PMATH347 - Groups and Rings (Class Notes)

Johnson Ng

October 2, 2017

Contents

List of Definitions

List of Theorems

List of Symbols

S_n	symmetric group on n letters
D_{2n}	dihedral group of order 2n
$A \times B$	Cartesian product of A and B
$A \simeq B$	A is isomorphic to B
$\ker(\phi)$	kernel of ϕ
$I_m(\phi)$	image set of ϕ
gH, Hg	left coset, right coset of H with coset representative g
$[G : H]$	index of the subgroup H in G
$H \triangleleft G$	H is a normal subgroup of G
$\mathrm{rem}_n(a)$	remainder of a when divided by n

Chapter 1

Lecture 1: Sept 8, 2017

1.1 Logistics

Textbook is relatively important. The level of the text is about the same as the class, so it works to read ahead. (Problem is, the syllabus is not listed in the course outline, so what should we read?)

1.2 Group theory: Dihedral and Permutation groups

Fix $n \geq 3$, regular n-gon on a plane. For e.g. n=7

Definition 1.2.1 (Symmetry)
Rigid motions in $\mathbb{R}^3$, in which we can move it(?) around in $\mathbb{R}^3$ and put it back to get the same region.

Definition 1.2.2 (Dihedral Group)
D_{2n} - set of all such symmetries (which is a "group").

Our interest: the end results

Two symmetries are the same if they have the same final position.

Fix a labelling of the vertices.

An element of D_{2n} determines and is determined by how it permutes the vertices (labels).

Definition 1.2.3 (Permutation)
A permutation of a set X is a bijection $\sigma : X \to X$. S_X is the set (or "group") of all permutations of X. $S_n := S_{\{1,...,n\}}$

So $D_{2n} \subset S_n$, we view $\sigma \in D_{2n}$ as the permutation $\{1, ..., n\} \to \{1, ..., n\}$. So $i \mapsto$ the vertex that the symmetry σ takes i to.

Not all permutations are symmetries!

Example 1.2.1
$n = 4$, with labels 1, 2, 3, 4

Let $\sigma \in S_4$ with mapping $1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3, 4 \mapsto 4$.

So $\sigma \notin D_8$

Claim 1.2.1
$|S_n| = n!$

Proof
There are n labels. Firstly, pick 1, then there will be n - 1 choices for 2. Then, pick 2, then there remains n - 2 choices. Continue this argument. This completes the proof.

Claim 1.2.2
$|D_{2n}| = 2n$

Proof
For each vertex, $i \in \{1, ..., n\}$, we have the rigid motion that takes vertex 1 to vertex i. Then we have a choice of placing vertex 2 at vertex i + 1 (where n + 1 = 1) or i - 1 (where 1 - 1 = n). Both choices are possible and give distinct symmetries. E.g. They take the pair (1, 2) to distinct pairs. So we have 2n elements in D_{2n} so far. But a symmetry is determined by where it takes (1, 2).

We can "multiply" the elements of D_{2n} – and also of S_n – by composition.

Given $\sigma, \tau \in S_n$, denote by $\sigma\tau$ the permutation that first does τ then does σ, and then does σ, r times is expressed as $\sigma^r := \sigma\sigma \ldots \sigma$.

Note

1. *If $\sigma, \tau \in D_{2n}$, then $\sigma\tau \in D_{2n}$. We can also "invert" elements of D_{2n}. If $\sigma \in S_n, \sigma^{-1} \in S_n$.*
2. *$\sigma \in D_{2n} \implies \sigma^{-1} \in D_{2n}$.*

3. $(\sigma^r)^{-1} = (\sigma^{-1})^r =: \sigma^{-r}$

In D_{2n}, we have a distinguished element called the **identity**, denoted by 1, which does nothing.

Convention: $\sigma \in S_n, \sigma^0 = 1$

Our proof that $|D_{2n}| = 2n$ actually showed us that:

Claim 1.2.3
Every element of D_{2n} can be written uniquely as $r^i s^k$ where $k = 0, 1$, $i = 0, ..., n-1$, r is the rotation of the n-gon by $\frac{2\pi}{n}$ radians (by one vertex), and $s =$ reflection across the line that passes through i and the origin.

Chapter 2

Lecture 2: Sept 11, 2017

2.1 Last time

$D_{2n} \subseteq S_n$ for $n \geq 3$.

Claim 2.1.1
Every element of D_{2n} can be written uniquely as $r^i s^k$ where $k = 0, 1$, $i = 0, ..., n-1$, r is the rotation of the n-gon by $\frac{2\pi}{n}$ radians (by one vertex), and $s =$ reflection across the line that passes through i and the origin.

2.2 Continuing on Dihedral groups

We can "compute" D_{2n}.

Example 2.2.1
Consider the element of D_{2n} given by $r_{-1}sr^2s$ which is equals to $r^{-1}r^{-2}ss = r^{-3}s^2 = r^{-3} = r^{n-3}$.

Note (General identities in D_{2n})

1. $sr^i = r^{-i}s \quad i = 0, ..., n-1$
2. $s^2 = 1$
3. $r^{-1} = r^{n-i}$

2.3 Groups

Definition 2.3.1 (Group)
A group is a non-empty set G equipped with a binary operation, i.e. a function

$$* : G \times G \to G \tag{2.1}$$

which is from ordered pairs of leemnts in G to G, satisfying the following three axioms:

1. *Associativity:* $\forall a, b, c \in G \; a * (b * c) = (a * b) * c$.
2. $\exists$ *identity element* $e \in G$ *with the property* $\forall a \in G \; a * e = e * a = a$.
3. $\forall a \in G \; \exists$ *an inverse* $a^{-1} \in G \quad a * a^{-1} = a^{-1} = e$.

Example 2.3.1
S_n *is a (finite) group with*

1. $* =$ *composition*
2. $e = 1$
3. $a^{-1} =$ *inverse permutation*

Example 2.3.2
D_{2n} *is a group.*

Definition 2.3.2 (Subgroup)
A subgroup of a group G is a non-empty subset $H \subseteq G$ that is closed under both $*$ and taking inverses, i.e.

- $a, b \in H \subseteq G \implies a * b \in H$
- $a \in H \subseteq G \implies a^{-1} \in H$

We denote H as a subgroup of G by $H \leq G$.

Remark
If $H \leq G$, then $* \restriction_{H \times H} : H \times H \to H$ and this makes H into a group.

Proof
$* \restriction_{H \times H}$ *is the fact that H is closed under $*$.*

Associativiy of $* \restriction_{H \times H}$ on H follows from associativity of $*$ on G.

For axiom (ii), take $a \in H$. So $a^{-1} \in H$. Then $a * a^{-1} \in H$. But since $a * a^{-1} = e \in G$ by axiom (iii). Thus $e \in H$.

Axiom (iii) is from the fact that H is closed under taking inverses.

Given a subgroup H of a group $(G, *)$, we call (H, $* \restriction_{H \times H}$) the induced group structure on H.

Example 2.3.3
$D_{2n} \leq S_n$

Example 2.3.4
(a) S_n

(b) D_{2n}

(c) $\mathbb{R}^*$ *= non-zero real numbers,* $*$ *= usual multiplication,* $a^{-1} = \frac{1}{a}, e = 1$.

(d) More generally, for $n \geq 1$, $GL_n(\mathbb{R})$ *= set of* $n \times n$ *invertible matrices with real entries* ($GL_n(\mathbb{R}) = \mathbb{R}^*$*),* $*$ *= matrix multiplication,* $e = I$*, inverse is* M^{-1} *if* $M \in GL_n(\mathbb{R})$.

This works with $\mathbb{R}$ *replaced by* $\mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$.

Definition 2.3.3 (Abelian Group)
A group $(G, *)$ *is called abelian if* $*$ *is commutative, i.e.* $a * b = b * a$ *for all* $a, b \in G$.

Example 2.3.5
From our previous example, (a) and (b) are non-abelian (for $n \geq 3$*). (c) is abelian. (d) is non-abelian for* $n > 1$.

Continuing the numbering of the example,

(e) The following are abelian groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}_p, +)$

where we have $* = +, e = 0, a^{-1} = -a$

Note (Multiplicative Notation)
We often write ab *for* $a * b$ *and we tend to write 1 for* e.

Note (Additive Notation)
*If we are working with a group (G, *) that we know is abelian, we often write* $a + b$ *instead of* $a * b$*. We write 0 instead of* e *and write* $-a$ *instead of* a^{-1}.

We never use Additive Notation if we are unsure about the commutativity of the group.

Chapter 3

Lecture 3: Sept 13, 2017

3.1 Properties of Groups

Proposition 3.1.1
Suppose G is a group.

1. *The identitiy element is unique.*
2. *For each $a \in G$, a has a unique inverse.*
3. $(a^{-1})^{-1} = a$
4. $(ab)^{-1} = b^{-1}a^{-1}$
5. *Generalised associativity law: $\forall a_1, ...a_n \in G$, then $a_1a_2...a_n$ gives the same value regardless of how we associate the expressions.*
6. *In any group G, $1^{-1} = 1$*

Proof

1. *Suppose $e, e' \in G$ are both identity elements (WTP $e = e'$).*

$$\begin{aligned} e &= e'e \quad \textit{since } e' \textit{ is an identity} \\ &= e' \quad \textit{since } e \textit{ is an identity} \end{aligned}$$

2. *Suppose $b, c \in G$ are both inverses of $a \in G$. So*

$$\begin{aligned} &ab = 1 = ac \\ &\implies b(ab) = b(ac) \\ &\implies (ba)b = (ba)c \quad \textit{associativity)} \\ &\implies 1b = 1c \quad \textit{(since } ba = 1\textit{)} \\ &\implies b = c \end{aligned}$$

3. *By defn of inverse,*

$$\begin{aligned} aa^{-1} &= 1 \\ a^{-1}a &= 1 \end{aligned}$$

   Thus a is the inverse of a^{-1}.

4. $\forall a, b \in G$

$$\begin{aligned} (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}(ab)) \\ &= b^{-1}((a^{-1}a)b) \\ &= b^{-1}(1b) \\ &= b^{-1}b = 1 \end{aligned}$$

   Similarly, $(ab)(b^{-1}a^{-1}) = 1$. Therefore $(ab)^{-1} = b^{-1}a^{-1}$.

5. *Proof for this proposition is intuitive, and we can use induction on n. See Dummit Section 1.1.*

6. $1 \cdot 1 = 1$

The fifth proposition allows us to drop the parenthesis without ambiguity.

Note (Notation)
$\forall a \in G \ n > 0$

$$a^n = a \cdot a \cdot \ldots \cdot a, \quad a^0 = 1, \quad a^{-n} = (a^n)^{-1}$$

Remark

1. *By Proposition (d), $a^{-n} = (a^n)^{-1}$*

2. *In general, $(ab)^n \neq a^n b^n$ (especially for non-abelian)*

Proposition 3.1.2 (Cancellation law)
For any $a, b, u, v \in G$

1. $au = av \implies u = v$ *(Left-cancellation)*
2. $ub = vb \implies u = v$ *(Right-cancellation)*

Proof

1.

$$\begin{aligned} au &= av \\ a^{-1}au &= a^{-1}av \\ u &= v \end{aligned}$$

2. *Similar to above.*

Remark
Note that 0 is not in a group, since every element must have an inverse but 0 does not.

3.2 Homomorphism

Definition 3.2.1 (Group Homomorphism)
A group homomorphism $\phi : G \to H$ where G, H are groups, is a function from G to H with with the property that for all $a, b \in G$

$$\phi(ab) = \phi(a)\phi(b)$$

(aka a morphism of groups)

Definition 3.2.2 (Isomorphism)
A homomorphism $\phi : G \to H$ is called an isomorphism if it is bijective.

We say that $G \simeq H$, and say that G is isomorphic to H, if there exists an isomorphism $\phi : G \to H$.

Remark
ab is a multiplication in G.

$\phi(a)\phi(b)$ is a multiplication in H.

Proposition 3.2.1
If $\phi : G \to H$ is a group homomorphism, then

1. $\phi(1_G) = 1_H$
2. $\forall a \in G \;\; \phi(a^{-1}) = \phi(a)^{-1}$

Proof

1. $1_H\phi(1_G) = \phi(1_G) = \phi(1_G 1_G) = \phi(1_G)\phi(1_G)$. *Thus, by Cancellation Law,* $1_H = \phi(1_G)$.
2. $\forall a \in G$

$$\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(1_G) = 1_H$$
$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1_G) = 1_H$$
$$\implies \phi(a^{-1}) = \phi(a)^{-1}$$

Definition 3.2.3 (Kernel)
If $\phi : G \to H$ *is a group homomorphism, then the kernal of* ϕ *is*

$$\ker(\phi) = \{a \in G : \phi(a) = 1\} \tag{3.1}$$

Proposition 3.2.2
$\ker(\phi) \leq G$

Proof
Suppose $a, b \in \ker(\phi)$.

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

So $ab \in \ker(\phi)$. *So* $\ker(\phi)$ *is closed under the group operation of* G.

Suppose $a \in \ker(\phi)$.

$$\phi(a^{-1}) = \phi(a)^{-}1 = 1_H^{-1} = 1_H$$

So $\ker(\phi)$ *is closed under inverses.*

Also, $\ker(\phi) \neq \emptyset$ *since* $\phi(1_G) = 1_H$ *by proposition 3(a), so* $1_G \in \ker(\phi)$.

Chapter 4

Lecture 4: Sep 15, 2017

4.1 Examples of Homomorphism

Example 4.1.1
Fix $n \geq 2$.

1. $\mathbb{Z}_n = \{0, 1, ..., n-1\}$

   addition: $a \oplus b$ *= remainder of* $a + b$ *when divided by* n

   multiplication: $a \otimes b$ *= remainder of* ab *when divided by* n

   $(\mathbb{Z}_n, \oplus)$ *is an abelian group with identity 0.*

   The fact that this is a (finite) group uses basic arithmetic of congruences.

2. $(\mathbb{Z}, +)$ *is an abelian group.*

   $\mathrm{rem} : \mathbb{Z} \to \mathbb{Z}_n$

   $\mathrm{rem}(a) =$ *remainder of* a *when divided by* n*.*

   This is a group homomorphism.

Proof

2. *Need to show* $\mathrm{rem}(a + b) = \mathrm{rem}(a) \oplus \mathrm{rem}(b)$

   We know

$$\begin{aligned} a &\equiv \operatorname{rem}(a) \mod n \\ b &\equiv \operatorname{rem}(b) \mod n \end{aligned}$$

$$\begin{aligned} \implies & a + b \equiv \operatorname{rem}(a) + \operatorname{rem}(b) \mod n \\ & \textit{and} \\ & a + b \equiv \operatorname{rem}(a+b) \mod n \end{aligned}$$

$$\implies \operatorname{rem}(a+b) \equiv (\operatorname{rem}(a) + \operatorname{rem}(b)) \mod n$$

But $0 \leq \operatorname{rem}(a+b) \leq n-1$. *Therefore,*

$$\begin{aligned} \operatorname{rem}(a+b) &= \textit{remainder when } (\operatorname{rem}(a) + \operatorname{rem}(b)) \textit{ is divided by } n \\ &= \operatorname{rem}(a) \oplus \operatorname{rem}(b) \end{aligned}$$

Note

$$\begin{aligned} \ker(\operatorname{rem}) &= \{an : a \in \mathbb{Z}\} \\ &= \{b \in \mathbb{Z} : n | b\} = n\mathbb{Z} \end{aligned}$$

So $n\mathbb{Z} \leq \mathbb{Z}$, *i.e.* $n\mathbb{Z}$ *is a subgroup of* $\mathbb{Z}$.

Example 4.1.2
$G = \mathbb{R}^{>0}$ *is a group under multiplication.*

Note: $\mathbb{R}^{>0} \leq R^X$

$H = (\mathbb{R}, +)$

$\exp : \mathbb{R} \to \mathbb{R}^{>0}$ *e.g.* $r \mapsto e^r$

Group homomorphism from $H \to G$: $\exp(a+b) = e^{a+b} = e^a e^b = \exp(a)\exp(b)$

$\exp(a+b)$ *is a group operation on* H.

$\exp(a)\exp(b)$ *is a group operation on* G.

So $\exp$ *is a group homomorphsim from the additive group of reals to the multiplicative group of the positive reals. In fact, it is an isomorphism since it is bijective.*

exp ***is injective***

$$\begin{aligned} e^a &= e^b \\ \implies \ln(e^a) &= \ln(e^b) \\ \implies a &= b \end{aligned}$$

exp ***is surjective***

$$r \in \mathbb{R}^{>0} \quad a = \ln(r)$$
$$\implies e^a = e^{\ln r} = r$$
$$\ln : (\mathbb{R}^{>0}, x) \to (\mathbb{R}, +) \textit{ is also a group homomorphism}$$
$$\ln(ab) = \ln(a) + \ln(b)$$
$$\exp \circ \ln : \mathbb{R}^{>0} \to \mathbb{R}^{>0} \quad r \mapsto r$$
$$\exp \circ \ln : id_G$$
$$\ln \circ \exp : id_H$$

Definition 4.1.1 (Inverse of a Group Homomorphism)
If $\phi : G \to H$ is a group homomorphism, then an inverse to ϕ is a group homomorphism

$$\psi : H \to G \tag{4.1}$$

such that

$$\psi \circ \phi = id_G$$
$$\phi \circ \psi = id_H$$

Example 4.1.3 (Exercise)
A group homomorphism is an isomorphism iff it has an inverse group homomorphism.

Note
$(\mathbb{R}, +) \simeq (\mathbb{R}^{>0}, \times)$

Proposition 4.1.1
Suppose $\phi : G \to H$ is a surjective group homomorphism. If G is abelian, then so is H

Proof

$$a, b \in H \qquad \exists r, s \in G \ a = \phi(r) \ b = \phi(s)$$
$$ab = \phi(r)\phi(s) = \phi(rs) = \phi(sr) = \phi(s)\phi(r) = ba$$

Corollary 4.1.1
If $G \simeq H$ then G is abelian iff H is abelian.

Example 4.1.4
$GL_1(\mathbb{C}) \not\simeq GL_2(\mathbb{C})$

$GL_1(\mathbb{C})$ *is abelian.*

$GL_2(\mathbb{C})$ *is not abelian.*

Example 4.1.5
$G = (\mathbb{Z}_4, \oplus)$

$H = (\mathbb{Z}_5^\times, \otimes)$

$\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$ — *identity = 1*

(Note $\mathbb{Z}_6^\times$ is not a group under $\otimes$)

$\phi : G \to H$

$$\begin{aligned} \phi(0) &= 1 \\ \phi(1) &= 2 \\ \phi(2) &= 3 \\ \phi(3) &= 4 \end{aligned}$$

But then $\phi(1 \oplus 1) = \phi(2) = 3$ and $\phi(1) \otimes \phi(1) = 2 \otimes 2 = 4$.

So $\phi(1 \oplus 1 \neq \phi(1) \otimes \phi(1)$.

***But** actually $G \simeq H$, since*

$$\begin{aligned} \psi(0) &= 1 \\ \psi(1) &= 2 \\ \psi(2) &= 4 \\ \psi(3) &= 3 \end{aligned}$$

is an isomorphism.

Chapter 5

Lecture 5: Sep 18, 2017

5.1 Group Actions

Definition 5.1.1 (Group Action)
A group action is a group G on a set A is a function

$$G \times A \to A \tag{5.1}$$

denoted by $\cdot$, i.e.

$$(g, a) \mapsto g \cdot a \in A \tag{5.2}$$

satisfying

1.

$$g_1 \cdot (g_2 \cdot a) = \overset{\text{multiplication in } G}{\overset{\downarrow}{(g_1 g_2)}} \underset{\text{group action}}{\underset{\uparrow}{\cdot}} a$$

2. $1 \cdot a = a$

forall $g_1, g_2 \in G,\ a \in A$.

If G acts on A, for each $g \in G$ we get $\sigma_g : A \to A$, i.e. $a \mapsto g \cdot a$

Lemma 5.1.1 (σ_g as a bijection)
G acts on A, $g \in G$. Then $\sigma_g : A \to A$ is a bijection.

Proof
For injection,

$$\begin{aligned} \forall a, b \in A\ \sigma_g(a) &= \sigma_g(b) \\ \implies g \cdot a &= g \cdot b \\ \implies g^{-1} \cdot (g \cdot a) &= g^{-1} \cdot (g \cdot b) \\ \implies (g^{-1}g) \cdot a &= (g^{-1}g) \cdot b \\ \implies 1 \cdot a &= 1 \cdot b \\ \implies a &= b \quad \textit{by property 2} \end{aligned}$$

For surjection,

$$\forall b \in A \quad \textit{Let } a = g^{-1} \cdot b$$
$$\sigma_g(a) = g \cdot a = g \cdot (g^{-1} \cdot b) = (gg^{-1}) \cdot b = b$$

Note (Warning)
Do not confuse the action of G on A and group operation on G, especially as we often write ga instead of $g \cdot a$ for the group action.

Hopefully, the difference is clear by context.

Note (Recall)
For any set A

$$S_a = \textit{ group of bijections of } \sigma : A \to A \textit{ under composition} \tag{5.3}$$

If G acts on A, we have just defined a function

$$G \to S_A \quad \textit{Lemma 5.1.1}$$
$$g \mapsto \sigma_g$$

Proposition 5.1.1 (Permutation Representation)
The function $G \to S_A$ given by $g \mapsto \sigma_g$ is a group homomorphism.

Proof
All we have to check is that for any $g, h \in G$

$$\sigma_{gh} = \sigma_g \circ \sigma_h \tag{5.4}$$

Both sides are permutations of A.

Let $a \in A$ be arbitrary.

$$\begin{aligned}\sigma_{gh}(a) &= (gh) \cdot a \\ &= g \cdot (h \cdot a) \\ &= g \cdot (\sigma_h(a)) \\ &= \sigma_g(\sigma_h(a))\end{aligned}$$

Exercise 5.1.1
Prove the converse of Proposition 5.1.1: Suppose G is a group, A is a set, and $\phi : G \to S_A$ is a group homomorphism. Then we get an action of G on A by

$$g \cdot a := \phi(g)(a) \in A \tag{5.5}$$

Moreover, the associated $G \to S_A$ which $g \mapsto \sigma_g$ is just ϕ.

Definition 5.1.2 (Trivial Homomorphism)
For G, H groups, the trivial homomorphism $\phi : G \to H$ is $\phi(g) = 1_H$ for all $g \in G$, i.e. $\ker(\phi) = G$.

Example 5.1.1

1. *Trivial action: Every group G acts on every set A by $g \cdot a = a$.*

   - $g_1 \cdot (g_2 \cdot a) = g_1 \cdot a = a = (g_1 g_2) \cdot a$

   The associated permuration representation $G \to S_A$ is the trivial homomorphism, i.e. $\sigma_g = \mathrm{id}_A : A \to A$ which $a \mapsto a$ for all $g \in G$. Everything is in the kernel of the action.

Definition 5.1.3 (Kernel of the Action)
Suppose G acts on A and $\phi : G \to S_A$ which $g \mapsto \sigma_g$ is the corresponding homomorphism. We call $\ker(\phi) \leq G$ the kernel of the action of G on A. It is the set of elements in G that acts trivially on A.

Example 5.1.2

2. *Grenary set A, S_A acts on A by*

$$\sigma \cdot a := \sigma(a) \tag{5.6}$$

   The corresponding homomorphism

$$S_A \to S_A \tag{5.7}$$

   is the identity homomorphism, i.e.

$$\sigma_\tau = \tau \quad \text{any } \tau \in S_A \tag{5.8}$$

3. V is an $\mathbb{R}$-vector space. Then scaloar multiplication

$$\mathbb{R}^\times \times V \to V$$
$$(r, v) \mapsto rv$$
$$r(sv) = (rs)v \quad \textit{is a vector space axiom}$$

Note: $\mathbb{R}^\times$ is the non-zero reals

So $(\mathbb{R}^\times, \times)$ acts on the vector space V.

The associated homomorphism from $\mathbb{R}^\times \to S_V$ is injection if V is nontrivial (exercise).

Note (Bad notation last lecture)

$$\mathbb{Z}_5^\times = \{1, 2, 3, 4\} \quad \textit{with } \otimes \tag{5.9}$$

but

$$\mathbb{Z}_6 \setminus \{0\} \tag{5.10}$$

is not a group.

($\mathbb{Z}_6^\times$ is something else, see homework)

Chapter 6

Lecture 5: Sep 20, 2017

6.1 Logistics

Note (Homework 1)
Q5 $(\mathbb{Z}_n, \oplus)$

Note (Midterm Confusion)
- check email

Note
symmetric group (S_A) = *permutation groups*

6.2 More on Group Actions

We continue with two important group actions:

Example 6.2.1

4. *Groups acting on themsevles by left multiplication:*

   Let G be a group. G acts on itself by

$$g \in G,\ a \in G \quad g \cdot a = ga \tag{6.1}$$

   associativity of group operation

$$\iff g \cdot (h \cdot a) = (gh) \cdot a \tag{6.2}$$

   group axiom about identity

$$\implies 1 \cdot a = a \tag{6.3}$$

Exercise 6.2.1
Multiplication on the right is not a group action.

We have a corresponding permutation representation

$$G \to S_G \tag{6.4}$$

Proposition 6.2.1
$G \to S_G$ is injective.

Proof
$\forall g, h \in G \ \sigma_g = \sigma_h$

In particular, $\sigma_g(1) = \sigma_h(1)$.

$$\sigma_g(1) = g \cdot 1 = g1 = g$$
$$\sigma_h(1) = h \cdot 1 = h1 = h$$

Therefore, $g = h$.

In particular, the kernel of this action is trivial, i.e., the subgroup $\{1\} \leq G$.

Definition 6.2.1 (Faithful)
A group action G on A is said to be faithful if the kernel of the action is trivial, i.e. the only group element fixing all of A pointwise is the identity element 1_G.

Definition 6.2.2 (Image Set)
Suppose $\phi : G \to H$ is a group homomorphism. Then $I_m(\phi) = \{h \in H : h = \phi(g) \text{ for some } g \in G\}$

Lemma 6.2.1 (Lemma 9)
Suppose $\phi : G \to H$ is a group homomorphism.

1. $I_m(\phi) \leq H$
2. *If ϕ is injective then it induces an isomorphism*

$$G \xrightarrow{\simeq} I_m(\phi) \tag{6.5}$$

Proof

1. *Suppose* $h_1, h_2 \in I_m(\phi) \implies \exists g_1, g_2 \in G\ \phi(g_1) = h_1\ \phi(g_2) = h_2$.

$$\begin{aligned} h_1h_2 &= \phi(g_1)\phi(g_2) \\ &= \phi(g_1g_2) \end{aligned}$$

Since $g_1g_2 \in G \implies h_1h_2 \in I_m(\phi)$

Also $\phi(1_G) = 1_H$ *so*

$$\begin{aligned} 1_G \in I_m(\phi) &\implies I_m(\phi) \neq \emptyset \\ &\implies I_m(\phi) \leq H \end{aligned}$$

2. $I_m(\phi)$ *is a group and*

$$\phi : G \to I_m(\phi) \tag{6.6}$$

is a bijection group homomorphism. Hence

$$G \simeq I_m(\phi) \tag{6.7}$$

Corollary 6.2.1 (Cayley's Theorem)
Every group is isomorphic to a subgroup of some permutation. Moreover, is a group G *is finite, i.e.* $|G| = n$ *for some* n*, then* G *is isomorphic to a subgroup* S_n*.*

Proof
Consider the action of G *on itself by left multiplication. By Proposition 6.2.1, this gives us an injective group homomorphism* $\phi : G \to S_G$*. By Lemma 6.2.1,* $G \simeq I_m(\phi) \leq S_G$*. Moreover, if* $|G| = n$*, then* $S_G \simeq S_n := S_{\{1,2,\ldots,n\}}$*.*

Example 6.2.2

5. *Groups acting on themselves by conjugation*

Definition 6.2.3 (Conjugation)
For a group G*,* $\forall g, h \in G$*. Then the conjugate of* h *by* g *is the element* ghg^{-1}*.*

Remark
If G *is abelian, then* $ghg^{-1} = hgg^{-1} = h$*, i.e. a conjugation does nothing in abelian groups. Thus the notion of a conjugation is only interesting for non-abelian groups.*

Example 6.2.3
Conjugation as an action of G *on itself, i.e. given* $g \in G,\ a \in G, g \cdot a := gag^{-1}$

Given $g, h \in G,\ g \cdot (h \cdot a) = g \cdot (hah^{-1}) = g(hah^{-1})g^{-1} = (gh)a(h^{-1}g^{-1}) = (gh)a(gh)^{-1} = (gh) \cdot a$*.*

$1 \cdot a = 1a1^{-1} = a$

Example 6.2.4
We get another permutation representation

$$\psi : G \to S_G \tag{6.8}$$

coming from G acting on itself by conjugation.

$\ker(\psi) = \{g \in G : ga = ag \ \forall a \in G\}$

Note that $gag^{-1} = a \iff ga = ag$

If G is abelian, this is the trivial action.

Definition 6.2.4 (Center of the Group)
For any group G,

$$Z(G) = \{g \in G : \forall h \in G \ gh = hg\} \tag{6.9}$$

*is called the **center of G**.*

Remark

1. *If G is abelian, then $Z(G) = G$.*
2. $Z(G) \leq G$ *since* $Z(G) = \ker(\psi)$ *which is the kernel of the action of G on itself by conjugation.*

Chapter 7

Lecture 7: Sep 22, 2017

7.1 Cosets

Definition 7.1.1 (Left Cosets)
Let G is a group and $H \leq G$.

A ***left coset*** *of H is a set of the form $aH = \{a \cdot h : h \in H\}$ for some $a \in G$*

Example 7.1.1

$$\begin{aligned} G &= S_3 \quad (= D_6) \\ &= < r, s | r^3 = s^2 = 1, r^2 s = sr > \\ &= \{1, r, r^2, s, rs, r^2 s\} \end{aligned}$$

$$H = \{1, s\} = \substack{\textit{subgroup generated by } s \\ \textit{smallest subgroup of } G \textit{ containing } s \\ (1 \in H, ss = 1 \in H)}$$

The left cosets of H are:

$$\begin{aligned} 1H &= H & &= \{1, s\} \\ rH &= \{r, rs\} \\ r^2 H &= \{r^2, r^2 s\} \\ sH &= \{s, s^2\} & &= \{1, s\} \\ rsH &= \{rs, rs^2\} & &= \{r, rs\} \\ r^2 sH &= \{r^2 s, r^2 s^2\} & &= \{r^2, r^2 s\} \end{aligned}$$

Observe that

1. $1H = sH = \{1, s\}$

   $rH = rsH = \{r, rs\}$

   $r^2H = r^2sH = \{r^2, r^2s\}$

2. $aH \neq bH \implies aH \cap bH = \emptyset$
3. $\bigcup_{a \in G} aH = G$
4. *All of the left cosets have the same size.*

Proposition 7.1.1 (Proposition 11)
Let G be a group and $H \leq G$, and $a, b \in G$. Then $aH = bH \iff a \in bH$.

Proof
Suppose $aH = bH$, then $a = a1$ and since $1 \in H$, $a1 \in aH = bH$.

Suppose $a \in bH$. Then $a = bh$ for some $h \in H$. For any $h' \in H$, $ah' = bhh'$ and since $hh' \in H$, $ah \in bH$. This implies that $aH \subset bH$.

For any $h'' \in H$, since $a = bh$ thus we have that $bh'' = ah^{-1}h''$ and since $h^{-1}h'' \in aH$. Thus $bH \subset aH$.

Therefore, $aH = bH$.

Corollary 7.1.1

1. $aH = bH \iff b^{-1}a \in H$

   $aH = H \iff a \in H$

2. $aH \cap bH \neq \emptyset \implies aH = bH$

Proof

1.

$$\begin{aligned} aH = bH &\iff a = bh \text{ for some } h \in H \\ &\iff b^{-1}a = h \text{ for some } h \in H \\ &\iff b^{-1}a \in H \end{aligned}$$

2. *Suppose $c \in aH \cap bH$. Then $c \in aH \implies cH = aH$ and $c \in bH \implies cH = bH$. Therefore $aH = bH$.*

Proposition 7.1.2

$$\bigcup_{a\in G} aH = G \tag{7.1}$$

Proof

$$\bigcup_{a\in G} aH \subset G$$

For any $g \in G$, $g \in gH \subset \bigcup_{a\in G} aH \implies G \subset \bigcup_{a\in G} aH$

Proposition 7.1.3
Let G *be a group,* $H \leq G, a \in G$. *Then the map*

$$\begin{aligned}\sigma_a : H &\to aH \\ h &\mapsto ah\end{aligned}$$

is a bijection of sets.

Proof
By definition of left cosets, aH, σ_a *is surjective, since* $ah = \sigma_a(h)$.

If $\sigma_g(h_1) = \sigma_a(h_2)$ *for* $h_1, h_2 \in H$, *then* $ah_1 = ah_2$, *which then* $h_1 = h_2$. *Thus* σ_a *is injective.*

Corollary 7.1.2
If H *is finite, then* $|H| = |aH|$ *for any* $a \in G$. *This means that all left cosets have the same size.*

Remark
We now know that

- *All left cosets have the same size.*
- G *is the union of all left cosets, and furthermore, it can be partitioned into all the distinct left cosets. Thus if* G *is finite, then*

  $$|G| = |H|(\textit{number of distinct left cosets}) \tag{7.2}$$

  We call the number of distinct left cosets of H *the index of* H *in* G, *denoted by* $[G : H]$.

Example 7.1.2

$$
\begin{gathered}
G = S_3 \\
H = \{1, s\} \\
rH = \{r, rs\} \\
r^2H = \{r^2, r^2s\} \\
G = \{1, s\} \cup \{r, rs\} \cup \{r^2, r^2s\} \\
|G| = 2 + 2 + 2 \\
[G : H] = 3
\end{gathered}
$$

Corollary 7.1.3 ((12) Lagrange's Theorem)
If G is a finite group and $H \leq G$, then

$$|H|\Big||G| \tag{7.3}$$

Proof
$|G| = |H|[G : H]$ *and* $[G : H] \in \mathbb{Z}$

Definition 7.1.2 (Order)
The order of a group G is the cardinality of G.

Example 7.1.3
In our previous example, note that S_3 cannot have a subgroup of order 4.

Example 7.1.4 (Subgroups of S_3)
$S_3 = \{1, r, r^2, s, rs, r^2s\}$

$$
\begin{gathered}
H \leq S_3 \implies |H| = 1 \text{ or } 2 \text{ or } 3 \text{ or } 6 \\
|H| = 1 \implies H = \{1\}|H| = 6 \implies H = S_3 \\
|H| = 2 \implies H = \{1, s\} \text{ or } \{1, rs\} \text{ or } \{1, r^2s\} \\
|H| = 3 \implies
\end{gathered}
$$

Suppose $|H| = 2$. Then $H = \{1, a\}$ for some $a \in G$.

$$a^2 \in H \implies a^2 = 1 \text{ or } a^2 = a$$

but $a^2 = a \implies a = 1$. So $\{1, s\} \leq G \iff a^2 = 1$ since $a^2 = 1 \implies a^{-1} = a \in H$.

Suppose $|H| = 3$. *Can* H *contain S? No, since if* $s \in H$*, then* $\{1, s\} \subset H$ *and* $\{1, s\}$*, but by (12) Lagrange's Theorem 7.1.3* $2 \not| 3$. *Likewise,* $rs, r^2 s \notin H$. *Thus*

$$
\begin{aligned}
H &= \{1, r, r^2\} \\
&= \text{smallest subgroup containing } r \\
&= \text{subgroup generated by } r
\end{aligned}
$$

Converse of (12) Lagrange's Theorem 7.1.3 is false.

There exists a finite group G and a positive integer $m||G|$ such that G does not have a subroup of order m.

Example 7.1.5

$$
\begin{aligned}
G &= A_4 \\
&= \text{ group of symmetries of a regular tetrahedron, order 12} \\
&= \{1, (1,2)(3,4), (1,4)(2,3), (1,3)(2,4), (2,3,4), (4,3,2), (1,3,4), (1,2,4), (4,2,1), (1,2,3), (3,2,1)\}
\end{aligned}
$$

A_4 *has no subgroup of order 6 (exercise)*

Chapter 8

Lecture 8: Sep 25, 2017

8.1 Continuing with Cosets

We can similarly define right cosets as

$$\forall a \in G\ H \leq G \quad H_a := \{ha : h \in H\} \tag{8.1}$$

Definition 8.1.1 (Set of Left Cosets)
Let $H \leq G$

$$G/H := \text{ set of all left cosets of } H \text{ in } G \tag{8.2}$$
$$:= \{aH : a \in G\} \tag{8.3}$$

which we call as G mod H.

Note
We have a natural action of G on G/H given by: $\forall g \in G$

$$g \cdot aH := (ga)H \tag{8.4}$$

$$\text{The kernel of this action} = \{g \in G : gaH = aH\ \forall a \in G\} \tag{8.5}$$
$$= \{g \in G : a^{-1}ga \in H\ \forall a \in G\} \tag{8.6}$$

Example 8.1.1
$G = (\mathbb{Z}, +) \quad d > 0\ H = d\mathbb{Z} \leq \mathbb{Z}$

$$\mathbb{Z}/d\mathbb{Z} = \{a + d\mathbb{Z} : a \in \mathbb{Z}\} \tag{8.7}$$
$$= \{[a]_d : a \in \mathbb{Z}\} \tag{8.8}$$

where $[a]_d = \{n \in \mathbb{Z} : n \equiv a \mod d\} = a + d\mathbb{Z}$.

So the congruence class of $a \mod d$ *is just the left coset of* $d\mathbb{Z}$ *by* a.

This has a natural group structure: $[a]_d + [b]_d = [a = b]_d$.

So left cosets generalises congruences classes to arbitrary groups.

We now try to put a natural group structure on G/H:

$$(aH)(bH) := abH \tag{8.9}$$

But in general, given any

$$X, Y \subseteq G$$
$$XY := \{xy : x \in X,\ y \in Y\} \subseteq G \tag{8.10}$$

Note that Equation 8.10 is a **natural definition**.

If

$$\begin{gathered} X = aH\ Y = bH \implies XY = \{ah_1bh_2 : h_1, h_2 \in H\} \\ abH = \{abh : h \in H\} \\ abH \subseteq XY \\ XY \not\subseteq abH \quad \text{in general} \end{gathered}$$

If G is abelian, then $XY = abH$ and Equation 8.9 is a good definition.

G abelian: $XY \subseteq abH$

Proof
$ah_1bh_2 = abh_1h_2$ *then we can just take* $h = h_1h_2$.

All we need for $abH = (aH)(bH)$ *is that for all* $h_1 \in H$, *for some* $h' \in H$, $h_1b = bh'$. *Then*

$$ah_1bh_2 = abh'h_2 = abh$$

by $h = h'h_2 \in H$.

Definition 8.1.2 (Normal Subgroup)
A subgroup $H \leq G$ *is normal if* $\forall b \in H\ Hb = bH$, *i.e.*

$$\forall h \in H\ \exists h' \in H \quad hb = bh' \tag{8.11}$$

We denote a normal subgroup by $H \triangleleft G$.

Lemma 8.1.1 (Lemma 13)
$H \leq G$. TFAE:

1. $H \lhd G$
2. $\forall b \in G\ b^{-1}Hb \subseteq H$
3. $b^{-1}Hb = H$

Proof
1 $\iff$ 3 *Suppose* $H \lhd G\ b \in G$

$$\begin{aligned} Hb &= \{hb : h \in H\} \\ bH &= \{bh : h \in H\} \\ b^{-1}Hb &= \{b^{-1}hb : h \in H\} \end{aligned}$$

$$\begin{aligned} &Hb = bH \\ \implies &b^{-1}Hb = H \end{aligned}$$

3 $\implies$ 2 *is straightforward*

2 $\implies$ 3 *Apply 2 to* b^{-1}*, so that*

$$\begin{aligned} (b^{-1})^{-1}H(b^{-1}) &\subseteq H \\ bHb^{-1} &\subseteq H \\ Hb^{-1} &\subseteq b^{-1}H \\ H &\subseteq b^{-1}Hb \end{aligned}$$

Therefore, $\forall b \in G\ H = b^{-1}Hb$

For 1 $\implies$ 3, we needed the following

Definition 8.1.3
$X \subseteq G$

$$\begin{aligned} bH &:= \{bx : x \in X\} \\ Xb &:= \{xb : x \in X\} \end{aligned}$$

Exercise 8.1.1
- $X = Y \implies bX = bY$
- $a(bX) = (ab)X$

Lemma 8.1.2 (Lemma 14)
If $H \triangleleft G$ and $a, b \in G$, then

$$\underbrace{(aH)(bH)}_{\textit{set product}} = (ab)H \tag{8.12}$$

Proof
is an exercise (yay) - it is what motivated the definition of a normal subgroup

Remark
Suppose $H \triangleleft G$. Let G act on G/H. The kernel of the action is H.

Proof

$$\begin{gathered} h \in H \ a \in G \ \exists h' \in H \\ haH = ah'H \quad (\textit{since } H \triangleleft G) = aH \end{gathered}$$

So h is in the kernel of the action.

Suppose $g \in G$ is in the kernel of the action. So

$$\forall a \in G \ gaH = aH$$

in part, take $a = 1$. So $gH = H \implies g \in H$.

Chapter 9

Lecture 9: Sep 27, 2017

9.1 Logistics

Midterm Change

Date: Friday (Oct 27)

Time: 7:30pm - 9:00pm

Location: TBA

9.2 Cyclic groups

Definition 9.2.1 (Cyclic Groups)
Given a group G, $\forall a \in G$, the cyclic subgroup of G generated by a is $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$

Proposition 9.2.1 (Proposition 15)

1. $\langle a \rangle \leq G$
2. $\langle a \rangle$ *is the smallest subgroup of G that contains a.*
3. *Suppose order of a is finite, say n. Then $\langle a \rangle := \{1, a, a^2, ..., a^{n-1}\}$ and $|\langle a \rangle| = n$.*
4. *If G is finite then every element of G has finite order.*
5. *If G is finite,* $\text{order}(a) \Big| |G|$.
6. *If G is finite, $|G| = n$, then $a^n = 1$.*

7. *If $|G|$ is prime, then G is cyclic, i.e. $G = \langle a \rangle$ by some $a \in G$.*
8. *Every subgroup of a cyclic group is cyclic. (Given without proof :( ) [This generalizes, but is proved similarly to A2Q1]*

Proof

1. $$a^n a^m = a^{n+m} \in \langle a \rangle$$
$$(a^n)^{-1} = (a^{-1})^n = a^{-n} \in \langle a \rangle$$
$$1 = a^0 \in \langle a \rangle$$

2. *$\langle a \rangle \leq G$ by (1). $a \in \langle a \rangle$ since $a = a^1$. If $H \leq G$ and $a \in H$, then since G is closed under group multiplication and inverses, $a^n \in H$ for all $n \in \mathbb{Z}$. So $\langle a \rangle \leq H$.*
3. *If $n = 1$, then $a = 1$. So $\langle a \rangle = \{1\}$. Assume $n > 1$. Let $m = qn + r \in \mathbb{Z} \quad 0 \leq r < n$.*
$$a^m = a^{qn+r} = (a^n)^q a^r = 1^q a^r = a^r \in \{1, ..., a^{n-1}\}$$
Thus $\langle a \rangle = \{1, a, ..., a^{n-1}\}$. Note that this only works for finite n.

Suppose, wlog, $0 \leq r \leq s < n$ with $a^r = a^s \implies a^{s-r} = a^s a^{-r} = 1$. But $0 \leq s-r < n$, which contradicts the definition of n being the least positive integer (or by minimality of order, $s - r = 0$). So $1, a, a^2, ..., a^{n-1}$ are all distinct and $|\langle a \rangle| = n$.
4. *$1, a, a^2, ...$ cannot all be distinct as G is finite. So for some $s > r \geq 1, a^s = a^r$. So $a^{s-r} = 1$.*
5. *By (1), $\langle a \rangle \leq G$. By (12) Lagrange's Theorem 7.1.3, $|\langle a \rangle| \Big| |G|$. By (4), a has finite order, thus (3) gives us that $\text{order}(a) = |\langle a \rangle|$.*
6. *By (4) and (5), order of a is finite, and $\text{order}(a) \Big| n$. let $l = \text{order}(a) \quad n = lk$ for some $k \in \mathbb{Z}$.*
$$a^n = a^{lk} = (a^l)^k = 1^k = 1$$
7. *Let $a \in G, a \neq 1$. Order of a is finite and $\text{order}(a) \Big| |G|$. Thus $\text{order}(a) = 1$ or $|G|$. But $\text{order}(a) = 1 \implies a = 1$. So $\text{order}(a) = |G|$. By (3), $\text{order}(a) = |\langle a \rangle|$. $\therefore \langle a \rangle = G$.*

9.3 Continuing with Normal Subgroups

Proposition 9.3.1 (Proposition 16)
If $H \triangleleft G$, then G/H = set of all left cosets is a group under set multiplication. Moreover, $\pi : G \to G/H$ given by $\pi(g) = gH$ is a surjective group homomorphism.

*G/H is called the **quotient group** and $\pi : G \to G/H$ is called the **quotient map**.*

Proof
Associativity:

$$\begin{aligned}(aHbH)cH &= (abH)cH) \quad \textit{Lemma } 8.1.2 \\ &= (ab)cH \quad \textit{Lemma } 8.1.2 \\ &= a(bc)H \quad \textit{by association} \\ &= aHbcH \quad \textit{Lemma } 8.1.2 \\ &= aH(bHcH) \quad \textit{Lemma } 8.1.2\end{aligned}$$

Inverse: Inverse of aH is $a^{-1}H$

$$\begin{aligned}aHa^{-1}H &= aa^{-1}H \quad \textit{Lemma } 8.1.2 \\ &= 1H = H = 1_{G/H}\end{aligned}$$

Similarly, $a^{-1}HaH = H = 1_{G/H}$. So $(aH)^{-1} = a^{-1}H$.

Identity: Identity in $G/HisH$.

$$\begin{aligned}aHH &= aH \\ HaH &= aH\end{aligned}$$

Therefore G/H is a group under set multiplication.

$$\begin{aligned}\pi(ab) &= abH = aHbH \quad \textit{Lemma } 8.1.2 \\ &= \pi(a)\pi(b)\end{aligned}$$

π surjective: Let $aH \in G/H$.

$$aH = \pi(a) \tag{9.1}$$

Remark
$\ker(\pi) = H$

Proof

$$\begin{aligned} \pi(a) = 1_{G/H} &\iff aH = H \\ &\iff a \in H \quad \textit{Proposition 7.1.1(1)} \end{aligned}$$

Chapter 10

Lecture 10: Sep 29, 2017

10.1 Continuing with Normal Subgroups

Note
$H \lhd G$ then G/H is a group under the set and

$$\begin{aligned} \pi : G &\to G/H \quad \textit{surjective} \\ a &\mapsto aH \end{aligned}$$

group homomorphism $\ker(\pi) = H$. *The function collapses each coset such that they become a single point, G/H.*

Example 10.1.1
1.

$$\langle 1 \rangle = \{1\} \lhd G$$
$$a 1 a^{-1} = 1 \quad \textit{for any } a \in G$$
$$\pi : G \to G/\langle a \rangle \quad \textit{quotient map}$$

π is an isomorphism:

$$\begin{aligned} \pi(a) = \pi(b) &\iff a\langle a \rangle = b\langle 1 \rangle \\ &\iff a = b \end{aligned}$$

2. *$H = G \lhd G$ since for any $a \in G$, $aGa^{-1} \subseteq G$*

$$\pi : G \to G/G$$

where G/G is the trivial group. For any $a, b \in G$, $b^{-1}a \in G \implies aG = bG$. In fact, $aG = G$.

3. *If G is abelian, every subgroup H of G is normal, i.e. $H \triangleleft G$, since*

$$\forall a \in H\ h \in H\ aha^{-1} = aa^{-1}h = h \in H$$
$$\therefore aHa^{-1} \subseteq H$$

Example: $G = (\mathbb{Z}, +) \quad H = d\mathbb{Z} \quad d \geq 0$

$$\mathbb{Z}/d\mathbb{Z} \quad \begin{matrix} d{=}0 \text{ in case (1)} \\ d{=}1 \text{ in case (2)} \\ d{>}1\ \mathbb{Z}/d\mathbb{Z} \text{ group of congruence classes modulo } d \end{matrix}$$
$$\mathbb{Z}/d\mathbb{Z} = \{[0]_d, ..., [d-1]_d\} \simeq \mathbb{Z}_d = \{0, 1, ..., d-1\}$$

4. *$\phi : G \to H$ is a group homomorphism then $\ker(\phi) \triangleleft G$.*

Proof
Let $a \in G$ and $b \in \ker(\phi)$

$$\begin{aligned} \phi(aba^{-1}) &= \phi(a)\phi(b)\phi(a)^{-1} \\ &= \phi(a)\phi(a)^{-1} \quad b \in \ker(\phi) \\ &= 1_H \quad \therefore aba^{-1} \in \ker(\phi) \end{aligned}$$

Thus we observe that $a\ker(\phi)a^{-1} \subseteq \ker(\phi)$. Therefore, $\ker(\phi) \triangleleft G$.

Note
When $n \geq 3$ is even, $Z(D_{2n}) = \{1, r^{\frac{n}{2}}\}$.

5. *$G = D_{10}$ = group of rigid transformations of a regular pentagon ($n = 5$, so $2n = 10$). Note that it's not an abelian group. This is also called a dihedral group of order 10 (recall).*

Note: $s \in D_{10}$ reflection. $\text{order}(s) = 2$.

$$\langle s \rangle = \{1, s\} \leq D_{10} \ntriangleleft D_{10}$$

Let $r = \frac{2\pi}{5}$ clockwise rotation.

$$\begin{aligned} rsr^{-1} &= rrs \\ &= r^2 s \neq 1 \\ &\neq s \end{aligned}$$

since every element in D_{10} *can be uniquely expressed as* $r^i s^k$ *for* $i = 0, 1, 2, 3, 4$ *and* $k = 0, 1$.

Note that

$$\begin{aligned} 1 &= r^0 s^0 \\ s &= r^0 s^1 \end{aligned}$$

So

$$\begin{aligned} r^2 s &\neq 1 \\ &\neq s \end{aligned}$$

$\therefore \langle s \rangle \ntriangleleft D_{10}$

On the other hand

$$\langle r \rangle = \{1, r, r^2, r^3, r^4\} \triangleleft D_{10}$$

since $\text{order}(r) = 5$.

Proof
Let $a \in D_{10}$ $a = r^i s^k$ *where* $i = 0, 1, ..., 4$ *and* $k = 0, 1$. *Let* $l = 0, ..., 4$.

$$\begin{aligned} ar^l a^{-1} &= r^i s^k r^l s^{-k} r^{-i} \\ (\textit{if } h = 0) \quad ar^l &= r^i r^l r^{-i} \\ &= r^{i-l-i} = r^l \in \langle r \rangle \\ (\textit{if } k = 1) \quad ar^{-l} a^{-1} &= r^i s r^l s^{-1} r^{-i} \\ &= r^i r^{-l} s s^{-1} r^{-i} \quad \textit{by A1Q1(b)} \\ &= r^i r^{-l} r^{-i} = r^{-l} \in \langle r \rangle \end{aligned}$$

Therefore,

$$\begin{aligned} ar^l a^{-1} \in \langle r \rangle \quad \therefore\ a \langle r \rangle a^{-1} &\leq \langle r \rangle \quad \textit{any } a \in D_{10} \\ \langle r \rangle &\triangleleft D_{10} \end{aligned}$$

$$\pi : D_{10} \to D_{10}/\langle r \rangle \quad \textit{quotient map}$$

What is $D_{10}/\langle r \rangle$*?*

$|D_{10}| = 10,\ |\langle r\rangle| = 5$ *by (12) Lagrange's Theorem 7.1.3*

There are exactly two cosets:

$$\langle r\rangle = \{1, r, r^2, r^3, r^4\}$$
$$s\langle r\rangle = \{s, sr, sr^2, sr^3, sr^4\}$$

It is clear that these two are disjoint.

So $D_{10}/\langle r\rangle$ *is a group of size (or order) 2. Up to isomorphism, there is only 1 group with two elements.*

$$G = \{1, a\}\ a \neq 1 \quad \textit{Cayley Group}$$

G	*1*	*a*
1	*1*	*a*
a	*a*	*1 (1)*

(1) :

$$a^2 - 1 \textit{ or } a$$
$$a^2 = a \implies a = 1$$
$$\textit{so } a^2 = 1$$

Chapter 11

Lecture 11: Oct 2, 2017

11.1 Continuing with Normal Subgroups

Example 11.1.1

6. $G = \mathbb{C}^\times$ mutiplicative group of complex numbers.

$$S := \{z \in \mathbb{C}^\times : |z| = 1\} \tag{11.1}$$

So $S \leq \mathbb{C}^\times$ (Note circle S is closed in multiplication)

Since $\mathbb{C}^\times$ is abelian, thus $S \triangleleft \mathbb{C}^\times$.

What is $\mathbb{C}^\times/S$? $\mathbb{C}^\times/S \simeq (\mathbb{R}^{>0}, \cdot)$

$$\pi : \mathbb{C}^\times \to \mathbb{C}^\times/S \tag{11.2}$$

A typical element of $\mathbb{C}^\times/S$ is a left coset $wS, w \in \mathbb{C}^\times$:

$$ws = \textit{circle of radius } |w| \tag{11.3}$$

Proof: $w \in S, |wz| = |w||z| = |w|$.

$$|0| = |w| \implies u = w \cdot \frac{u}{w}, \left|\frac{u}{w}\right| = \frac{|u|}{|w|} = 1$$

$\therefore \frac{u}{w} \in S$

So $\mathbb{C}^\times/S$ = set of all circles in the complex plane centered at the origin.

$$uS \cdot wS = uwS = \text{ circle of radius } |uw| = |u||w|$$

In $\mathbb{C}^\times/S$, we multiply circles by multiplying radii.

11.2 Quotient Maps

Definition 11.2.1 (Fibre)
Given $H \triangleleft G$, $\pi : G \to G/H$ quotient map. Given an element $aH \in G/H$, the fibre (the pullback) $\pi^{-1}(\underbrace{aH}_{\in G/H}) = aH \subseteq G$.

Remark
Why $\pi^{-1}(\underbrace{aH}_{\in G/H}) = aH \subseteq G$?

$\forall b \in G, \pi((b) = aH \iff bH = aH \iff a^{-1}b \in H \iff a^{-1}b = h$ *for some* $h \in H \iff b = ah$ *for some* $h \in H \iff b \in aH$.

Remark
$aH = bH \iff a^{-1}b \in H \iff a \in bH \iff b \in aH$

Since $H = \ker(\pi)$, the fibres of π are all left cosets of the kernel (true for any group homomorphism).

Proposition 11.2.1 (Proposition 17)
Let $\phi : G \to H$ be a group homomorphism. Let $K = \ker(\phi) \triangleleft G$. The nonempty fibres of ϕ are the left cosets of K.

Proof
$h \in I_m(\phi) \leq H$. *Fix* $a \in \phi^{-1}(h) := \{g \in G : \phi(g) = a\}$.

Claim: $\phi^{-1}(h) = aK$. *Let* $b \in G$, *then*

$$\begin{aligned} b \in \phi^{-1}(h) &\iff \phi(b) = h \\ &\iff \phi(b) = \phi(a) \\ &\iff \phi(a)^{-1}\phi(b) = 1_H \\ &\iff \phi(a^{-1}b) = 1_H \\ &\iff a^{-1}b \in K \\ &\iff b \in aK \end{aligned}$$

Conversely, let aK be a left coset.

$$\begin{aligned} b \in aK &\implies b = ak \text{ for some } k \in K \\ &\implies \phi(b) = \phi(a)\phi(k) = \phi(a) \text{ since } k \in K = \ker(\phi) \\ &\implies b \in \phi^{-1}(\phi(a)) \\ &\therefore aK \subseteq \phi^{-1}(\phi(a)) = bK \end{aligned}$$

By the previous part, $\phi^{-1}(\phi(a)) = bK$ for some $b \in G \implies aK = bK = \phi^{-1}(\phi(a))$.

Corollary 11.2.1 (Corollary 18)
A group homomorphism $\phi : G \to H$ is injective iff $\ker(\phi) = \langle a \rangle$

Proof
By Proposition 11.2.1 the nonempty fibres of ϕ are cosets $a\ker(\phi)$. ϕ is injective iff the nonempty fibres are singletons. Since $\ker(\phi) \to a\ker(\phi)$ which $x \mapsto ax$ is an injection, we get that

$$\begin{aligned} a\ker(\phi) \text{ is a singleton} &\iff \ker(\phi) \text{ is a singleton} \\ &\iff \ker(\phi) = \langle 1 \rangle \end{aligned}$$

Remark
Proposition 11.2.1 and Corollary 18 11.2.1 are about group homomorphisms.

Given $\phi : G \to H$ as a group homomorphism, then we know that $\ker(\phi) \lhd G$. Consider $\pi : G \to G/\ker(\phi)$ as the quotient homomorphism. $\ker(\pi) = \ker(\phi)$

Definition 11.2.2 (Universal)
Suppose $N \lhd G$. If $\phi : G \to H$ is any group homomorphism with $\ker(\phi) \geq N$, then $\exists!$ group homomorphism $\bar{\phi} : G/N \to H$ such that

$$G \xrightarrow{\phi} H \quad G \xrightarrow{\pi} G/N \quad G/N \xrightarrow{\bar{\phi}} H \tag{11.4}$$

This means for any $a \in G$,

$$\bar{\phi}\pi(a) = \phi(a) \tag{11.5}$$

*We say $\bar{\phi}$ is **induced** by ϕ*

Theorem 11.2.1 ((19) Universal Property of Quotients)
Suppose $N \lhd G$. Then $\pi : G \to G/N$, the quotient map, is universal with respect to all group homomorphisms on G whose kernel contains in N.

Proof

Define $\bar{\phi} : G/N \to H$ *by, for any* $a \in G$,

$$\bar{\phi}(aN) = \phi(a) \tag{11.6}$$

$\bar{\phi}$ *is well defined: Suppose* $aN = bN$.

$$\begin{aligned}
&\implies b^{-1}a \in N \leq \ker(\phi) \\
&\implies \phi(b^{-1}a) = 1_H \\
&\implies \phi(b^{-1})\phi(a) = 1_H \\
&\implies \phi(a) = \phi(b)
\end{aligned}$$

$\bar{\phi}$ *is a homomorphism:*

$$\begin{aligned}
\bar{\phi}((aN)(bN)) &= \bar{\phi}(abN) \\
&= \phi(ab) = \phi(a)\phi(b) \\
&= \bar{\phi}(aN)\bar{\phi}(bN)
\end{aligned}$$

Commuting diagram: For $a \in G$

$$\bar{\phi}(\pi(a)) = \bar{\phi}(aN) = \phi(a) \tag{11.7}$$

Uniqueness of $\bar{\phi} : G \to H$ *as a homomorphism: (exercise)*

Chapter 12

Lecture 12: Oct 4, 2017