MAT 2143 Midterm Summary Sheet

Equivalence Classes and Relations

Equivalence Relations

$\sim$ is an equivalence relation on a set X if it is

- ***Reflexive:*** $x \sim x \; \forall x \in X$
- ***Symmetric:*** $x \sim y \iff y \sim x \; \forall x, y \in X$
- ***Transitive:*** $x \sim y \wedge y \sim z \implies x \sim z \; \forall x, y, z \in X$

We say $\approx$ is a refinement of $\sim$ if $a \approx b \implies a \sim b \; \forall a, b \in X$

An *equivalence class* is denoted by

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

Theorems

Theorem. *Let X be a set with an equivalence relation. Then*

$$[x] \cap [y] \neq \emptyset \implies [x] = [y]$$

Theorem. Let X be a set with an equivalence relation. Then the equivalence classes form a partition of X.

Theorem. Let R_j form a partion of X. Say that $x \sim y$ means $x, y \in R_j$ for some j. Then $\sim$ is an equivalence relation on X.

Operations

An operation is *well-defined on equivalence classes* if

$$\left.\begin{matrix} x \sim y \\ w \sim z \end{matrix}\right\} \implies x \cdot w \sim y \cdot z$$

Or equivalently,

$$\left.\begin{matrix} [x] = [y] \\ [w] = [z] \end{matrix}\right\} \implies [x \cdot w] = [y \cdot z]$$

Example: $X = \mathbb{R} \times \mathbb{R}$ $(a, b) \sim (c, d)$ means $a^2 + b^2 = c^2 + d^2$ Is addition well defined? Let

$$\begin{cases} (a, b) \sim (c, d) \\ (e, f) \sim (g, h) \end{cases} \implies \begin{cases} a^2 + b^2 = c^2 + d^2 \\ e^2 + f^2 = g^2 + h^2 \end{cases}$$

Then

$$\begin{cases} (a, b) + (e, f) = (a + e, b + f) \\ (c, d) + (g, h) = (c + g, d + h) \end{cases}$$

Now we have to check if

$$(a + e)^2 + (b + f)^2 = (c + g)^2 + (d + h)^2$$

Number Theory

Fact: *Every Non-empty $S \subseteq N$ has a minimum element d in S*

Prop: Let $a, b \in \mathbb{Z}$ with $b > 0$, then $\exists! q, r \in \mathbb{Z}$ with $a = bq + r$ for $0 \leq r < b$

GCD

Definition: *Let $a, b \in \mathbb{Z}$, if d is a positive integer with*

- $d \mid a$ and $d \mid b$
- if $c \mid a$ and $c \mid b$, then $c \mid d$

then d is the gcd of a and b

Theorem: *For every $a, b \in \mathbb{Z}$, $\exists! d = \gcd(a, b)$. Furthermore, $\exists x, y \in \mathbb{Z}$ such that $d = ax + by$. Furthermore d is the largest common divisor of a, b*

Corollary: $\gcd(a, b) = 1 \implies \exists x, y$ *s.t* $ax + by = 1$

Corollary: $\gcd(a, b) = d \implies \{ax + by : x, y \in \mathbb{Z}\} = d\mathbb{Z}$

LCM

Definition: *let $a, b \in \mathbb{Z}$ if m is a positive integer with*

- *$a \mid m$ and $b \mid m$*
- *if $a \mid n$ and $b \mid n$, then $m \mid n$*

then m is a lcm *of a, b.*

Theorem: *For every a, b $\exists!$* lcm *m*

Cayley Tables

$\cdot$	ϵ	a_1	a_2	$\cdots$
ϵ	ϵ	a_1	a_2	$\cdots$
a_1	a_1	$\cdots$	$\cdots$	$\cdots$
a_2	a_2	$\cdots$	$\cdots$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Properties:

- Symmetric $\implies$ Operation is commutative
- row and column is the header $\implies$ corresponding element is the identity
- every row has the identity $\implies$ each element an inverse
- Only one row and column can match the header (in other words there is only one identity)
- Each row and column contains each element *exactly* once (since the group is closed)

Isomorphisms

Isomoprhism

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

Automorphism

If $\phi : G \to G$ is an isomorphism, then ϕ is an automorphism. We denote the set of all automorphisms as $\mathrm{aut}(G)$

Cyclic Groups

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

Facts and Notation

- $|g|$ = order of an element, $|g| = \infty \iff g^k \neq \epsilon \; \forall k \in \mathbb{Z}$
- $\{k : g^k = \epsilon\} = |g| \cdot \mathbb{Z}$, so $g^k = \epsilon \iff |g| \mid k$
- $|x| = |y| \iff (x^k = \epsilon \iff y^k = \epsilon)$
- G is cyclic $\implies$ G is abelian
- G is cyclic $\implies$ All subgroups of G are cyclic
- G is cyclic with with no subgroups other than $\{\epsilon\} \iff |G| = n$ is prime. *(We say G is cyclic of prime order)*
- If G, H are both cyclic, then $G \cong H \iff |G| = |H|$
- $|g^k| = \frac{n}{\gcd(n,k)}$
- Generators are exactly $\{g^k : \gcd(n, k) = 1\}$

Complex Numbers

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

$$\mathbb{C} = \{re^{i\theta} : r, \theta \in \mathbb{R} \text{ s.t } r \geq 0, 0 \leq \theta < 2\pi\}$$

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

$$z = re^{i\theta} = re^{i(\theta + 2k\pi)} = -re^{i(\theta + (2k+1)\pi)}$$

$$z = re^{i\theta} = r\cos\theta + ir\sin\theta$$

$$a = r\cos\theta \text{ and } b = ir\sin\theta$$

$$|z| = |a + bi| = \sqrt{a^2 + b^2} = r$$

$$\frac{b}{a} = \tan\theta$$

Roots of Unity and The Circle Group $\mathbb{T}$

The nth root of unity is the solution to $z^n = 1$

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

Circle Group $\mathbb{T}$

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

R Group

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

Properties:

- $|z|$ is finite $\forall z \in R$
- $|R|$ is infinite
- R is abelian but *not* cyclic
- Every finite subset is contained in a finite subgroup
- Every finite subgroup is cyclic
- Every infinite subgroup is not cyclic

$$R = \langle\{e^{\frac{2\pi i}{n}} : n \geq 1\}\rangle = \langle\{e^{\frac{2\pi i}{n}} : n \geq k\}\rangle$$

For any k

Subgroup Hierarchy:

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

Symmetric Group

Ω is some set, a *permutation* of Ω is a bijection $\Omega \mapsto \Omega$. S_Ω = the set of all permutations of Ω, which is called the *symmetric group* S_n. $S_n = S_\Omega$ for $\Omega = \{1, 2, \ldots, n\}$. so $|\Omega| = n$.
A subgroup of S_n is called a permutation group.

Theorems

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

Cycle Notation

If $\sigma \in S_n$ then

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

Cycles

$\sigma \in S_n$ is a cycle if $\exists a_1, \ldots, a_k$ such that

$$\begin{cases} \sigma(a_j) = a_{j+1} \\ \sigma(a_k) = a_1 \\ \sigma(x) = x,\ x \neq a_j \end{cases}$$

Cycle Order

- A k-cycle has $a_1, \ldots, a_k$ terms
- 2-cycles are called *transpositions*

More Notation

Two-Line Notation:

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

One-Line Notation:

$$\sigma = \begin{pmatrix} 1 & 3 & 5 & 4 \end{pmatrix}(2)(6) = \begin{pmatrix} 1 & 3 & 5 & 4 \end{pmatrix}$$
$$\sigma^{-1} = \begin{pmatrix} 4 & 5 & 3 & 1 \end{pmatrix}$$

Supports

The support of a permutation π is $\{x : \pi(x) \neq x\}$. Permutations are *disjoint* if their supports are disjoint. **Example:**

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix},\ \text{support}(\sigma) = \{1, 4, 5\}$$

Cycle Types & Order

The *cycle type* of a permutation π is the list of the lengths of its disjoint cycles. The order is the lcm of the cycle types.

Example: List all the possible orders and cycle-types of permutations in S_7

Cycle-Type	Order
7	7
6	6
5,2	10
5	5
4,3	12
4,2	4
4	4
3,3	3
3,2,2	6
3,2	6
3	3
2,2,2	2
2,2	2
2	2
1	1

Dihedral Group

D_n is the group of symmetries of a regular n-gon with

- ρ = reflection by $\frac{1}{n}$ circle = $\begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix}$
- μ = reflection through corner 1 =

$$\begin{cases} (1)\begin{pmatrix} 2 & 2m \end{pmatrix}\begin{pmatrix} 3 & 2m-1 \end{pmatrix}\ldots\begin{pmatrix} m & m+2 \end{pmatrix}(m+1) \\ (1)\begin{pmatrix} 2 & 2m+1 \end{pmatrix}\begin{pmatrix} 3 & 2m \end{pmatrix}\ldots\begin{pmatrix} m+1 & m+2 \end{pmatrix} \end{cases}$$

For $n = 2m$, and $m = 2m + 1$ respectively.

$$D_n = \{\mu^i \rho^j\} = \{\rho^j \mu^i\}$$

Theorem: D_n is a subgroup of S_n

Conjugation

$\sigma, \pi \in S_n$, we say π is conjugated by σ for $\sigma\pi\sigma^{-1}$. Suppose $\pi(i) = j$, then

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

Proposition: $\alpha, \beta \in S_n$ have the same cycle type $\iff$ $\beta = \sigma\alpha\sigma^{-1}$ for some $\sigma \in S_n$.

Important Facts/Theorems

**Note: Some of these are repeats but are very important*

- $|g^k| = \frac{n}{\gcd(n,k)}$
- If G, H are both cyclic, then
  $G \cong H \iff |G| = |H|$
- Cyclic $\implies$ Abelian
- Disjoint permutations commute
- $x \in \text{support}(\pi) \implies \pi(x), \pi(\pi(x)), \ldots \in \text{supp}(\pi)$
- Order of a permutation is the lcm of the cycle types
- Every permutation can be written as products of disjoint cycles
- S_n is generated by the set of all cycles
- k-cycles can be written as the product of $k - 1$ transpositions
- The set of all transpositions generates S_n, so
  $S_n = \langle\{\begin{pmatrix} a & b \end{pmatrix} : 1 \leq a < b \leq n\}$
- The following are minimal generating sets of S_n

$$\{\begin{pmatrix} 1 & a \end{pmatrix} : 2 \leq a \leq n\}$$

$$\{\begin{pmatrix} a & a+1 \end{pmatrix} : 1 \leq a \leq n-1\}$$
$$\{\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & \ldots & n \end{pmatrix}\}$$

- If G is abelian and H is not, then they are never isomorphic.

Lagrange Theorem

Let G be a finite group and H be a subgroup of G. Then

$$|G| = [G : H] \cdot |H| \implies [G : H] = \frac{|G|}{|H|}$$

$[G : H]$ is the number of left cosets of G in H.

Corollaries

Corollary:

$$H < G \implies |H| \text{ divides } |G|$$

Proof.

$$|H| \cdot [G : H] = |G|$$

Corollary:

$$g \in G \implies |g| \text{ divides } |G|$$

Proof.

$$|g| = |\langle g \rangle| \quad |\langle g \rangle| \cdot [G : \langle g \rangle]$$

Corollary:

$$|G| \text{ prime } \implies G = \langle a \rangle \; \forall a \neq \epsilon$$

If

$$K < H < G$$

then

$$|G| = [G : H][H : K]|K|$$

$$[G : K] = [G : H][H : K]$$

Cosets

H is s subgroup of G, g is any fixed element in G. Then the left coset of H in G is

$$gH = \{gh : h \in H\}$$

The right coset of H in G is

$$Hg = \{hg : h \in H\}$$

Properties

- G abelian $\implies gH = Hg \; \forall g \in G \; H \leq G$
- $H \leq Z(G) \implies gH = Hg \; \forall g \in G$
- $g \in Z(G) \implies gH = Hg \; \forall H \leq H$

Equivalent Statements

Let $H \leq G$ $g_1, g_2 \in G$

- $g_1 H = g_2 H$
- $H g_1^{-1} = H g_2^{-1}$
- $g_1 H \subseteq g_2 H$ (or $g_2 H \subseteq g_1 H$)
- $g_1 \in g_2 H$ (or $g_2 \in g_1 H$)
- $g_2^{-1} g_1 \in H$ (or $g_1^{-1} g_2 \in H$)