2.1 Equivalence Relations

Define $R = \{(x, y): x, y \in X, x \sim y\} \subseteq X \times X$
R: set of all pairs that are equivalent

$\sim$ is an equivalence relation if it satisfies:
- Reflexive: $x \sim x \ \forall x \in X$
- Symmetric: $x \sim y \leftrightarrow y \sim x$
- Transitive: If $x \sim y$ and $y \sim z$, then $x \sim z$

2.2 Equivalence Classes

$[x] = \{y \in X: y \sim x\}$

3.1 Well-Defined Operations

An operation $\cdot$ is well defined if:
$\left.\begin{matrix} x \sim y \\ w \sim z \end{matrix}\right\} \rightarrow (x \cdot w) \sim (y \cdot z)$

Note: $x \sim y \leftrightarrow [x] = [y]$

+ Theorems

- Let X be a set with an equivalence relation, then $[x] \cap [y] \neq \emptyset \rightarrow [x] = [y]$
- Equivalence classes are either disjoint or equal
- Let X be a set with an equivalence relation, then the equivalence classes form a partition of X
- Let R_j ($j \in J$, for some index set J) form a partition of X. Say that $x \sim y$ means $x, y \in R_j$ for some j, then $\sim$ is an equivalence relation on X

3.2 Number Theory

- Any non-empty set $S \subseteq \mathbb{N}$ has a unique $d \in S$ such that $\forall x \in S,\ d \leq x$
- For $a, b \in \mathbb{Z},\ b > 0$, then $\exists!\, q, r \in \mathbb{Z}$ such that $a = bq + r,\ 0 \leq r < b$

3.3 Refinements

For two equivalence relations $\approx$ and $\sim$, we say $\approx$ is a refinement of $\sim$ if each equivalence class of $\approx$ is contained in an equivalence class of $\sim$
In other words, $a \approx b \rightarrow a \sim b$

5.1 Divisibility and Modulo

$m \mid n$ means $\exists x \in \mathbb{Z}$ such that $n = mx$
$a \equiv b \bmod n$ means $n \mid (a - b) \rightarrow \dfrac{a-b}{n} \in \mathbb{Z}$

+ Theorems

- Congruence modulo n is an equivalence relation
- If $a \equiv a' \pmod n$ and $b \equiv b' \pmod n$, then:
  - $a + b \equiv a' + b' \pmod n$
  - $ab \equiv a'b' \pmod n$
- $\mathbb{Z}_n = \{[k]_n: k \in \mathbb{Z}\}$, contains n elements
  For $n = 5$, $[2] = \{\dots, -3, 2, 7, \dots\} \in \mathbb{Z}_5$
- $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n: x \text{ has a multiplicative inverse} \in \mathbb{Z}_n^*\}$
  $=$ The set of elements that are coprime with n

5.2 Prime and Irreducible

For $p \in \mathbb{Z}$ where $p > 1$:
- p is irreducible if the only divisors of p are 1 and p
- p is prime if whenever $p \mid ab$, then $p \mid a$ and $p \mid b$

+ Theorems

- p is prime $\leftrightarrow$ p is irreducible
- For $n > 1$, $\exists! \begin{cases} p_1, \dots, p_s \text{ primes} \\ e_1, \dots, e_s \text{ positives} \end{cases}$ s.t $n = p_1^{e_1} \times \cdots \times p_s^{e_s}$

5.3 GCD and LCM

- $d = \mathrm{GCD}(a, b)$ if and only if:
  - $d \mid a$ and $d \mid b$
  - If $c \mid a$ and $c \mid b$, then $c \mid d$
- $m = \mathrm{LCM}(a, b)$ if and only if:
  - $a \mid m$ and $b \mid m$
  - If $a \mid n$ and $b \mid n$, then $m \mid n$

+ Theorems

- $\forall a, b \in \mathbb{Z},\ \exists!$ GCD d and $\exists x, y \in \mathbb{Z}$ such that $d = ax + by$
- $\forall a, b \in \mathbb{Z},\ \exists!$ LCM m
- If $\mathrm{GCD}(a, b) = 1$, then $\exists x, y$ such that $ax + by = 1$
- If $\mathrm{GCD}(a, b) = d$, then $\{ax + by: x, y \in \mathbb{Z}\} = d \times \mathbb{Z}$
- $\mathrm{GCD}(a, b) \times \mathrm{LCM}(a, b) = |ab|$

6.1 Groups

For some set S and an operation $\cdot$, $(S, \cdot)$ is a group if:
- Closure: $ab \in S$
- Associativity: $(ab)c = a(bc)$
- Identity: $\exists \epsilon \in S$ such that $x\epsilon = \epsilon x = x$
- Inverses: $\forall x \in S, \exists y \in S$ such that $xy = yx = \epsilon$

9.1 Laws of Exponents

For a group G with some operation $\cdot$:
- $x^n = x \cdot x \cdot \ldots \cdot x$ (n times)
- $x^{-n} = (x^{-1})^n = (x^n)^{-1}$
- $x^m \cdot x^n = x^{m+n}$
- $(x^m)^n = x^{mn}$

If $xy = yx\ \forall x, y \in G$, then G is abelian (commutative)

9.2 - 10.1 Properties of Groups

- The identity is unique
- The inverse of each element is unique
- $ax = b$ has a unique solution $x\ \forall a, b \in G$
- $ab = ac \rightarrow bc$
- $(ab)^{-1} = b^{-1}a^{-1}$, $\quad (abc)^{-1} = c^{-1}b^{-1}a^{-1}$
- $(a^{-1})^{-1} = a$
- If $xy = x$ for some $x, y \in G$, then $y = \epsilon$
- If $xy = \epsilon$ for some $x, y \in G$, then $y = x^{-1}$

8.1 Cayley Tables

$\cdot$	a	b	…
a	a	b	…
b	b	$a \cdot b$	…
$\vdots$	$\vdots$	$\vdots$	$\ddots$

9.3 Properties of Cayley Tables

- Only one row and column matches the header completely and no other row or column matches the header in a single position
- Each row and column contains each element once

9.4 Product of Groups

For two groups G, H, their product is defined as:
$G \times H = \{(g,h): g \in H,\ h \in H\}$
$(x,a) \ \cdot_{G\times H} \ (y,b) = (x \ \cdot_G \ a, \quad y \ \cdot_H \ b)$

+ Theorems

- The product of groups is a group
- For $x = (a_1, \dots, a_t) \in G_1 \times \dots \times G_t$, then $|x| = \text{LCM}(|a_1|, \dots, |a_t|)$
- $G_1 \times \dots \times G_t$ is cyclic $\leftrightarrow \begin{cases} \text{Each } G_i \text{ is cyclic} \\ \text{GCD}\left(|G_i|, |G_j|\right) = 1 \ \ \forall i \neq j \end{cases}$

9.5 Isomorphisms

If $\phi: G \to H$ is a bijection with $\phi(x \cdot_G y) = \phi(x) \cdot_H \phi(y)$
Then ϕ is an isomorphism, and G, H are isomorphic

If G, H are isomorphic, then permuting the Cayley Table of G gives the Cayley Table of H

9.6 Isomorphisms

If $\phi: G \to G$ is an isomorphism, then ϕ is an automorphism
$aut(G) =$ The set of all automorphisms of G and it's a group

6.2 Symmetries

$S = \{\alpha, \beta, \dots\}$ is the set of symmetries of some object with the operation composition

- Example of Symmetries:
  $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$
- Example of Composition:
  $\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{matrix} \curvearrowright \beta \\ \curvearrowright \alpha \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

6.3 Properties of Symmetries

- $\alpha \circ \beta$ is a symmetry $\forall \alpha, \beta \in S$
- $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma) \ \ \forall \alpha, \beta, \gamma \in S$
- $\exists \epsilon \in S$ such that $\epsilon \circ \alpha = \alpha \circ \epsilon = \alpha \ \ \forall \alpha \in S$
- $\forall \alpha \in S,\ \exists \beta \in S$ such that $\alpha \circ \beta = \epsilon$

11.4 Generating Sets

If $\forall g \in S$, g can be written with α, β, then $\{\alpha, \beta\}$ generates S

11.1 Subgroups

For a group G with operation $\cdot$, if $H \subseteq G$, and it's a group with the same operation $\cdot$, then H is a subgroup
Notation:
If H is a subgroup of G, we write $H \leq G,\ H < G$ (if $H \neq G$)

11.2 Subgroup Test

Suppose H is a subset of G, then if:

- $H \neq \emptyset$
- $x, y \in H \to x \cdot y \in H$
- $x \in H \to x^{-1} \in H$

Then H is a subgroup

+ Theorems

- If $H \leq G$, then $\epsilon_G \in H$ and $\epsilon_H = \epsilon_G$
- If $H_1 \leq G$ and $H_2 \leq G$, then $H_1 \cap H_2 \leq G$
- If $K \leq H_1$ and $K \leq H_2$, then $K \leq H_1 \cap H_2$
- For $H_1 \leq G$ and $H_2 \leq G$:
  If $H_1 \cup H_2 \leq G$, then $H_1 \leq H_2$ or $H_2 \leq H_1$

11.5 Product Set

If $S \subseteq G$, then $\langle S \rangle$ is the set of all possible products of elements in S and their inverses

+ Theorems

- $S \subseteq G \to \langle S \rangle \leq G$
- If $H_1 \leq K$ and $H_2 \leq K$, then $\langle H_1 \cup H_2 \rangle \leq K$

11.7 Greatest Lower Bound

If $\exists \alpha \in X$ such that $\begin{cases} \alpha \leq x,\ \ \alpha \leq y \\ z \leq x \ \text{ and } \ z \leq y \to z \leq \alpha \end{cases} \forall x, y \in X$,
then α is the greatest lower bound of x, y, denoted $glb(x, y)$

11.8 Least Upper Bound

If $\exists \beta \in X$ such that $\begin{cases} x \leq \beta,\ \ y \leq \beta \\ x \leq z \ \text{ and } \ y \leq z \to \beta \leq z \end{cases} \forall x, y \in X$,
then β is the least upper bound of x, y, denoted $lub(x, y)$

11.6 Lattices

A lattice is the set X with operation $\leq$ such that $glb(x, y)$ and $lub(x, y)$ exists $\forall x, y \in X$

It's a diagram of subgroups, where each line connecting H and K (with K vertically higher than H in the diagram) means $H \leq K$

Note: If $H \leq K$, and we have some subgroup F such that $H \leq F \leq K$, then $F = H$ or $F = K$

11.3 Symmetries of a Square Example

To show a square has at most 8 symmetries:
Let γ be some symmetry, then:

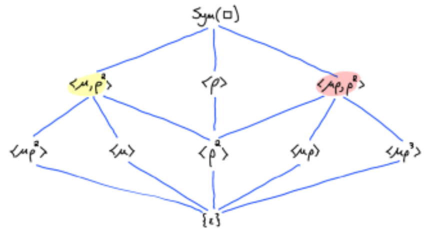
- $\gamma(1)$ (1st corner) has 4 options
- $\gamma(2)$ (2nd corner) is adjacent to $\gamma(1)$, so 2 options
- $\gamma(4)$ (4th corner) is adjacent to $\gamma(1)$, so 1 option left
- $\gamma(3)$ (3rd corner) has 1 option left

So $4 \times 2 \times 1 \times 1 = 8$ possibilities

To show a square has at least 8 symmetries, we show the above 8 symmetries are all possible, with matrices form

To find the subgroups of the symmetries of a square, we go through the product set of every subset of G, for instance: $\langle\epsilon\rangle,\ \langle\mu\rangle,\ \langle\rho\rangle,\ \langle\mu,\rho\rangle, \ldots$

If the product set generates G, it's not a subgroup, otherwise, it is, and we can use the subgroups to draw the lattice:



14.1 Cyclic Groups

G is cyclic $\leftrightarrow \exists$ a generator $g \in G$ s.t $G = \langle g\rangle = \{g^k : k \in \mathbb{Z}\}$
The order of g is the smallest positive integer n with $g^n = \epsilon$

Notation:

- $|g|$ = Order of an element, $|g| = \infty \leftrightarrow g^k \neq \epsilon\ \forall k \in \mathbb{Z}$
- $|G|$ = Size of a group

The set $\{k : g^k = \epsilon\} = |g|\mathbb{Z}$, so $g^k = \epsilon \leftrightarrow |g|$ divides k

$|x| = |y|$ is equivalent to $x^k = \epsilon \leftrightarrow y^k = \epsilon$

If G is a group with n elements and $|g| = n < \infty$ then:

- $G = \langle g\rangle = \{g, g^2, \ldots, g^n = \epsilon\}$
- $|G| = |g|$
- $|g^k| = \dfrac{n}{\mathrm{GCD}(n,k)}$
- Generators of G are exactly $\{g^k : GCD(n,k) = 1\}$

To check if a group is cyclic or not, check all the generators, if the order of some generator g is the length of the group, then the group is cyclic

+ Theorems

- G is cyclic $\rightarrow G$ is abelian (commutative)
- G is cylic $\rightarrow$ All subgroups are cyclic
- G has no subgroups other than $\{\epsilon\}$ and G
  $\leftrightarrow G$ is cyclic of prime order
  $\leftrightarrow |G| = n$ is prime
- If G, H are both cyclic, then $G \cong H \leftrightarrow |G| = |H|$

15.1 Complex Numbers

$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$
$\mathbb{C} = \{re^{i\theta} : r, \theta \in \mathbb{R}\}$ where $r \geq 0$ and $0 \leq \theta < 2\pi$

$re^{i\theta} = r\cos\theta + ri\sin\theta \rightarrow e^{i\theta} = \cos\theta + i\sin\theta$

For $z \in \mathbb{C}$:

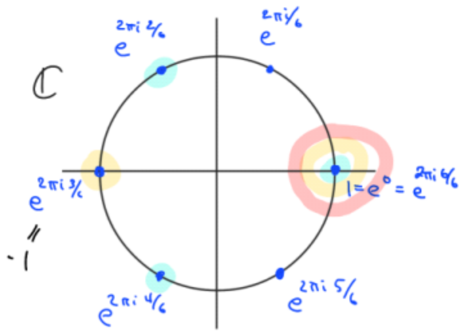
- $|z| = |a + bi| = \sqrt{a^2 + b^2} = r$
- $\dfrac{b}{a} = \tan\theta$

15.2 Roots of Unity

The nth root of unity is the solution to $z^n = 1$ for $z \in \mathbb{C}$

$R_n = \left\{e^{i2\pi\times\frac{1}{n}},\ e^{i2\pi\times\frac{2}{n}}, \ldots, e^{i2\pi\times\frac{n}{n}}\right\} = \left\langle e^{\frac{i2\pi}{n}}\right\rangle$

<u>Example:</u> R_6



$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\} = \{e^{i\theta} : \theta \in \mathbb{R}\}$

$\mathbb{T}$ is a subgroup of $\mathbb{C}^\times$

R_n is a subgroup of $\mathbb{T}$ (and of $\mathbb{C}^\times$)

Let $R = \bigcup_{n=1}^{\infty} R_n = \left\{e^{\frac{2\pi i j}{n}} : 0 \leq j < n,\ \ n \geq 1\right\}$

15.3 Subgroup Hierarchy

$R_n < R < \mathbb{T} < \mathbb{C}^\times$

15.4 Properties of R

- $|z|$ is finite $\forall z \in R$
- $|R|$ is infinite
- It's abelian but not cyclic
- Every finite subset is contained in a finite subgroup
- Every finite subgroup is cyclic
- Every infinite subgroup is not cyclic
- $R = \left\langle\left\{e^{\frac{2\pi i}{n}} : n \geq 1\right\}\right\rangle = \left\langle\left\{e^{\frac{2\pi i}{n}} : n \geq k\right\}\right\rangle\ \forall k$

15.5 Subgroups of $\mathbb{T}$

- $R = \left\{e^{\frac{2\pi i j}{n}} :\ \ 0 \leq j < n,\ \ n \geq 1\right\}$
- $Z = \{e^{ik} :\ k \in \mathbb{Z}\}$

17.1 Permutations

S_Ω is the set of all bijections $\Omega \to \Omega$, S_Ω is a symmetric group
S_Ω is denoted as S_n if $|\Omega| = n$
A subgroup of S_n is called a permutation group
If $\sigma \in S_n$, then $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

+ Theorems

- S_Ω with the operation composition is a group
- $|S_n| = n!$

17.2 Cycles and Cycle Notation in S_n

$\sigma \in S_n$ is a cycle if $\exists a_1, \dots, a_k$ such that $\begin{cases} \sigma(a_j) = a_{j+1} \\ \sigma(a_k) = a_1 \\ \sigma(x) = x, \quad x \neq a_j \end{cases}$

17.3 Cycle Order

- A k-cycle has $a_1, \dots, a_k$ terms based on the above defition
- All 1-cycles can be omitted
- 2-cycles are called transpositions

17.4 Cycle Notations

- Two-line notation:
  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix}$
- One-Line Notation:
  $\sigma = (1 \quad 3 \quad 5 \quad 4)\,(2)\,(6) = (1 \quad 3 \quad 5 \quad 4)$
  $\sigma^{-1} = (1 \quad 4 \quad 5 \quad 3) = (4 \quad 5 \quad 3 \quad 1)$, just σ inverted

17.5 Multiplying Cycles

For $\alpha = (1 \quad 3 \quad 4 \quad 7)$ and $\beta = (2 \quad 3 \quad 5 \quad 7)$, we perform multiplication:

x	$\beta(x)$	$\alpha(\beta(x))$
1	$\beta(1) = 1$	$\alpha(1) = 3$
2	$\beta(2) = 3$	$\alpha(3) = 4$
3	$\beta(3) = 5$	$\alpha(5) = 5$
4	$\beta(4) = 4$	$\alpha(4) = 7$
5	$\beta(5) = 7$	$\alpha(7) = 1$
6	$\beta(6) = 6$	$\alpha(6) = 6$
7	$\beta(7) = 2$	$\alpha(2) = 2$

$\to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 7 & 1 & 6 & 2 \end{pmatrix}$

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

18.1 Supports

The support of a permutation π is $\{x\colon \pi(x) \neq x\}$
Two permutations are disjoint if their supports are disjoint
Example:
$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}, \qquad \text{support}(\alpha) = \{1,4,5\}$

18.2 Cycle Types

The cycle type of a permutation π is the list (with repetition) of the length of its disjoint cycles

+ Theorems

- Disjoint permutations commute: $\alpha(\beta(x)) = \beta(\alpha(x))$
- $x \in \text{support}(\pi) \to \pi(x), \qquad \pi(\pi(x)), \dots \in \text{support}(\pi)$
- Order of a permutation π is the LCM of the lengths of its disjoint cycles, so the LCM of its cycle type
- Every permutation π can be written as a product of disjoint cycles
- S_n is generated by the set of all cycles
- k-cycles can be written as product of $k-1$ transpositions
- $(a_1 \quad a_2 \quad \dots \quad a_k) = (a_1 \quad a_k)\,(a_1 \quad a_{k-1}) \dots (a_1 \quad a_2)$
  $= (a_1 \quad a_2)\,(a_2 \quad a_3) \dots (a_{k-1} \quad a_k)$
- The set of all transpositions generates S_n,
  so $S_n = \langle \{ (a \quad b)\colon 1 \leq a < b \leq n \} \rangle$
- The following are minimal generating sets for S_n:
  - $\{(1 \quad a)\colon\ 2 \leq a \leq n\}$
  - $\{(a \quad a+1)\colon\ 1 \leq a \leq n-1\}$
  - $\{(1 \quad 2),\ (1 \quad 2 \quad \dots \quad n)\}$

18.3 Dihedral Group

It's the symmetries of a regular n-gon with the following:
- ρ = rotation by $\frac{1}{n}$ circle $= (1 \quad 2 \quad \dots \quad n)$
- μ = reflection through corner 1
$= \begin{cases} (1)\,(2 \quad 2m)\,(3 \quad 2m-1) \dots (m \quad m+2)\,(m+1), & n = 2m \\ (1)\,(2 \quad 2m+1)\,(3 \quad 2m) \dots (m+1 \quad m+2), & n = 2m+1 \end{cases}$

$D_n = \{\mu^i \rho^j\} = \{\rho^j \mu^i\}, \qquad 0 \leq i \leq 1, \qquad 0 \leq j \leq n-1$

$D_n = \{\mu, \rho\colon\ \mu^2 = \epsilon,\ \rho^2 = \epsilon,\ \rho\mu = \mu\rho^{-1}\}$

+ Theorems

D_n is a subgroup of S_n

20.1 Conjugation

$\sigma\pi\sigma^{-1}$ is the conjugation of π by σ

$\pi(i) = j \leftrightarrow (\sigma\pi\sigma^{-1})(\sigma(i)) = \sigma(j)$

Conjugation Example:

$\sigma = (1 \quad 3 \quad 4 \quad 5)\,(7 \quad 9) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 4 & 5 & 1 & 6 & 9 & 8 & 7 \end{pmatrix}$

$\pi \quad = (1 \quad 7 \quad 3)\,(4 \quad 6 \quad 9)\,(8 \quad 2)$
$\quad\ \ \downarrow \ \downarrow \ \downarrow \ \downarrow \ \downarrow \ \downarrow \ \downarrow \ \downarrow$ by σ
$\sigma\pi\sigma^{-1} = (3 \quad 9 \quad 4)\,(5 \quad 6 \quad 7)\,(8 \quad 2)$

+ Theorems

$\alpha, \beta \in S_n$ have the same cycle type $\leftrightarrow \beta = \sigma\alpha\sigma^{-1}$ for $\alpha \in S_n$