in X^G \implies |X^G| \geq 1$. $p \mid |X^G| \implies \exists a \in G \setminus 1_G$ such that $(a \cdots a) \in X^G \implies a^p = 1_G, a \neq 1_G \implies a = p$. ⊠

§7.2 p-groups

p-groups are groups G such that $|G| = p^n$ for $n \in \mathbb{N}$.

Proposition 7.1. Let p be a prime, G a group of order p^n. Then G has a chain of normal subgroups of order p^k for all $k \leq n$. For example, there exists

$$\{1_G\} \trianglelefteq G_1 \trianglelefteq G_2 \cdots \trianglelefteq G_n = G$$

such that $G_i \trianglelefteq G$ for all $0 \leq i \leq n$, $|G_i| = p^i$.

Proof. We prove this proposition by induction. Assume $n \geq 1$. Then $|Z(G)| = p^k$ for some $k \geq 1$. By Cauchy's Lemma, there exists some $g \in Z(G)$ such that g has order p. Set $N = \langle g \rangle \trianglelefteq G$. $n = 1 : \{1_G\} \trianglelefteq G$, $|\{1_G\}| = p^0, |G| = p^1$. Assume the hypothesis is true for $|G| = p^{n-1}$. To show the hypothesis is true for $|G| = p^n$: Consider $\pi \colon G \to G/N$. We have $|G/N| = \frac{|G|}{|N|} = \frac{p^n}{p} = p^{n-1}$. By the induction hypothesis there exists $\{1_G\} \trianglelefteq \overline{G_1} \trianglelefteq \overline{G_2} \cdots \trianglelefteq \overline{G_{n-1}} = G/N$. Verify that $G_{i+1} := \pi^{-1}(\overline{G_i}) \trianglelefteq G$, $\left|\pi^{-1}(\overline{G_i})\right| = p^{i+1}$, and $\{1_G\} \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ (G_1 has order p). It is crucial that n is in the center of G. ⊠

§7.3 Sylow Theorems

p denotes a prime, and G a group of order $p^r m$ where $p \nmid m, r \in \mathbb{N}$.

Definition 7.1 (Sylow)**.** A *Sylow p-subgroup* of G is a subgroup of G of order p^r.

Theorem 7.1. *G is a group of order $p^r m$ where p is a prime, $p \nmid m$, $m \in \mathbb{N}$, $r \in \mathbb{N}$. Then*

1. *Sylow p-subgroups exist,*
2. *They are all conjugate (in particular they are isomorphic),*
3. *Every p-subgroup of G lies within a Sylow p-subgroup,*
4. *$n_p :=$ the number of Sylow p-subgroups of G, $n_p = [G : N_G(P)]$ where P is a Sylow p-subgroup (P-Sylow a p-subgroup). In particular, $n_p \mid m$,*
5. *$n_p \equiv 1 \pmod p$,*
6. *$n_p = 1 \iff$ there is a unique Sylow p-subgroup which is normal in G.*

When you do the proof, things will just "click" together.

Example 7.1. Let G be a group of order $6 = 2 \cdot 3$. So 2-Sylows, 3-Sylows exists. $n_2 \equiv 1 \pmod 2$, $n_2 \mid 3 \implies n_2 = 1$ or 3. $n_3 \equiv 1 \pmod 3$, $n_3 \mid 2 \implies n_3 = 1$. $n_2 = n_3 = 1 \implies G \simeq P_2 \times P_3$ where P_2 is the 2-Sylow and P_3 is the 3-Sylow. $n_2 = 3$ and $n_3 = 1$ happens when $G \simeq S_3$.

Wow, this was a dense lecture.

§8 September 14, 2020

§8.1 Class Introductions (not math)

Zoom classes suck: time for brief introductions. About Dr. Ciperiani: Number Theory, Elliptic Curves, Princeton, Albania, Smith $\implies$ France, Colombia, MSRI, UT! Swimming and Traveling, two kids (2 and 6).

I'm omitting the rest of the personal introductions for privacy, but all my class mates are very interesting and cool people.

§8.2 Sylow Theory

Last time: Sylow Theorems. Let p be a prime.

Theorem 8.1. *Let G be a group of order $p^r m$ where $p \nmid m, r \in \mathbb{N}$. Then*

1. *Sylow p-subgroups exist,*
2. *They are all conjugate,*
3. *Every p-subgroup of G lies in some Sylow p-subgroup of G,*
4. *Let $n_p :=$ the number of Sylow p-subgroups of G, P be a Sylow p-subgroup. Then $n_p = [G : N_G(P)]$, where $N_G(P)$ is the normalizer of P in G. In particular, $n_p \mid m = [G : P]$.*
5. *$n_p \equiv 1 \pmod p$,*
6. *$n_p = 1$ if and only if $P \trianglelefteq G$.*

We introduce our key lemma:

Lemma 8.1. *Let P denote any maximal p-subgroup of G, $N = N_G(P)$. If Q is any p-subgroup of N, then $Q \subseteq P$. Consequently, $p \nmid [N : P]$.*

Proof. Consider the map
$$\pi \colon N \to \overline{N} = N/P.$$
Then $\pi(Q) = \overline{Q}$. Q a p-subgroup $\implies$ $|\overline{Q}| = p^m$. $\pi^{-1}(\overline{Q}) = QP \supseteq P$, $|QP| = |\overline{Q}| \cdot |P| = p^m \cdot |P| \implies QP = P$, P is maximal. So QP is a p-subgroup, $p^m = 1$, $p \mid [\overline{N} : P] \implies p \mid |N/P| \implies$ by Cauchy's Lemma that there exists a $g \in N/P$ such that $\operatorname{ord} g = p$. Take $\pi^{-1}\langle g\rangle = \langle P, g\rangle$, $|\pi^{-1}\langle g\rangle| = p|P|$. $\pi \colon \langle P, g\rangle \to \langle g\rangle$, $\ker \pi|_{\langle P,g\rangle} = P$.

$$O \to \underset{\ker\pi}{P} \to \langle P, g\rangle \xrightarrow{\pi} \underset{\operatorname{im}\pi}{\langle g\rangle} \to O$$

implies
$$kP, g > | = |\operatorname{im}\pi| \cdot |\ker \pi| = p|P|,$$
$\langle P, g\rangle \not\supseteq P$, since P is maximal. ⊠

Now let's prove the theorem.

Proof. Let P be a maximal p-subgroup of G. We have

$$X = \{gPg^{-1} \mid g \in\}$$

Observe that

1. $|X| = [G : N_G(P)]$,
2. Every element of X is a maximal p-subgroup of G, $gPg^{-1} \not\subseteq Q$ a p-subgroup $\implies P \not\subseteq g^{-1}Qg$ which is false since P is a maximal p-subgroup,

Fine. (One of Dr. Ciperiani's (lovingly) idiosyncracies). We have P acting on X by conjugation. The only fixed point of X under the action of P is P, ie, $X^P = P$.

Claim. If $gPg^{-1} \in X^p \iff P \subseteq N_G(gPg^{-1})$, ie, $h(gPg^{-1})h^{-1} = gPg^{-1}$ for all $h \in P$, then (??) $P = gPg^{-1}$.

The first claim said that $|X^P| = |\{p\}| = 1$. Nontrivial orbits of X under the action of P have size dividing $|P|$. This implies that the size is equal to p^k for some $k \in \mathbb{N}$. $|X| = |X^P| + \sum$ sizes of distinct larger orbits, all of which are powers of p. Since $X^P| = 1$, we have $|X| \equiv 1 \pmod{p}$. Whoops, we're a little overtime. We have one more claim to prove before completing the proof of the Sylow Theorems, then we will be done. ⊠

§9 September 16, 2020

Last time: we were proving a big theorem. Let's move onto our second claim:

§9.1 Proving the Sylow Theorems

Claim. X contains all maximal p-subgroups of G.

Proof. Suppose Q is a maximal p-subgroup of G such that $Q \notin X$. Consider the action of Q on X by conjugation (since Q is a subgroup of G).Examine X^Q, the set of fixed points of X under the action of Q. $X^G \ni gPg^{-1}$ for some $g \in G$. Then

$$X^Q \ni gPg^{-1} \iff Q \subseteq N_G(gPg^{-1}).$$

But by our key lemma, $Q \subseteq gPg^{-1}$, both sets are maximal. So $Q = gPg^{-1}$, a contradiction, since we assumed $Q \notin X$. ⊠

Claim. This is the second claim: $X^Q = \varnothing$ implies $X = \amalg$ nontrivial orbits of X under the action of Q. But all of the orbits have size p^k for some $k \in \mathbb{N}$, which implies

$$|X| = \sum_{i=1} p^{k_i} \equiv 0 \pmod p$$

for $k_i \in \mathbb{N}$, a contradiction. Wait, did we just reach a contradiction twice? We assumed the assumtion failed and then got this, concluding the proof of Claim 2.

We want to find the order of P: We have

$$\begin{tikzcd} G \arrow[d, dash, "{[G:N_G(P)]=|X|\equiv 1 \pmod p}"] \\ N_G(P) \arrow[d, dash, "{[N_G(P):P]\not\equiv 0 \pmod p \quad \text{by the lemma}}"] \\ P \end{tikzcd}$$

which implies $P \mid [G : P]$. $|G| = [G : P] \cdot |P| \implies |P| = p \implies P$ is a Sylow p-subgroup of G. Claim 2 implies $n_p = |X| = [G : N_G(P)]$. Then this implies $n_p \mid [G : P] = \frac{m \cdot p^r}{p^r} = m$. For 5, $n_p = |X| \equiv 1 \pmod p$ by Claim 1(b), and for 6, $n_p = 1 \iff |X| = 1 \iff X = \{p\} \iff p \trianglelefteq G$, and we are done. ⊠

§9.2 Applications to Simple Groups

Definition 9.1 (Simple Groups)**.** A group G is simple if its only normal subgroups are $\{1_G\}$ and G.

Example 9.1. Let G be a p-group, ie $|G| = p^n$ for $n \in \mathbb{N}$. $Z(G) = p^r, r \geq 1 \implies$ there exists a $g \in Z(G)$ such that $\operatorname{ord} g = p$. This implies $\langle g \rangle \trianglelefteq G$ has order p. So G is normal if and only if $|G| = p$. (Was it supposed to be simple?)

Example 9.2. Let G be a group of order pq where p, q are primes, $p \neq q$. Assume $p < q$. Then $n_q \mid p$ and $n_q \equiv 1 \pmod q$. Together, these imply that $n_q = 1 \implies p$-Sylow of G is normal in G. So G is not simple.

§9.3 Groups of Order 12 Are Not Simple

Example 9.3. Let G be a group of order $p^2 q$ where p, q are distinct primes. Say $p > q$. Then $n_p \equiv 1 \pmod p$ and $n_p \mid q$, which together imply that $n_p = 1$ and G is not simple.

Now assume $p < q$: then $n_p \equiv 1 \pmod p$ and $n_p \mid q$. So we have two possibilities: $n_p = 1$ or q (if $q \equiv 1 \pmod p$). Look at the q-Sylows, so we have $n_q \equiv 1 \pmod p$ and $n_q \mid p^2$. This implies $n_q = 1$ or p^2 if $p^2 \equiv 1 \pmod q$. We just argued that $q \nmid p - 1$ since $p < q$, so $q \mid p + 1$. The only way this happens is if the equality with p^2 holds. So $p = 2$ and $q = 3$, there's no other scenario.

We conclude that G is not simple ($n_q = 1$) or $|G| = 2^2 \cdot 3$. Can this group be simple? Also, can we have $|G| = p^2 q$ such that $p < q$ and $n_p = p, n_q = p^2$? $n_q = p^2 \implies G$ has p^2 distinct subgroups of order $q \implies$ has $(q-1) \cdot p^2$ distinct elements of order q. S is the set of elements of G with order q. $G \setminus S \supseteq$ Sylow p-subgroups, $|G \setminus S| = p^2 q - (q-1)p^2 = p^2$. So we have space for exactly one Sylow p-subgroup. Therefore $n_p = 1$, a contradiction, so G is not simple.

Corollary 9.1. *Let G be a nontrivial group of order less than 60. Then G is simple if and only if $|G|$ is prime.*

Proof. $|G| \in \{p^n, pq, p^2 q, 2 \cdot 3 \cdot 5, 2^3 \cdot 3, 2^3 \cdot 5, 2^3 \cdot 7, 3^3 \cdot 2\}$, where p, q are distinct primes. We have to refute these possibilites, to be continued next time. ☒

§10 September 18, 2020

Last time: proving a corollary. I wish I was in the Canvas... We deal with many many cases.

Example 10.1. $|G| = 2 \cdot 3 \cdot 5$.

- $n_5 = 1$ or $6 \implies G$ has $(5-1)6$ elements of order 5.
- $n_3 = 1$ or $10 \implies G$ has $(3-1)6$ elements of order 3.

So $|G| > 4 \cdot 6 + 20 = 44$, which is false since $|G| = 30$. Now let $|G| = 2 \cdot 3 \cdot 7$. $n_7 = 1 \implies G$ is not simple. $|G| = 2^3 \cdot \implies n_3 = 1$ or 4, $n_2 = 1$ or 3. Let P_2 be the 2-Sylow: $[G : P_2] = 3$. We have an older theorem: there exists an $N < P_2$ such that $N \trianglelefteq G$ and $3 \leq [G : N] \mid 3! = 6$, which implies N is nontrivial or the full group, so G is not simple.

§10.1 Representation Theory

We have group actions connected to some representations, and we use these representations to talk about our groups. Representation theory is the study of linear algebra to deduce things about groups.

Claim. Group actions of G gives rise to representations of G. (The other way holds, but is not as useful).

We have seen for a group G acting on a set X, we have a bijective map $\varphi\colon G \to S_X$ a group homomorphism. Each group action corresponds to a homomorphism, that is,

$$g \cdot x \longrightarrow \varphi\colon g \mapsto (x \mapsto g \cdot x).$$

For the other way around,

$$g \cdot x := \varphi(g)(x) \longleftarrow \varphi.$$

Definition 10.1 (Representations)**.** A representation of G on an $\mathbb{F}$-vector space V is a homomorphism

$$\varphi\colon G \to \mathrm{GL}(V),$$

where $\mathrm{GL}(V)$ is just the set of automorphisms $\mathrm{Aut}(V \to V)$ from V onto V (automorphisms are just invertible linear maps).

§10.2 Linear Actions

How are group actions related to representation theory?

Definition 10.2. A group action G on the vector space V is *linear* if the maps induced by the elements of your group $v \to g \cdot v$ are linear for all $g \in G$.

Proposition 10.1. Linear actions of G are in bijection with representations of G. To see this, $g \cdot v \longrightarrow \varphi\colon g \mapsto (v \mapsto g \cdot v)$, $v \in V$, $g \in G$. Verify that φ is a homomorphism. For the other way, $\varphi\colon G \to \mathrm{GL}(V)$, $g \cdot v = \varphi(g)(v)$.

Proof. Things we have to do:

1. Verify that $g \cdot v$ is a linear group action.
2. Verify that $\varphi(g) \in \mathrm{GL}(V)$. Also verify that φ is a homomorphism (this is trivial).

$\boxtimes$

Let G a group acting on a set X. We want to construct a linear action of G using this given action. Let $V = \bigoplus \mathbb{F}e_x$, where e_x is a basis element. Then the action of G on V is defined as follows: let

$$v \in V \implies v = \sum_{x \in X} a_x e_x$$

where $a_x \in \mathbb{F}$, $a_x = 0$ for all but finitely many $x \in X$ (denoted by the convention "almost all"). Then

$$g \cdot := \sum a_x e_{g \cdot x} \in V.$$

Claim. The action of G on V is linear. Verify this in your free time.

§10.3 Regular Representations

Definition 10.3 (Regular Representations)**.** Consider the corresponding representation $\varphi \colon G \to \mathrm{GL}(V)$. This representation has a special name: observe $\varphi(g)$ is a *permutation matrix* whos entries are 0 or 1 if x is finite. Permutation matrices simply permute (rearrange) the basis elements. This is called the *regular* representation.

Example 10.2. Consider the action G on G by left multiplication. Then

$$V_{\mathrm{reg}} := \bigoplus_{g \in G} \mathbb{F}e_g, \quad \varphi_{\mathrm{reg}} \colon G \to \mathrm{GL}(V_{\mathrm{reg}}).$$

is the regular representation of G. If G is finite, then V_{reg} is finite dimensional. Multiplicity, irreducability (throwback to last semester!). We call a space irreducable if we can't find a subspace such that we can restrict this homomorphism to the subspace.

If this is gibberish, just know that the regular representation will contain **all** the information you need to know about your group (wow!).

Definition 10.4. Let V be a finite dimensional vector space over $\mathbb{F}$. Then the *character* of a representation $\varphi \colon G \to \mathrm{GL}(V)$ is defined as

$$\mathrm{char}\, \varphi \colon G \to F, \quad g \mapsto \mathrm{tr}\, \varphi(g).$$

The amazing thing is that your character will determine your representation uniquely. Let's continue this next time (this is making much more sense than Sylow whatever).