PMATH 347 Notes

Groups and Rings

Spring 2023

Based on Professor David McKinnon's Lectures

Contents

Lecture 1, 2023/05/08

1 Groups and Subgroups

Before we talk about the formal definition, informally speaking, a **group** is just a bunch of things we can multiply and divide (add and subtract) in a sensible way.

Example 1.1. The real numbers $\mathbb{R}$ is a group under addition and multiplication.

Example 1.2. The nonzero real numbers $\mathbb{R}^*$ is a group under multiplication and division.

Example 1.3. Let $n \geq 1$, define:

$$\mathrm{GL}_n(\mathbb{R}) = \{n \times n \text{ invertible matrices in } \mathbb{R}\}$$

This is a group under multiplication.

Example 1.4. The set $\{z \in \mathbb{C} : |z| = 1\}$ is a group under multiplication.

Example 1.5. Let $n \geq 1$ and define:

$$S_n = \{f : \{1, \cdots, n\} \to \{1, \cdots, n\} \mid f \text{ is bijective}\}$$

Then S_n is a group under function composition.

But what exactly do we mean by "in a sensible way"? This leads to the following definition.

Definition. A **group** is an ordered pair $(G, \cdot)$ where G is a set and $\cdot$ is a function $\cdot : G \times G \to G$ satisfying the following properties:

(1) If $a, b, c \in G$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(2) There exists $e \in G$ such that for all $a \in G$ we have $e \cdot a = a \cdot e = a$. (We usually just denote $e = 1$).

(3) If $a \in G$, there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = e$.

Definition. A **subgroup** of a group $(G, \cdot)$ is a group $(H, \cdot)$ where $H \subseteq G$ is a subset.

Example 1.6. Let $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, then $\{z \in \mathbb{C} : |z| = 1\}$ is a subgroup of $\mathbb{C}^*$ under multiplication.

Example 1.7. For $n \geq 1$, define:

$$\mathrm{SL}_n(\mathbb{R}) = \{n \times n \text{ matrices in } \mathbb{R} \text{ with determinant } 1\}$$

Then $\mathrm{SL}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$ under multiplication, because:

$$\det(AB) = \det(A)\det(B) = 1$$

given $A, B \in \mathrm{SL}_n(\mathbb{R})$ and $I_n \in \mathrm{SL}_n(\mathbb{R})$.

Theorem 1.8 (Subgroup Theorem). Let G be a group and $H \subseteq G$ be a nonempty subset of G. Then H is a subgroup of G if and only if:

(1) For all $a, b \in H$ we have $a \cdot b \in H$.

(2) For all $a \in H$ we have $a^{-1} \in H$.

Proof. ($\Rightarrow$). This is trivial.

($\Leftarrow$). We want to show H is a subgroup of G. First, $ab \in H$ for $a, b \in H$ implies the multiplication:

$$\cdot : H \times H \to H$$

is well-defined. We need to prove (1),(2),(3) as in the definition. (1) is trivial because the operation comes from the group G. To show $e \in H$, we pick $a \in H$, then since $a^{-1} \in H$ we have $e = aa^{-1} \in H$. And (3) is also trivial. $\square$

Lecture 2, 2023/05/10

Let us look at these two subgroups of $\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$.

Example 1.9. Recall that:

$$\mathrm{SL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) = 1\}$$

This is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Example 1.10. Define the set:

$$\mathrm{SO}_n(\mathbb{R}) = \{A \in \mathbb{M}_n(\mathbb{R}) : \|u - v\| = \|Au - Av\| \text{ for all } u, v \in \mathbb{R}^n\}$$

This is the set of matrices in $\mathbb{M}_n(\mathbb{R})$ that preserves distance. It turns out this is a subgroup of $\mathrm{GL}_n(\mathbb{R})$ under multiplication.

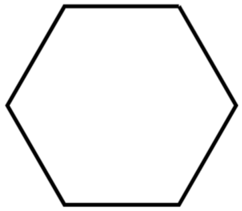
Remark. The above two subgroups tells us that, if a subset S of a group G is defined by "all elements in G that do not change something", then S is probably a subgroup. Using the second example, if A and B both preserves distance, then AB also preserves distance.

Example 1.11. Is $\mathbb{Z}_7$ (Integer modulo 7) a subgroup of $\mathbb{Z}$? NO! Because it is not even a subset of $\mathbb{Z}$! Elements in $\mathbb{Z}_7$ are not integers, they are residue classes.

Let us consider a hexagon (6-gon) H in $\mathbb{R}^2$, where the rightmost vertex is $(1, 0)$. Define the set:

$$D_6 = \{2 \times 2 \text{ invertible martices that map } H \to H\}$$

This is the set of functions that map H to itself. Which matrices are in D_6?



Say $M \in D_6$, then $M(0,1)^T$ is another vertex in H. Let Mv be some vertex next to $M(0,1)^T$, then there are 6 choices for $M(0,1)^T$ and 2 choices for Mv. Therefore D_6 has at most 12 elements. In fact, D_6 consists of 6 rotations and 6 reflections. In general, we have the following definition:

Definition. For $n \in \mathbb{N}$, we define:

$$D_n = \{A \in \mathrm{GL}_n(\mathbb{R}) : A \text{ maps } H \text{ to } H\}$$

where H is the regular n-gon in $\mathbb{R}^2$. This is called the **dihedral group of a regular n-gon**.

Let us now consider another very important group.

Definition. For $n \in \mathbb{N}$, define S_n to be the **symmetric group on n elements**, defined by:

$$\begin{aligned} S_n &= \{\text{bijections } f : \{1, \cdots, n\} \to \{1, \cdots, n\}\} \\ &= \{\text{permutations of } \{1, \cdots, n\}\} \end{aligned}$$

Example 1.12. Consider the following bijection from $\{1, 2, 3, 4, 5\}$ to itself.

n	1	2	3	4	5
$f(n)$	2	5	3	1	4

We use the notaiton (1254)(3) to denote this permutation. Why? We read the (1254) first. This means 1 maps to 2, 2 maps to 5, 5 maps to 4 and 4 maps to 1. And the (3) means 3 maps to 3 itself.

This is called the **disjoint cycle notation** for a permutation $\sigma \in S_n$. We denote the identity permutation as (1). In general, we can construct the disjoint cycle notation of $\sigma \in S_n$ this way:

(1) First, we write down a cycle:

$$(1, \sigma(1), \sigma(\sigma(1)), \cdots)$$

We keep iterating σ until it gets back to 1.

(2) If there are any elements of $\{1, \cdots, n\}$ that are left, start over at step (1) with the smallest element of them.

(3) Keep going until we are done.

Definition. The **order** of an element $g \in G$ is the smallest positive integer n satisfying $g^n = 1$. If there is no such integer, we say g has infinite order.

Definition. The **order** of a group G is just the cardinality of G.

Example 1.13. The group S_n has order $n!$ and D_6 has order 12.

Example 1.14. Say $\sigma \in S_n$ has the disjoint cycle notaiton $\sigma = \tau_1 \cdots \tau_\ell$ where τ_i are cycles. Then the order of σ is the lcm of the length of these cycles.

Example 1.15. Define the **Quaternion group** Q_8 to be:

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \right\}$$

under multiplication.

Lecture 3, 2023/05/12

Definition. We say a group G is **abelian** if for all $a, b \in G$ we have $ab = ba$.

Definition. The **direct product** of groups G, H is the group:

$$G \times H = \{(g, h) : g \in G, \ h \in H\}$$

and the multiplication is defined by $(g, h) \cdot (g', h') = (gg', hh')$.

2 Group Homomorphisms

Definition. Let G and H be groups. A **homomorphism** from G to H is a function $f : G \to H$ satisfying $f(ab) = f(a)f(b)$ for all $a, b \in G$.

Note that $f(1_G) = 1_H$ because:

$$H \ni f(1_G) = f(1_G \cdot 1_G) = f(1_G)f(1_G) \in H$$

thus $f(1_G) = 1_H$.

Definition. A group **isomorphism** from G to H is a homomorphism $f : G \to H$ with an inverse homomorphism $f^{-1} : H \to G$. We say groups G, H are **isomorphic** if there exists an isomorphism $f : G \to H$. In this case we write $G \cong H$.

Remark. An isomorphism is NOT defined to be a bijective homomorphism. There are some bijective homomorphism whose inverse is not a homomorphism. But in the case of groups, they are the same.

Theorem 2.1. A homomorphism $f : G \to H$ is an isomorphism if and only if it is bijective.

Proof. ($\Rightarrow$). This is trivial.

($\Leftarrow$). Let $f : G \to H$ be a bijectitve homomorphism, since f is bijective, it has an inverse $f^{-1} : H \to g$. We want to show f^{-1} is a homomorphism. Let $a, b \in H$, we want to show $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$. It is enough to show $f(f^{-1}(ab)) = f(f^{-1}(a)f^{-1}(b))$ since f is injective. Indeed:

$$f(\underbrace{f^{-1}(a)}_{\in G}\underbrace{f^{-1}(b)}_{\in G}) = f(f^{-1}(a))f(f^{-1}(b)) = ab$$

and clearly $f(f^{-1}(ab)) = ab$, we are done the proof. $\square$

Example 2.2. The map $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ given by the determinant is a homomorphism because:

$$\det(AB) = \det(A)\det(B)$$

by linear algebra. But this is NOT an isomorphism since it is not injective.

Example 2.3. Let $q : \mathbb{Z} \to \mathbb{Z}_7$ by $q(n) = [n]$. Recall that $[n]$ denotes the congruence class:

$$[n] = \{n + 7k : k \in \mathbb{Z}\}$$

Here $\mathbb{Z}$ and $\mathbb{Z}_7$ are groups under addition. Then $q(n + m) = q(n) + q(m)$, so q is a homomorphism. But this is NOT an isomorphism since $q(0) = q(7)$.

Example 2.4. Let $i : S_n \to S_{n+1}$ be defined in the following way. Given $\sigma \in S_n$, define:

$$i(\sigma) \in S_{n+1} \quad \text{by} \quad i(\sigma)(k) = \begin{cases} n+1 & \text{if } k = n+1 \\ \sigma(k) & \text{if } k \in \{1, \cdots, n\} \end{cases}$$

This is a injective homomorphism but NOT an isomorphism.

Example 2.5. The map $\log : \mathbb{R}^+ \to \mathbb{R}$ is a homomorphism. Here R^+ is a group under multiplication and $\mathbb{R}$ is a group under addition. This is just because $\log(xy) = \log x + \log y$. This is clearly bijective, so it is an isomorphism.

Example 2.6. Let $f : G \to G$ by $f(a) = 1$. This is clealry a homomorphism and it is called the **trivial homomorphism** from G to G.

Lecture 4, 2023/05/15

3 Group Actions

Definition. An **action** of a group G on a set S is a homomorphism $\phi : G \to \mathrm{Sym}(S)$, where:

$$\mathrm{Sym}(S) = \{f : S \to S \mid f \text{ is bijective}\}$$

This is basically turning every element in G into a bijection from S to itself.

Example 3.1. The map $\phi : \mathrm{GL}_n(\mathbb{R}) \to \mathrm{Sym}(\mathbb{R}^n)$ defined by:

$$\phi(A) : \mathbb{R}^n \to \mathbb{R}^n \text{ by } \phi(A)(v) = Av$$

This is an action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathbb{R}^n$.

Example 3.2. The map $\phi : \mathrm{GL}_n(\mathbb{R}) \to \mathrm{Sym}(\mathbb{R}^n)$ defined by:

$$\phi(A) : \mathbb{R}^n \to \mathbb{R}^n \text{ by } \phi(A)(v) = (\det A)v$$

This is an action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathbb{R}^n$ as well.

Example 3.3. The map $\phi : S_n \to S_n$ by $\phi(\sigma) = \sigma$ defines an action of S_n on $\{1, \cdots, n\}$.

Example 3.4. The map $\phi : G \to \mathrm{Sym}(S)$ by $\phi(g) = \mathrm{id}$. This is the trivial action of G on S.

Example 3.5. Let S be the regular n-gon. The map $\phi : D_n \to \mathrm{Sym}(S)$ by $\phi(\sigma) = \sigma$ is an action of D_n on the regular n-pgon.

Definition. We say an action $\phi : G \to \mathrm{Sym}(S)$ is **free** if:

$$\phi(g)(x) = x \text{ for some } x \in S \implies g = 1$$

This is saying that, for every non-trivial g, we must have that $\phi(g)$ does not fix anything!

Definition. We say an action $\phi : G \to \mathrm{Sym}(S)$ is **faithful** if:

$$\phi(g)(x) = x \text{ for all } x \in S \implies g = 1$$

This means ϕ is injecitve. This says that if g and h acts on the S in the same way, then $g = h$.

Definition. We say an action $\phi : G \to \mathrm{Sym}(S)$ is **transitive** if for every $x, y \in S$, there exists $g \in G$ such that $\phi(g)(x) = y$.

Remark. Note that by definition, ϕ is free $\implies$ ϕ is faithful.

Example 3.6. The action in Example 1.22 is faithful. If $\phi(A) = \phi(B)$, then $Av = Bv$ for all v, which implies $A = B$ and it follows that ϕ is injective. This is not necessarily free. Some non-identity matrix A has eigenvalue 1, then $\phi(A)(x) = Ax = x$ for some $x \neq 0$ but $A \neq I_n$. This is also not transitive. If $v_1 \neq 0$ and $v_2 = 0$, then $Av_1 \neq 0$ for any A as A is invertible.

Example 3.7. The action in Example 1.23 is not even faithful. Note that:

$$\det \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = 1 = \det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

This means ϕ is not injective. So ϕ is not faithful, hence not free. This is also not transitive. If v, w are not multiples of each other, then $(\det A)v \neq w$ for any A.

Notation. Note that if $\phi : G \to \mathrm{Sym}(S)$ is an action on S and $x \in S$. We may write:

$$g \cdot x = gx = \phi(g)(x)$$

if the action ϕ is clear from the context.

Definition. Let $\phi : G \to \mathrm{Sym}(S)$ be an action and let $x \in S$ be an element. The **Orbit** of x is:

$$\mathcal{O}_x = \{gx : g \in G\} \subseteq S$$

Note that if $x \in \mathcal{O}_y$, then $gy = x$ so that $y = g^{-1}x$ and $y \in \mathcal{O}_x$. Since $x \in \mathcal{O}_x$ for all $x \in S$, we can see that orbits $\{\mathcal{O}_x : x \in S\}$ partitions S.

Definition. Let $x \in S$. The **Stabilizer** of x is:

$$\mathrm{Stab}(x) = \{g \in G : gx = x\}$$

Example 3.8. For $G = S = \mathrm{GL}_n(\mathbb{R})$, then:

$$\begin{aligned} \mathrm{Stab}(x) &= \{A \in \mathrm{GL}_n(\mathbb{R}) : Ax = x\} \\ &= \{A \in \mathrm{GL}_n(\mathbb{R}) : A \text{ has eigenvalue } 1 \text{ and } x \text{ is an eigenvector}\} \end{aligned}$$

Lecture 5, 2023/05/17

4 Cayley's Theorem

Example 4.1. Let G be a group, then G acts on itself by left multiplication. That is:

$$\phi : G \to \mathrm{Sym}(G) \;\text{ by }\; g \cdot x = gx$$

Here gx literally means g multiplied by x in the group G. This is indeed an action. Note:

(a) This action is free. We have:

$$gx = x \iff gxx^{-1} = xx^{-1} \iff g = 1$$

(b) This is transitive. For any $x, y \in G$ we have $y = (yx^{-1})x$. Hence:

$$\phi(yx^{-1})(x) = yx^{-1}x = y$$

(c) For any $x \in G$ we have $\text{Stab}(x) = 1$ and $\mathcal{O}_x = G$.

Example 4.2. Say G is a finite group, then we can enumerate the elements of G by:

$$G = \{x_1, \cdots, x_n\}$$

Therefore we have:

$$\text{Sym}(G) \cong \text{Sym}(\{1, \cdots, n\}) \cong S_n$$

This action in Example 1.30 is free, thus faithful. It means this action defines gives an injective homomorphism $G \to S_n$. The image of G under a homomorphism is a subgroup of S_n (Exercise!). It follows that G is isomorphic to a subgroup of S_n. In particular, every finite group G is isomorphic to a subgroup of S_n, wehre $n = |G|$. This is the famous **Cayley's Theorem**.

Theorem 4.3 (Cayley). Every finite group G is isomorphic to a subgroup of S_n, where $n = |G|$.

Example 4.4. Let G be a group and $\phi : G \to \text{Sym}(G)$ by:

$$\phi(g)(x) = g \cdot x = gxg^{-1}$$

This is indeed an action and is called the **action by conjugation**. We say gxg^{-1} is the **conjugate** of x by g. Note that:

(a) If $G \neq \{1\}$, then we let $g = x \neq 1$. Hence:

$$g \cdot x = gxg^{-1} = xxx^{-1} = x$$

However $g \neq 1$, so the action is NOT free.

(b) This is sometimes faithful, sometimes not.

(c) This is NOT transitive.

$$g \cdot 1 = g(1)g^{-1} = 1$$

Hence 1 is fixed, so it cannot be sent to another element in G.

(d) For all $x \in G$, we have:

$$\text{Stab}(x) = \{g \in G : g \cdot x = gxg^{-1} = x\} = \{g \in G : xg = gx\}$$

This is called the **Centralizer** of x. And:

$$\mathcal{O}_x = \{gxg^{-1} : g \in G\}$$

is called the **Conjugacy class** of x.

Lecture 6, 2023/05/19

5 Cyclic Groups

Definition. Let G be a group and $g \in G$ be any element. The **subgroup generated by** x is:

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} = \{\cdots, g^{-2}, g^{-1}, 1, g, g^2, \cdots\}$$

Since $\langle g \rangle$ is closed under multiplication and inversion, so it is a subgroup.

Remark. Note that $\langle g \rangle$ is the smallest subgroup of G that contains g.

Definition. A **cyclic group** is a group G such that there exists $g \in G$ with $G = \langle g \rangle$.

Example 5.1. Let $G = \mathbb{Z}$ under addition. Let $g = 1$, then:

$$\langle g \rangle = \{\cdots, -2, -1, 0, 1, 2, \cdots\} = \mathbb{Z}$$

Therefore $\mathbb{Z}$ is a cyclic group.

Example 5.2. Let $G = \mathbb{Z}_n$ and $g = [1]$, then:

$$\langle g \rangle = \{[0], [1], [2] \cdots, [n-1]\} = \mathbb{Z}_n$$

Therefore $\mathbb{Z}_n$ is a cyclic group.

These are two examples of cyclic groups, it turns out that they are all cyclic groups!

Theorem 5.3. Let G be a group and $g \in G$ be any element. If g has infinite order, then $\langle g \rangle \cong \mathbb{Z}$. If g has finite order, then $\langle g \rangle \cong \mathbb{Z}_n$, where n is the order of g.

Proof. Define a homomorphism $\phi : \mathbb{Z} \to \langle g \rangle$ by $\phi(k) = g^k$. Then ϕ is clearly onto, as $g^k = \phi(k)$ for $k \in \mathbb{Z}$. If g has infinite order, then ϕ is injective:

$$\phi(n) = \phi(m) \iff g^n = g^m \iff g^{n-m} = 1 \iff n = m$$

This is because g has infinite order, so $g^{n-m} = 1$ implies $n - m = 0$. Hence ϕ is an isomorphism and $\mathbb{Z} \cong \langle g \rangle$. Now suppose g has order $n < \infty$, so $g^n = 1$. Define another homomorphism:

$$\tilde{\phi} : \mathbb{Z}_n \to \langle g \rangle \ \text{ by } \ \tilde{\phi}([k]) = g^k$$

Here $[k]$ denotes the congruence class in $\mathbb{Z}_n$. We claim that this is well-defined and injective!

$$\phi([k]) = \phi([\ell]) \iff g^k = g^\ell \iff g^{k-\ell} = 1 \iff n \mid (k - \ell) \iff [k] = [\ell]$$

This is a map between two finite sets. It is injecitve, so it must be surjective. Hence $\tilde{\phi}$ is an isomorphism and $\mathbb{Z}_n \cong \langle g \rangle$. $\square$

6 Lagrange's Theorem

Theorem 6.1 (Lagrange). Let G be a finite group and $H \subseteq G$ be a subgroup. Then $|G|$ is divisible by $|H|$.

Proof. Consider an action of H on G by left multiplication. That is:

$$\phi : H \to \mathrm{Sym}(G) \ \text{ by } \ h \cdot g = hg$$

The orbit of 1 is just all of H. The orbit of g is:

$$Hg := \mathcal{O}_g = \{hg : h \in H\}$$

and there is a bijection $H \to Hg$ by $h \mapsto hg$. Since G is a disjoint union of orbits, so:

$$G = \bigcup_{k=1}^{n} Hg_k$$

for some $g_1, \cdots, g_k \in G$. It means there are k orbits of this action. Each Hg_k has size $|H|$. Hence:

$$G = k \cdot |H|$$

It follows that $|G|$ is divisible by $|H|$. $\square$

Remark. We say Hg is a **right coset** of H in G and the number of right cosets (the number of orbits) is called the **index** of H in G and is written as $[G : H]$. If G is finite, then Lagrange's Theorem says that:

$$[G : H] = \frac{|G|}{|H|} = \text{number of orbits (right cosets) in } G$$

Corollary 6.2. Let G be a finite group and $x \in G$. Then $|G|$ is divisible by the order of x.

Proof. Apply Lagrange's Theorem to the subgroup $\langle x \rangle$. $\square$

Lecture 7, 2023/05/23

Definition. Let G be a group and $S \subseteq G$ a subset of G (not necessarily a subgroup). The **subgroup generated by** S is defined by:

$$\begin{aligned}\langle S \rangle &= \bigcap \{H \subseteq G : S \subseteq H \text{ and } H \text{ is a subgroup of } G\} \\ &= \{a_1^{n_1} \cdots a_r^{n_r} : a_i \in S,\ n_i \in \mathbb{Z},\ r \in \mathbb{N}\}\end{aligned}$$

This is the smallest subgroup of G that contains S.

Example 6.3. If $S = \{a, b\}$, then $\langle S \rangle = \{a^{n_1} b^{k_1} \cdots a^{n_r} b^{n_r} : n_i \in \mathbb{Z}\}$ and $\langle \emptyset \rangle = \{1\}$

Definition. The **kernel** of a group homomorphism $f : G \to H$ is:

$$\ker f = \{g \in H : f(g) = 1\}$$

Theorem 6.4. A group homomorphism $f : G \to H$ is injecitve if and only if $\ker f = \{1\}$.

Proof. $(\Rightarrow)$. Since $f(1) = 1$ and f is injecitve, so $\ker f = \{1\}$.

$(\Leftarrow)$. Assume $\ker f = \{1\}$. Let $a, b \in G$ with $f(a) = f(b)$. Then $f(ab^{-1}) = 1$ and thus $ab^{-1} \in \ker f = \{1\}$. Hence $ab^{-1} = 1$ and $a = b$. $\square$

Remark. Note that $\ker f$ is a subgroup of G. Also, if $a \in \ker f$ and $g \in G$, then:

$$f(gag^{-1}) = f(g)f(a)f(g)^{-1} = f(g)(1)f(g)^{-1} = 1$$

It means $gag^{-1} \in \ker f$. This means $\ker f$ is closed under conjugation.

7 Quotient Groups

Definition. Let $H, K \subseteq G$ be a subgroup. Then HK is the smallest subgroup containing both H and K. In fact we have $HK = \{hk : h \in H, k \in K\}$.

Definition. A subgroup $H \subseteq G$ is **normal** in G if for every $h \in H$ and $g \in G$, we have $ghg^{-1} \in H$. In other word, H is normal if $gHg^{-1} \subseteq H$.

Proposition 7.1. Let $f : G \to H$ be a group homomorphism, then $\ker f \subseteq G$ is normal in G.

Proof. By the above remark. $\square$

Example 7.2. $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$. If $A \in \mathrm{SL}_n(\mathbb{R})$ so $\det(A) = 1$. Let $P \in \mathrm{GL}_n(\mathbb{R})$, then we have:

$$\det(PAP^{-1}) = \det(P)\det(A)\det(P^{-1}) = \det(P)\det(P^{-1}) = 1$$

It follows that $PAP^{-1} \in \mathrm{SL}_n(\mathbb{R})$. We can prove it in a different way. The map $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ has kernel $\ker(\det) = \mathrm{SL}_n(\mathbb{R})$, therefore $\mathrm{SL}_n(\mathbb{R})$ is normal in $\mathrm{GL}_n(\mathbb{R})$.

Remark. If G is abelian, then every subgroup $H \subseteq G$ is normal in G. Indeed, if $g \in G$ and $h \in H$, we have $ghg^{-1} = gg^{-1}h = h \in H$. However, the converse is not true! Consider the Quaternion Q_8. Every subgroup is normal but Q_8 is NOT abelian.

Example 7.3. Let $G = D_n$, the symmetry of regular n-gon. Let H be the subgroup of all rotations. It is a normal subgroup, consider the homomorphism $\phi : D_n \to \mathbb{Z}_2$ by:

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is a rotation} \\ 1 & \text{if } \sigma \text{ is a reflection} \end{cases}$$

It can be proved that this is a homomorphism and $\ker\phi = \{\text{all rotations}\}$.

From the examples above, we saw that we can prove a subgroup is normal in G by proving it is the kernel of some homomorphism from G to another group. This is in fact always true!

Theorem 7.4. Let $H \subseteq G$ be a subgroup, then H is normal if and only if there is a group P and a homomorphism $g : G \to P$ such that $\ker\phi = H$.

Proof. ($\Leftarrow$). This is trivial.

Lecture 8, 2023/05/24

($\Rightarrow$). Say H is normal, we want to define a group P and a homomorphism $\phi : G \to P$ with $\ker\phi = H$. Let us think about how we could construct P. Once we get ϕ, it wil map $H \to \{1\} \subseteq P$. If $g \notin H$, then $\phi(g) \neq 1$ in P. If g_1, g_2 satisfies $\phi(g_1) = \phi(g_2)$, then:

$$\phi(g_2^{-1}g_1) = \phi(g_2^{-1})\phi(g_1) = \phi(g_2)^{-1}\phi(g_1) = 1 \implies g_2^{-1}g_1 \in H$$

It follwos that $g_1 \in g_2H$, the left coset of H. We define a group:

$$P = \{gH : g \in G\}$$

via the multiplication $(g_1H)(g_2H) = (g_1g_2)H$. Is this multiplication well-defined? That is:

$$g_1H = g_1'H \text{ and } g_2H = g_2'H \implies g_1g_2H = g_1'g_2'H$$

Lemma: If H is normal, then for all $g \in G$ we have $gH = Hg$.

Proof (Lemma): Let $g \in G$ and suppose $gh \in gH$ for some $h \in H$. We want to show $gh \in Hg$. Since H is normal, we have:

$$ghg^{-1} \in H \implies gh \in Hg$$

More explicity, write $ghg^{-1} = h' \in H$, then $gh = h'g \in Hg$. The other inclusion is similar, this proved the lemma. **(QED Lemma)**

Now assume $g_1H = g_1'H$ and $g_2H = g_2'H$, we have:

$$g_1g_2H = g_1g_2'H = g_1Hg_2' = g_1'Hg_2' = g_1'g_2'H$$

This proved that the group operation is well-defined. This makes P into a group with identity $1_P = H$ and the inverse of gH is $g^{-1}H$. Now define:

$$\phi : G \to P \text{ by } \phi(g) = gH$$

This is clearly a homomorphism and $gH = H \iff g \in H$, so $\ker\phi = H$, as desired! $\square$

Definition. Let G be a group and $H \subseteq G$ a normal subgroup. The **quotient group** of G by H is defined to be:

$$G/H = \{gH : g \in G\}$$

with multiplication $(g_1H)(g_2H) = (g_1g_2)H$. We proved in the above proof that this is a group.

Notation. If $g_1H = g_2H$ in G/H, we also write $g_1 \equiv g_2 \pmod H$. This is the same as the notation in number theory. We write $a \equiv b \pmod n$ when $n \mid (a - b) \iff a + n\mathbb{Z} = b + n\mathbb{Z}$.

Example 7.5. Consider $G = \mathbb{Z}$ and $N = 4\mathbb{Z} = \{4k : k \in \mathbb{Z}\}$. Then:

$$\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$$

We can send $i + 4\mathbb{Z}$ to $[i]$ in $\mathbb{Z}_4$ and it shows that $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$. In general, we have $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Notation. Let $\phi : G \to H$ and let $\operatorname{Im}\phi = \{\phi(g) : g \in G\}$ is the image of ϕ. It is easy to see that $\operatorname{Im}\phi$ is a subgroup of H.

Lecture 9, 2023/05/26

Theorem 7.6 (Universal Property of Quotients). Let G be a group and $N \subseteq G$ a normal subgroup of G. Let $f : G \to H$ be a group homomorphism. Let $q : G \to G/N$ be the projection map by $q(g) = gH$. Then there exists a homomorphism $\tilde{f} : G/N \to H$ satisfying $f = \tilde{f} \circ q$ if and only if $N \subseteq \ker f$. In this case, we have $\operatorname{Im} \tilde{f} = \operatorname{Im} f$ and $\ker \tilde{f} = q(\ker f)$.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "q"'] & H \\ G/N \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

Remark. Why is this theorem important? If we have a quotient group G/N and H and we want to find a homomorphism $G/N \to H$. However, if we define a map from $G/N \to H$ directly, it might not even be well-defined. For example, consider $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}$ by $f(x + 5\mathbb{Z}) = 3x$, then:

$$18 = f(6 + 5\mathbb{Z}) = f(1 + 5\mathbb{Z}) = 3$$

This means f is not a well-defined map. This happens because we defined our map f based on the "representative" g of an element $g+N \in G/N$. To avoid this, we will use a different way to construct a homomorphism $G/N \to H$.

(1) Let G, H be groups and let $N \subseteq G$ be a normal subgroup.

(2) Find a group homomorphism $f : G \to H$ such that $N \subseteq \ker f$.

(3) Applying UPQ, we get a map $\tilde{f} : G/N \to H$.

Let us see some examples of this idea.

Example 7.7. Consider $G = \mathrm{GL}_n(\mathbb{R})$ and $H = \mathbb{R}^*$. Consider the map $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$. Its kernel is exactly $\mathrm{SL}_n(\mathbb{R})$. Hence we get a homomorphism $\tilde{\det} : \mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \to \mathbb{R}^*$

$$\begin{tikzcd} \mathrm{GL}_n(\mathbb{R}) \arrow[r, "\det"] \arrow[d, "q"'] & \mathbb{R}^* \\ \mathrm{SL}_n(\mathbb{R}) \arrow[ur, dashed, "\tilde{\det}"'] & \end{tikzcd}$$

It satisfies that $\tilde{\det} \circ q = \det$ and $\operatorname{Im}(\tilde{\det}) = \operatorname{Im}(\det) = \mathbb{R}^*$, so $\tilde{\det}$ is surjective. Also:

$$\ker(\tilde{\det}) = q(\ker(\det)) = q(\mathrm{SL}_n(\mathbb{R})) = 0 + \mathrm{SL}_n(\mathbb{R})$$

Hence $\tilde{\det}$ has trivial kernel, so it is injecitve. Hence $\tilde{\det}$ is an isomorphism, which gives:

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$$

Example 7.8. Let $G = \mathbb{Z}^2$ and $N = \langle(1,2)\rangle$. What does G/N look like? We want to find a group H and a homomorphism $f : \mathbb{Z}^2 \to H$ such that $\langle(1,2)\rangle \subseteq H$. Let $H = \mathbb{Z}$ and define $f(a,b) = 2a - b$, then this is clearly a homomorphism. Also we have $N \subseteq \ker f$. By UPQ we get a homomorphism:

$$\tilde{f} : \mathbb{Z}^2/\langle(1,2)\rangle \to \mathbb{Z} \text{ by } \tilde{f}((a,b)+N) = 2a - b$$

Note that we exactly have $N = \ker f$, hence $\tilde{f}$ is injecitve. Also, for all $b \in \mathbb{Z}$ we have $f(0,-b) = b$. Hence f is onto, which implies $\tilde{f}$ is onto as well as $\operatorname{Im} f = \operatorname{Im} \tilde{f}$. Hence $\tilde{f}$ is an isomorphism and:

$$\mathbb{Z}^2/\langle(1,2)\rangle \cong \mathbb{Z}$$

Proof of Theorem 7.6 (UPQ). ($\Rightarrow$). We want to show $N \subseteq \ker f$. Indeed, if $n \in N$ then we have:

$$f(n) = \tilde{f}(q(n)) = \tilde{f}(1) = 1$$

It follows that $n \in \ker f$ and thus $N \subseteq \ker f$.

($\Leftarrow$). Now suppose $N \subseteq \ker f$, we define $\tilde{f} : G/N \to H$ by:

$$\tilde{f}(gN) = f(g)$$

We will show that $\tilde{f}$ is well-defined. Indeed, if $g_1N = g_2N$ then $g_1g_2^{-1} = n$ for some $n \in N$. Then:

$$\tilde{f}(g_1N) = f(g_1) = f(g_2n) = \tilde{f}(g_2nN) = \tilde{f}(g_2N)$$

Clearly $\tilde{f}$ is a homomorphism and $f = \tilde{f} \circ q$. The uniqueness and other two properties are easy to check as well. □

Lecture 10, 2023/05/29

Theorem 7.9 (First Isomorphism Theorem). Let $f : G \to H$ be a group homomorphism, then we have $G/\ker f \cong \operatorname{Im} f$.

Proof. We have a homomorphism $\tilde{f} : G/\ker f \to H$ by UPQ. The kernel of $\tilde{f}$ is exactly $q(\ker f) = 0 + \ker f$, which is the identity in $G/\ker f$. Hence $\tilde{f}$ is injecitve. If we restrict the codomain to $\operatorname{Im} f = \operatorname{Im} \tilde{f}$, this map is surjective. Hence $\tilde{f} : G/\ker f \to \operatorname{Im} f$ is an isomorphism. □

Corollary 7.10. Let $f : G \to H$ be a homomorphism and G is finite. Then $|\ker f| \cdot |\operatorname{Im} f| = |G|$.

Proof. This is clearly since $|G/\ker f| = |G|/|\ker f|$ by Lagrange's Theorem. Then apply FIT. □

8 Conjugacy Classes

Definition. Recall that every group G acts on itself by conjugation. (Example 4.4). Let $g \in G$ act on G by $g \cdot x = gxg^{-1}$. The orbits of g under this action is called the **conjugacy classes** of g.

Remark. Note that the map $x \mapsto gxg^{-1}$ is an isomorphism from G to G. Thus elements of the same conjugacy calss are "algebraically identical". This is analogous to similar matrices in linear algebra: two matrices are similar if they represent the same linear map in different bases.

Definition. Recall that the stabilizer of $x \in G$ under this action is called the **centralizer** of x, denoted by $\text{Cent}(x)$. We have:

$$g \in \text{Stab}(x) \iff g \cdot x = x \iff gxg^{-1}x \iff xg = gx$$

In other words, $\text{Stab}(x)$ consists of all elements of G that commute with x.

Definition. The **center** of a group G is the set:

$$Z(G) = \{z \in G : zg = gz \text{ for all } g \in G\} = \bigcap_{g \in G} \text{Cent}(g)$$

This is the subgroup of G consisting of elements that commute with every element in G!

Example 8.1. Conjugacy classes in $\text{GL}_n(\mathbb{R})$ is similarity.

Example 8.2. If G is abelian, then $gxg^{-1} = gg^{-1}x = x$ for all $x, g \in G$. Therefore conjugacy is trivial and every conjugacy class in G has one element.

Theorem 8.3 (Chinese Remainder Theorem). Let $m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$. Then:

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

given by the map $\phi(x + mn\mathbb{Z}) = (x + m\mathbb{Z}, x + n\mathbb{Z})$.

Proof. This is clearly a well-defined group homomorphism. To show it is bijectitve, it suffices to show it is injecitve since both $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ both have mn elements. Let $x + mn\mathbb{Z} \in \ker \phi$, then we have that:

$$x \equiv 0 \pmod{m}$$
$$x \equiv 0 \pmod{n}$$

By the usual Chinese Remainder Theorem (the version from MATH 135/145), we know $x \equiv 0 \pmod{mn}$. Hence this is an isomorphism. $\square$

Question: In general, when can we have $G \cong H \times K$? If $G \cong H \times K$, then subgroups of G would correspond to subgroups of $H \times K$.

Theorem 8.4. Let G be a group and M, N be normal subgroups of G satisfying:

(1) $N \cap M = \{1\}$.

(2) $nm = mn$ for all $m \in M$ and $n \in N$.

(3) For all $g \in G$, there exist $m \in M$ and $n \in N$ with $mn = g$.

Then we have $G \cong M \times N$ by $\phi : M \times N \to G$ with $\phi(m, n) = mn$.

Proof. We just need to check ϕ is an isomorphism. It is clearly a homomorphism:

$$\begin{aligned} \phi((m_1, n_1)(m_2, n_2)) &= \phi(m_1 m_2, n_1 n_2) = m_1 m_2 n_1 n_2 \\ &= m_1 n_1 m_2 n_2 && \text{(by (2))} \\ &= \phi(m_1, n_1)\phi(m_2, n_2) \end{aligned}$$

Note that if $\phi(m, n) = mn = 1$, then $m = n^{-1} \in M \cap N$. By (1), we know $m = n = 1$ and $(m, n) = (1, 1)$. It means $\ker \phi$ is trivial and ϕ is injective. Clearly ϕ is onto by (3). $\square$

Lecture 11, 2023/05/31

Example 8.5. Let $G = D_n$ and $H \subseteq D_n$ be the subgroup of rotations. Is there a subgroup $N \subseteq D_n$ such that $D_n \cong H \times N$? NO! Note that $|H| = n$, so if such H exists then $|N| = 2$. Now, note that H is abelian. Also N is abelian since $N \cong \mathbb{Z}/2\mathbb{Z}$. Hence $H \times N$ is abelian, which is impossible since D_n is not abelian.

Hölder's Program: If we understand N and G/N, can we understand G?

Sadly this is not that simple. Note that $D_n/H \cong \mathbb{Z}/2\mathbb{Z}$ but:

$$(H \times \mathbb{Z}/2\mathbb{Z})/(H \times \{1\}) \cong \mathbb{Z}/2\mathbb{Z}$$

Nevertheless, if a group G has a non-trivial normal subgroup N, then this idea has some merit: We can use N and G/N to understand G better.

Definition. A group G is **simple** if its only normal subgroups are $\{1\}$ and G.

Example 8.6. The group $\mathbb{Z}/p\mathbb{Z}$ is simple for all prime p.

9 Generators and Relations

Definition. Let S be a set. The **free group on** S is the set of equivalence classes of finite strings:

$$\{x_1 \cdots x_r : x_i = s \text{ or } s^{-1} \text{ for } s \in S,\ r \in \mathbb{N} \cup \{0\}\}/\sim$$

where the equivalence relation is the transitive closure of:

$$\begin{aligned} x_1 \cdots x_r &\sim x_1 \cdots x_n s s^{-1} x_{n+1} \cdots x_r \\ &\sim x_1 \cdots x_n s^{-1} s x_{n+1} \cdots x_r \end{aligned}$$

The group operation is concatenation. This group is denoted by F_S.

Example 9.1. If $S = \emptyset$ then $F_S = \{1\}$.

Example 9.2. If $S = \{a\}$ then $F_S \cong \mathbb{Z}$. This is because F_S is strings of a's or a^{-1}'s, Define a homomorphism $\phi : \mathbb{Z} \to F_S$ by:

$$\phi(n) = \begin{cases} \underbrace{a \cdots a}_{n \text{ times}} & \text{if } n \geq 0 \\ \underbrace{a^{-1} \cdots a^{-1}}_{-n \text{ times}} & \text{if } n < 0 \end{cases}$$

This is an isomorphism.

Example 9.3. If $S = \{a, b\}$, then F_S is huge! It has elements like $aba^{-1}b$, $abba^{-1}b^{-1}a^{-1}$. Now, suppose G is a group with $G = \langle g_1, g_2 \rangle$. Define $\phi : F_2 \to G$ by:

$$\phi(\text{string}) = \text{same string with} \begin{cases} a \mapsto g_1 \\ a^{-1} \mapsto g_1^{-1} \\ b \mapsto g_2 \\ b^{-1} \mapsto g_2^{-1} \end{cases}$$

For example, $\phi(abba^{-1}b^{-1}a) = g_1g_2g_2g_1^{-1}g_2^{-1}g_1$. This is clearly an onto homomorphism. The kernel of ϕ is called the relations satisfied by g_1, g_2.

Lecture 12, 2023/06/02

Theorem 9.4. Every group is the quotient of a free group.

Proof. Suppose $G = \langle S \rangle$, where $S \subseteq G$ is a subset. Define a homomorphism $\phi : F_S \to G$ by:

$$\phi(\text{string}) = \text{string as elements of } G$$

This is onto. Therefore by UPQ, we know ϕ induces an isomorphism $\tilde{\phi} : F_S / \ker \phi \to G$. $\square$

Definition. By this theorem, we may write $G = \langle S \mid R \rangle$, where R is a subset of F_S such that $\ker \phi$ is the smallest normal subgroup of F_S containing R. We call S the **generators** of G and R is called the **relations**.

Example 9.5. We claim that $D_n = \langle x, y \mid x^2, y^n, xyxy \rangle$. Let $G = \langle x, y \mid x^2, y^n, xyxy \rangle$, we want to find an isomorphism $G \to D_n$. There is a homomorphism $\phi : F_2 \to D_n$ by:

$$\begin{aligned} \phi(x) &= \text{ reflection } s \\ \phi(y) &= \text{ rotation } r \text{ by } \frac{2\pi}{n} \text{ radians} \end{aligned}$$

Then ϕ is onto. Note that $\phi(x^2) = s^2 = \text{id}$ and $\phi(y^n) = \text{rotation by } 2\pi = \text{id}$. Also note that $\phi(xyxy) = \text{id}$. Let N be the smallest normal subgroup containing $x^2, y^n, xyxy$. Hence $N \subseteq \ker\phi$ and UPQ gives a homomorphism $\tilde{\phi} : F_2/N \to D_n$ as follows:

$$\begin{tikzcd} F_2 \arrow[r, "\phi"] \arrow[d, "q"'] & D_n \\ F_2/N \arrow[ur, dashed, "\tilde{\phi}"'] & \end{tikzcd}$$

We know $\tilde{\phi}$ is onto as well, now we want to show it is injecitve. Since $|D_n| = 2n$, it suffices to show F_2/N has at most $2n$ elements (this implies $\tilde{\phi}$ is injecitve as well). An element of F_2/N is of the form mN where m is a string of x, y, x^{-1}, y^{-1}. First, $x^2 \equiv 1 \pmod N$ means that the string $m \pmod N$ need not have consecutive x's or x^{-1}'s. Similarly $y^n \equiv 1 \pmod N$ means m need not have string of n or more y's or y^{-1}'s. For example:

$$\underbrace{xx}_{\equiv 1} xyy \underbrace{y \cdots y}_{n \text{ terms}} \underbrace{x^{-1}x^{-1}}_{\equiv 1} y \equiv xyyx^{-1}x^{-1}y = xyyy \pmod N$$

Using the relation $xy = y^{-1}x$ we can see that $m \pmod N$ can start with a string of x's and end with a string of y's. Thus mod N, the string m can be written as either:

$$y^i \text{ for } i \in \{0, 1, \cdots, n-1\} \quad \text{or} \quad xy^i \text{ for } i \in \{0, 1, \cdots, n-1\}$$

Hence there mN has at most $n + n = 2n$ chocies, which means $|F_2/N| \leq 2n$. Hence $\tilde{\phi}$ is an isomorphism.

10 Alternating Groups

The group S_n acts on $\mathbb{R}^n$ by permutating coordinates. For example, $\sigma = (12)(45)$ acts on $\mathbb{R}^5$ by:

$$\sigma \cdot (a, b, c, d, e) = (b, a, c, e, d)$$

So we get a homomorphism $\phi : S_n \to \text{Sym}(\mathbb{R}^n)$. In fact this action defines a linear map, so we get a homomorphism $\phi : S_n \to \text{GL}_n(\mathbb{R})$. We can get a homomorphism $\sigma : S_n \to \mathbb{R}$ by:

$$\text{sgn}(\sigma) = \det \phi(\sigma)$$

Clearly $\text{sgn}(\sigma) \in \{1, -1\}$. Why? We know that for a square matrix A, swapping two rows changes the determinant by ± 1. Well, $\phi(\sigma)$ is the matrix after permutating the rows of I_n, which must have determinant ± 1. It is not always 1 and not always -1. For example $\sigma = (12) \in S_n$, then:

$$\operatorname{sgn}(\sigma) = \det \left(\begin{array}{cc|c} 0 & 1 & \\ 1 & 0 & O \\ \hline \multicolumn{2}{c|}{O} & I_{n-2} \end{array} \right) = -1$$

Therefore $\operatorname{sgn} : S_n \to \{\pm 1\}$ is a surjective homomorphism whose kernel has $n!/2$ elements.

Definition. The subgroup $\ker \operatorname{sgn} \subseteq S_n$ is called A_n, the **alternating group** on n letters. This means A_n is a normal subgroup of S_n. Elements of A_n are called **even permutations** and other elements of S_n are called **odd permutations**.

Example 10.1. The identity (1) is even and every 2-cycle is odd.

Lemma 10.2. Every m-cycle in S_n can be written as a product of 2-cycles.

Proof. Let $\sigma = (a_1 \cdots a_m)$ be an m-cycle. Then:

$$(a_1 \cdots a_m) = (a_m a_{m-1})(a_{m-1} a_{m-2}) \cdots (a_2 a_1)$$

The number of 2-cycles is $(m-1)$. □

Remark. By this lemma, we see that every odd cycle is an even permutation and every even cycle is an odd permutation. This is because:

$$\operatorname{sgn}(a_1, \cdots, a_m) = \operatorname{sgn}(a_m a_{m-1}) \cdots \operatorname{sgn}(a_2 a_1) = (-1)^{m-1} = \begin{cases} 1 & \text{if } m \text{ is odd} \\ -1 & \text{if } m \text{ is even} \end{cases}$$

Remark. This lemma also says that 2-cycles generate S_n. This is because every permutation admits a disjoint cycle representation and each cycle is a product of 2-cycles. Hence any subgroup of S_n containing all of the 2-cycles is S_n.

Lecture 13, 2023/06/05

11 Orbit-Stabilizer and Class Equation

Theorem 11.1 (Orbit-Stabilizer). Let G be a finite group acting on a set X. Let $x \in X$, then:

$$|\mathcal{O}_x| \cdot |\operatorname{Stab}(x)| = |G|$$

where $\mathcal{O}_x$ denotes the orbit of x and $\operatorname{Stab}(x)$ is the stabilizer of x under this action.

Proof. By definition, we have a homomorphism $\phi : G \to \mathrm{Sym}(X)$. There is a function $\psi : G \to \mathcal{O}_x$ by $g \mapsto g \cdot x$. Using this ψ we the equality:

$$|G| = |\psi^{-1}(\mathcal{O}_x)| = \sum_{y \in \mathcal{O}_x} |\psi^{-1}(\{y\})| \tag{1}$$

We claim that $|\psi^{-1}(\{y\})| = |\operatorname{Stab}(x)|$ for all $y \in \mathcal{O}_x$. First note that:

$$\psi^{-1}(\{x\}) = \{g \in G : gx = x\} = \operatorname{Stab}(x)$$

Now suppose $x \neq y \in \mathcal{O}_x$, then $y = hx$ for some $h \in G$. We claim that $\psi^{-1}(\{y\}) = h^{-1} \cdot \operatorname{Stab}(x)$. For the first inclusion: If $g \in \psi^{-1}(\{y\})$ then $gx = y$. Hence:

$$(h^{-1}g)x = h^{-1}(gx) = h^{-1}y = x$$

Therefore $h^{-1}g \in \operatorname{Stab}(x)$, so $g = hh^{-1}g \in h \cdot \operatorname{Stab}(x)$. On the other hand, if $h^{-1}g \in \operatorname{Stab}(x)$ then we have $(h^{-1}g)x = h^{-1}y = x$. Hence $h^{-1}g \in \psi^{-1}(\{y\})$. Hence $\psi^{-1}(\{y\}) = h^{-1} \cdot \operatorname{Stab}(x)$ and:

$$|\psi^{-1}(\{y\})| = |h^{-1} \cdot \operatorname{Stab}(x)| = |\operatorname{Stab}(x)|$$

Combining this an equation (1) we have:

$$|G| = \sum_{y \in \mathcal{O}_x} |\operatorname{Stab}(x)| = |\mathcal{O}_x| \cdot |\operatorname{Stab}(x)|$$

As desired. $\square$

Let G be a finite group, with disjoint conjugacy classes $K_1, \cdots, K_r$. Pick some $g_i \in K_i$ for each i. By definition, each $K_i = \mathcal{O}_{g_i}$ is the orbit of g_i under the action by conjugation. In this action, the stabilizer of $g \in G$ is the centralizer $\operatorname{Cent}(g) = \{h \in G : gh = hg\}$. Hence:

$$|G| = |\mathcal{O}_{x_i}||\operatorname{Stab}(g_i)| = |K_i||\operatorname{Cent}(g_i)|$$

By reordering, assume $K_1, \cdots, K_j$ are the singleton conjugacy classes. That is, $K_1 \cup \cdots \cup K_j = Z(G)$ is the center of G. Since G is the disjoint union of all conjugacy classes, we have:

$$|G| = \sum_{i=1}^{r} |K_i| = \sum_{i=1}^{j} |K_i| + \sum_{i=j+1}^{r} |K_i| = |Z(G)| + \sum_{i=j+1}^{r} \frac{|G|}{|\operatorname{Cent}(g_i)|}$$

Theorem 11.2 (Class Equation). Let G be a finite group and let $g_1, \cdots, g_r$ be the representatives of the non-singleton conjugacy classes. Then:

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|\operatorname{Cent}(g_i)|}$$

12 Simplicity of Alternating groups

Remark. Say $\tau \in S_n$, then:

$$\tau(a_1 a_2 \cdots a_r)\tau^{-1} = (\tau(a_1)\tau(a_2)\cdots\tau(a_r))$$

In general, the permutation $\tau\sigma\tau^{-1}$ yields the same permutation σ only with a_i replaced by $\tau(a_i)$. This is saying that the conjugacy classes in S_n are the set os permutaion with the same "shape" when writing in the disjoint cycle representation.

Example 12.1. In S_3, all conjugacy classes are $\{(1)\}$, $\{(12),(13),(23)\}$, $\{(123),(132)\}$.

Example 12.2. In S_5, all conjugacy classes and their sizes are:

Conjugacy Classes	$\{(1)\}$	$\{(ab)\}$	$\{(abc)\}$	$\{(abcd)\}$	$\{(abcde)\}$	$\{(ab)(cd)\}$	$\{(ab)(cde)\}$
Size	1	10	20	30	24	15	20

Lecture 14, 2023/06/07

Theorem 12.3. A_5 is a simple group!

To prove it we need a lemma.

Lemma 12.4. Let G be a group and $H \subseteq G$ be a subgroup. Then H is normal in G if and only if H can be written as a union of conjugacy classes in G.

Proof. ($\Rightarrow$). Assume H is normal, if $x \in H$ then $gxg^{-1} \in H$ for all $g \in G$. This means the entire conjugacy class $\mathcal{O}_x$ is contained in H. Hence:

$$H = \bigcup_{x \in H} \mathcal{O}_x$$

($\Leftarrow$). Let $x \in H$, then $\mathcal{O}_x \subseteq H$. Hence $gxg^{-1} \in \mathcal{O}_x \subseteq H$ for all $g \in G$. $\square$

Plan to prove Theorem 12.3. We already found out all the conjugacy classes of S_5 are and these will give us the conjugacy classes of A_5. Now we are going to show that if $H \subseteq A_5$ is normal, then $|H| = 1$ or $|H| = |A_5| = 60$ so that $H = \{1\}$ or A_5. Our strategy is to show that for any choices of conjugacy classes, the sum of their sizes is not equal to $|H|$ unless $|H| = 1$ or 60, which means H is not a union of conjugacy classes unless $H = \{1\}$ or $H = A_5$ (apply the above lemma).

Proof of Theorem 12.3. The only difficult part is to figure out the conjugacy classes of A_5. Note that two permutations in the same conjugacy class in A_5 also have the same shape, but the converse is not true! It is possible that two permutations have the same shape but they belong to two different conjugacy classes in A_5. Let us first consider the possible cycle types in A_5:

Conjugacy Classes?	$\{(1)\}$	$\{(abc)\}$	$\{(abcde)\}$	$\{(ab)(cd)\}$
Size in S_5	1	20	24	15

Clearly $\{(1)\}$ is also a conjugacy class in A_5. For $\sigma \in A_5$ we let $\operatorname{Cent}_{A_5}(\sigma)$ and $\operatorname{Cent}_{S_5}(\sigma)$ denote the stabilizer of σ in A_5 and S_5, respectively. Also we let σ^{A_5} and σ^{S_5} denote the conjugacy class of σ in A_5 and S_5, respectively. By the Orbit-Stabilizer theorem:

$$|\sigma^{S_5}| = \frac{120}{|\operatorname{Cent}_{S_5(\sigma)}|} \quad \text{and} \quad |\sigma^{A_5}| = \frac{60}{|\operatorname{Cent}_{A_5}(\sigma)|} \tag{1}$$

Moreover we have $\operatorname{Cent}_{A_5}(\sigma) = \operatorname{Cent}_{S_5}(\sigma) \cap A_5$ and $\sigma^{A_5} \subseteq \sigma^{S_5}$.

$$\begin{tikzcd}
\operatorname{Cent}_{S_5}(\sigma) \arrow[r] & S_5 \arrow[r, "\operatorname{sgn}"] & \{\pm 1\} \\
\operatorname{Cent}_{A_5}(\sigma) \arrow[r] \arrow[u, hook] & A_5 \arrow[r, "\operatorname{sgn}"] \arrow[u, hook] & \{1\} \arrow[u, hook]
\end{tikzcd}$$

Note that $\operatorname{sgn}(\operatorname{Cent}_{S_5}(\sigma)) = \{\pm 1\}$ or $\{1\}$.

$$\begin{aligned}
\operatorname{sgn}(\operatorname{Cent}_{S_5}(\sigma)) = \{1\} &\implies \operatorname{Cent}_{S_5}(\sigma) \subseteq A_5 \implies \operatorname{Cent}_{A_5}(\sigma) = \operatorname{Cent}_{S_5}(\sigma) \\
\operatorname{sgn}(\operatorname{Cent}_{S_5}(\sigma)) = \{\pm 1\} &\implies 2 \cdot |\operatorname{Cent}_{A_5}(\sigma)| = |\operatorname{Cent}_{S_5}(\sigma)|
\end{aligned}$$

Combining this with (1) we have the following observation:

$$\sigma^{A_5} = \sigma^{S_5} \iff \operatorname{Cent}_{A_5}(\sigma) \subsetneq \operatorname{Cent}_{S_5}(\sigma) \iff \sigma \text{ commutes with some } \tau \in S_5 \setminus A_5$$

Now let us consider the centralizer of each σ of the shape $(abc), (abcde), (ab)(cd)$.

(1). Let $\sigma = (123)$. Then $(123)(45) = (45)(123)$ and $(45) \notin A_5$. Therefore $(123)^{A_5} = (123)^{S_5}$.

(2). Note that $\operatorname{Cent}_{S_5}((12345)) = \langle (12345) \rangle \subseteq A_5$, so $(12345)^{S_5}$ splits into a union of two conjugacy classes (each has size 12) in A_5 and we have:

$$(12345)^{S_5} = (12345)^{A_5} \cup (13452)^{A_5}$$

(3). Let $\sigma = (12)(34)$. Note that σ commutes with $(12) \notin A_5$, hence the conjugacy class of σ in A_5 and S_5 coincide and it has size 15.

Lecture 15, 2023/06/09

By our above analysis, the conjugacy classes of A_5 are given by the table:

Conjugacy Classes	$\{(1)\}$	$\{(123)\}$	$\{(12345)\}$	$\{(13452)\}$	$\{(12)(34)\}$
Size	1	20	12	12	15

Now let $\{1\} \neq H \subseteq A_5$ be a nontrivial normal subgroup. Then H has size dividing 60, by Lagrange's theorem. Therefore $|H| \in \{2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\} = S$. By Lemma 12.4 we know H is the disjoint union of some conjugacy classes of A_5. Since H is a subgroup it must include the class $\{(1)\}$. However, by some basic arithmetic we can see that the sum of 1 and some of $20, 12, 12, 15$ cannot be one of S, except for 60. Hence $|H| = 60$ and $H = A_5$. Therefore A_5 is simple! $\square$

Theorem 12.5. A_n is simple for $n \geq 5$.

Proof. Let $n \geq 5$. We have done it for $n = 5$. Now suppose $H \subseteq A_n$ is normal and $H \neq \{(1)\}$, we want to show $H = A_n$. Let $(1) \neq \sigma \in H$. For any $\sigma \in A_n$ we have $\sigma\tau\sigma^{-1} \in H$, as H is normal in A_5. If we choose τ to be a 3-cycle, then τ^{-1} is a 3-cycle and $\sigma\tau^{-1}\sigma$ is a 3-cycle. This means the permutation $\tau\sigma\tau^{-1}\sigma^{-1} \in H$ moves at most 6 things (because it is a product of two 3-cycles and each 3-cycle moves at most 3 things). We choose τ carefully so that $\tau\sigma\tau^{-1}\sigma^{-1}$ moves between 2 and 5 things. Call $\alpha = \tau\sigma\tau^{-1}\sigma^{-1} \in H$. Suppose $K = \{a, b, c, d, e\}$ contains all the numbers that α moves. Define the following subgroup:

$$B = \{\sigma \in A_n : \sigma x \neq x \implies x \in \{a, b, c, d, e\}\}$$

to be the subgroup of A_n that only moves elements in K. Then $B \cong A_5$ as groups. Note that $H \cap B$ is normal in B. Since $B \cong A_5$ is simple and $\alpha \in H \cap B \neq \emptyset$, we must have $H \cap B = B$. Hence we have $B \subseteq H$. Note that the permutation (abc) is in B, hence $(abc) \in H$. Therefore H contains a 3-cycle. To show that H contains all the 3-cycles, we can note that (abc) commutes with (de) for some $d, e \notin \{a, b, c\}$. This is possible because $n \geq 5$. By the argument in the proof of A_5, we know the conjugacy class in S_n does not split in A_n, so H contains all the 3-cycles!! Now we finish the proof that $H = A_n$ by showing A_n is generated by 3-cycles.

Lecture 16, 2023/06/12

Lemma 12.6. The 2-cycles generate S_n for $n \geq 2$.

Proof. It suffices to show every cycle is a product of 2-cycles. Let $\sigma = (a_1, \cdots, a_k)$ then:

$$(a_1, \cdots, a_k) = (a_1 a_k) \cdots (a_1 a_3)(a_1 a_2)$$

As desired. $\square$

Lemma 12.7. The 3-cycles generate A_n for $n \geq 3$.

Proof. Let $H \subseteq A_n$ be the subgroup generated by all the 3-cycles. Let $\sigma \in A_n$. By the lemma above, we can write $\sigma = t_1 \cdots t_r$, where each t_i is a 2-cycle. Note that $\text{sgn}(t_i) = -1$ for all i, so r must be even as $\text{sgn}(\sigma) = 1$. Now we show that $(ab)(cd)$ is a product of 3-cycles. If $(ab) = (cd)$ then $(ab)(cd) = (ab)(ab) = (1) = (123)(123)(123)$ is a product of 3-cycles. Now assume $(ab) \neq (cd)$. If $\{a,b\} \cap \{c,d\} = \emptyset$ then we have $(ab)(cd) = (abc)(bcd)$. Otherwise, $\{a,b\} \cap \{c,d\}$ has one element. WLOG assume $b = c$, then $(ab)(cd) = (ab)(bd) = (abd)$ is a product of 3-cycles. Therefore, if we write $r = 2k$ then:

$$\sigma = \underbrace{t_1 t_2}_{\in H} \cdots \underbrace{t_{2k-1} t_{2k}}_{\in H} \in H$$

It follows that $H = A_n$, so 3-cycles generate A_n. $\square$

Proof of Theorem 12.5 Continued. We have proved that A_n is generated by 3-cycles. Since H contains all 3-cycles, we must have $H = A_n$. This completes the proof. $\square$

Example 12.8. Note that $A_1 = A_2 = \{(1)\}$ are simple.

Example 12.9. Note $A_3 = \{(1), (123), (132)\} \cong \mathbb{Z}/3\mathbb{Z}$ is simple because 3 is prime.

Example 12.10. Finally, A_4 has 12 elements. Its conjugacy classes are:

Conjugacy Classes	$\{(1)\}$	$\{(123)\}$	$\{(132)\}$	$\{(12)(34)\}$
Size in A_4	1	4	4	3

This can be obtained with the same analysis as in A_5, by considering their centralizers. A normal subgroup of A_4 contains (1) and is a union of conjugacy classes. By Lagrange's theorem, the only possibility is $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. This is indeed a subgroup! Hence it is normal in A_4. It follows that A_4 is not simple.

Theorem 12.11. Let $n \in \mathbb{N}$, then A_n is simple for all $n \neq 4$.

13 Sylow's Theorems

Definition. Let p be a prime. A **p-group** is a finite group G such that $|G|$ is a power of p.

Definition. Let p be a prime and G be a finite group of order $|G| = p^a m$, where $p \nmid m$. A **p-Sylow subgroup** of G is a subgroup of order p^a.

Definition. Let G be a group and $S \subseteq G$. The **normalizer** of S in G is:

$$N_G(S) := N(S) := \{g \in G : gSg^{-1} = S\}$$

It is the largest subgroup of G such that S is normal in it. [Well, S is not required to be a subgroup, so we really mean $N(S)$ is the largest subgroup of G containing S such that S is closed under conjugating by elements in $N(S)$.]

Theorem 13.1 (Sylow's Theorem). Let p be a prime number. Let G be a group with $p^a m$ elements such that $p \nmid m$. Then:

(1) G has a p-Sylow subgroup.

(2) Any p-subgroup of G is contained in a p-Sylow subgroup.

(3) Any two p-Sylow subgroups are conjugate. That is, if H_1 and H_2 are two p-Sylow subgroups, then $gH_1g^{-1} = H_2$ for some $g \in G$.

(4) Let N_p denote the number of p-Sylow subgroups of G. Then $N_p \equiv 1 \pmod p$ and $N_p \mid |G|$. Moreover, we have $N_p = [G : N(P)]$ for any p-Sylow subgroup P.

Example 13.2. Let G be a group of 15 elements. Then $|G| = 3 \cdot 5$. By the Sylow's theorem, it has a 3-Sylow subgroup H and a 5-Sylow subgroup K. Note that $N_3 \equiv 1 \pmod 3$ and $N_3 \mid 15$. Hence $N_3 = 1$. Similarly $N_5 = 1$ as well. It means $[G : N(H)] = 1$, so $N(H) = G$. Therefore H is normal in G. Similarly K is normal in G. Now we claim that:

$$G \cong H \times K$$

by applying Theorem 8.4. Note that $H \cap K = \{1\}$ because $H \cap K$ has order dividing both 3 and 5. We also need to check $HK = G$. Note that $HK = \{hk : h \in H, k \in K\}$ has at most 15 elements, so we need to show it has at least 15 elements. If $h_1k_1 = h_2k_2$, then $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\}$. Hence $h_1 = h_2$ and $k_1 = k_2$. It follows that HK has at least 15 elements and $HK = G$. Finally, let $h \in H$ and $k \in K$ we want to show $hk = kh$. Note $hkh^{-1} \in K$ and $kh^{-1}k^{-1} \in K$ so that $hkh^{-1}k^{-1} \in H \cap K = \{1\}$. It follows that $hk = kh$. Thus $G \cong H \times K$. Since $|H| = 3$ and $|K| = 5$, so $H \cong \mathbb{Z}/3\mathbb{Z}$ and $K \cong \mathbb{Z}/5\mathbb{Z}$. It follows that:

$$G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$$

This means $\mathbb{Z}/15\mathbb{Z}$ is the ONLY group of order 15, up to isomorphism!

Lecture 17, 2023/06/14

Theorem 13.3 (Cauchy). Let p be a prime and G be a finite group such that p divides $|G|$. Then G contains an element of order p.

Proof. We first prove a small lemma:

Lemma: Cauchy's Theorem holds when G is abelian.

Proof (Lemma): We perform induction on $|G|$. If $|G| = 1$ then there is no prime dividing 1, so the lemma holds vacuously. Suppose $|G| \geq 2$ and let p be a prime dividing $|G|$. Take $1 \neq a \in G$ and consider $H = \langle a \rangle$. If p divides $|H|$ then $a^{|H|/p}$ has order p. Otherwise $p \mid [G : H]$ because p is a prime number and $[G : H]|H| = |G|$ by Lagrange's theorem. Hence p divides $|G/H| = [G : H]$. By induction, since $|G/H| < |G|$ we know G/H has an order $\bar{x} = xH$ of order p. [Note that G/H is a group since G is abelian.] Let m be the order of x in G. Then:

$$(xH)^m = x^m H = H \implies p \mid m$$

It follows that $x^{m/p} \in G$ has order p, as desired. **(QED Lemma)**

Now consider the general case. We induce on $|G|$ again. If $|G| = 1$ then we are done. If p divides $|Z(G)|$, then since $Z(G)$ is abelian it contains an element $x \in Z(G) \subseteq G$ of order p. Then we are done! Otherwise, by the class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|\operatorname{Cent}(g_i)|}$$

for some $g_i \in G$ not in the center. Since $p \nmid |Z(G)|$, we also have $p \nmid \sum_{i=1}^{r} \frac{|G|}{|\operatorname{Cent}(g_i)|}$. Hence there exists i such that $p \nmid \frac{|G|}{|\operatorname{Cent}(g_i)|}$. Note that $|G|$ has a factor of p, so $|\operatorname{Cent}(g_i)|$ must have a factor of p as well! If $|\operatorname{Cent}(g_i)| = |G|$ then $\operatorname{Cent}(g_i) = G$ and $g_i \in Z(G)$, which is a contradiction by the choice of g_i. Therefore $|\operatorname{Cent}(g_i)| < |G|$ and by induction, $\operatorname{Cent}(g_i)$ has an element of order p. This completes the proof. $\square$

Note. This is not the proof Professor McKinnon gave in class. In fact, I think he forgot to prove this theorem (lol) and he used this theorem in the proof of Sylow's theorem.

Proof of Theorem 13.1 (Sylow). (1). We prove it by induction on $|G|$. If $|G| = 1$, there is nothing to prove. Assume $|G| \geq 2$ and assume $|G| = p^a m$ for $p \nmid m$. If p divides $|Z(G)|$ then by Cauchy's theorem, there is an element $x \in Z(G)$ of order p. Let $N = \langle x \rangle$, so $|N| = p$. Also N is normal in G because $N \subseteq Z(G)$. Hence G/N has fewer elements than G, so G/N has a p-Sylow subgroup $\bar{P}$. Note that $|G/N| = p^{a-1}m$, so $|\bar{P}| = p^{a-1}$. Let $P = \{g \in G : gN \in \bar{P}\} \subseteq G$. Then

$|P| = p^a$ as $|\bar{P}| = p^{a-1}$ and $|N| = p$. It follows that P is a p-Sylow subgroup of G. Now consider the case when $p \nmid |Z(G)|$. By the class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|\operatorname{Cent}(g_i)|}$$

for $g_i \in G$ not in $Z(G)$. Since $p \nmid |G|$, we know $p \nmid \sum_{i=1}^{r} \frac{|G|}{|\operatorname{Cent}(g_i)|}$. Hence there exists i such that p does not divide $\frac{|G|}{|\operatorname{Cent}(g_i)|}$. Since $|G| = p^a m$, we know $|\operatorname{Cent}(g_i)|$ must have a factor of p^a as well! However, $|\operatorname{Cent}(g_i)|$ divides $|G|$ by Lagrange's theorem. Thus p^{a+1} does not divide $|\operatorname{Cent}(g_i)|$. We can thus write $|\operatorname{Cent}(g_i)| = p^a n$ for some n. Since $\operatorname{Cent}(g_i)$ is a proper subgroup of G, it contains a p-Sylow subgroup of size p^a by induction! This gives a p-Sylow subgroup of G.

Lecture 18, 2023/06/16

(2). Let $P = P_1$ be a p-Sylow subgroup. Let $S = \{P_1, \cdots, P_r\}$ be the set of conjugates of P. That is, it is the orbit of P under the action of G by conjugation. Let Q be a p-Sylow subgroup of G. Then Q acts on S by conjugation. Let $\mathcal{O}_1, \cdots, \mathcal{O}_s$ be the orbits of this Q-action.

Lecture 19, 2023/06/19

14 Finite Groups of small order

Proposition 14.1. Let p be a prime. Every group of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof. This follows from Lagrange's theorem. $\square$

Let G be a finite group and $|G| = n$. We will classify all finite group of order n for $n \leq 15$. We are going to use the tools developed so far: Lagrange's theorem, Group actions and Sylow's theorem and the following result from an assignment:

Theorem 14.2. Let p be a prime. Every group of order p^2 is either $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Example 14.3 ($n = 1$)**.** In this case G is the trivial group.

Example 14.4 ($n = 2$)**.** Let $|G| = 2$. Then $G \cong \mathbb{Z}/2\mathbb{Z}$.

Example 14.5 ($n = 3$)**.** Let $|G| = 3$. Then $G \cong \mathbb{Z}/3\mathbb{Z}$.

Example 14.6 ($n = 4$)**.** Let $|G| = 4$. Then $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example 14.7 ($n = 5$)**.** Let $|G| = 5$. Then $G \cong \mathbb{Z}/5\mathbb{Z}$.

Example 14.8 ($n = 6$)**.** Let $|G| = 6$. This is the first nontrivial case. Note that $6 = 2 \cdot 3$, so it has a 3-Sylow subgroup P_3 and a 2-Sylow subgroup P_2. Moreover $N_3 \equiv 1 \pmod 3$ and $N_3 \mid 6$, so $N_3 = 1$. Hence P_3 is a normal subgroup. Now there are two cases.

Case 1. If P_2 is normal, then by the same proof as Example 13.2 we can show that:

$$G \cong P_2 \times P_3 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$$

Case 2. Assume P_2 is not normal, so $N_2 \neq 1$. By Sylow's theorem, since $N_2 \equiv 1 \pmod 2$ and $N_2 \mid 6$ we must have $N_2 = 3$. Call thes 2-Sylow subgroups $K = \{P_2, Q_2, R_2\}$. Then G acts transitively on K by $g \cdot P = gPg^{-1}$. This action defines a group homomorphism $\phi : G \to \mathrm{Sym}(K) \cong S_3$. Note that:

$$\ker \phi = \{g \in G : gP_2g^{-1} = P_2,\ gQ_2g^{-1} = Q_2,\ gR_2g^{-1} = R_2\}$$

Since this action is transitive, K is the unique orbit of 3 elements. Each of $\mathrm{Stab}(P)$ has 2 elements for $P \in K$, by the Orbit-Stabilizer theorem. Note that $P \subseteq \mathrm{Stab}(P)$ because $gPg^{-1} = P$ for $g \in P$. Since $|\mathrm{Stab}(P)| = |P| = 2$, we have $P = \mathrm{Stab}(P)$ for all $P \in K$. Hence $\mathrm{Stab}(P) \cap \mathrm{Stab}(Q) = P \cap Q = \{1\}$ for $P \neq Q$ in K. It follows that $\ker \phi = \{1\}$ so that ϕ is injecitve. Since $|G| = |S_3| = 6$, we know ϕ is an isomorphism. Therefore $G \cong S_3$.

Example 14.9 ($n = 7$). Let $|G| = 7$. Then $G \cong \mathbb{Z}/7\mathbb{Z}$.

Before we consider the case $n = 8$, we will first prove this useful lemma.

Lemma 14.10. Let G be a group and $H \subseteq G$ be a subgroup of index 2. Then H is normal in G.

Proof. Define a map $\phi : G \to \{\pm 1\}$ by:

$$\phi(g) = \begin{cases} 1 & \text{if } g \in H \\ -1 & \text{if } g \notin H \end{cases}$$

We claim that ϕ is a group homomorphism. Clearly $\phi(1) = 1$ because H is a subgroup. Now let $a, b \in G$ be arbitrary. If $a, b \in H$ then $\phi(a) = \phi(b) = 1$ and $\phi(ab) = 1$ as well. If $a, b \notin H$, we claim that $ab \in H$. Indeed, $[G : H] = 2$ implies there are only two left cosets H and gH for some $g \in G$. Note that $(gH)^2 = H$. Since $a, b \notin H$ we have $aH = bH = gH$. Moreover:

$$(ab)H = (aH)(bH) = (gH)(gH) = (gH)^2 = H$$

It follows that $ab \in H$. Hence $\phi(a) = \phi(b) = -1$ and $\phi(ab) = 1$. Finally assume $a \in H$ and $b \notin H$. Then $aH = H$ and $bH = gH$. Then $abH = gH \neq H$, so $ab \notin H$! Thus $\phi(a) = 1$ and $\phi(b) = -1$ and $\phi(ab) = -1$. This proved that ϕ is a group homomorphism. It is clear that $\ker \phi = H$, which proved that H is noraml in G. [Becasuse kernel is always a normal subgroup.] $\square$

Example 14.11 ($n = 8$). Let $|G| = 8 = 2^3$. There are three different cases.

(1). If there exists an element of order 8, then $G \cong \mathbb{Z}/8\mathbb{Z}$.

(2). If every element of G has order 2. Let $a, b \in G$, then $a = a^{-1}$ and $b = b^{-1}$. Then $(ab)^2 = 1$, so $abab = 1$. It follows that $ab = b^{-1}a^{-1} = ba$, so G is abelian. Let $1 \neq a, b, c$ be three distinct elements in G, then by Theorem 8.4 we have:

$$G \cong \langle a \rangle \times \langle b \rangle \times \langle c \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

(3). Suppose there exists $x \in G$ of order 4. Then $H = \langle x \rangle$ has index 2 in G, so H is normal in G by the Lemma above. Let $y \notin H$, then $yxy^{-1} \in H$ and we can write $yxy^{-1} = x^a$ for some $a \in \mathbb{N}$. Note that conjugation does not change the order, so $x^a = yxy^{-1}$ has order 4 as well. Hence $a \in \{1, 3\}$. If $a = 1$ then $xy = yx$.

Lecture 22, 2023/06/26

15 Rings and Ideals

Informally, a **ring** is a bunch of things we can add, subtract and multiply.

Example 15.1. $\mathbb{Z} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{C}[x]$ are all rings, with usual addition and multiplication.

Example 15.2. $\mathbb{R}[x, y] = \{\text{polynomials in } x \text{ and } y \text{ with } \mathbb{R}\text{-coefficient}\}$ is a ring.

Example 15.3. $\mathbb{M}_n(\mathbb{R}) = \{n \times n \text{ matrices over } \mathbb{R}\}$ with usual addition and multiplication is a ring.

Example 15.4. $\mathbb{Z}_n = \{[k] : 0 \leq k \leq n-1\}$ is a ring for all $n \in \mathbb{N}$.

Definition. A **ring** is a triple $(R, +, \cdot)$, where $+$ and $\cdot$ are binary operations on R such that $(R, +)$ is an abelian group (with identity 0) satisfying:

(1) For all $a, b, c \in R$ we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(2) There exists $0 \neq 1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

(3) For all $a, b, c \in R$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

We say $x \in R$ is a **unit** if there exists $y \in R$ such that $xy = yx = 1$. We let $R^\times$ (or R^*) denote the set of all units of R.

Remark. In some texts the author does not assume a ring has property (2) above. They call a ring that has 1 a **unital ring** and a ring only need to satisfy property (1) and (3). However, in this course we always assume a ring has a multiplicative identity 1.

Proposition 15.5. Let R be a ring. Then $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$.

Proof. Since $(R, +)$ is an abelian group we know $0 + 0 = 0$. Multiplying by a on the right on both sides and apply (3), we have:

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$$

Adding the inverse $-(0 \cdot a)$, we have $0 = 0 \cdot a$ as desired. Similarly $0 = a \cdot 0$ as well. $\square$

Corollary 15.6. Let R be a ring and $a \in R$. Then $-a = (-1) \cdot a = a \cdot (-1)$.

Proof. Let $a \in R$, then by the Proposition above:

$$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 - 1) \cdot a = 0 \cdot a = 0$$

Hence $(-1) \cdot a = -a$. Similarly $a \cdot (-1) = -a$. $\square$

Definition. A ring R is **commutative** if $ab = ba$ for all $a, b \in R$.

Definition. A ring R is a **division ring** if every nonzero $x \in R$ is a unit. Equivalently, $R^\times = R \backslash \{0\}$.

Definition. A **field** is a commutative division ring.

Definition. Let R be a ring. An element $a \in R$ is a **zero divisor** if $a \neq 0$ and there exists $0 \neq b \in R$ such that $ab = 0$ or $ba = 0$.

Definition. A ring R is an **integral domain** (or just **domain**) if R has no zero divisors.

Example 15.7. The ring $\mathbb{Z}_6$ is not a domain because $[2] \cdot [3] = [0]$.

Theorem 15.8. Let R be a ring. If a is a unit, then a is not a zero divisor.

Proof. Suppose $ab = 0$, then $b = a^{-1}ab = a^{-1}0 = 0$. □

Corollary 15.9. Every division ring is a domain.

Example 15.10. $\mathbb{Z}$ is a domain but not a division ring. The only units of $\mathbb{Z}$ are ± 1.

Example 15.11. $\mathbb{Q}$ and $\mathbb{R}$ are fields.

Example 15.12. If $n \geq 2$, then $\mathbb{M}_n(\mathbb{R})$ is not commutative and not a domain. It is clearly not commutative. If we let E_{ij} be the matrix whose ij-entry is 1 and all the other entries are 0, then we note that $E_{1n}^2 = 0$ but $E_{1n} \neq 0$. Hence E_{1n} is nilpotent and a zero divisor of $\mathbb{M}_n(\mathbb{R})$.

$$\mathbb{M}_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R}) = \{n \times n \text{ invertible matrices}\}$$

Example 15.13. $\mathbb{R}[x]$ is commutative domain and $\mathbb{R}[x]^\times = \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$.

Definition. Let $(R, +, \cdot)$ be a ring. A **subring** of R is a subset $S \subseteq S$ such that $(S, +, \cdot)$ is a ring. This means $a + b, a \cdot b \in S$ for all $a, b \in S$ and identities of S are the same as identities of R.

Lecture 23, 2023/06/28

Theorem 15.14 (Subring Theorem). Let R be a ring. $S \subseteq R$ is a subring if and only if:

(1) $1 \in S$.

(2) S is closed under subtraction. That is, $a - b \in S$ for all $a, b \in S$.

(3) S is closed under multiplication. That is $ab \in S$ for all $a, b \in S$.

Proof. $(\Rightarrow)$. This is the definition.

$(\Leftarrow)$. Since $1 \in S$, then $1 - 1 = 0 \in S$. The other properties are easy to check. □

Example 15.15. Let $R = \mathbb{C}$ and let $\zeta_5 = e^{2\pi i/5}$ be the primitive 5-th root of unity. Let:

$$S := \mathbb{Z}[\zeta_5] := \{a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 + e\zeta_5^4 : a, b, c, d, e \in \mathbb{Z}\}$$

It is easy to check that S is a subring of $\mathbb{C}$. The closure under multiplication can be checked using the relation that $\zeta_5^5 = 1 = 1 + 0\zeta_5 + 0\zeta_5^2 + 0\zeta_5^3 + 0\zeta_5^4$.

Definition. Let R and T be rings. A **ring homomorphism** from R to T is a function $f : R \to T$ such that $f(1_R) = 1_T$ and $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$. An **isomorphism** is a homomorphism with an inverse homomorphism.

Proposition 15.16. A ring homomorphism is an isomorphism if and only if it is a bijection.

Example 15.17. $\mathbb{Z} \times \mathbb{Z}$ is a ring by $(a, b) \cdot (c, d) = (ac, bd)$. Then $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $f(a, b) = a$ is a ring homomorphism.

Example 15.18. The map $f : \mathbb{R}[x] \to \mathbb{C}$ by $f(p(x)) = p(i)$ is a group homomorphism.

Remark. In general, plugging stuff in for the variable is always a homomorphism.

Definition. Let $\phi : R \to T$ be a homomorphism. The **image** of ϕ is:

$$\text{im}\phi = \{\phi(r) : r \in R\}$$

The **kernel** of ϕ is:

$$\ker(\phi) = \{r \in R : \phi(r) = 0\}$$

Theorem 15.19. Let $\phi : R \to T$ be a homomorphism. Then $\text{im}\phi$ is a subring of T but $\ker(\phi)$ is NOT a subring of R.

Proof. Note that $\phi(1_R) = 1_T$, so $1_T \in \text{im}\phi$. It is clear to check the other properties. If $\ker(\phi)$ is a subring of R then $1 \in \ker(\phi)$, so $1_T = \phi(1) = 0_T$. This is a contradiction. $\square$

Definition. Let R be a ring. An R**-module** is a bunch of things we can add, subtract and multiply by elements in R. [Essentailly it is the vector space over the ring R.] Formally, an R**-module** is an abelian group M with a function $\cdot : R \times M \to M$ satisfying:

(1) For all $r_1, r_2 \in R$ and $m \in M$ we have $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$.

(2) For all $r \in R$ and $m_1, m_2 \in M$ we have $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.

(3) For all $r_1, r_2 \in R$ and $m \in M$ we have $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$.

Let M be an R-module. We say $N \subseteq M$ is an R**-submodule** of M is also an R-module with the same operations. Note that if $\mathbb{F}$ is a field, then an $\mathbb{F}$-module is exactly a vector space over $\mathbb{F}$.

Lecture 24, 2023/06/30

Note. From now on, every ring we deal with is commutative.

Example 15.20. Let R be a ring. Then R is an R-module, where the scalar multiplication by elements in R is just multiplication in R.

Example 15.21. Let $\phi : R \to T$ be a ring homomorphism, then $\ker \phi$ is an R-submodule of R. We say $\ker \phi$ is an ideal (see below).

Example 15.22. The even integers $2\mathbb{Z}$ is an $\mathbb{Z}$-module.

Definition. Let R be a ring. An **ideal** of R is an R-submodule of R. That is, $I \subseteq R$ is an ideal if for all $a, b \in I$ and $r \in R$ we have $ra + b \in I$.

16 Quotient Rings

Question: Is every ideal of R the kernel of some homomorphism?

Answer: YES! Take the quotient.

If R is a ring and I is an ideal of R. We want to find a ring T and a homomorphism $\phi : R \to T$ such that $\ker \phi = I$. If such a ring and a homomorphism exists. For all $t \in T$:

$$\phi^{-1}(t) = \{r \in R : \phi(r) = t\}$$

Suppose $\phi(r) = t$ and since $\phi(I) = 0$, we have $\phi^{-1}(t) = r + I = \{r + i : i \in I\}$. This motivates our following definition:

Definition. Let R be a ring and $I \subseteq R$ is an ideal. For $r \in R$ define $r + I = \{r + i : i \in I\}$. Let:

$$R/I = \{r + I : r \in R\}$$

Then R/I is a ring with addition and multiplication by:

$$(r_1 + I) + (r_2 + I) := (r_1 + r_2) + I$$
$$(r_1 + I) \cdot (r_2 + I) := (r_1 r_2) + I$$

This operation is well-defined. We call R/I the **quotient ring** of R by I.

Example 16.1. Note that $6\mathbb{Z}$ is an ideal of $\mathbb{Z}$, so $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$ is the quotient ring.

Remark. Note that R/I is NOT a subring of R! For example, $\mathbb{Z}/6\mathbb{Z}$ is not (isomorphic to) a subring of $\mathbb{Z}$ because every subring of $\mathbb{Z}$ is infinite.

Theorem 16.2 (Universal Property of Quotients). Let R and T be rings and $\phi : R \to T$ be a ring homomorphism. Let $I \subseteq R$ be an ideal. Let $q : R \to R/I$ be the quotient map. There exists a homomorphism $\tilde{\phi} : R/I \to T$ if and only if $I \subseteq \ker \phi$.

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "q"'] & T \\ R/I \arrow[ur, dashed, "\tilde{\phi}"'] & \end{tikzcd}$$

Furthermore, we have $\mathrm{im}\tilde{\phi} = \mathrm{im}\phi$ and $\ker \tilde{\phi} = q(\ker \phi)$.

Proof. Same as the proof of UPQ for quotient groups. $\square$

Proposition 16.3. A ring homomorphism $\phi : R \to T$ is injecitve if and only if $\ker \phi = \{0\}$.

Proof. Let $\phi : R \to T$ be a ring homomorphism, then:

$$\begin{aligned} \phi \text{ is injective } &\iff \forall x, y \in R : \phi(x) = \phi(y) \implies x = y \\ &\iff \forall x, y \in R : \phi(x - y) = 0 \implies x - y = 0 \\ &\iff \forall a \in R : \phi(a) = 0 \implies a = 0 \\ &\iff \ker \phi = \{0\} \end{aligned}$$

This completes the proof. $\square$

Example 16.4. Consider the ring $\mathbb{R}[x]$. Define the ideal $I = \{p(x) \in \mathbb{R}[x] : p(1) = 0\}$. What does the quotient ring $\mathbb{R}[x]/I$ look like? Define $\phi : \mathbb{R}[x] \to \mathbb{R}$ by $\phi(p(x)) = p(1)$. By definition we have $\ker \phi = I$. Note that for any $\alpha \in \mathbb{R}$ we have $\phi(\alpha) = \alpha$, so ϕ is surjective. By the UPQ we have a surjective homomorphism $\tilde{\phi} : \mathbb{R}[x]/I \to \mathbb{R}$. Note that it is injective because:

$$\ker \tilde{\phi} = q(\ker \phi) = q(I) = 0$$

Therefore $\tilde{\phi}$ is injecitve and thus $\mathbb{R}[x]/I \cong \mathbb{R}$ as rings.

Lecture 25, 2023/07/05

Definition. Let R be a ring. An ideal $I \subseteq R$ is a **maximal ideal** if $I \neq R$ and for any ideal J satisfying $I \subseteq J \subseteq R$ we have $J = I$ or $J = R$. That is, there is no proper ideal that contains I.

Example 16.5. Let $R = \mathbb{Z}$. What are the ideals of $\mathbb{Z}$? Let $0 \neq I \subseteq \mathbb{Z}$ be a nonzero ideal. There exists $n \in \mathbb{Z}$ of minimal absolute value such that $n \in I$. WLOG assume $n > 0$. [If $n < 0$ then because $-n \in I$ so we may replace n with $-n$.] We claim that $I = n\mathbb{Z}$. It suffices to show $I \subseteq n\mathbb{Z}$.

Let $a \in I$, then by the division algorithm we can write $a = nq + r$ for some $0 \leq r < n$. Since $a, n \in I$ we have $r \in I$. However, $r < n$ implies $r = 0$. Hence $a = nq \in n\mathbb{Z}$, as desired.

Note that $n\mathbb{Z}$ is a maximal ideal if and only if n is a prime. If n is not prime, then $p \mid n$ for some prime p, so we have $n\mathbb{Z} \subsetneq p\mathbb{Z}$. Note that $\mathbb{Z}/p\mathbb{Z}$ is a field! This is true in general.

Lecture 26, 2023/07/07

17 Prime and Maximal Ideals

Definition.

18 Basic Module Theory

19 Finitely Generated Abelian Groups

20 Localization and Fraction Fields

21 The Chinese Remainder Theorem