Contents

Chapter 2

Groups

Beginning of Jan. 29, 2021

2.1 What is a Group?

Definition 2.1.1

A **group** $(G, \cdot)$ is a non-empty set G with a binary operation $\cdot : (a,b) \mapsto a \cdot b$ from $G \times G$ to G satisfying

(1) associative law: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$,

(2) identity: $\exists\, e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$, and

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

If in addition $a \cdot b = b \cdot a$ then G is **commutative** or **Abelian**. The fact that $a, b \in G \implies a \cdot b \in G$ is callused **closure**. Sometimes we omit the $\cdot$ and simply write ab.

Some examples and nonexamples of groups:

(1) $(\mathbb{Z}, +)$ is a group with identity 0 and $x^{-1} := -x$.

(2) $(\mathbb{Z} \setminus \{0\}, +)$ is *not* a group since there's no additive identity.

(3) $(\mathbb{Z}, \times)$ is *not* a group since some elements don't have inverse.

(4) $(\mathbb{Q} \setminus \{0\}, \times)$ is a group with identity 1 and inverse $x^{-1} := 1/x$.

(5) $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ is a group, where $\mathrm{GL}_2(\mathbb{R})$ (General Linear group) denotes the set of all *invertible* 2-by-2 real matrices and $\cdot$ is the normal matrix multiplication.

> ***Proof.***
>
> (1) Closure: $\det(A)\det(B) = \det(AB)$ and so AB is invertible. It's trivial that the entries are also real, so $AB \in \mathrm{GL}_2(\mathbb{R})$.
>
> (2) Associativity: matrix multiplications are already associative.

(3) Existence of identity: $I_{2\times 2}$.

(4) Existence of inverse: $(AB)^{-1} = B^{-1}A^{-1} \in \mathrm{GL}_2(\mathbb{R})$.

□

(6) $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ is a group.

(7) $(\mathrm{SL}_n(\mathbb{R}), \cdot)$ is a group where $\mathrm{SL}_2(\mathbb{R})$ is the set of n-by-n matrices with determinants 1.

(8) $(O_n(\mathbb{R}), \cdot)$ is a group where $O_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R})$ denotes all n-by-n symmetric, invertible matrices.

Definition 2.1.2

For $n \in \mathbb{Z}^+$, the **symmetric group** S_n is the group of **permutations** of n objects, i.e., the set of bijective functions from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$.

Proof that S_n is a group.

(1) Closure: pick $\sigma, \tau \in S_n$. Since the composition of bijections is bijective, we see that $\sigma \circ \tau$ is by definition another permutation of n elements.

(2) Associativity: this follows from the fact that composition of functions functions are associative.

(3) Existence of identity: the identity map $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$.

(4) Existence of inverse: the inverse σ^{-1} of bijective σ exists.

□

Beginning of Feb. 1, 2021

Example 2.1.3. Let $\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\tau := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. What is $\sigma\tau$?

Solution

$$\begin{cases} \tau(1) = 3 \\ \tau(2) = 2 \\ \tau(3) = 1 \end{cases} \text{and} \begin{cases} \sigma(1) = 2 \\ \sigma(2) = 3 \\ \sigma(3) = 1 \end{cases} \implies \begin{cases} \sigma\tau(1) = \sigma(3) = 1 \\ \sigma\tau(2) = \sigma(2) = 3 \\ \sigma\tau(3) = \sigma(1) = 2 \end{cases}$$

Remark. It's no true in general that groups are commutative / Abelian. In fact, S_3 is the smallest non-Abelian group.

What is the structure of S_3, or in general any given group? How to determine?

(1) **Cayley Table**: exhaustive method, puting multiplication table by brute force. OK for small group.

(2) **Generators**: synthetic method, using "special" elements and the relations between them to generate the rest of the group. This is called a **presentation**.

(3) **Representation theory method**: interpret the group as the symmetries of same kind of space. In practice, understanding a group often amounts to finding a nice representation.

Digression: Notation

We often use lower case Greek letters to refer to premutations: τ, σ, ρ, etc., and we formally write

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

but we usually condense the above notation into one line, named **cycle notation**. For example, consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 2 & 1 & 6 & 7 \end{pmatrix}.$$

Going from 1, we loop through $1-3-5-1$ and we write $(1\,3\,5)$. Then we have the cycle $(2\,4)$. Then (6) and finally (7). Since we've exhausted every element in the set, we are done. We write

$$\sigma = (7)(6)(2\,4)(1\,3\,5) = (2\,4)(1\,3\,5)$$

and by convention we drop all the 1-cycles.

> **Remark.** This way of writing σ is not unique. For example $\sigma = (4\ 2)(5\ 1\ 3)$ too. Also, for the cycle notations, since the cycles commute we can rearrange the cycles in any order.

Beginning of Feb. 3, 2021

Consider S_3 again. Let $\sigma := (2\,3\,1)$ and $\tau := (1\,3)$. It's not hard to verify that $\sigma^3 = \tau^2 = e$.

Speaking of its structure — $S_3 = \{e, (1\,2\,3), (1\,3\,2), (1\,2), (1\,3), (2\,3)\}$ with $\cdot$ as the bianry operation. Alternatively, S_3 consists of $e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2$. It turns out that $\tau\sigma = \sigma^2\tau$ and $\tau\sigma^2 = \sigma\tau$. A Cayley Table for S_3:

$\cdot$	1	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
e	e	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	e	$\tau\sigma^2$	τ	$\tau\sigma$
σ^2	σ^2	e	σ	$\tau\sigma$	$\tau\sigma^2$	τ
τ	τ	$\tau\sigma$	$\tau\sigma^2$	e	σ	σ^2
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	τ	σ^2	e	σ
$\tau\sigma^2$	$\tau\sigma^2$	τ	$\tau\sigma$	σ	σ^2	e

So S_3 is generated by σ and τ where $\sigma^3 = \tau^2 = e$ and $\sigma\tau = \tau\sigma^2$.

Upshot: this is a *quotient object* in the sense that S = all strings of symbols in letters "a" and "b" with R being the relation $a^2 = 1, b^2 = 1, ab = ba^2$. Then $S_3 \cong S/R$. We will write

$$S_3 = \left\langle a, b \mid a^2 = b^2 = 1, ab = ba^2 \right\rangle.$$

This is called a **presentation**.

Beginning of Feb. 5, 2021

The Representation Theory Approach

Idea: interpret G as symmetries of spaces.

Consider $\mathcal{S} = \{1, 2, 3\}$, an unstructured, finite space. Its symmetries are the permutations, i.e., elements of S_3. This is called the **permutation representation**.

On the other hand, there are other ways to represent G as symmetries of other, more structured spaces.

Example 2.1.4. Let D_n be the symmetries of a regular n-gon.

Let E be an equilateral triangle with vertices $1, 2, 3$.

(1) The trivial symmetry — doing nothing.

(2) The rotating symmetry, R — rotating the triangle for 120 degrees. $1-2-3$ to $2-3-1$.

(3) R^2, rotating the triangle by 240 degrees, to $3-1-2$.

(4) Reflection across L_1 (endpoint at 1 and bisects the opposite side), $1-2-3$ to $1-3-2$.

(5) Reflection across L_2: $1-2-3$ to $3-2-1$.

(6) Reflection across L_3: $1-2-3$ to $2-1-3$.

Now we have $D_3 = \{1, R, R^2, F_1, F_2, F_3\}$. And we have $G = \left\langle a, b \mid a^3 = b^2 = e, ab = ba^2 \right\rangle$.

The relationship? Consider the mapping $G \to D_3$ by $a \mapsto R$ and $b \mapsto F_2$. It's easy to check that $a^3 = b^2 = e$ and $b = ba^2$. That we represented a by rotation and b by reflection is called a **linear representation**.

The algebraic objects are rigid but "unstructured", but the representation theory approach interprets or "structures" algebraic objects.

(1) Say we have $A \in \mathrm{GL}_2(\mathbb{R})$. It's a mapping that acts on $\mathbb{R}^2$.

(2) What kind of group can we say about $\mathrm{GL}_n(\mathbb{R})$? It represents symmetries on $\mathbb{R}^n$.

(3) For example, consider $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ a nontrivial rotation matrix and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ a reflection matrix across the 45° line. It's easy to verify that $BAB^{-1} = A^{-1}$.

(4) Now we let the rotation matrix to be a and the reflection matrix b. It follows that we just represented the group $\left\langle a, b \mid a^4 = b^2 = 1, bab^{-1} = a^{-1} \right\rangle$ by symmetries (of D_4) on $\mathbb{R}^2$, with a, b being those two matrices.

Beginning of Feb. 8, 2021

Remark. Fact, to be shown later: every group can be represented as a group of symmetries on $\mathbb{R}^n$ for some n. However sometimes these representations can be extremely complex, e.g., the monster group.

Another example: take C_n the cyclic group $\langle g \rangle := \langle g \mid g^n = 1 \rangle$. A nice presentation of this is by roots of unity, a matrix group of form

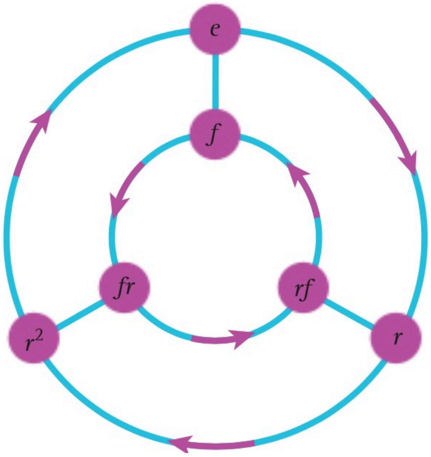
$$\begin{bmatrix} \cos 2\pi/n & -\sin 2\pi/n \\ \sin 2\pi/n & \cos 2\pi/n \end{bmatrix}.$$

Cayley Graphs

(1) Start with $S \subset G$ that generates G. For example for $D_3 = \langle a, b \mid a^2 = b^3 = 1, a^2b = ba \rangle$ we start with $\langle a, b \rangle$.

(2) Draw a Cayley graph by drawing edges connecting vertex g to sg for $s \in S$ starting with e. See p.53 on book.

(3) Leave arrows that only go one direction. Drop the ones that go both directions.



Cayley graph of D_3

2.3 More examples on Groups and Some Basic Facts

$\mathbb{Z}/n\mathbb{Z}$ is can be viewed as a cyclic group of order n and represented by the rotation matrices of $2\pi/n$.

Definition 2.3.1

The **group of units mod n**, $(\mathbb{Z}/n\mathbb{Z}^\times, \cdot)$ is defined by

$$\mathbb{Z}/n\mathbb{Z}^\times = \{[a] \mid \gcd(a, n) = 1\}.$$

The operation is defined by $[a][b] := [ab]$. We call these elements **units** in $\mathbb{Z}/n\mathbb{Z}$.

Beginning of Feb. 10, 2021

Notice that $\mathbb{Z}/n\mathbb{Z}^\times$ = the collection of $[a]$'s where there exists b such that $ab \equiv 1 \pmod{n}$ (by Bezout's identity).

Definition 2.3.2

$|\mathbb{Z}/n\mathbb{Z}|^\times$ is defined as to be the **Euler φ-function**, $\varphi(n)$.

Theorem 2.3.3

If $x = \prod_{i=1}^{k} p_i^{e_i}$ then $\varphi(x) = x \cdot \prod_{i=1}^{k}(1 - 1/p_i)$.

Example 2.3.4. The **general linear group** $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ with p prime is defined as

$$\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z}) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad \cdot bc \in \mathbb{Z}/p\mathbb{Z}^{\times} \right\}$$

under matrix multiplication.

Remark. What about the size of $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$. The first row can be anything but $[0\ 0]$ so there are $p^2 - 1$ options. Once the first row has been determined, since the second row can be anything besides a scalar multiple of the first row (including 0 times it), there are $p^2 - p$ options. Multiplying them together we get $(p^2 - 1)(p^2 - p)$ distinct elements in this group. The cardinality of $\mathrm{GL}(n, \mathbb{Z}/p\mathbb{Z})$ is

$$(p^n - 1)(p^n - p) \ldots (p^n - p^{n-1}).$$

Theorem 2.3.5

$a \in G$ has a unique inverse.

Proof. Suppose b and c are both inverses. Then

$$b = b(ac) = (ba)c = c.$$

□

Corollary 2.3.6

Every row of the multiplication table of a finite group is a permutation of the first row.

Proof. Define a function $L_a : G \to G$ by $g \mapsto ag$. Then L_a is injective by cancellation law. L_a is surjective because bg^{-1} is always a solution to $ag = b$.. Then every row is a permutation of the first as L_a is bijective. □

Beginning of Feb. 12, 2021

2.4 Subgroups

Definition 2.4.1

A subset $H \subset G$ of a group G that also satisfies the group axioms is a **subgroup** of G. If $H \neq \{e\}$ and $H \neq G$ then it's a **proper subgroup**; otherwise it's called a **trivial subgroup**.

We have seen many examples of subgroups already:

(1) $\{1, (13)\}$ is a subgroup of S_3 since $(13)^2 = 1$.

(2) $\{1, (123), (132)\}$ is another subgroup of S_3.

(3) D_4 is a subgroup of S_4: think of labelling the edges of a square by $1, 2, 3, 4$ – obviously a permutation.

Definition 2.4.2

The **integer powers** of an element $a \in G$ are elements of form a^n where n is an integer. Immediately notice that $a^{-n} = (a^{-1})^n$.

Definition 2.4.3

The **order** of an element $a \in G$, written $o(a)$, is the smallest positive integer n such that $a^n = e$. If there is no such n, we define $o(a) := \infty$.

Proposition 2.4.4: Two-Step Subgroup Test

Suppose G is a group and $H \subset G$ such that $H \neq \varnothing$. If, for all $a, b \in H$,

(1) $a \cdot b \in H$, and

(2) $a^{-1} \in H$,

then H is a subgroup of G.

Corollary 2.4.5: One-Step Subgroup Test

Same as above, except the condition is that for all $a, b \in H$, $ab^{-1} \in H$.

Proof. If $H \neq \varnothing$ then there exists $a \in H$. Therefore $aa^{-1} = e \in H$. We have identity.
Now for $b \in H$, $eb^{-1} = b^{-1} \in H$. Inverse exists.
Finally, for $a, b \in H$, $a(b^{-1})^{-1} = ab \in H$, closure. □

Example 2.4.6. The (unique) cyclic subgroups of the additive group $(\mathbb{Z}/8\mathbb{Z}, +)$ include $\langle [0] \rangle, \langle [1] \rangle$, $\langle [2] \rangle$, $\langle [4] \rangle$.

Definition 2.4.7

The **center** of a group G is

$$Z(G) := \{a \in G \mid ax = xa \text{ for all } x \in G\},$$

i.e., "the largest Abelian component" that commutes with everything in the group.

Proposition 2.4.8

$Z(G)$ is a commutative subgroup of G.

Proof. Commutativity is clear. It remains to show $Z(G)$ is indeed a subgroup. We'll use the two-step test, i.e., showing it's closed under multiplication and has inverses.
For inverses, pick $a \in Z(G)$ (it's not empty; at least the identity is inside it). By assumption $ax = xa$ for all

$x \in G$, and so

$$a^{-1}ax = a^{-1}xa \implies x = a^{-1}xa \implies xa^{-1} = a^{-1}xaa^{-1} = a^{-1}x \text{ for all } x \in G.$$

For closure, take $a, b \in Z(G)$. Then

$$abx = a(bx) = a(xb) = (ax)b = (xa)b = xab \implies ab \in Z(G).$$

□

Example 2.4.9. We now show that the center of S_n, $n \geqslant 3$, is trivial, i.e., just the identity. Pick arbitrary $\sigma \neq e$. Then for some $i \neq j$ we have $\sigma(i) = j$. Now let $k \neq i, j$. Now define $\tau := (ik)$, i.e., $\tau(i) = k$ and $\tau(k) = i$. Then

$$\sigma(\tau(i)) = \sigma(k) \neq j \text{ since } \sigma(i) = j, \text{ and } \tau(\sigma(i)) = \tau(j) = j.$$

Then σ and τ are not commutative! Therefore only $e \in Z(S_n)$. □

Beginning of Feb. 17, 2021

Example 2.4.10. Let $G = \mathrm{GL}(2, \mathbb{R})$. Find $Z(G)$.

Claim: the center only consists of (nonzero) scalar multiples of I. Indeed the set of multiples of I is a subset of G. Now we show the other inclusion. Assume

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(G).$$

Then,

$$uw \neq 0 \implies \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} u & v \\ 0 & w \end{bmatrix} = \begin{bmatrix} u & v \\ 0 & w \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

(We picked the bottom-left entry of the arbitrary matrix to be 0 to simplify the calculations.) Then

$$\begin{bmatrix} au & av + bw \\ cu & cv + dw \end{bmatrix} = \begin{bmatrix} au + cv & bu + dv \\ cw & dw \end{bmatrix}$$

Since $au = au + cv$ and $vw \neq 0$ we know $c = 0$. Similarly using $\begin{bmatrix} u & 0 \\ v & w \end{bmatrix}$ one can show $b = 0$. Then $av + bw = bu + dv \implies av = dv \implies a = d$.

2.5 Cyclic Groups

Definition 2.5.1

A group G is **cyclic** if it's generated by some $a \in G$, i.e., $G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$.

Proposition 2.5.2

Assume $G = \langle a \rangle$ with $o(a) = n$, then

(1) $a^i = a^j \iff i \equiv j \pmod{n}$,

(2) $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$,

(3) $a^k = e \implies n \mid k$,

(4) $\left\langle a^k \right\rangle = \langle a \rangle \iff \gcd(n,k) = 1$,

(5) $\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle$, and

(6) $|a^k| = n/\gcd(n,k)$.

We use the above propositions to prove the following important fact:

Theorem 2.5.3

Suppose G is a finite cycle group of order $|G|$. Then,

(1) Any subgroup H of G is cyclic,

(2) The order of any subgroup divides that of G, i.e., $|H| \mid |G|$ (Lagrange),

(3) For every divisor d of $|G|$, there is a unique subgroup of order d. If $G = \langle a \rangle$ then such subgroup is $H = \left\langle a^{n/d} \right\rangle$.

Proof of (1). Suppose $G = \langle a \rangle$ and pick any H other than $\{e\}$. Let m be the smallest positive integer such that $a^m \in H$. Pick $a^t \in H$. By division algorithm, $t = mq + r$ where $0 \leqslant r < m$. Therefore

$$a^r = a^{t-mq} = a^t a^{-mq}$$

and so the RHS $\in H$. Since $r < m$ the only possibility if the LHS $\in H$ is if $r = 0$, i.e., a^t is a power of a^m. Hence $H = \langle a^m \rangle$. □

Beginning of Feb. 19, 2021

Example 2.5.4. Since $(\mathbb{Z}/9\mathbb{Z}, \times)$ has order 6, in fact $(\mathbb{Z}/9\mathbb{Z}, \times) \cong (\mathbb{Z}/6\mathbb{Z}, +)$.

Proof of (3). Assume $d \mid n := |G|$. Then $\left\langle a^{n/d} \right\rangle$ has order d since $(n/d)/\gcd(n, n/d)$ is indeed d. Now for uniqueness, suppose $\langle a^m \rangle$ is another subgroup of G of order d. By (5) in the previous theorem,

$$\langle a^m \rangle = \left\langle a^{\gcd(m,n)} \right\rangle =: \left\langle a^k \right\rangle = K.$$

Immediately we see $k \mid n$. Notice that $d = o(a^k) = n/\gcd(n,k) = n/k$, so indeed $n/d = k$. □

Theorem 2.5.5

Assume $G = \langle a \rangle$ where $o(a) = n < \infty$. If $d \mid n$ then the number of elements of order d is $\varphi(d)$.

Proof. By (3) above, there is a unique subgroup $H = \langle b \rangle$ with $|H| = d$. Any other element with order d must also be in H or else it generates some H', contradicting uniqueness of H. □

Example 2.5.6. If p is a prime then $(\mathbb{Z}/p\mathbb{Z}, +)$ has $\varphi(p) = p - 1$ generators since any positive integer $< p$ is coprime with p.

Example 2.5.7. We later prove $\mathbb{Z}/p\mathbb{Z}^\times$ is cyclic. For now, notice that $\mathbb{Z}/p\mathbb{Z}^\times$ has order $p - 1$, but $\underline{\text{not}}$ all elements of $\mathbb{Z}/p\mathbb{Z}^\times$ are **primitive roots**. A characterization of when this is true — if and only if $n = 2, 4, p^r$, or $2p^r$ where p is an odd prime. [*430 flashback intensifies*]

Chapter 3

More on Groups

3.1 Groups of Permutations

Beginning of Feb. 22, 2021

Proposition 3.1.1

(1) Each permutation in S_n can be written as product of disjoint cycles.

(2) Disjoint cycles commute.

(3) The order of a product of disjoint cycles is the lcm of the cycle lengths.

Quick proof: $(\alpha\beta)^k = \alpha^k\beta^k = e \iff \alpha^k = \beta^k = e$.

Note that if

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

then

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Also notice that (in cycle notation) $(a_1a_2\dots a_n)^{-1} = (a_ra_{r-1}\dots a_1)$.

We now try to rewrite “big” permutations into small permutations which are called permutations.

Definition 3.1.2

A permutation (ab) is called a **transposition** or **2-cycle** if it permutes two elements. If σ can be written as an even number of tranpositions it is an **even permutation**, otherwise an **odd permutation**. In fact, the **parity** (even or odd) is unique.

Note that every permutation can be broken down into products of transpositions:

$$(x_1x_2\dots x_n) = (x_1x_n)(x_1x_{n-1})\dots(x_1x_2).$$

Lemma 3.1.3

Every transposition can be written as a product of an odd number of adjacent transpositions.

Proposition 3.1.4

The notion of even and oddness of a permutation is well defined. (Parity is unique.) Suppose $\sigma = \alpha_1\alpha_2\dots\alpha_r$ and $\sigma = \beta_1\beta_2\dots\beta_s$, then $r \equiv s \pmod 2$.

Proof. Define

$$V(x_1,\dots,x_n) \coloneqq \prod_{1\leqslant i<j\leqslant n}(x_i - x_j)$$

and define the **action** of a permutation $\sigma \in S_n$ on the polynomial by

$$(\sigma V)(x_1,\dots,x_n) = V(x_{\sigma(1)}, x_{\sigma(2)},\dots,x_{\sigma(n)}).$$

Notice that whatever appears as $x_i - x_j$ also appears as some $x_{\sigma(m)} - x_{\sigma(n)}$ so $V(x_1,\dots,x_n)$ and $(\sigma V)(x_1,\dots,x_n)$ differ by at most the sign. We define

$$\operatorname{sgn}(\sigma) = \frac{V(x_{\sigma(1)}, x_{\sigma(2)},\dots,x_{\sigma(n)})}{V(x_1,x_2,\dots,x_n)}.$$

In particular, if we can show

$$(\sigma V)(\cdot) = \operatorname{sgn}(\sigma)V(\cdot) \text{ where } \operatorname{sgn}(\sigma) = \begin{cases} 1 & \sigma \text{ even} \\ -1 & \sigma \text{ odd} \end{cases}$$

then the proposition follows. Below we will show some propositions related to $\operatorname{sgn}(\sigma)$ (so no QED yet!). □

Proposition 3.1.5

Suppose $\alpha, \beta, \sigma \in S_n$. Then

(1) $\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$:

$$\begin{aligned}\operatorname{sgn}(\alpha\beta) &= \frac{V(x_{\alpha\beta(1)},\dots,x_{\alpha\beta(n)})}{V(x_1\dots,x_n)} = \frac{V(x_{\alpha(\beta(1))},\dots,x_{\alpha(\beta(n))})}{V(x_{\beta(1)},\dots,x_{\beta(n)})}\cdot\frac{V(x_{\beta(1)},\dots,x_{\beta(n)})}{V(x_1,\dots,x_n)} \\ &= \operatorname{sgn}(\alpha)(\operatorname{sgn}(\beta).\end{aligned}$$

(2) sgn of a transposition is -1. (Odd number of products of adjacent transpositions.)

(3) $\operatorname{sgn}(\sigma)$ is (-1) raised to the power of number of transpositions of σ. This proves the previous proposition, as the sign of σ cannot vary.

Beginning of Feb. 24, 2021

Definition 3.1.6

The **alternating group** is $A_n : \{\sigma \in S_n \mid \sigma \text{ is even}\}$.

Remark. One immediately sees that A_n is a subgroup of S_n. Pick $\sigma, \tau \in A_n$ where $\sigma = \alpha_1 \dots \alpha_r$ and $\beta = \beta_1 \dots \beta_s$ (product of transpositions). Then $\sigma\tau$ is simply the product of $r + s$ transpositions, and the inverse is simply the product of inverse, in the reverse order.

Proposition 3.1.7

$|A_n| = |S_n|/2$.

Proof. Define $T : A_n \to S_n \smallsetminus A_n$ by $T(\sigma) = (12)\sigma$. This is a bijection.
Injective: if $T(\sigma) = T(\tau)$, i.e., $(12)\sigma = (12)\tau$. Then $(12)^2\sigma = (12)^2\tau \implies \sigma = \tau$.
Surjective: if $\tau \in S_n \smallsetminus A_n$ then $(12)\tau \in A_n$ and $(12)[(12)\tau] = \tau$. □

3.2 Isomorphisms and Cayley's Theorem

Now we start talking about structures of groups.

Definition 3.2.1

Suppose G and G' are groups. A function $T : G \to G'$ is called a **group isomorphism** if an only if T is bijective and it preserves group operations, i.e., for $x, y \in G$,

$$T(xy) = T(x)T(y).$$

If such T exists, we say G is **isomorphic to** G', written $G \cong G'$.

An intuitive example includes the isomorphism between the cyclic group C_n and $(\mathbb{Z}/n\mathbb{Z}, +)$. Indeed, the map $T : \mathbb{Z}/n\mathbb{Z} \to C_n$ defined by $[k] \mapsto a^k$ is a bijection. (Notice that this is well-defined since if $[x] = [y]$ then $n \mid x - y$ and thus $a^x = a^y$.)

Beginning of March 1, 2021

Remark. It is possible that two sets have the same cardinality (i.e., there exists a bijection) but are not isomorphic. For example $(\mathbb{Z}/6\mathbb{Z}, +)$ is abelian while S_3 is not. If there were an isomorphism T from $\mathbb{Z}/6\mathbb{Z} \to S_3$ then $xy = yx \implies T(xy) = T(yx) \implies T(x)T(y) = T(y)T(x)$ for all $T(x), T(y) \in S_3$.

Immediately, we have the following results:

(1) An isomorphism sends identity to identity. *Indeed,* $T(x) = T(xe) = T(x)T(e)$ *where the first equality is from the fact that* $x = xe$*, and likewise for the other direction.*

(2) For all $x \in G$ and $T : G \to G'$ isomorphic, $T(x^{-1}) = (T(x))^{-1}$.

(3) The order of $T(x) \in G'$ is the same as the order of $x \in G$. *Trivial since* $T(x^{-1}) = T(x^{-1})T(x) = e' \in G'$.

Theorem 3.2.2: Cayley's Theorem

If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Proof. Recall that for any $g \in G$ we have a bijection $L_g : G \to G$ defined by $x \mapsto gx$. Notice that this L_g permutes elements of G (maybe some, maybe all).

Let $\{g_1, \dots, g_n\}$ be an enumeration of G. Let σ_a be the permutation such that $L_a(g_i) = ag_i := g_{\sigma_a(i)}$ where $a \in G$ is chosen arbitrarily. Notice that such $\sigma_a \in S_n$ is unique since G is a group and cancellation holds.

We define $T : G \to S_n$ by $a \mapsto \sigma_a$. Notice that T is injective. If $\sigma_a = \sigma_b$, picking $g_k = e$ gives $a = ag_k = g_{\sigma_a(k)} = g_{\sigma_b(k)} = b$. In addition, it preserves group structure: for any g,

$$g_{\sigma_{ab}(i)} = abg_i = a(bg_i) = a(g_{\sigma_b(i)}) = g_{\sigma_a \circ [\sigma_b(i)]},$$

which implies $T(ab) = \sigma_{ab} = \sigma_a\sigma_b = T(a)T(b)$. Clearly $T(G)$ being a subgroup is trivial. □

Beginning of March 3, 2021

Definition 3.2.3

A **group homomorphism** from $(G, *)$ to $(G', \cdot)$ is a function $f : G \to H$ satisfying

$$f(u * v) = f(u) \cdot f(v).$$

Definition 3.2.4

An isomorphism from $(G, \cdot)$ to itself is called an **automorphism**, and such function is called a **group automorphism**. Set set of all automorphisms of G is called $\text{Aut}(G)$ which forms a group under compositions of functions.

Definition 3.2.5

Take a fixed element $g \in G$. Define its **conjugation funtion** $C_g(x) := g^{-1}xg$ for all $x \in G$. Claim: $C_g : G \to G$ is an automorphism.

Proof. We check its an isomorphism. Suppose $g^{-1}xg = g^{-1}yg$, then applying g on the left and g^{-1} on the right we obtain $x = y$ and so C_g is injective. For surjectivity: pick $y \in G$. Notice that for $gyg^{-1} \in G$ we have $C_g(gyg^{-1}) = g^{-1}gygg^{-1} = y$. Now for preservation of group structure:

$$C_g(xy) = g^{-1}xyg = (g^{-1}xg)(g^{-1}yg) = C_g(x)C_g(y).$$

□

Remark. Automorphisms defined this way are called **inner automorphisms**, written $\text{Inn}(G)$. Those that are not are **outer automorphisms**, written $\text{Out}(G)$.

There are automorphisms that are not detectable inside G. For example: $G = GL(2, p^n)$ with $T : G \to G$ defined by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a^p & b^p \\ c^p & d^p \end{bmatrix}$$

is not detectable by conjugation. But by FLT, $a \equiv a^p \pmod{p}$ suggests this is an automorphism.

Note that if the group is abelian, the C_g is not so interesting, since $g^{-1}xg = x$. Thus, for an abelian group, $\operatorname{Inn}(G)$ simply consists of the identity mapping.

Definition 3.2.6

If $y = g^{-1}xg$ for some $g \in G$, we say that x and y are **conjugate elements** of G.

One very useful notion in group theory:

Definition 3.2.7

The **conjugacy class** of an element x in a group G is

$$x^G = \{g^{-1}xg \mid g \in G\}.$$

Recall the definition of similar matrices. A and B are similar if for some C we have $A = C^{-1}BC$, and the idea is that A and B refer to the same transformation up to some change in basis. Properties of similar matrices include same eigenvalues or same characteristic polynomials.

Beginning of March 5, 2021

3.3 Cosets, Lagrange's Theorem, & Normal Subgroups

Consider how we partitioned $\mathbb{Z}$ into $\mathbb{Z}/n\mathbb{Z}$. We want to generalize this to arbitrary groups. The first part is to come up with an equivalence relation.

Definition 3.3.1

If H is a subgroup of G, and $g \in G$, we say that a **left coset** of H is a set of form $gH = \{gh \mid h \in H\}$. Similarly, the **right coset** is defined by $Hg = \{hg \mid h \in H\}$. The set of all left cosets is written G/H and the set of all right cosets as $H \backslash G$.

Note that gH is simply the image of H under left multiplication L_g. These cosets will give us the equivalence classes we want to "divide" G.

Example 3.3.2. Let $G = (\mathbb{Z}, +)$. Let $H = n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$. The left cosets G/H are $\mathbb{Z}/n\mathbb{Z}$.

$$[0] = 0 + n\mathbb{Z}, [1] = 1 + n\mathbb{Z}, [2] = 2 + n\mathbb{Z}, \ldots$$

All of these $[\cdot]$ are cosets.

Example 3.3.3. Let $G = (\mathbb{Z}/15\mathbb{Z}^{\times}, \cdot)$ and $H = \langle [4] \rangle$. We know

$$G = \{[1],[2],[4],[7],[8],[11],[13],[14]\} \text{ and } H = \{[4],[1]\}.$$

For the cosets:

$$\begin{aligned}
[1]H &= H \\
[2]H &= \{[2],[8]\} \\
[4]H &= \{[1],[4]\} = [1]H \\
[7]H &= \{[13],[7]\} \\
[8]H &= \{[2],[8]\} = [2]H \\
[11]H &= \{[14],[11]\} \\
[13]H &= \{[7],[13]\} = [7]H \\
[14]H &= \{[11],[14]\} = [11]H
\end{aligned}$$

Therefore there are four (distinct) cosets and so $G/H = \{[1]H, [2]H, [7]H, [11]H\}$.

Proposition 3.3.4

Suppose H is a subgroup of a finite group G. The following are true.

(1) $|H| = |Hg| = |gH|$ for all $g \in G$. *Trivial by the bijectivity of $L_g : H \to gH$.*

(2) We have an equivalence relation on G by

$$x \sim y \text{ if and only if } x^{-1}y \in H.$$

The equivalence classes are just the (left) cosets of H.

(3) $|G/H| = |G|/|H|$. *By the previous parts, G is a disjoint union of cosets of the same order. We'll cover this next time.*

Beginning of March 8, 2021

Theorem 3.3.5: Lagrange's Theorem

Suppose H is a subgroup of a finite group G. Then $|H|$ divides $|G|$.

Corollary 3.3.6

(1) If G is a finite group, then the order of any $g \in G$ divides $|G|$. *Proof: consider $\langle g \rangle$ and apply Lagrange.*

(2) Any G of prime order is cyclic. *Proof: subgroup has order 1 or $|G|$. Then $a \neq e \implies \langle a \rangle = G$.*

(3) **Fermat's Little Theorem**. If $a \in \mathbb{Z}/p\mathbb{Z}$ with p prime then $a^p \equiv a \pmod{p}$.

Proof. Trivial if $a \equiv 0 \pmod{p}$. *If* $a \not\equiv 0 \pmod{p}$ *then* $a \in \mathbb{Z}/p\mathbb{Z}^\times$ *and thus* $o(a)$ *divides* $|\mathbb{Z}/p\mathbb{Z}^\times| = p - 1$. *Therefore* $a^{p-1} \equiv 1 \pmod{p} \implies a^p \equiv a \pmod{p}$.

Definition 3.3.7

A subgroup H of G is called a **normal subgroup** if and only if $g^{-1}Hg = H$ for all $g \in G$. In other words, for all $g \in G$ we have $H = \{g^{-1}hg \mid h \in H\}$. The notation is $H \lhd G$.

Proposition 3.3.8

The following are equivalent:

(1) H is a normal subgroup of G.

(2) Every right coset is a left coset.

(3) Every right coset Hg is exactly the coset corresponding to the same g, i.e., $Hg = gH$ for all $g \in H$.

Proof. (3) $\implies$ (2) is trivial. (2) $\implies$ (3) needs some justification. Assume $g'H = Hg$. We know $e \in H$, so $eg = g \in Hg$. Thus $g \in g'H$. Notice that $g \in gH$ as well. Since cosets form a partition, the only possibility is if $gH = g'H$.

(3) $\implies$ (1): assume $Hg = gH$ for all $g \in G$. Then left-multiplying everything by g^{-1} gives $g^{-1}Hg = g^{-1}gH = H$. Hence H is normal. □

Beginning of March 10, 2021

Example 3.3.9. $Z(G)$, the center of G is always a normal subgroup of G. Obviously true, since $a \in Z(G)$ commutes with all $g \in G$ and thus $g^{-1}ag = g^{-1}ga = a$.

Example 3.3.10. The group generated by r is normal in D_3, i.e., $\langle r \rangle \lhd D_3$. (Refer to HW5: index 2 subgroups are normal.)

Proof. Decall that $D_3 = \left\langle r, f \mid r^3 = f^2 = 1, frf = r^2 \right\rangle$. Conjugation by r is clearly trivial. If we conjugate by f, then $fr^nf = (frf)^n$ since $f = f^{-1}$ and the middle f's cancel out. Since $frf = r^2$ in D_3, clearly the conjugated element is still in $\langle r \rangle$. □

3.4 Quotient Groups G/H

Definition 3.4.1

If H is a normal subgroup of G, we define the **quotient group** G/H to be the set G/H of left cosets with multiplication $(aH)(bH) = (ab)H$ for $a, b \in G$.

Theorem 3.4.2

If G is a group and H a normal subgroup, then the above defines a group.

Proof. Closure under multiplication: pick $aH, bH \in G/H$. Then $(aH)(bH) = a(bH)H = abH$ since $Hb = bH$ as H is normal.

Identity: H itself (or equivalently eH). Obviously $aHeH = aeH = eaH = eHaH$.

Inverse: for clarity, define $S^{-1} = \{s^{-1} \mid s \in S\}$. Notice that $H^{-1} = H$. The inverse of $aH = a^{-1}H$ as $(a^{-1}H)(aH) = a^{-1}aHH = H$ and $(aH)(a^{-1}H) = aa^{-1}HH = H$.

Associativity follows directly from that of G and $H \triangleleft G$. □

Example 3.4.3. Let $G = D_3$ and $H = \langle r \rangle$. Then $G/H = \{\langle r \rangle, f\langle r \rangle\}$.

Beginning of March 15, 2021

Example 3.4.4. Consider $G = \mathrm{Aff}(5)$ and H the subgroup generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. (This is normal.) Below we compute G/H.

Since $|G| = 4 \cdot 5 = 20$ and $|H| = 5$, $|G/H| = 4$. The identity of $G/H = H$. The other three elements in G/H are left cosets left multiplied by

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix}.$$

Notice that the multiplication table of G/H looks very nice!

$$\begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} H \cdot \begin{bmatrix} y & 0 \\ 0 & 1 \end{bmatrix} H = \begin{bmatrix} xy & 0 \\ 0 & 1 \end{bmatrix} H,$$

where xy is taken modulo 5. Note that $G/H \cong \mathbb{Z}/5\mathbb{Z}^\times \cong \mathbb{Z}/4\mathbb{Z}$, and $H \cong \mathbb{Z}_5$. However, G is much more complicated than either H or G/H, and this is what makes algebra much harder.

Definition 3.4.5

A **simple** group G is a group whose only normal subgroups are $H = \{e\}$ and $H = G$.

The classification of all finite simple groups was one of the major projects during the 20th century.

Beginning of March 17, 2021

3.5 Group Homomorphisms

Definition 3.5.1

If G and G' are groups, a function $T : G \to G'$ is called a **group homomorphism** if and only if $T(xy) = T(x)T(y)$ for all $x, y \in G$.

Example 3.5.2. Isomorphism is much stronger than homomorphism. Consider $T : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $n \mapsto [n]$. Clearly this is not injective and thus not an isomorphism. However, we indeed have $[x + y] = [x] + [y]$, and thus T is a homomorphism.

Example 3.5.3. Consider $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^x$ with $A \mapsto \det(A)$. This is obviously not injective but, yes, again, it is a homomorphism.

Example 3.5.4. Consider $S_n \mapsto \{\pm 1\}$ by $\sigma \mapsto \mathrm{sgn}(\sigma)$. Again, not injective but indeed a homomorphism.

It follows naturally that we want to know how "far" T is from being injective.

Definition 3.5.5

Suppose G, G' are groups and $T : G \to G'$ is a group homomorphism. The **kernel** of T, written $\ker(T)$, is defined by

$$\ker(T) = \{g \in G \mid T(g) = e'\}$$

where e' is the identity of G'.

Lemma 3.5.6

$T : G \to G'$ is injective if and only if $\ker(T) = \{e\}$.

Proof. For $\Longrightarrow$, assume T is injective. First we show $T(e) = e'$:

$$T(e)T(x) = T(ex) = T(x) \implies T(e) = e'.$$

On the other hand, $\ker(T) = \{e\}$ the singleton because T is injective, namely there can only be one element in G that gets sent to $e' \in G'$.

For $\Longleftarrow$, assume $\ker(T) = \{e\}$. Note that $T(x^{-1})T(x) = T(x^{-1}x) = T(e) = e'$ and likewise $T(x)T(x^{-1}) = e'$. Therefore if $T(x) = T(y)$ then $T(x)(T(y))^{-1} = T(x)T(y^{-1}) = e'$ and so $xy^{-1} = e$, namely that $y^{-1} = x^{-1}$. Hence $y = (y^{-1})^{-1} = (x^{-1})^{-1} = x$. □

Lemma 3.5.7

If G, G' are groups and $T : G \to G'$ is a group homomorphism, then $\ker(T)$ is a normal subgroup of G.

Proof. Two steps: showing that $\ker(T)$ is a subgroup and that $\ker(T) \lhd G$.

For the first one, we use the one-step test ($ab^{-1} \in \ker(T)$). Suppose $x, y \in \ker(T)$. Then

$$T(xy^{-1}) = T(x)T(y^{-1}) = T(x)(T(y))^{-1} = e'(e')^{-1} = e'.$$

Now it remains to show that $g^{-1}(\ker(T))g = \ker(T)$. Let $g \in G$ be given and pick any $x \in \ker(T)$. Then

$$T(g^{-1}xg) = T(g^{-1})T(x)T(g) = T(g^{-1})T(g) = T(g^{-1}g) = e'$$

and so $g^{-1}(\ker(T))g \subset \ker(T)$. For the other direction, simply notice that

$$g^{-1}(\ker(T))g \subset \ker(T) \implies g\left[g^{-1}(\ker(T))g\right]g^{-1} \subset g(\ker(T))g^{-1}.$$

This is equivalent to $\ker(T) \subset \tilde{g}^{-1}(\ker(T))\tilde{g}$ since $\tilde{g}$ is arbitrarily chosen. (If we pick $\tilde{g} \in G$, simply let $g := \tilde{g}^{-1}$.) □

Example 3.5.8. Recall the map $T : S_n \to \{\pm 1\}$ by $\sigma \mapsto \operatorname{sgn}(\sigma)$. The kernel is the set of even permutations, i.e., A_n, and thus $\underline{A_n \text{ is normal!}}$

Example 3.5.9. Let $F : \{f : \mathbb{R} \to \mathbb{R}\}$ and $D : \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ differentiable everywhere}\}$. Let both have function addition, i.e., $f(x) + g(x) = (f+g)(x)$. Define $T : D \to F$ by $f \mapsto f'$. This is a homomorphism. The identity of F is the zero function, so $\ker(T)$ is the set of constant functions.

Definition 3.5.10

Suppose G, G' are groups and $f : G \to G'$ is a group homomorphism. The **image group** of G under f is

$$f(G) := \{f(x) \mid x \in G\}.$$

Check: this is a group.

Theorem 3.5.11: First Isomorphism Theorem

Suppose G, G' are groups and $f : G \to G'$ is a group homomorphism. Then the quotient group $G/\ker(f)$ is isomorphic to the image group under the mapping

$$F : G/\ker(f) \to f(G) \text{ defined by } g\ker(f) \mapsto f(g).$$

We will prove this theorem next lecture. For now, some examples first.

Example 3.5.12. Consider $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $m \mapsto [m]$. Then $\ker(f) = n\mathbb{Z}$. The FIT says that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}. \text{ Okay...}$$

Example 3.5.13. Let $G := (\mathbb{R}, +)$ and $G' := (\{x \in \mathbb{C} \mid |x| = 1\}, \cdot)$. Let $f : G \to G'$ be defined as $x \mapsto e^{2\pi i x}$.

Then $\ker(f) = \mathbb{Z}$ and $f(G) = S^1$. Then the FIT says

$$\mathbb{R}/\mathbb{Z} \cong S^1[!!]$$

Beginning of March 19, 2021

Proof of the F.I.T.. For simplicity denote $\ker(f)$ by K. First notice that $F : G/K \to f(G)$ is well-defined. Indeed, if $aK = bK$ then $be = ax$ for some $x \in K$. Then, since $K = \ker(f)$,

$$F(bK) = F(axK) = f(ax) = f(a)f(x) = f(a) = F(aK).$$

To show that F is a homomorphism:

$$F[(aK)(bK)] = F(abK) = f(ab) = f(a)f(b) = F(aK)F(bK).$$

To show that F is bijective (in fact, injective suffices as surjectiveness in this definition is trivial). Suppose $F(aK) = F(bK)$. Then $f(a) = f(b)$ and thus $f(ab^{-1}) = e' \implies ab^{-1} \in K$. Therefore $b = ax$ for some $x \in K$ and thus

$$bK = axK = aK \implies f \text{ is injective.}$$

□

Theorem 3.5.14: Third Isomorphism Theorem

Suppose $H \triangleleft K, H \triangleleft G$, and $K \triangleleft G$. Then

$$G/K \cong (G/H)/(K/H).$$

Proof. We first show that $(G/H)/(K/H)$ is well-defined:

$$(gH)^{-1}(kH)(gH) = g^{-1}kgH \in K/H$$

since $K \triangleleft G \implies g^{-1}kg \in K$.

Let $T : G/H \to G/K$ be defined by $gH \mapsto gK$. (Check that T is a homomorphism.) Also, T is guaranteed to be surjective as any gK is the image of $T(gH)$. Therefore $T(G/H) = G/K$. By the F.I.T.,

$$(G/H)/\ker(T) \cong G/K.$$

Therefore it remains to show that $\ker(T) = K/H$. What is the kernel though? It contains all the gH such that $gK = K$. What does this tell us? $gK = K$ if and only if $g \in K$, i.e., $gH \in \ker(T)$ if and only if $gH \in K/H$. Therefore $\ker(T) = K/H$ and we are done! □

3.6 Direct Product of Groups

Definition 3.6.1

Give G, H groups, we define a larger group consisting of ordered paired called the **direct product** (or sum) of G and H, denoted $G \oplus H$ (or $G \times H$), defined by

$$G \oplus H = \{(g,h) \mid g \in G, h \in H\}$$

with the operation of component-wise multiplication: $(g,h)(g',h') = (gg',hh')$.

Example 3.6.2. Consider $G := \mathbb{R} \oplus \mathbb{R}$ and $T := (\{x \in \mathbb{C} \mid |x| = 1\}, \cdot)$ and define $G := T \oplus T$. Define $\rho : G \to G'$ by

$$(x,y) \mapsto (e^{2\pi i x}, e^{2\pi i y}).$$

Then $\ker(\rho) = \mathbb{Z} \oplus \mathbb{Z}$, and by the F.I.T.,

$$(\mathbb{R} \oplus \mathbb{R})/(\mathbb{Z} \oplus \mathbb{Z}) \cong T \oplus T = \text{ the torus!}$$

Beginning of March 22, 2021

Example 3.6.3. The **Klein 4-group**, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, is written as $\mathbb{Z}/2\mathbb{Z}^2$ or $\mathbb{Z}_2^2$ for shorthand notation. It consists of ordered pairs of 0's and 1's with component-wise addition mod 2.

Similar to the order of permutations in cycle notations, if for $a \in G$, $b \in H$ we have $o(a) = m$ and $o(b) = n$ then the order of (a,b) in $G \oplus H$ is $\operatorname{lcm}(m,n)$.

Proposition 3.6.4

If $G = \langle a \rangle$ and $H = \langle b \rangle$ then $G \oplus H$ is cyclic if and only if $\langle G \rangle, \langle h \rangle$ are co-prime. *Clear enough.*

Example 3.6.5. Let m and n be co-prime. Let $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ be defined by $x \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$. Then f is a homomorphism. Note that $\ker(f) = mn\mathbb{Z}$.
Then, the F.I.T. gives us the following:

$$\mathbb{Z}/mn\mathbb{Z} = f(\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Example 3.6.6. $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \ncong \mathbb{Z}/32\mathbb{Z}$ as the former has <u>no</u> element of order 32.

Example 3.6.7. Some of the groups of order 8 include:

$$D_4, \quad \mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z}^3.$$

There is one more called the *quarternion group*.

Most of the times, set-theoretic constructions do not create a group. In general, even if H, K are subgroups of G,

$$HK = \{hk \mid h \in H, k \in K\}$$

is not a group. However, normality can change things:

Lemma 3.6.8

If H, K are subgroups of G and $H \lhd G$ then HK is a subgroup. One between the two being normal suffices.

Proof. Claim: if $H \lhd G$ then $HK = KH$. Indeed, for all $k \in K$ we have $Hk = kH$.

(1) Identity: trivial.

(2) Inverse: $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.

(3) Closure: $(hk)(h'k') = h(kh')k' = h(\tilde{h}'\tilde{k})k' = (h\tilde{h}')(\tilde{k}k') \in HK$.

□

Beginning of March 24, 2021

Example 3.6.9. Let G, H be groups with $H \lhd G$. Then

$$\bigoplus_{i=1}^{n} G / \bigoplus_{i=1}^{n} H \cong \bigoplus_{i=1}^{n} (G/H).$$

Proof. Consider the *canonical projection*

$$\varphi : \bigoplus_{i=1}^{n} G \to \bigoplus_{i=1}^{n} (G/H) \text{ by } g \mapsto gH \text{ component-wise.}$$

Then the claim just follows from the F.I.T. □

3.7 Group Actions

To understand abstract groups, it is often helpful to interpret them as some kind of symmetry of spaces. This is called **group action** or **group representation**, as we've briefly discussed before. Recall how we were given a multiplication table of D_4 and represented them (the group generated by a, b satisfying $a^4 = b^2 = 1$ and $bab = a^{-1}$) by the collection of symmetries generated by $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, which then describes the symmetries of $\mathbb{R}^2$ by rotation and reflection.

With intuition provided, we now introduce the formal definition of group actions.

Definition 3.7.1

A group G is said to **act on a set X on the left** (X need not to be a group!!) if there is a function $\Theta : G \times X \to X$, written $\Theta(\sigma, x) = \sigma \cdot x = \sigma x$ for all $\sigma \in G, x \in X$, that satisfies the following:

(1) *** $(\sigma\tau)x = \sigma(\tau x)$ for all $\sigma, \tau \in G$ and $x \in X$, and

(2) if e is the identity of G then $ex = x$ for all $x \in X$.

We've seen several examples already.

Example 3.7.2. The group G acts on itself by left multiplication $Lg(x) := gx$. Indeed, for $g_1, g_2 \in G$ and $x \in G$ we have

$$(g_1 g_2)x = g_1(g_2 x) \text{ and } ex = x.$$

Example 3.7.3. The symmetric group S_n acts on the set $X = \{1, 2, \ldots, n\}$ via $\sigma x = \sigma(x)$ for all $x \in X$:

$$\Theta : S_n \times X \to X \text{ by } (\sigma, x) \mapsto \sigma x.$$

Indeed, we have

$$(\sigma\tau)x = \sigma(\tau x) \text{ and } ex = x \text{ where } e \text{ is the identity permutation.}$$

Example 3.7.4. Let X be the set of variables with four variables $x_1, \ldots, x_4$. Let $P(x_1, x_2, x_3, x_4) = x_1x_3 - x_2x_4$ and let $G = S_4$ that permutes the order of the variables.
For example, let $\sigma = (12)(34)$ and $\tau = (123)$. Then $(\sigma P)(x_1, \ldots, x_4) = x_2x_4 - x_1x_3$ and $(\tau P)(x_1, \ldots, x_4) = x_2x_1 - x_3x_4$. Since $\tau\sigma = (123)(12)(34) = (134)$ so $(\tau\sigma P)(x_1, \ldots, x_4) = x_3x_4 - x_2x_1$. One can check that this agrees with $\tau(\sigma P)(x_1, \ldots, x_4)$.

Example 3.7.5. $\mathrm{GL}(n; \mathbb{R})$ acts on $\mathbb{R}^n$ by $(M, x) \mapsto Mx$.

Definition 3.7.6

Assume that G acts on X. The **orbit** of $x \in X$ is $\mathrm{Orb}(x) = \{\sigma x \mid \sigma \in G\}$, namely "everywhere G pushes x".

Lemma 3.7.7

Assume G acts on X. We have an equivalence relation on X given by $x \sim y$ if and only if $y \in \mathrm{Orb}(x)$.

Proof. We check the three postulates one by one:

(1) Reflexivity: $ex = x$ so $x \sim y$.

(2) Symmetry: if $x \sim y$, i.e., $y \in \mathrm{Orb}(x)$ so $y = gx$ for some $g \in G$. Then $x = g^{-1}gx = g^{-1}y$.

(3) Transitivity: if $y = gx$ and $z = hy$ then $z = hy = hgx = (hg)x$ where $hg \in G$. □

Therefore, given an action on X, we are able to partition X by these orbits.

Beginning of March 26, 2021

Definition 3.7.8

Assume that G acts on set X. The **stabilizer** of $x \in X$ is

$$G_x = \operatorname{Stab}(x) = \{\sigma \in G \mid \sigma x = x\},$$

and the **fixed points** of $\sigma \in G$ are

$$\operatorname{Fix}(\sigma) = \{x \in X \mid \sigma x = x\}.$$

Remark. It is clear that $\operatorname{Stab}(x)$ is a subgroup of G.

Theorem 3.7.9: Orbit / Stabilizer Theorem

Assume that the finite group G acts on the finite set X. Then for any $x \in X$,

$$|\operatorname{Orb}(x)| = |G|/|\operatorname{Stab}(x)|.$$

Proof. Since $\operatorname{Stab}(x)$ is a subgroup, $G/\operatorname{Stab}(x)$ is a collection of cosets and clearly $|G/\operatorname{Stab}(x)| = |G|/|\operatorname{Stab}(x)|$. We can define $F : G/\operatorname{Stab}(x) \to \operatorname{Orb}(x)$ by $\sigma \operatorname{Stab}(x) \mapsto \sigma x$. We will show that this is bijective.

(1) Well-definedness: assume $\alpha \operatorname{Stab}(x) = \beta \operatorname{Stab}(x)$. Then $\alpha\beta^{-1} \in \operatorname{Stab}(x)$. (Recall that $kH = gH \implies g^{-1}kH = H$ and since H is a group, this is true if and only if $g^{-1}k \in H$.) Therefore by definition of stabilizer $\alpha\beta^{-1}x = x$ and $\alpha\beta^{-1}(\beta x) = \beta x$. On the other hand, clearly $\alpha\beta^{-1}\beta x = \alpha(\beta\beta^{-1})x = \alpha x$, so $\alpha x = \beta x$.

(2) Injectivity: assume $\alpha x = \beta x$. Then $\beta^{-1}\alpha x = x \implies \beta^{-1}\alpha \in \operatorname{Stab}(x)$ and so $\beta \operatorname{Stab}(x) = \alpha \operatorname{Stab}(x)$.

(3) Surjectivity is trivial. □

Theorem 3.7.10: Burnside's Lemma

Assume that the finite group G acts on the finite set X. Then the number of orbits of the group action is

$$\#\text{orbits} = \frac{1}{|G|}\sum_{\sigma \in G} |\operatorname{Fix}(\sigma)|.$$

Proof. By definition,

$$\sum_{g\in G} |\operatorname{Fix}(g)| = \sum_{g \in G} |\{x \in X : gx = x\}| = |\{(g, x) \mid g \in G, x \in X, gx = x\}|.$$

Then we can interchange the summation and transform summation of $\operatorname{Fix}(\sigma)$ into of $\operatorname{Stab}(x)$:

$$\sum_{g\in G} |\operatorname{Fix}(g)| = \sum_{x\in X} |\{g \in G \mid gx = x\}| = \sum_{x \in X} |\operatorname{Stab}(x)|$$

Beginning of March 29, 2021

Recall that Orbit-Stabilizer theorem gives $|\mathrm{Stab}(x)| = |G|/|\mathrm{Orb}(x)|$. Therefore,

$$\sum_{x\in X}|\mathrm{Stab}(x)| = \sum_{x\in X}|G|/|\mathrm{Orb}(x)| = |G|\sum_{x\in X}\frac{1}{|\mathrm{Orb}(x)|}.$$

Now pick one orbit O. Note that every $x \in O$ contributes $1/|O|$ to the sum, so all elements in O contribute exactly 1 to the sum. Now there may be other orbits, but given any orbit, all elements of the orbit contribute precisely 1 to the sum. Therefore $\sum_{x\in X}\frac{1}{|\mathrm{Orb}(x)|}$ is precisely the number of orbits!! Therefore,

$$\sum_{g\in G}|\mathrm{Fix}(g)| = \sum_{x\in X}|\mathrm{Stab}(x)| = |G|\cdot\#\text{orbits}.$$

□

Example 3.7.11. Let G act on G by conjugation $T_g(x) = gxg^{-1}$ for $x, g \in G$. It follows that $\mathrm{Orb}(x) = x^G$ the conjugacy class of x. The stabilizer of x is the **centralizer** of x, defined by

$$C_G(x) = \{g \in G \mid gxg^{-1} = x\}.$$

Also recall that the center $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$. This gives the **class equation**.

Proposition 3.7.12: Class Equation

Let $x_1^G, \dots, x_t^G$ be the nontrivial conjugacy classes in G (i.e., $|x_i^G| > 1$). Then

$$|G| = |Z(G)| + \sum_{i=1}^{t}\frac{|G|}{|C_G(x_i)|}.$$

Proof. Pick $x_i \notin Z(G)$. The Orbit-Stabilizer theorem says $|x_i^G| = |G|/|C_G(x_i)|$. Recall that the orbits form a partition of the group! Therefore $|G|$ is the sum of the order of all (trivial or nontrivial) orbits! The trivial ones are the ones in $Z(G)$ ($|\mathrm{Orb}(x)| = 1$ if and only if $x \in Z(G)$), and so

$$|G| = |Z(G)| + \sum_{i=1}^{t}\frac{|G|}{C_G(x_i)}.$$

□

Beginning of March 31, 2021

Theorem 3.7.13: Cauchy's Theorem

If a prime p divides $|G|$ (G finite), then G has an element of order 0.

Proof. We proceed by strong induction. Clearly if $|G| = 1$ or 2 the claim holds. For the inductive step, two cases:

(1) G is abelian. If it has no proper subgroup then G is cyclic with $|G| = p$. Therefore any non-identity element of G has to generate G and thus has order p.

If G has a proper subgroup and H a proper subgroup, $H \lhd G$ since G is abelian. If p divides $|H|$ we are done. If not, since $H \lhd G$ we may consider $|G/H|$. By strong induction, since $|G/H| < |G|$ it admits an element of p. Then if $o(gH) = p$ in G/H, we also have $o(g) = p$ in G, and the claim follows.

(2) G is not abelian. Recall that $C_G(x) = \{g \in G : xg = gx\}$ is the centralizer of x. Suppose $x \notin Z(G)$ (this is possible since G is not abelian) and p does not divide $|G/C_G(x)|$ (not necessarily a group, but indeed a collection of cosets and thus a set; we'll deal with the other case where p divides the order of this set later). Lagrange's theorem says

$$|G| = |C_G(x)| \cdot |G/C_G(x)|.$$

It follows that p divides $|C_G(x)|$. By assumption, $x \notin Z(G)$ so there is some $g \in G$ with which x does not commute. Therefore $|C_G(x)| < |G|$. By strong induction, $C_G(x)$ has an element of order p, and thus element must also have order p in G.

Finally, assume that p divides the order of $|G/C_G(x)|$ for all $x \notin Z(G)$. Recall the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{t} \frac{|G|}{C_G(x_i)}.$$

Since p divides $|G|$ but not the denominators, the sum on the RHS and $|G|$ both divides p. Therefore p divides $|Z(G)|$. Again, by induction $|Z(G)| < |G|$ and so $Z(G)$ has an element of order p. So does G.

The claim follows after we are done with our induction. □

We will soon present a generalization of Cauchy's theorem, called *Sylow theorems*.

Definition 3.7.14

For a prime p, a ***p*-group** means the group with order as a power of p.

Definition 3.7.15

A **Sylow *p*-subgroup** of a finite group G is a maximal p-subgroup of G.

Theorem 3.7.16: Sylow's Theorems

(1) If $|G| = p^e n$ with $\gcd(p, n) = 1$, then there is a subgroup H_i of G with $|H_i| = p^i$ for all $1 \leqslant i \leqslant e$. In particular, there is a Sylow p-subgroup of G of order p^e.

(2) If H is a subgroup of G and $|H| = p^i$, then H is contained in some Sylow p-subgroup of G.

(3) *** If $|G| = p^e n$ where $\gcd(p, n) = 1$, then all Sylow p-subgroups are conjugate (by p) and the number N_p of Sylow p-subgroups is a divisor of $|G|$ and $N_p \equiv 1 \pmod{p}$.

Example 3.7.17. A_4 has order $12 = 2^2 \cdot 3$. Then Sylow's third theorem gives $N_2 \equiv 1 \pmod{2}$, i.e., the total number of Sylow 2-subgroups of A_4 is odd.

Beginning of April 2, 2021

Example 3.7.18. All groups of order 15 are cyclic.

By Sylow-3 (theorem), $N_3 \equiv 1 \pmod 3$ and $N_3 \mid 15$ so $N_3 = 1$. Likewise, $N_5 = 1$. Let A be the unique Syloe 3-subgroup. It follows that for any $g \in G$, the conjugation gAg^{-1} must also be A. Hence A is normal. Similarly, the only Sylow 5-subgroup B must also be normal. Clear enough, $A \cap B = \{e\}$. Since they are normal (in fact one suffices), AB is a subgroup of G and it must also have order 15. Then see Ex.3.7.14 in HW7.

Proof of Sylow-2. Assuming Sylow-1 holds, there exists a Sylow p-subgroup which we call P_1. Define

$$\mathcal{S} = \{P_1, \dots, P_k\} = \{gP_1g^{-1} \mid g \in G\}.$$

Notice that this is not a circular reasoning with Sylow-3 since $\mathcal{S}$ is defined to be all groups obtained by conjugation, not that all Sylow p-subgroups.

Claim: $p \nmid k$. To see this, let G act on $\mathcal{S}$ by conjugation, i.e., $gP_i = gP_ig^{-1}$. Notice that this indeed is a group action. Then,

$$\text{Stab}(P_i) = \{g \in G \mid gP_ig^{-1} = P_i\},$$

the **normalizer** of P_i, written $N_G(P_i)$. Also, by definition, $\text{Orb}(P_i) = \mathcal{S}$. Now we invoke the Orbit-Stabilizer theorem:

$$|\text{Orb}(P_1)| = \frac{|G|}{|\text{Stab}(P_1)|} \implies |\mathcal{S}| = \frac{|G|}{|N_G(P_1)|}.$$

Since $N_G(P_1)$ contains P_1 (simple let $e \in G$ act on P_1), the fraction exhausts all powers of p and thus $p \nmid |\mathcal{S}| \implies p \nmid k$.

Back to the proof: we want to show that any H is contained in some P_i. Let H act on $\mathcal{S}$ by conjugation. Then, the orbits of this action partition $\mathcal{S}$. Suppose the disjoint orbits are $\text{Orb}(P_{i,1}), \dots, \text{Orb}(P_{i,n})$. Then clearly

$$|\mathcal{S}| = |\text{Orb}(P_{i,1})| + \cdots + |\text{Orb}(P_{i,n})|. \tag{Δ}$$

On the other hand,

$$\text{Stab}(P_{i,n}) = \{g \in H \mid gP_{i,n}g^{-1} = P_{i,n}\} = H \cap N_G(P_{i,n}).$$

By the Orbit-Stabilizer theorem,

$$|\text{Orb}(P_{i,n})| = \frac{|H|}{|H \cap N_G(P_{i,n})|}.$$

We know that $p \nmid |\mathcal{S}|$, so clearly one of the $|\text{Orb}(P_{i,n})|$'s on the RHS of (Δ) does not divide p. Let it be $|\text{Orb}(P_{i,j})|$. Therefore it has to be 1, as $|H| = p^i$ by assumption (so the divisors are either 1 or nontrivial powers of p), Therefore

$$|H| = |H \cap N_G(P_{i,j})|$$

and so $H = H \cap N_G(P_{i,j}) = H \cap P_{i,j}$. The red = relies on the lemma (which we didn't prove) that, *if H is a p-subgroup and if Q a Sylow p-subgroup then*

$$H \cap N_G(Q) = H \cap Q. \qquad \square$$

Beginning of April 5, 2021

Application: Counting

Suppose, say, we want to consider the number of necklaces one can make using using beads with two colors located at the vertices of a hexagon.

Problem 3.7.1

Given a necklace consisting of 6 beads, each of which can either be red or blue, how many "essentially different" necklaces are there? That is, if one pattern can be obtained by reflecting or rotating another one, they are considered the same.

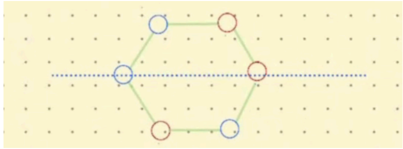
First question: what is the symmetry group of a necklace?
Answer: D_6 (rotation doesn't matter; neither does reflection).

Intuitively one would come up with something like 2^6 possible coloring of numbered vertices of a hexagon. Let X be the set of all these colored hexagons / necklaces. Let $G := D_6$ act on these necklaces, e.g., rotating by 60 degrees, rotating by 120 degrees, reflecting and then rotating by 240 degrees, etc.

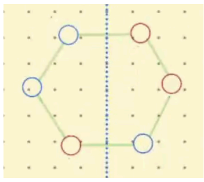
Notice that our original question asks how many essentially different necklaces are there? Here two necklaces are *essentially different* if one cannot be obtained by applying group actions to the other (e.g., reflection, rotation, etc.). Magically, all the essentially same necklaces fall into the same orbit, so the original question is equivalent to asking how many orbits are there under this group action.

This cries out for Burnside's Lemma. There are 12 elements in $G = D_6$, and we can classify them into three major types:

(1) Flipping across an axis that goes through the vertices: 3 elements, namely fr, fr^3, fr^5. Pick any one of them, for example the following screenshot from lecture: clearly the two vertices can be of any color, and we can freely color the two on the top without any restriction. Then the bottom two are automatically decided. Hence there are 2^4 choices, i.e., 2^4 fixed points.



(2) Flipping across an axis that goes through the midpoints of opposite sides: 3 elements, namely f, fr^2, fr^4. Similar to above but this time only $2^3 = 8$ fixed points.



(3) Rotating by 60 degrees: 2 elements, namely r and r^5. 2 fixed points only: every vertex must be of the same color to the one on its left (or right, depending on direction of rotation), so they are either all blue or all red.

(4) Rotating by 120 degrees: 2 elements, namely r^2 and r^4.Similar to above, vertices $1, 3, 5$ must have the same color and vertices $2, 4, 6$ must have the same color. Thus there are $2^2 = 4$ fixed points.

(5) Rotating by 180 degrees: 1 element, namely r^3. 2^3 fixed points by the same token.

(6) Finally, do nothing: 1 element, namely the identity e. Obvious: 2^6 fixed points.

Now we invoke Burnside's Lemma:

Group element σ	Number of such elements	$\lvert\text{Fix}(\sigma)\rvert$
Identity	1	2^6
Flip w/ vertices	3	2^4
Flip w/ midpoints	3	2^3
Rotation by 60 deg	2	2
Rotation by 120 deg	2	2^2
Rotation by 180 deg	1	2^3

It follows that

$$\text{number of orbits} = \text{number of essentially different necklaces} = \frac{1}{|G|}\sum_{\sigma\in G}|\text{Fix}(\sigma)| = \frac{156}{12} = 13.$$

Chapter 4

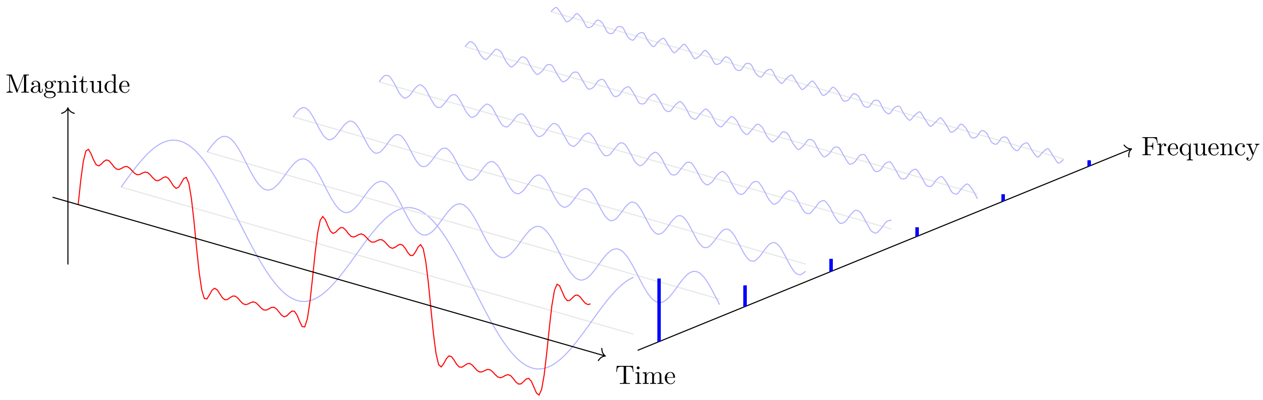
Midterm II Project: Finite Fourier Transforms on Groups

4.0 But What is a Fourier Transform?

A magical theorem in mathematical analysis says the following:

> A *suitably nice* function $f : \mathbb{R} \to \mathbb{R}$ can be approximated *nicely* by a combination of basic trigonometric polynomials of form $\sin(nx)$ and $\cos(nx)$ where $n \in \mathbb{Z}$.

Heuristically, think of the sounds that our ears hear every day. We hear a wide range of pitches (frequencies of sound waves) and levels of loudness (amplitudes). Among all these chaotic combinations of sounds, how can we even tell what we are actually hearing? It turns out that our inner ears, in particular the *basilar membrane*, automatically carry out **Fourier transforms**: the original sound wave, a function of time, is expressed as a "combination" of a bunch of simpler, nicer sound waves that resemble the sine curves with different frequencies. Our brains then receives the latter, i.e., the "frequency decomposition" of these sound waves. This explains why we are able to identify musical chords consisting of multiple notes.



Our focus today, however, is on finite Fourier transforms on groups (this is 410 not 425 after all).

For the remainder of this presentation, we assume $(G,+)$ is a finite cyclic group of order n where $+$ denotes the usual addition (so it can be identified with $\mathbb{Z}/n\mathbb{Z}$).

4.1 Preliminaries and Basic Definitions

Complex Numbers

We begin by bringing up some basic definitions and properties, some of which hopefully you have seen elsewhere:

(1) For $z = a + bi \in \mathbb{C}$, the **modulus** of z, written $|z|$, is defined to be $\sqrt{a^2 + b^2}$ (the distance to origin).

(2) For $z = a + bi \in \mathbb{C}$, the **conjugate** of z, written $\overline{z}$, is defined to be $a - bi$.

(3) Let S^1 be the **unit circle** in $\mathbb{C}$, that is, $S^1 \coloneqq \{z \in \mathbb{C} : |z| = 1\}$.

(4) **Euler's formula**: $e^{i\theta} = \cos(\theta) + i\sin(\theta)$. More importantly, each $z \in S^1$ can be uniquely represented by $e^{i\theta}$ for some $\theta \in [0, 2\pi)$.

Convolution (on Finite Groups): A $*$ is Born

Yes, it looks like a fancy multiplication symbol, and yes, it is an "upgraded" version of function multiplication (which we'll show very soon).

It is probably more intuitive to think of convolutions in probability theory. Suppose we are rolling two unfair (just to make the idea clearer) six-sided dices. Let X be the outcome of the first dice and let Y that of the second. What would be the distribution of the sum $Z = X + Y$?
For example, what events would lead to $Z = 7$, given X, Y can output any integer in $[1, 6]$? The answer is clear: 7 can be written as $1 + 6, 2 + 5$, ..., all the way till $6 + 1$. Therefore the probability of $Z = 7$ is given by

$$P(Z = 7) = \sum_{i=1}^{6} P(X = i)P(Y = 7 - i),$$

and more generally,

$$P(Z = z) = \sum_{i=1}^{6} P(X = i)P(Y = z - i)$$

as long as both functions on the RHS make sense (e.g., to get $Z = 8$, both rolls must be at least 2 as $1 + 6 < 8$).

Definition: Convolution (on finite group)

Let f, g be functions $G \to \mathbb{C}$. We define the **convolution** of f, g written $f * g$ and read "f splat g", by

$$(f * g)(a) = \frac{1}{|G|} \sum_{b \in G} f(a - b)g(b) \text{ for any } a \in G.$$

Definition: Indicator Function

For any $a \in G$, we define the **indicator function** $\delta_a : G \to \{0, 1\}$ by $\delta_a(x) = 1$ if $x = a$ and $\delta_a \equiv 0$ otherwise.
Relate this to the Dirac delta function if you have any Fourier background.

Convolution is extremely useful in a variety of fields. From the definitions above, we will be able to derive a list of "nice" properties of convolutions (on finite groups):

(1) $|G|\delta_0$ is the identity for convolution (note that $|G|$ is just a constant):

$$(f * |G|\delta_0)(a) = \frac{1}{|G|}\sum_{b\in G} f(a-b)(|G|\delta_0)(b) = \frac{1}{|G|}\cdot f(a)|G| = f(a) \qquad \text{for all } a \in G$$

because $(|G|\delta_0)(b)$ only evaluates to nonzero (to 1) when $b = a$.

(2) $*$ is commutative, i.e., $f * g = g * f$ (a nice property to have in 410, right?):

$$\begin{aligned}(f * g)(a) = \frac{1}{|G|}\sum_{b\in G} f(a-b)g(b) &= \frac{1}{|G|}\sum_{a-b\in G} f(a-(a-b))g(a-b)\\ &= \frac{1}{|G|}\sum_{b\in G} f(a-(a-b))g(a-b) && \sum_{a-b\in G} = \sum_{b\in G}\text{: they sum over the same elements}\\ &= \frac{1}{|G|}\sum_{b\in G} f(b)g(a-b) = (g * f)(a).\end{aligned}$$

(3) $*$ is (left) distributive, i.e., $f * (g+h) = f * g + f * h$:

$$\begin{aligned}[f * (g+h)](a) &= \frac{1}{|G|}\sum_{b\in G} f(a-b)[g(b)+h(b)]\\ &= \frac{1}{|G|}\sum_{b\in G} f(a-b)g(b) + \frac{1}{|G|}\sum_{b\in G} f(a-b)h(b)\\ &= (f * g)(a) + (f * h)(a).\end{aligned}$$

(4) $*$ is associative, i.e., $f * (g * h) = (f * g) * h$ (this is really just done by brutal computation along with some slick ways to rewrite the summations; similar to (2)):

$$\begin{aligned}[(f * g) * h](a) &= \frac{1}{|G|}\sum_{b}(f * g)(a-b)h(b)\\ &= \frac{1}{|G|}\sum_{b}\left[\frac{1}{|G|}\sum_{c} f(a-b-c)g(c)\right]h(b)\\ &= \frac{1}{|G|^2}\sum_{b}\sum_{c} f(a-b-c)g(c)h(b)\\ &= \frac{1}{|G|^2}\sum_{b'}\sum_{c'} f(a-b)g(b-c)h(c) && \text{setting } b' := b+c \text{ and } c' := b\\ &= \frac{1}{|G|^2}\sum_{b}\sum_{c} f(a-b)g(b-c)h(c) && \sum_{b'} = \sum_{b} \text{ and } \sum_{c'} = \sum_{c}\\ &= \frac{1}{|G|}\sum_{b} f(a-b)\left[\frac{1}{|G|}\sum_{c} g(b-c)h(c)\right]\\ &= \frac{1}{|G|}\sum_{b} f(a-b)(g * h)(b)\\ &= [f * (g * h)](a).\end{aligned}$$

Dual Groups

Consider the two groups $(G, +)$ and $(S^1, \cdot)$ [notice that the latter is indeed a group by Euler's formula]. Between groups we have various morphisms, and this leads to the following definition:

Definition: Dual Group

Let G be defined as above. We define $\hat{G}$, the **dual group** of G, to be the group of homomorphisms $\chi\colon G \to S^1$. The group operation is simply defined to be function multiplication, i.e., for any $\chi_1, \chi_2 \in \hat{G}$ and $g \in G$, we have $(\chi_1\chi_2)(g) = \chi_1(g) \cdot \chi_2(g)$. (*These χs are called **characters**.*)

> **Remark.** It might help to simply not try to understand what an abstract homomorphism $\chi : G \to S^1$ looks like. We are more interested in the group itself, i.e., the collection of these homomorphisms and the interactions among them. Not a big deal if this definition seems too abstract on first glance; hopefully it will come along nicely later.

4.2 Fourier Transform of $f\colon G \to \mathbb{C}$

4.2.1 Fourier Transform of $f\colon G \to \mathbb{C}$

But why do we need to abruptly introduce the notion of a dual group?

Recall from the very beginning that, when our ears hear something, they decompose the sound waves, a function $f\colon \mathbb{R} \to \mathbb{C}$ of time, i.e., $f(t)$, into a function $\hat{f}\colon \hat{\mathbb{R}} \to \mathbb{C}$ of frequencies, i.e., $\hat{f}(\xi)$. By doing so, our brain understands what the decomposition of the sound looks like. The underlying magic here is that the **Pontryagin dual** $\hat{\mathbb{R}}$ of $\mathbb{R}$ is in fact $\mathbb{R}$ itself, and this explains why f and $\hat{f}$ are ultimately both functions $\mathbb{R} \to \mathbb{C}$.

The upshot of the above paragraph is that under Fourier transform, a function $f\colon \mathbb{R} \to \mathbb{C}$ becomes a function $\hat{f}\colon \hat{\mathbb{R}} \to \mathbb{C}$. Connecting this to our finite cyclic group G, the Fourier transform of a function $f\colon G \to \mathbb{C}$ is, unsurprisingly, a function $\hat{f}\colon \hat{G} \to \mathbb{C}$ (yeah it's still abstract...). To put formally:

Definition: Fourier Transform

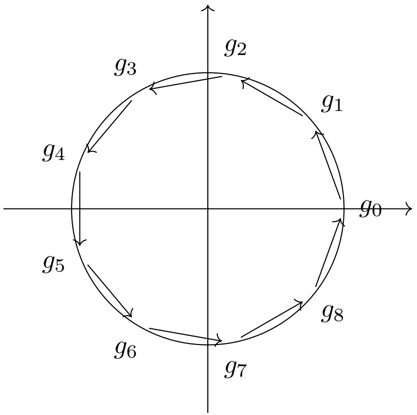
We define the **Fourier transform** $\hat{f}\colon \hat{G} \to \mathbb{C}$ of a function $f\colon G \to \mathbb{C}$ by

$$\hat{f}(\chi) = \frac{1}{|G|} \sum_{y \in G} f(y)\overline{\chi(y)}.$$

(To wrap your head around it: χ is an element of $\hat{G}$, i.e., a homomorphism $\chi : G \to S^1$, $\chi(y)$ a complex number, and $\overline{\chi(y)}$ the complex conjugate of $\chi(y)$.)

In our case, since $(G, +)$ can be identified with $\mathbb{Z}/n\mathbb{Z}$, we see $\hat{G}$ is in fact the set of all homomorphisms from G to the multiplicative groups of roots of unity in $\mathbb{C}$.

Heuristically, suppose $G = \langle g \rangle$ and $\chi(g)$ corresponds to the vertex labeled g_1 in the diagram (by Euler's formula, this point is $e^{2\pi i/n}$). Traversing through the list $(g, g^2, \ldots, g^{n-1}, g^n)$ under multiplication by g is equiva-



lent to traversing through the list of vertices of the polygon since $e^{2k\pi i/n}$ is precisely the vertex g_k. (Similar to how g^n is the identity of the group G of order n, we define $g_n \coloneqq g_0 = 1$, the identity element of the multiplicative group of roots of unity in $\mathbb{C}$.) To put this into mathematical language:

Definition

Suppose $a, b \in G = \mathbb{Z}/n\mathbb{Z}$. We define $\chi_a \in \hat{G}$ by $\chi_a(b) = e^{2\pi iab/n}$. Note that since $e^{2\pi i} = e^{2\pi in/n} = 1$, the exponent already takes care of the "modulo n" part.

4.2.2 The Space $L^2(\mathbb{Z}/n\mathbb{Z})$

Now we consider the space of functions $L^2(\mathbb{Z}/n\mathbb{Z}) \coloneqq \{f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}\}$. Notice that our previously discussed χ_as are all in this space. In fact, this is an **inner product space** (a vector space equipped with an inner product) where the inner product is given by

$$\langle f, g \rangle \coloneqq \sum_{x \in \mathbb{Z}/n\mathbb{Z}} f(x)\overline{g(x)}.$$

In addition, $L^2(\mathbb{Z}/n\mathbb{Z})$ is $\underline{n\text{-dimensional}}$ and — you might have guessed — a basis is naturally given by χ_as where $a \in G$. Even better, they don't just form a basis — they are an $\underline{\text{orthogonal basis}}$.

Theorem: $\{\chi_a\}$ is Orthogonal

For $a, b \in \mathbb{Z}/n\mathbb{Z}$, define $\chi_a(b) = e^{2\pi iab/n}$ (as above). Then $\{\chi_a : a \in \mathbb{Z}/n\mathbb{Z}\}$ forms an orthogonal set, i.e.,

$$\langle \chi_a, \chi_b \rangle = \begin{cases} n & a \equiv b \pmod{n} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The inner product gives $\langle \chi_a, \chi_b \rangle = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_a(x)\overline{\chi_b(x)} = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} e^{2\pi iax/n} e^{-2\pi ibx/n} = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_{a-b}(x)$. If $n \mid a - b$ then we are immediately done since there are n elements in $\mathbb{Z}/n\mathbb{Z}$ and each $\chi_{a-b}(x)$ is $e^{2\pi i(a-b)/n} = 1$.

On the other hand, if $n \mid a - b$, for convenience write $c = a - b$ and $S = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_x(x)$ the RHS. Notice that

$$\{\chi_c(0), \chi_c(1), \ldots, \chi_c(n-1)\} = \{\chi_c(1), \chi_c(2), \ldots, \chi_c(n)\},$$

i.e., the set is invariant under right shift $x \mapsto x + 1$. Therefore,

$$\chi_c(1)S = \chi_c(1) \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_c(x) = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_c(1)\chi_c(x) = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_c(x+1) = S,$$

which can happen only if $\chi_c(1) = 1$ or $S = 0$. Note that $\chi_c(1) = \chi_{a-b}(1) = e^{2\pi i(a-b)/n}$. Since $n \mid a - b$ by assumption, this expression cannot be 1, and therefore $S = 0$, as desired. □

4.2.3 Properties of the Fourier Transform

One of the best things about Fourier transform is that it reduces the complicated convolution to a much simpler form.

Theorem

Let $G = \mathbb{Z}/n\mathbb{Z}$ and let $\chi \in \hat{G}$. Then:

(1) The Fourier transform of the convolution of $f, g\colon G \to \mathbb{C}$ is equal to the element-wise product of their Fourier transforms:

$$\widehat{f * g}(\chi) = \hat{f}(\chi) \cdot \hat{g}(\chi).$$

(2) Given all the Fourier transforms $\hat{f}(\chi)$, we can recover f via the *Fourier inversion formula*

$$f(x) = \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x).$$

Proof of (1). Hopefully, by now you are fairly comfortable with the notion of convolution (so I won't need to use different colors on different variables).

$$\begin{aligned}
\widehat{f * g}(\chi) &= \frac{1}{|G|} \sum_{z \in G} (f * g)(z)\overline{\chi(z)} \\
&= \frac{1}{|G|} \sum_{z \in G} \left[\frac{1}{|G|} \sum_{y \in G} f(z - y)g(y) \right] \overline{\chi(z)} \\
&= \frac{1}{|G|^2} \sum_{z \in G} \sum_{y \in G} f(z - y)g(y)\overline{\chi(z)} \\
&= \frac{1}{|G|^2} \sum_{y \in G} g(y) \sum_{w \in G} f(w)\overline{\chi(w + y)} && \text{setting } w \coloneqq z - y \\
&= \left[\frac{1}{|G|} \sum_{y \in G} g(y)\overline{\chi(y)} \right] \left[\frac{1}{|G|} \sum_{w \in G} f(w)\overline{\chi(w)} \right] \\
&= \hat{f}(\chi) \cdot \hat{g}(\chi).
\end{aligned}$$

□

Proof of (2). First recall that $\overline{\chi_a(y)} = e^{-2\pi i a y/n} = e^{2\pi i(-ay)/n} = \chi_a(-y)$ for all $a, y \in \mathbb{Z}/n\mathbb{Z}$. Then,

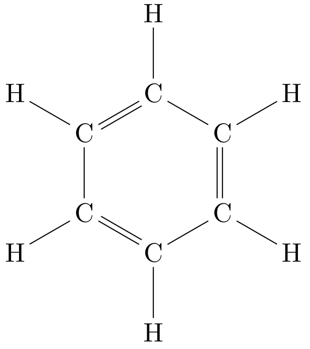
$$\begin{aligned}
\sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x) &= \sum_{\chi \in \hat{G}} \chi(x) \left[\frac{1}{|G|} \sum_{y \in G} f(y)\overline{\chi(y)} \right] \\
&= \sum_{y \in G} f(y) \left[\frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(x)\overline{\chi(y)} \right] \\
&= \sum_{y \in G} f(y) \left[\frac{1}{|G|} \langle \chi_x, \chi_y \rangle \right].
\end{aligned}$$

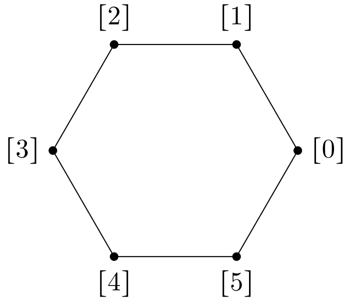
By the orthogonality theorem previously proven, $\langle \chi_x, \chi_y \rangle / |G|$ is 1 if $y = x$ and 0 otherwise, so indeed the RHS evaluates to $f(x)$, and we recover the Fourier inversion formula. □

4.3 Application: Stability of Benzene

4.3.1 Benzene *&* Some *Black Boxes*

In chemistry, Benzene, C_6H_6, is known to be very stable due to its *delocalized π-electrons*. The most notable feature of its structure (diagram on the left) is its hexagonal ring, which highly resembles the Cayley graph $X(\mathbb{Z}/6\mathbb{Z}, S)$ (middle) where $S \coloneqq \{\pm 1 \pmod 6\}$.





$$A = \begin{bmatrix} 0 & 1 & & & & 1 \\ 1 & 0 & 1 & & & \\ & 1 & 0 & 1 & & \\ & & 1 & 0 & 1 & \\ & & & 1 & 0 & 1 \\ 1 & & & & 1 & 0 \end{bmatrix}$$

With a few *black boxes* (which you need to take for granted...), we are able to show why is Benzene stable. The **adjacency matrix** of this Cayley graph is the matrix A on the right.

Black box #1: we can view this adjacency matrix as a matrix of the *adjacency operator* acting on complex-valued functions $f(x)$ for x in the Cayley graph $X(\mathbb{Z}/6\mathbb{Z}, S)$. If we generalize the notion of indicator function by defining

$$\delta_S(x) = \begin{cases} 1 & x \in S \\ 0 & \text{otherwise,} \end{cases}$$

then the action of this *adjacency operator* is given by

$$Af(x) = \sum_{s \in S} f(x+s) = f(x-1) + f(x+1) = \sum_{s \in S} \delta_S(x-s) f(s) = n(\delta_S * f)(x).$$

Black box #2 (or not): the **Spectral Theorem** says that $L^2(\mathbb{Z}/n\mathbb{Z})$ has an orthonormal basis of eigenfunctions (generalizations of eigenvectors) of A.

Upshot. In fact, we know what these eigenfunctions are: by linearity of χ_b for any $b \in \mathbb{Z}/6\mathbb{Z}$, we have

$$A\chi_b(x) = \chi_b(x+1) + \chi_b(x-1) = (\chi_b(1) + \chi_b(-1))\chi_b(x).$$

Therefore χ_b's are the eigenfunctions and $(\chi_b(1) + \chi_b(-1))$ the eigenvalues. Recall from Euler's formula

$$\begin{aligned} \chi_b(1) + \chi_b(-1) &= e^{2\pi i b/6} + e^{-2\pi i b/6} \\ &= \cos(2\pi b/6) + i\sin(2\pi b/6) + \cos(-2\pi b/6) + i\sin(-2\pi b/6) \\ &= 2\cos(2\pi b/6). \end{aligned}$$

Letting b vary in $\mathbb{Z}/6\mathbb{Z}$ we obtain the **spectrum** of A, written $\Lambda(A)$, i.e., the set of eigenvalues of A:

$$\begin{aligned} \Lambda(A) = \{2\cos(2\pi b/6) \mid b \in \mathbb{Z}/6\mathbb{Z}\} &= \{2\cos(0), 2\cos(2\pi/6), \ldots, 2\cos(10\pi/6)\} \\ &= \{2, 1, -1, -2, -1, 1\}. \end{aligned}$$

Black box #3: [Hückel, 1932] the stability of a chemical compound is determined by its **rest mass energy**

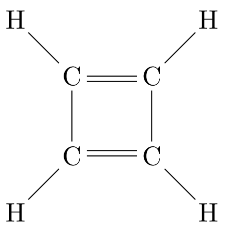
$$E := \left(\sum_{\substack{\text{top } n/2 \\ \lambda \in \Lambda(A)}} \lambda \right) \cdot \frac{2}{n},$$

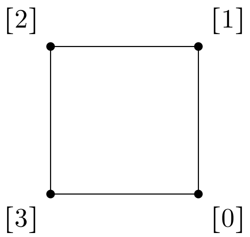
where the summation is taken over the larger half of $\Lambda(A)$. The larger the value E, the more stable the compound.

Upshot. Applying this theorem to the adjacency matrix of Benzene, we see that $E(C_6H_6) = (2+1+1)/3 \approx 1.33$.

4.3.2 Benzene C_6H_6 is More Stable than Cyclobutadiene C_4H_4

To wrap this presentation up, we present one more highly analogous example and show that cyclobutadiene, C_4H_4, is less stable than benzene is. Below from left to right are (1) the structure diagram of cyclobutadiene, (2) the Cayley graph $X(\mathbb{Z}/4\mathbb{Z}, \{\pm[1]\})$ that (1) resembles, and (3) the corresponding adjacency matrix.





$$B = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

Analogously, we have $Bf(x) = f(x-1) + f(x+1)$ and the eigenfunctions are χ_b, $b \in \mathbb{Z}/4\mathbb{Z}$. Hence the spectrum is

$$\{2\cos(2\pi b/4) \mid b \in \mathbb{Z}/4\mathbb{Z}\} = \{2\cos(0), 2\cos(\pi/2), 2\cos(\pi), 2\cos(3\pi/2)\} = \{2, 0, -2, 0\},$$

and by Hückel,

$$E(C_4H_4) = \frac{2}{4}(2+0) = 1,$$

indeed smaller than $E(C_6H_6)$. Therefore cyclobutadiene is less stable, as claimed.

End of Project

Chapter 5

Rings

5.1 Why Rings?

Beginning of April 12, 2021

When we work with $\mathbb{Z}$ or $\mathbb{Q}$, we usually work with more than just one operation that is present in a group. Therefore it's natural that we ask if we can add another operation, and this gives rise to a ring.

We will consider certain "nice" kinds of rings of which we can say a great deal. One such example is a *field*, which is highly structured.

Many constructions we introduced for groups (quotients, products, etc.) have natural analogues for rings. Behold!

5.2 What is a Ring?

Definition 5.2.1

A **ring** $R := (R, +, \cdot)$ is an Abelian group under the notion of addition, denoted $+$, with a binary operation of multiplication, denoted $\cdot$, which is

(1) associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, and

(2) (left and right) distributive: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

For simplicity we usually write $x \cdot y$ as xy.

Notice the following:

(1) Since $(R, +)$ is a group there exists an additive identity, denoted 0.

(2) If a ring does have a multiplicative identity, we say R is a **ring with identity** (counter e.g.: $2\mathbb{Z}$).

(3) Some books (e.g. Artin) defines a ring to be a ring with identity. We will not ignore the difference here.

(4) If multiplication is commutative then we say R is a **commutative ring** (counter e.g.: matrices).

Properties of Rings

Let R be any ring. For $a, b, c \in R$ we have the following facts where $-a$ denotes the additive inverse of a:

(1) $a \cdot 0 = 0 \cdot a = 0$: *notice that* $0 + a \cdot 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ *and the claim follows since* $(R, +)$ *is a group.*

(2) $a(-b) = (-a)b$: *since* $a(-b) + ab = a \cdot (-b + b) = a \cdot 0 = 0 \cdot b = (-a + a)b = (-a)b + ab$. *Done.*

(3) $(-a)(-b) = ab$,

(4) $a(b - c) = ab - ac$, and

(5) if R has an identity (which we call 1) then $(-1)a = -a$ and $(-1)(-1) = 1$.

Definition 5.2.2

Let R be a ring. If S is a nonempty subset of R which is a ring under the same operations as R, then S is called a **subring** of R. Clearly $\{0\}$ is a subring of any ring (*but it is not a ring with identity*).

Proposition 5.2.3

The subring test says that a nonempty $S \subset R$ is a subring of R if and only if S is closed under subtraction and multiplication. *We choose subtraction over addition because the one-step subgroup test uses inverse, in which case the inverse of addition is subtraction.*

Example 5.2.4. $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ for all $n \in \mathbb{Z}$.

Example 5.2.5. $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. Indeed,

$$(a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{Z}[i]$$

and

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i].$$

Example 5.2.6. $\mathbb{Z}$ is a subring of $\mathbb{Z}[-\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$.

Example 5.2.7. Just like how the union of two groups is in general not a group, the union of two subrings is in general not a subring. For example, $2\mathbb{Z} \cup 5\mathbb{Z}$ is not a subring of $\mathbb{Z}$: clearly $2 + 5 = 7 \notin 2\mathbb{Z} \cup 5\mathbb{Z}$.

Example 5.2.8. A remedy to the above non-example is by considering $2\mathbb{Z} + 5\mathbb{Z} := \{2n + 5m \mid m, n \in \mathbb{Z}\}$. This is indeed a subring of $\mathbb{Z}$. In fact, Bézout's identity tells us $2\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$.

Beginning of April 14, 2021

Recall in group theory that a unit is an "invertible" element, for example how $\mathbb{Z}/n\mathbb{Z}$ is a group under addition but only $\mathbb{Z}/n\mathbb{Z}^\times$ is a group under multiplication.

Definition 5.2.9

Suppose R is a ring with identity for multiplication (which we call 1 and $1 \neq 0$). The **units** in R are the invertible elements for multiplication in R. To put formally,

$$R^\times = \{a \in R \mid \exists b \in R \text{ such that } ab = 1 = ba\}.$$

If so we write $b = a^{-1}$.

Remark. Clearly $0 \in R$ but $0 \notin R^\times$. It follows that:

(1) $(R, +)$ is a (abelian) group,

(2) $(R, \cdot)$ is not a group because 0 has no multiplicative inverse,

(3) $(R^\times, +)$ is not a group because it has no identity (0), and

(4) $(R^\times, \cdot)$ is indeed a group! See below.

Proposition 5.2.10

If R is a ring with identity then $(R^\times, \cdot)$ is a group.

Proof.

(1) Closure: assuming (2), (3), and (4),

$$(ab)b^{-1}a^{-1} = abb^{-1}a^{-1} = 1$$

and likewise for the other direction.

(2) Associativity: this follows from the axioms of a ring directly.

(3) Existence of identity: this follows from the assumption that R is a ring with identity.

(4) Existence of inverse: for $a \in R^\times$, the corresponding b is its inverse.

□

Example 5.2.11. Let $\mathbb{Z}[x]$ denote the ring of polynomials, i.e., all polynomials with integer coefficients. We claim that this is a ring.

(1) Closure of addition is clear; closure of multiplication is also true since a degree m polynomial times a degree n polynomial simply gives a degree $m + n$ polynomial.

(2) Additive identity: the zero polynomial.

(3) Additive associativity: clear enough.

(4) Additive inverse: flip the signs of each coefficients.

(5) Multiplicative identity: the constant polynomial $f(x) = 1$.

(6) Multiplicative associativity and distributivity: a mess but true...

Since $\deg(fg) = \deg(g) + \deg(g)$ and the degree of $f(x) = 1$ is 0, all units in $\mathbb{Z}[x]$ must have degree 0. Furthermore, since $\mathbb{Z}^\times = \{\pm 1\}$, these are the only possible units for $\mathbb{Z}[x]$.

Example 5.2.12. Consider $M_2(\mathbb{Z})$ the set of all 2×2 matrices with integer entries. What is $M_2(\mathbb{Z})^\times$? Notice that these matrices all have integer determinants, and the only possibility that $\det(A)\det(B) = 1$ (for $A, B \in M_2(\mathbb{Z})$) is if $\det(A) = \det(B) = 1$ or both $= -1$. It is very easy to verify all matrices of form $\det(A) = \pm 1$ is in $M_2(\mathbb{Z})^\times$ by brute force computation (and the ivnerse formula).

Beginning of April 16, 2021

5.3 Nice Rings: Integral Domains & Fields

In this section we consider "nice" rings that resemble more of $\mathbb{Z}$ or $\mathbb{Q}$.

Definition 5.3.1

If R is a commutative ring, we say $0 \neq a \in R$ is a **zero divisor** if $ab = 0$ for some $b \neq 0$.

Example 5.3.2. In $\mathbb{Z}/8\mathbb{Z}$, the zero divisors are $[2]$ and $[4]$.

Definition 5.3.3

Now we define a "nice ring": an **integral domain**. We say R a commutative ring with identity for multiplication is an **integral domain** if it has no zero divisors. (We also assume $1 \neq 0$.)

Example 5.3.4. $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ are all integral domains. Also, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime.

Proposition 5.3.5

Integral domains are nice because they enjoy the **cancellation property**: if $a, b, c \in R$ and $a \neq 0$ then $ab = ac \implies b = c$. (Indeed, $ab = ac \to a(b - c) = 0$ and since $a \neq 0$ we must have $b = c$.)

Now we provide an even better ring that even allows division (the best one!!):

Definition 5.3.6

a **field** F is a commutative ring with identity for multiplication such that every nonzero element $a \in F$ has a multiplicative inverse $a^{-1} \in F$. In other words, $F^\times = F \setminus \{0\}$.

Proposition 5.3.7

Any field F is an integral domain, and any finite integral domain D is a field.

Proof. For $a, b \in F$, if $ab = 0$ but $a \neq 0$, then $b = a^{-1}ab = a^{-1} \cdot 0 = 0$. This shows F is an integral domain. For the other statement, assume D is a finite integral domain. We want to show that $D^{\times} = D \setminus \{0\}$. Since D is closed under multiplication by definition, it suffices to check that every $d \in D \setminus \{0\}$ has an inverse. Since D is finite, so is the order of a (i.e., $a^n = 1$ for some n). Therefore a^{n-1} is the inverse we are looking for. □

Example 5.3.8. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{Z}$ is not: 2, for example, has no multiplicative inverse.

Beginning of April 19, 2021

$$\begin{tikzcd}
 & \text{fields} \arrow[d] & \\
 & \text{integral domains} \arrow[dl] \arrow[dr] & \\
\text{commutative rings} \arrow[dr] & & \text{rings with identity} \arrow[dl] \\
 & \text{rings} &
\end{tikzcd}$$

Another particularly nice thing about fields is that we are able to easily classify all finite fields. In fact, there are not many finite fields besides $\mathbb{Z}/p\mathbb{Z}$ for prime p.

Example 5.3.9. We define $\mathbb{F}_9 := \mathbb{Z}/3\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}/3\mathbb{Z}\}$ where $i^2 = -1$. We define

$$(a + bi) + (c + di) = (a + c) + (b + d)i \text{ and } (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

To show $\mathbb{F}_9$ is a field, we begin by picking an arbitrary $a + bi \in \mathbb{Z}/3\mathbb{Z}[i]$. We want to find its inverse:

$$\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2}.$$

Note that $a^2 + b^2 \neq 0$ as long as $a \neq 0$ or $b \neq 0$. (It's easy to verify that $x^2 \equiv 0$ or $1 \pmod 3$ so if two of these add up to 0 they must be both 0.) Clearly $\mathbb{F}_9$ has 9 elements and it is indeed a finite field (and its order is not prime!).

Remark. In fact, all fields have the form (isomorphic) $\mathbb{F}_{p^n}$ for some prime p.

Definition 5.3.10

The **characteristic** of a ring R is the smallest $z \in \mathbb{Z}^+$ such that $nx = x + \ldots + x = 0$ for all $x \in R$. If no such n exists we say R has characteristic 0 (or ∞ in some books).

Proposition 5.3.11

Suppose R is a ring with identity 1 for multiplication.

(1) If the additive order of 1 is not finite, then the characteristic of R is 0.

(2) If the additive order of 1 is n then so is the characteristic of R.

(3) Suppose that R is an integral domain. Then the characteristic of R is either prime or 0.

Example 5.3.12. Clearly $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic 0. $\mathbb{Z}/3\mathbb{Z}$ has characteristic 3.

Example 5.3.13. $\mathbb{Z}/p\mathbb{Z}[x]$, the collection of polynomials with coefficients mod p, has characteristic p, even if the ring is not finite.

Beginning of April 21, 2021

Similar to different definitions derived from a group, we have many analogous definitions for rings and fields as well.

Definition 5.3.14

A subset F of a field E is a **subfield** if it is a field under the operations of E. We also say E is an **extension field** of F.

Proposition 5.3.15: Subfield test

Suppose E is a field. Then a nonempty subset $F \subset E$ is a subfield if and only if for $a, b \in F$ with $b \neq 0$, we have $a - b$ and $ab^{-1} \in F$.

Lemma 5.3.16

Suppose that R is an integral domain of nonzero characteristic p (which must be a prime), then for all $x, y \in R$, we have the **Freshman's Dream**:

$$(x+y)^p = x^p + y^p.$$

Proof. By the binomial theorem,

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}.$$

The binomial coefficient is a multiple of p unless $k = p$ or 0, in which cases it evaluates to 1. My dream holds! □

5.4 Building Rings from Old: Quotient and Direct Sums

Definition 5.4.1

Two rings R, S are **isomorphic** if there is a bijective function (a **ring isomorphism**) $f : R \to S$ preserving the ring structure. We write $R \cong S$ if this is the case.

Example 5.4.2. Claim: $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. First step is checking the cardinality: indeed they are the same. For the actual structure-preserving map:

$$f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \text{ by } [x] \mapsto ([x]_3, [x]_2),$$

i.e., mapping x to $(x \pmod 3), x \pmod 2)$. By the Chinese remainder theorem this is bijective, and clearly by properties of $\mathbb{Z}/n\mathbb{Z}$ this map is structure-preserving.

To construct quotient rings, what is the analogous concept to a normal subgroup (so that the quotient is a ring)?

Definition 5.4.3

A nonempty subset A of a ring R is called a (two-sided) **ideal** if and only if A is an additive subgroup of R such that $ra \in A$ and $ar \in A$ for all $r \in R, a \in A$. Trivial ideals include R itself and $\{0\}$.

Example 5.4.4. $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$. Indeed, multiplying anything in $n\mathbb{Z}$ by another integer still gives something in $n\mathbb{Z}$ and multiplication is commutative. In fact, $n\mathbb{Z}$ is a **principal ideal** generated by n and we write $n\mathbb{Z} = \langle n \rangle$.

Definition 5.4.5

Given a ring R and an element $a \in R$, the (2-sided) **ideal generated by a**, denoted $\langle a \rangle$, consists of elements ra and ar for all $r \in R$. Such an ideal is called a **principal ideal**. Similarly the ideal $\langle S \rangle$ **generated by a subset** S of R is the smallest ideal containing S.

Example 5.4.6. Consider $\mathbb{Z}$ the ring and $a, b \in \mathbb{Z}$. Then $\langle \{a, b\} \rangle$ is simply the ideal generated by $\gcd(a, b)$.

in In “nice rings” we can factor ideals uniquely into a product of “prime” ideals, although the elements themselves may fail to have unique factorization. (Whatever that means; we’ll get to it later.)

Example 5.4.7. $\mathbb{Z}[\sqrt{-5}]$ is not a **unique factorization domain**, i.e., there are different ways of factoring elements in this ring. For example,

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3.$$

Beginning of April 23, 2021

We will now show that the notion of ideal is what really gives rise to quotient rings. Clearly our goal is to construct some quotient ring R/A, analogous to G/H for groups. We need **cosets**, which are defined by

$$[x] = x + A = \{x + a \mid a \in A\}.$$

This gives rise to the equivalence classes defined by equivalence relation $x \sim y$ if and only if $x - y \in A$.

Then, we can define addition and multiplication

$$[x] + [y] := [x + y] \qquad [x] \cdot [y] := [xy].$$

Theorem 5.4.8

Suppose A is a subring of the ring R. Then with the definitions above, R/A is a ring if and only if A is an ideal. (*Compare this to its analogous counterpart in groups.*)

Proof. For $\implies$, assume A is an ideal. We first need to check if $+$ and $\cdot$ as defined above are well-defined. Indeed, if A is an ideal of R then, viewing R as an abelian group, A is a normal subgroup of R and addition is therefore well-defined. (Alternatively, $x - x', y - y' \in A \implies (x + y) - (x' + y') \in A$.)
For multiplication, if $[x] = [x']$ and $[y] = [y']$ then we want to show that $xy - x'y' \in A$. Indeed,

$$xy = x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y') \in A.$$

Now that the notions are well-defined, we need to verify that R/A is indeed a ring. Indeed it has an identity $[0] = A$, and for $[a] \in R/A$, its inverse is $[-a]$. The associativity and distributivity laws follow from those in R.
For $\implies$, if R/A is a ring, then multiplication in R/A must be well-defined. Certainly, we need $[0][a] = [a][0] = [0]$. Since a is arbitrary, that $[0][a] = [0]$ tells us $AR \subset A$ and likewise $RA \subset A$. Also, $[0] = [0] \pm [0]$, so taking any $a, b \in A$, we have $a + b \in A$ and $a - b \in A$, i.e., A is closed under addition and subtraction. □

Beginning of April 26, 2021

Example 5.4.9. Consider $\mathbb{Z}/2\mathbb{Z}[x]$, polynomials with coefficients in $\mathbb{Z}/2\mathbb{Z}$. Consider ideal $A := \langle x^2 + x + 1 \rangle = \{f(x)(x^2 + x + 1) \mid f(x) \in \mathbb{Z}/2\mathbb{Z}[x]\}$. What is $\mathbb{Z}/2\mathbb{Z}[x]/\langle x^2 + x + 1 \rangle$ as a ring?

First thing to note: there are 2^{n+1} polynomials of degree $\leqslant n$ in $\mathbb{Z}/2\mathbb{Z}[x]$.
Also notice that $[x^2 + x + 1] = [0]$ by definition of a quotient ring. This also means $[x^2] + [x] + [1] = [0]$, i.e., $[x^2] = [x] + [1]$ because $[x] = [-x]$ (and so $[1] = [-1]$) in $\mathbb{Z}/2\mathbb{Z}$. This means we are able to reduce any polynomial of degree > 1 (for example, $[x^3] = [x][x^2] = [x][y] = [z]$).
Now we can figure out what's in this quotient ring: clearly we have $[0]$ and $[1]$. We also have $[x]$ and $[x+1]$. Anything of higher degree can be reduced as shown above.
Now we know what the set is, but what is the ring structure? First notice that $x^2 + x + 1$ is **irreducible**, meaning that it does not have factors other than degree 0 or that of itself. It follows that this quotient ring is an integral domain.

Better than that, we claim that $\mathbb{Z}/2\mathbb{Z}[x]/\left\langle x^2+x+1\right\rangle$ is a field:

$$[1]\cdot[1]=[1]$$
$$[x]\cdot[1+x]=[x+x^2]=[-1]=[1]$$

We started with an ordinary ring and we obtain a field[!]

Definition 5.4.10

When is R/A an integral domain? This leads to the following definition.

We say A is a **prime ideal** if $ab\in A \implies a\in A$ or $b\in A$.

Lemma 5.4.11

For R a commutative ring with identity and A ideal, the quotient ring R/A is an integral domain if and only if A is a prime ideal.

Proof. We know R/A is a ring for sure, so it suffices to verify that it's an integral domain. If there is a zero advisor, then for some $a,b\in R$ we have

$$[a][b]=[0] \text{ with } [a],[b]\neq 0.$$

This means $ab\in A$ whereas $a,b\notin A$, contradicting A's being a prime ideal. This proves $\Longleftarrow$. The other direction follows direction from the same argument. □

Definition 5.4.12

When is R/A a field?

A proper ideal A is a **maximal ideal** in R if and only if, for any ideal B of R, if $A\subset B$ then $B=A$ or $B=R$.

Theorem 5.4.13

If A is an ideal in R (commutative; identity), then R/A is a field if and only if A is maximal.

Beginning of April 28, 2021

Proof. Assume R/A is a field and $A\subset B\subset R$ with $A\neq B$. It follows that there exists $x\in B-A$, so $[x]\neq[0]\in R/A$. Since R/A is a field $[x]$ admits a multiplicative inverse, which we call $[y]$. Therefore $[x][y]=[1]$ and $[xy-1]=[0]$, i.e., $xy-1\in A$, or $1=xy-u$ for some $u\in A$. Since $x\in B$ and B is an ideal, so is xy. Then $xy\in B$ and $u\in B$, so $1\in B$ and by definition of an ideal, $1r\in B$ for all $r\in R$.

For the other direction, suppose A is maximal. Pick $[x]\neq[0]$. Consider $B:=\{a+rx\mid a\in A, r\in R\}$. Certainly $A\subset B$ and $A\neq B$. Then $B=R$. Therefore $1\in B$ and $1=a+rx$ for some $a\in A, r\in R$. Then $[r][x]=[rx]=[1]-[a]$ but $[a]$ is just $[0]$. Thus $[r][x]=[1]$, and the claim follows. □

Example 5.4.14. The only ideals in a field F is $\{0\}$ and F itself. Suppose $A \neq \{0\}$ is an ideal in F. If we pick $a \in A$ then $a^{-1} \in F$, and $aa^{-1} = 1 \in A \implies A = F$.

Example 5.4.15. Claim: $0 \oplus \mathbb{Z}$ is a prime ideal of $\mathbb{Z} \oplus \mathbb{Z}$ but it's not maximal.

Indeed, if $(a,b)(c,d) = (0,x)$ then $ac = 0$ which means either $a = 0$ or $c = 0$, i.e., either $(a,c) \in 0 \oplus \mathbb{Z}$ or $(b,d) \in 0 \oplus \mathbb{Z}$.

To use the lemma above: we claim that $\mathbb{Z} \oplus \mathbb{Z}/0 \oplus \mathbb{Z} \cong \mathbb{Z}$. If so, since $\mathbb{Z}$ is an integral domain but not a field, $0 \oplus \mathbb{Z}$ is a prime ideal but is not maximal. To prove the isomorphism, consider $T : \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}/0 \oplus \mathbb{Z}$ by $a \mapsto [(a, \cdot)]$ where the second argument doesn't matter ($[(a,0)] = [(a,1)]$, for example).

Example 5.4.16. What are the maximal ideals in $\mathbb{Z}/18\mathbb{Z}$?

Recall that $\mathbb{Z}/18\mathbb{Z}$ can be generated (and only generated) by $[1],[5],[7],[11],[13],[17]$, i.e., the numbers in the group coprime to 18.

Note that, for example, since $2 \cdot 5 = 10$ and $10 \cdot 5^{-1} = 2$ (multiplicative inverse),

$$\langle [2] \rangle = \langle [10] \rangle = \langle [14] \rangle = \langle [8] \rangle = \langle [4] \rangle$$

$$\langle [3] \rangle = \langle [15] \rangle, \langle [6] \rangle = \langle [12] \rangle, \text{ and we also have } \langle [9] \rangle \text{ alone.}$$

It follows that $\langle [2] \rangle$ and $\langle [3] \rangle$ are the (only) possible maximal ideals.

End of Course