Final Review

4b. Isometry

dot product: $<\vec{u},\vec{v}>=\vec{u}^T\vec{v}$, length: $|\vec{v}|=<\vec{v},\vec{v}>$, distance: $|\vec{u}-\vec{v}|$.

isometry of $\mathbb{R}^n$: a distance preserving map $f:\mathbb{R}^n\to\mathbb{R}^n$, $\forall\vec{u},\vec{v}\in\mathbb{R}^n$, $|f(\vec{u})-f(\vec{v})|=|\vec{u}-\vec{v}|$

Lemma. If f,g are isometries on $\mathbb{R}^n$, then $f\circ g$ is also an isometry on $\mathbb{R}^n$.

Each $\vec{a}\in\mathbb{R}^n$ induces a translation map: $t_{\vec{a}}:\mathbb{R}^n\to\mathbb{R}^n$, $\vec{u}\mapsto\vec{u}+\vec{a}$. It is an isometry.

$T:\mathbb{R}^n\to\mathbb{R}^n$ is a linear operator if:

1. $\forall\vec{u},\vec{v}\in\mathbb{R}^n, T(\vec{u}+\vec{v})=T(\vec{u})+T(\vec{v})$
2. $\forall c\in\mathbb{R},\vec{u}\in\mathbb{R}^n, T(c\vec{u})=cT(\vec{u})$

orthogonal linear operator if it is a linear operator s.t. $\forall\vec{u},\vec{v}\in\mathbb{R}^n$, $<T(\vec{u}),T(\vec{v})>=<\vec{u},\vec{v}>$.

invertible A is orthogonal if $A^{-1}=A^T$.

orthogonal linear group $O_n(\mathbb{R})$: the set of all $n\times n$ orthogonal matrices, a subgroup of $GL_n(\mathbb{R})$.

T is an orthogonal linear operator $\iff$ A is an orthogonal matrix.

Lemma. The determinant of an orthogonal matrix is 1 or -1.

The kernel of $O_n(\mathbb{R})$: $SO_n(\mathbb{R})=\{A\in O_n(\mathbb{R})|\det(A)=1\}$

$M_n=T_n\rtimes O_n$ where M_n is group of isometry on $\mathbb{R}^n$, T_n is group of translations, O_n is orthogonal linear group, $O_n(\mathbb{R})=SO_n(\mathbb{R})\cup SO_n(\mathbb{R})r$.

Every isometry $f=t_{\vec{a}}\cdot\phi$, where $t_{\vec{a}}$ is the translation along $\vec{a}$, ϕ is an orthogonal linear operator.

When $n=2$, $f=t_{\vec{a}}\cdot\rho_\theta$ or $f=t_{\vec{a}}\cdot\rho_\theta\cdot r$,

where rotation $\rho_\theta=SO_2(\mathbb{R})=\begin{bmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{bmatrix}$ — rotation of angle θ around origin

reflection $r=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ — reflection with respect to x-axis

- $\phi\cdot t_{\vec{a}}=t_{\phi(\vec{a})}\cdot\phi$
  - In particular, for $\mathbb{R}^2$, $\rho_\theta t_{\vec{a}}=t_{\rho_\theta(\vec{a})}\rho_\theta$, $rt_{\vec{a}}=t_{r(\vec{a})}r$
- $t_{\vec{a}}+t_{\vec{b}}=t_{\vec{a}+\vec{b}}$, $t_{\vec{a}}^{-1}=t_{-\vec{a}}$
- $\rho_\alpha\cdot\rho_\beta=\rho_{\alpha+\beta}$, $\rho_\theta^{-1}=\rho_{-\theta}$
- $r^2=id$, $r^{-1}=r$
- $r\rho_\theta=\rho_{-\theta}r$ and $\rho_{-\theta}=r\rho_\theta r=r\rho_\theta r^{-1}$

dihedral group: $D_n=\{\rho_\theta^i r^j\in O_2|0\leq i\leq n-1, 0\leq j\leq 1\}$, where $\theta=\frac{2\pi}{n}$, finite subgroup of O_2

Properties: $|D_n|=2n$, $|\rho|=n$, $|r|=2$, $|<\rho>|=2$

4c. Groups Actions

A group action of G on a nonempty X is a function: $G \times X \to X$, $(g, x) \mapsto g.x$satisfying:

1. $1.x = x$ for any $x \in X$
2. $g_1.(g_2.x) = (g_1 g_2).x$ for any $g_1, g_2 \in G$, $x \in X$

orbit of x: $O(x) = \{y \in X | g.x = y \text{ for some } g \in G\}$, distinct orbits form a partition of X

stabilizer of x: $G_x = \{g \in G : g.x = x\}$, a subgroup of G

transitive action if there's only one orbit.

transitive action $\iff$ $\forall x, y \in X$, there exists $g \in G$ such that $y = g.x$.

Counting Formula: $|G| < \infty$, $|G| = |O(x)| \cdot |G_x|$

i.e. $|O(x)| = |G : G_x|$, $|G_x| = |G : O(x)|$

Class Equation: $|G| < \infty$, $|G| = |Z(G)| + \sum_{x \in S} |C_x| = |Z(G)| + \sum_{x \in S} \frac{|G|}{|N(x)|}$ where S is a set of representations of conjugacy classes with at least two elements. It decomposes G into the disjoint union of conjugacy classes C_x (orbits of G acting on itself by conjugation $g.x = gxg^{-1}$).

Examples:

- S_n acts on $X = \{1, 2, ..., n\}$ by $\sigma.k = \sigma(k)$
- $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by matrix multiplication
- G acts on G by left multiplication: $g.x = gx$
- G acts on G by conjugation: $g.x = gxg^{-1}$
    - stabilizer in this case is called normalizer $G_x = N_x = \{g \in G | gxg^{-1} = x\}$
    - $Z(G) \subseteq N_x$, $O(x) = C_x$

Property:

- Fix $g \in G$, we get a bijection map $X \to X$, $x \mapsto g.x$

  More generally, a group action corresponds to a homomorphism $G \to \text{Per}(X)$

More results:

- Cauchy's Theorem. $|G| < \infty$, $p \mid |G|$, then G has an element of order p.
- Fixed Point Theorem. G acts on X. $|G| = p^k$, $k > 0$. If $p \nmid |X|$, then there exists a fixed point $x \in X$ under this action, i.e. $g.x = x$ for any $g \in G$.
- H, K are subgroups of a finite group G. Then $|HK| = \frac{|H| \times |K|}{|H \cap K|}$.
- Groups of order p^2 are abelian.

5. Classification of Groups

p-subgroup: $|G| = p^e m$, p prime, $p \nmid m$. subgroup H s.t. $|H| = p^r$, $r > 0$.

Sylow p-subgroup: $|G| = p^e m$, p prime, $p \nmid m$. subgroup H s.t. $|H| = p^e$.

Sylow Theorem. $|G| = p^e m$, p prime, $p \nmid m$.

1. There exists a Sylow p-subgroup of G.
2. H is a Sylow p-subgroup of G, K is a p-subgroup of G, then $\exists g \in G$ s.t. $K \subset gHg^{-1}$.
3. $n_p \mid m$, $n_p \equiv 1 \pmod p$

Cor. There's unique Sylow p-subgroup $H \iff H$ is a normal subgroup of G, $H \lhd G$.

semidirect product with respect to $\phi : G' \to Aut(G)$: the group $G \rtimes_\phi G'$, composition: $(g_1, g_1')(g_2, g_2') = (g_1 \phi_{g_1'}(g_2), g_1' g_2')$

$G = H \rtimes K$. It means that $f : H \rtimes_\phi K \to G$ is an isomorphism, where $\phi : K \to Aut(H)$, $\phi_k(h) = khk^{-1}$, $f(h,k) = hk$.

$G = H \times K \iff H \cap K = \{1\}$, $HK = G$, and $H, K \lhd G$

$G = H \rtimes K \iff H \cap K = \{1\}$, $HK = G$, and $H \lhd G$

Results for classification:

- $|G| = p$, $G \cong \mathbb{Z}/p\mathbb{Z}$
- $|G| = 2p$, $G \cong \mathbb{Z}/2p\mathbb{Z}$ or $G \cong D_p$
- $|G| = p^2$, $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

6. Rings

ring $(R, +, \cdot)$: a set R with $+$ and $\cdot$, that satisfy:

1. $(R, +)$ forms an abelian group
2. "$\cdot$" is associative and there is a multiplicative identity $1 \in R$ s.t. $1 \cdot r = r \cdot 1 = r, \forall r \in R$
3. $\forall a, b, c \in R$, $(a+b)c = ac + bc$, $c(a+b) = ca + cb$

commutative ring: if "$\times$" is commutative

Prop. $\forall a, b \in R$, $0 \cdot a = a \cdot 0 = 0$, $-a = (-1) \cdot a$, $-(ab) = (-a)b = a(-b)$.

Examples:

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, where $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields
2. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, $\bar{a} + \bar{b} = \overline{a+b}$, $\bar{a}\bar{b} = \overline{ab}$
3. M_n, ring of $n \times n$ matrices (non-commutative when $n > 1$)

unit u: if $\exists u^{-1} \in R$, $uu^{-1} = 1$.

group of units, $R^\times$: the set of units of a ring R respect to multiplication

x is associated to y: $x, y \in R$ if $\exists u \in R^\times$ such that $x = uy$.

field: R with $R^\times = R \setminus \{0\}$, i.e., all the nonzero elements are units.

polynomial ring $R[x]$: the set of all polynomials with coefficients in R

A polynomial is monic if its leading coefficient is 1.

degree of a polynomial: the biggest power of x with nonzero coefficient.

Division Algorithm: If $f(x) \in R[x]$ is a monic polynomial, then for any $g(x) \in R[x]$, $\exists! q(x) \in R[x]$, $r(x) \in R[x]$ such that $g(x) = q(x)f(x) + r(x)$, with $\deg(r) < \deg(f)$.

ring homomorphism: $f : R \to R'$ s.t.

1. $\forall a, b \in R$, $f(a + b) = f(a) + f(b)$
2. $\forall a, b \in R$, $f(ab) = f(a)f(b)$
3. $f(1) = 1'$

kernel $\ker(f) = \{r \in R, f(r) = 0'\}$

Substitution Principle. $f : R \to R'$ is a ring homomorphism, $\alpha \in R'$. Then there is a unique ring homomorphism $F : R[x] \to R'$ that agrees with f on constant polynomials and sends x to α.

ideal: nonempty subset I of a ring R if:

1. $\forall a, b \in I$, $a + b \in I$
2. $\forall \alpha \in I$, $\forall r \in R$, $\alpha r \in I$

Prop. The kernel of a ring homomorphism $f : R \to R'$ is an ideal of R.

Prop. $(I, +)$ is a subgroup of $(R, +)$

Prop. $I \neq R \iff I \cap R^{\times} = \emptyset$, $I = R \iff I \cap R^{\times} \neq \emptyset \iff 1 \in I$

principal ideal generated by $a \in R$: $(a) = \{ar \in R | r \in R\}$

An ideal I is proper if $I \neq \{0\}$ and $I \neq R$.

Cor. principal ideal (a) is proper $\iff a \notin R^{\times} \cup \{0\}$

Cor. A nonzero ring is a field $\iff$ it has no proper ideal

integral domain: R if $ab = 0 \to a = 0$ or $b = 0$.

e.g. All fields are integral domains. All finite integral domains are fields.

e.g. $\mathbb{Z}/n\mathbb{Z}$ is an integral domain $\iff$ n is prime.

Principle Ideal Domain (PID): an integral domain all of whose ideals are principal.

Prop. $\mathbb{F}$ is a field. Then $\mathbb{F}[x]$ is a PID.

quotient ring: $R/I = \{r + I\}_{r \in R}$, I is ideal, $r_1 + I = r_2 + I \iff r_2 - r_1 \in I$

addition: $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$

multiplication: $(r_1 + I)(r_2 + I) = r_1 r_2 + I$

e.g. $R = \mathbb{Z}$, $I = n\mathbb{Z}$, $R/I = \mathbb{Z}/n\mathbb{Z}$

First Isomorphism Theorem. $f : R \to R'$ is a surjective homomorphism. $I = \ker(f)$. Then there exists a unique ring isomorphism $F : R/I \to R'$ such that $f = F \circ \pi$.

Cor. $R/\ker(f) \cong \mathrm{Im}(f)$.

maximal ideal: proper ideal I if for any ideal J of R that $I \subseteq J$, either $J = I$ or $J = R$.

Prop. I is a maximal ideal $\iff R/I$ is a field.

$\mathbb{F}$ is a field. $p(x) \in \mathbb{F}[x]$ is irreducible if it is not constant or a product of two polynomials.

Prop. $(p(x))$ is maximal in $\mathbb{F}[x] \iff p(x)$ is irreducible

so $\mathbb{F}[x]/(p(x))$ is a field $\iff p(x)$ is irreducible

Example: $R[x]/(x^2+1) \cong \mathbb{C}$