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

§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. ⊠

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

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

$\boxtimes$

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). ⊠

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

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

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

Conclusion. Two finite sets X, Y have the same cardinality if there exists a bijection $g \colon X \to Y$. This bijection gives rise to the map $\phi_g \colon S_y \to S_x$ 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

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

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

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

If $I_1 = \emptyset$, we are done: $s = c$. If $I_1 \neq \emptyset$: $k_2 = \min I_1$. Set $\iota_2 = (k_2\, s(k_2) \dots)$ 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: $I_2 = i_1 \setminus \{k_2, s(k_2), \dots, s^{e_2-1}(k_2)\}$. If $I_2 = \emptyset$ then we are done, verify $s = c_1 c_2$. If $I_2 \neq \emptyset$ then $k_3 = \min I_2$. Repeat the steps until $I_j = \emptyset \implies s = c_1 \dots c_j$ 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

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

is equal to

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

where each $\operatorname{ord} c_i$ 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.

⊠

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. $1_G \in G_x \iff (1_G, x) = x$,
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. $x \in X$, $G_x \leftrightarrow G/G_x \implies |G_x| = |G/G_x| \,\big|\, |G|$. ⊠

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.

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. ⊠