1 Chapter 1

Definition 1.1 (Matrix). A $m \times n$ matrix is a collection of mn numbers arranged in a rectangle like so:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \ldots & \cdots & \ldots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

Matrix multiplication is distributive:

$$A(B + B') = AB + AB', \quad (A + A')B = AB + A'B$$

And associative:

$$(AB)C = A(BC)$$

But not communative: $AB \neq BA$. Note that this also works in exactly the same fashion with block matrices.

Definition 1.2 (unit matrix). e_{ij} is 1 at entry i, j and zero everywhere else.

Definition 1.3 (elementary matrices). There are three types of elementary $n \times n$ matrices:

(i) One nonzero off-diagonal entry is added to the identity matrix at (i,j). In this case, EX adds a of row j of X to row i. (draw it out) (ii) The ith and jth diagonal entries of the identity matrix are replaced with zeros and 1's are added in the (i, j) and (j, i) positions. In this case when we have EX, we just swap rows i and j of X. (iii) One diagonal entry of the identity matrix is replaced by a nonzero scalar c. EX simply scales up row i by (a).

All elementary matrices are invertible. Their inverses are also elementary matrices.

Definition 1.4 (Row Echelon matrix). A row echelon matrix, M has the following properties:

- if row i of M is zero, then row j is zero $\forall j > i$
- if row i isn't zero, its first nonzero entry is 1. This is called a pivot
- if row $i + 1$ isn't zero, the pivot in row i+1 is to the right of the pivot in row i.
- The entries above and below a pivot are zero

Definition 1.5 (Permutation). A permutation is a mapping from a set to another set. The notation here is new. Basically, suppose we have a set of numbers $\{1, 2, 3, 4, 5\}$. Then, we have something that looks like this that represents p:

$$p = (341)(25)$$

This means that $3 \to 4$, $4 \to 1$, $1 \to 3$, etc.

Each group within parentheses is considered a n-cycle. 2-cycles are denoted transpositions. Note that when you have a permutation and elements are not listed, they are implicitly identity. Each permutation has a permutation matrix associated with it, which performs the permutation on a matrix.

The inverse of a permutation matrix is its transpose.

Definition 1.6 (random properties of invertible matrices).

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

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

2 Chapter 2

Definition 2.1 (Function types). For a function $f : X \to Y$ (domain to codomain):
surjective is at least one arrow per ele in codomain (codomain overmapped): $\forall y \in Y \exists x \in X$ s.t. $y = f(x)$
injective is at most one in arrow per ele in codomain (codomain undermapped): $\forall x, x' \in X, f(x) = f(x') \implies x = x'$
bijective is one to one: both surjective and injective

Definition 2.2 (Law of Composition). A function of two variables:

$$S \times S \to S$$

Where $S \times S$ is the product of two sets (set of pairs).

Definition 2.3 (Examples of laws of composition). Here's two examples:

- (ab) c = a(bc) (associative law)
- ab = ba (communative)

Definition 2.4 (Group). A group is a set G and a law of composition with the following properties:

- The law of composition is associative: $(ab)c = a(bc)$
- G contains an identity element 1 s.t. $1a = a$ and $a1 = a$ forall a in G
- Every element a of G has an inverse, an element b s.t. $ab = 1$ and $ba = 1$

A group's order (number elemenets) is its cardinality.

Definition 2.5 (Abelian Group). A group whose law of composition is commutative. That is to say, $ab = ba$. Also denoted a **commutative group**

And now for some common groups...

Definition 2.6 ($n \times n$ Common groups). General linear group: group of all invertible n by n matrices. Denoted GL_n
Special linear group: group of all n by n matrices with determinant 1. Denoted SL_n.
Alternating group: set of even permutations. Denoted A_n

Definition 2.7 (permutation group). The group of permutations of the set of n indices is called the **symmetric group**. This includes all permutations of those n indices.

Definition 2.8 (Subgroup). A subset H of a group G is a subgroup if it has the following properties:

- Closure: if a and b are in H, then ab is in H
- Identity: 1 is in H
- Inverses: If a is in H, then a^{-1} is also in H

There are two *trivial* subgroups for any group G. The subgroup containing every element in G, and the subgroup only containing the identity. Subgroups that are not *trivial* are denoted *proper*.

Definition 2.9 (divides). Given two integers a and b, we say a divides b if there is an integer c such that $b = ac$. E.g. a divides b if b is a multiple of a. Equivalently, if a is a factor of b.

Definition 2.10 (Subgroup of Additive Group of Integers). A subset of a group G with law of composition written additively is a subgroup if it has these properties:

- Closure: if a and b are in S then $a + b$ is in S
- Identity: 0 is in S
- Inverses: If a is in S then $-a$ is in S

Define an additive subgroup notationally like this:

$$\mathbb{Z}a = \{n \in \mathbb{Z} | n = ka \text{ for some } k \in \mathbb{Z}\}$$

Also union of two groups is gcd, difference is lcm.

Definition 2.11 (bracket notation). $< x >$ means smallest subgroup generated by single element x in group G. Using multiplicative notation, this means:

$$< x >= \{\ldots, x^{-1}, 1, x, x^2\}$$

Definition 2.12 (order of element). The order of an element n in a group G is the smallest positive integer with the property $x^n = 1$

Definition 2.13 (homomorphism). Let G and G' be groups written with multiplicative notation. A homomorphism $\phi : G \to G'$ is a map from G to G' s.t. $\forall a, b \in G$:

$$\phi(ab) = \phi(a)\phi(b)$$

Trivial homomorphism maps every element in G to the identity in G'.

Note that this preserves both identity and inverse relations.

The image of a homomorphism is the set elements mapped to in G' from G THIS IS A SUBSET OF G. This is a subgroup of the range.

$$\phi(G) = \text{im}\phi = \{x \in G' | \exists a \text{ s.t. } x = \phi(a)\}$$

The kernel of a homomorphism is the set of elements of G that map to G'_{id}. This is also a subgroup.

$$\ker \phi = \{a \in G | \phi(a) = \text{id}\}$$

The kernel is a normal subgroup of G.

If the kernel is trivial, then this implies the mapping is injective because $a^{-1}b \in \ker \phi \implies \phi(a) = \phi(b)$. But we can't have this by defn b/c then the kernel is no longer trivial.

Congruence relation is defined to be elements a, b s.t. $\phi(a) = \phi(b)$

Definition 2.14 (cosets). Let H be a subgroup of a group G and a be an element of G. Then define:

$$aH = \{g \in G | g = ah \forall h \in H\} \text{ (left coset)}$$
$$Ha = \{g \in G | g = ha \forall h \in H\} \text{ (right coset)}$$

The number of left cosets in a subgroup is called **index** of H in G and denoted $[G : H]$. Let $G \subset H \subset K$ be subgroups of a group G. Then $[G : K] = [G : H][H : K]$

If is normal subgroup, left and right cosets are equal.

Definition 2.15 (conjugate). If a and g are elements of a group G, then the element gag^{-1} is the conjugate of a by g.

Definition 2.16 (normal subgroup). A subgroup N of a group G is a normal subgroup if for every a in N and every g in G, the conjugate gag^{-1} is also in N.

Definition 2.17 (center of group). The center of group G, denoted Z, is defined as:

$$Z = \{z \in G | zx = xz \forall x \in G\}$$

This is always normal (because commutivity)

Definition 2.18 (isomorphism). An isomorphism $\phi : G \to G'$ between groups G and G' is a **bijective** group homomorphism. E.g. each element is only mapped to once. This means there is another isomorphism $\phi^{-1} : G' \to G$. We denote isomorphic to as $G \approx G'$.

Definition 2.19 (Isomorphic Class). The groups isomorphic to a given group G form what is called the isomorphism class of G.

Definition 2.20 (Automorphism). An automorphism on G is defined to be a isomorphism $\phi : G \to G$.

Definition 2.21 (Conjugation). Let g be a fixed element of a group G. Conjugation by g is the map $\phi(x) = gxg^{-1}$. This is (fairly obviously) an automorphism.

Definition 2.22 (commuting in a group). The **commutator** $aba^{-1}b^{-1}$ is an element associated with a pair (a, b) in a group. Two elements a and b of a group commute, eg $ab = ba$, iff

$$aba^{-1} = b \longleftrightarrow aba^{-1}b^{-1} = 1$$

Definition 2.23 (partition). A partition Π of a set S is a subdivision of S into nonoverlapping, nonempty subsets.

Definition 2.24 (equivalence relation). An equivalence relation on a set S is a relation that holds between certain pairs of elements of S. We denote this $a \sim b$. Requirements are:

- **transitive**: if $a \sim b$ and $b \sim c$, then $a \sim c$
- **symmetric**: if $a \sim b$, then $b \sim a$
- **reflexive**: $\forall a, a \sim a$

With group homomorphisms, the equivalence relation is defined by:

$$\phi(a) = \phi(b) \to a \equiv b$$

Definition 2.25 (equivalence classes). An equivalent relation defines a partition (and vice versa). All the elements in one of the subsets in the partition are equivalent by $\sim$. These subsets are denoted **equivalence classes**. Bar is used to denote equivalence class. The set of equivalence classes from a set S is denoted $\bar{S}$. An equivalence class of element b is denoted $\bar{b}$.

Definition 2.26 (maps). For a map of sets $f : S \to T$, the inverse image, or $fibre$ is defined:

$$f^{-1}(t) = \{s \in S | f(s) = t\}$$

Non-empty fibres are equivalence classes for equivalence relation $a \sim b$ if $f(a) = f(b)$.

Definition 2.27 (Counting Formula). Note that all left cosets aH of a subgroup H of a group G have the same order, $|H|$, because the mapping is bijective (any element a has an inverse so you can undo whatever you did). We also know that these cosets partition G (each element in g times the id element in H means g is in some coset). As a result:

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

Colloraries:

- Langrange's theorem states if H is a subgroup of finite group G, then the order of H divides the order of G. Another collorary is (noting that the kernel is a subgroup), $|G| = |\ker \phi| * |\operatorname{im} \phi|$ Note that to prove this, use the fact $[G : \ker \phi] = |\operatorname{im} \phi|$. This holds true because the LHS is the number of nonempty fibres in G', and the RHS is the number of elements mapped to in G'.

- $|\operatorname{im}\phi|$ also divides G' b/c the image is a subgroup of G' (follows from lagrange).

Definition 2.28 (**Congruence Relation).** Given some subgroup H of a group G, right and left congruence are defined as follows:

$$a \equiv b \text{ if } b = ah \text{ for some } h \in H (\text{left congruence})$$

$$a \equiv b \text{ if } b = ha \text{ for some } h \in H (\text{right congruence})$$

These cosets both individually partition G.

Definition 2.29 (**congruence classes modulo n).** Denoted $\mathbb{Z}/\mathbb{Z}n$, $\mathbb{Z}/n\mathbb{Z}$, or $\mathbb{Z}/(n)$. Means set of congruence classes modulo n :congruence classes $\mathbb{Z}i$ for $i \in [0, n-1]$.

Definition 2.30 (**restricting homomorphism).** Let $\psi : G \to G'$ be a homomorphism and let H be a subgroup of G. We may restrict ϕ to H to get the homomorphism:

$$\phi|_H : H \to G'$$

Same map ϕ, smaller domain.

Definition 2.31 (**Correspondence Theorem).** Let $\phi : G \to G'$ be a surjective homomorphism with kernel K. There is a bijective correspondence between subgroups of G' and subgroups of G that contain K. Then we have that that map is:

$$\text{subgroup H of G that contains K} \to \text{ its image } \phi(H) \in G'$$

$$\text{a subgroup H' of G'} \to \text{ its inverse image } \phi^{-1}(H') \in G$$

If H and H' are corresponding subgrupos, then H is normal in G iff H' is normal in G'.

If H and H' are corresponding subgroups, then $|H| = |H'||K|$ (follows naturally from counting formula).

Definition 2.32 (**Product group).** A product group is defined to be cartesian product of two groups with pairs. Multiplication is pairwise– $(a, b) \cdot (a', b') = (aa', bb')$. It's denoted $G \times G'$. Mapping from product group back to G or G' is called a projection.

Definition 2.33 (**Quotient Group).**

$$\bar{G} = G/N \text{ is the set of cosets of a normal subgroup} N \text{ in group} G$$

A theorem for why quotient groups are useful:

Let N is a normal subgroup of a group G, and let $\bar{G}$ denote the set of cosets of N in G. There is a law of composition of $\bar{G}$ that makes this set into a group s.t. the map $\phi : G \to \bar{G}$ defined by $\pi(a) \to \bar{a}$ is a surjective homomorphism whose kernel is N.

π is denoted **canonical map** from G to $\bar{G}$.

Definition 2.34 (Proper Subgroup). The subgroup is an actual subset; e.g. G and H (H is subset of G) are not the same.

Definition 2.35 (Product Set). If A and B are subsets of a group G, then AB denotes the set of products:

$$AB = \{x \in G | x = ab \text{ for some } a \in A, b \in B\}$$

Definition 2.36 (First Isomorphism Theorem). Let $\phi : G \to G'$ be a surjective group homomorphism with kernel N. The quotient group $\bar{G} = G/N$ is isomorphic to the image G'. If $\pi : G \to G'$ is the canonical map, then there is a unique isomorphism $\bar{\phi} : \bar{G} \to G'$ s.t. $\phi = \bar{\phi} \circ \pi$:

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"] & G' \\ \bar{G} \arrow[ur, "\bar{\phi}"] & \end{tikzcd}$$