

Chapter 1: Matrix Operations

Section 1.2: Row Reduction

Def: There are three types of **elementary matrices**:

Type	Definition	Action	Determinant
1.	$I + ae_{ij}$	Replace i th row X_i by $X_i + aX_j$	1
2.	$I + e_{ij} + e_{ji} - e_{ii} - e_{jj}$	Swaps row i with row j	-1
3.	$I + (c - 1)e_{ii} (c \neq 0)$	Multiply row i by a nonzero scalar c	c

Lma: Elementary matrices are invertible, and their inverses are also elementary matrices.

Def: The process of multiplying by elementary row operations on a matrix A , resulting in a matrix A' is called **row reduction** or **Gaussian elimination**.

Prop: The solutions of $A'X = B'$ are the same as those of $AX = B$.

Def: A matrix in **row echelon** form has the properties: A. The first nonzero entry in every row is 1. This entry is called a **pivot**. B. The first nonzero entry of row $i + 1$ is to the right of the first nonzero entry of row i . C. The entries above a pivot are zero.

Prop: Let $M' = [A'|B']$ be a row echelon matrix. Then the system of equations $A'X = B'$ has a solution if and only if there is no pivot in the last column B' . In that case, an arbitrary value can be assigned to the unknown x_i if column i does not contain a pivot.

Cor: every system $AX = 0$ of m homogenous equations in n unknowns with $m < n$ has a solution X in which some x_i is nonzero.

Prop: Let A be a square matrix. The following conditions are equivalent: A. A can be reduced to the identity by a sequence of elementary row operations. B. A is a product of elementary matrices. C. A is invertible. D. The system of homogeneous equations $AX = 0$ has only the trivial solution $X = 0$.

Cor: If a row of a square matrix A is zero, then A is not invertible.

Cor: Let A be an invertible matrix. To compute its inverse A^{-1} , apply elementary row operations E_1, \dots, E_k to A , reducing it to the identity matrix. The same sequence of operations, when applied to I , yields A^{-1} .

Prop: Let A be a square matrix which has either a left inverse $B: BA = I$, or a right inverse $AB = I$. Then A is invertible, and B is its inverse.

Section 1.3: Determinants

Def: The **determinant** of a 1×1 matrix is the value of its only element. For $n \times n$ matrices with $n > 1$, let the determinant be defined recursively as:

$$\det A = a_{1,1} \det A_{1,1} - a_{2,1} \det A_{2,1} + \dots \pm a_{n,1} \det A_{n,1}.$$

Some properties of the determinant:

$\det A$ is linear in the rows of the matrix.

If two adjacent rows of a matrix A are equal, then $\det A = 0$.

If a multiple of one row is added to another row, the determinant is unchanged.

If two rows are interchanged, the determinant is multiplied by -1 .

If a row of A is zero, then $\det A = 0$.

Thm: The determinant function is the *only* one with these properties.

Cor: A square matrix A is invertible if and only if $\det A \neq 0$.

Thm: Let A, B be any two $n \times n$ matrices. Then $\det(AB) = (\det A)(\det B)$.

Cor: If A is invertible, $\det(A^{-1}) = \frac{1}{\det A}$.

Prop: Let A^t denote the transpose of A . Then $\det A = \det A^t$.

Cor: The above properties hold when swapping the word *row* for *column*.

Section 1.4: Permutation Matrices

Def: A **permutation matrix** P is a matrix such that the operation of left multiplication by P is a permutation of the rows of a matrix.

Note: When we permute the *entries* of a vector $(x_1, \dots, x_n)^t$ according to a permutation p , the *indices* are permuted in the opposite way.

Prop: Let P be the permutation matrix associated to a permutation p . A. the j th column of P is the column vector $e_{p(j)}$. B. P is a sum of n matrix units: $P = \sum e_{p(j),j}$.

Prop: A. Let p, q be two permutations, with associated permutation matrices P, Q . Then the matrix associated to the permutation pq is the product PQ . B. A permutation matrix P is invertible, and its inverse is the transpose matrix: $P^{-1} = P^t$.

Section 1.5: Cramer's Rule

Def: Let A be an $n \times n$ matrix. The **adjoint** of A is the $n \times n$ matrix whose (i, j) entry $(\text{adj } A)_{ij}$ is $(-1)^{i+j} \det A_{ij} = \alpha_{ji}$, where A_{ij} is the matrix obtained by crossing out the i th row and the j th column.

Thm: Let $\delta = \det A$. Then $(\text{adj } A) \cdot A = \delta I$, and $A \cdot (\text{adj } A) = \delta I$.

Cor: Suppose that the determinant δ of A is not zero. Then $A^{-1} = \frac{1}{\delta}(\text{adj } A)$.

Chapter 2: Groups

Section 2.1: The Definition of a Group

Prop: Suppose an associative law of composition is given on a set S . There is a unique way to define, for every integer n , a product of n elements a_1, \dots, a_n of S with the following properties: 1. The product $[a_1]$ is the element itself. 2. The product $[a_1 a_2]$ is the law of composition itself. 3. For any integer i between 1 and n , $[a_1 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$.

Def: A **group** is a set G paired with a composition law \cdot such that 1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associative law) 2. $\exists e \in G$ such that $x \cdot e = x = e \cdot x \forall x \in G$ (identity). 3. $\forall x \in G, \exists y \in G$ such that $xy = e = yx$ (inverses).

Def: A group G is **abelian** if the law of composition is **commutative**, or: $ab = ba \forall a, b \in G$.

Prop (*Cancellation Law*): Let G be a group with $a, b, c \in G$. If $ab = ac$, then $b = c$. If $ba = ca$, then $b = c$.

Ex: The set of $n \times n$ invertible matrices with entries in a field \mathbb{F} is the $n \times n$ **general linear group**, denoted $\text{GL}_n(\mathbb{F})$.

Ex: The group of permutations of the set $\{1, 2, \dots, n\}$ is called the **symmetric group** denoted by S_n .

Section 2.2: Subgroups

Def: A subset H of a group G is called a **subgroup** if it has the following properties: 1. **Closure**: $\forall a, b \in H, ab \in H$. 2.

Identity: $e \in H$. 3. **Inverses**: If $a \in H$, then $a^{-1} \in H$. A subgroup is denoted $H \leq G$. Two immediate subgroups of a group G are $\{e\}$ and G . A subgroup is **proper** if it is neither of these.

Prop: For any integer b , the subset $b\mathbb{Z}$ is a subgroup of \mathbb{Z}^+ . Moreover, every subgroup H of \mathbb{Z}^+ is of the type $H = b\mathbb{Z}$ for some integer b .

Prop: Let a, b be integers, not both zero, and let d be the positive integer which generates the subgroup $a\mathbb{Z} + b\mathbb{Z}$. Then:

A. d can be written in the form $d = ar + bs$ for some integers r and s . B. d divides a and b . C. If an integer e divides a and b , it also divides d .

Lma: For a group G and an element $x \in G$, the set S of integers n such that $x^n = 1$ is a subgroup of \mathbb{Z}^+ .

Def: A **cyclic group of order m** is a group $H = \{1, x, \dots, x^{m-1}\}$ such that each element given is distinct and $x^m = 1$.

Def: The **order** of a group is the number of its elements, denoted $|G|$.

Ex: The **Klein four group** V is the simplest group which is not cyclic, consisting of four matrices $\begin{bmatrix} \pm 1 & \\ & \pm 1 \end{bmatrix}$.

Ex: The **quaternion group** $H = \{\pm 1, \pm i, \pm j, \pm k\}$ is a small subgroup of $\text{GL}_2(\mathbb{C})$.

Section 2.3: Isomorphisms

Def: An **isomorphism** φ from G to G' is a bijective map which is compatible with the laws of composition: $\varphi(ab) = \varphi(a)\varphi(b) \forall a, b \in G$. Two groups G and G' are **isomorphic** if there exists an isomorphism $\varphi : G \rightarrow G'$.

Def: An **automorphism** is an isomorphism from a group to itself. An example automorphism for any group G is **conjugation** by an element $b \in G$, defined as the map $a \mapsto bab^{-1}$. The element bab^{-1} is called the **conjugate** of a by b . a and a' are **conjugates** if $a' = bab^{-1}$ for some $b \in G$.

Section 2.4: Homomorphisms

Def: A **homomorphism** $\varphi : G \rightarrow G'$ is any map satisfying $\varphi(ab) = \varphi(a)\varphi(b)$.

Prop: A group homomorphism $\varphi : G \rightarrow G'$ carries the identity to the identity, and inverses to inverses: $\varphi(1_G) = 1_{G'}$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Def: The **image** of a homomorphism is denoted $\text{im } \varphi = \{x \in G' \mid \exists a \in G, x = \varphi(a)\}$. The **kernel** of a homomorphism is denote $\ker \varphi = \{x \in G \mid \varphi(x) = 1_{G'}\}$.

Ex: The kernel of the determinant homomorphism is the subgroup of matrices whose determinant is 1, called the **special linear group** denoted $\text{SL}_n(\mathbb{F})$.

Ex: The kernel of the sign homomorphism is the **alternating group** on n elements: A_n .

Def: A subgroup $N \leq G$ is called a **normal subgroup** if: $\forall a \in N, \forall b \in G, bab^{-1} \in N$, denoted $N \trianglelefteq G$.

Def: The **center** of a group G is the set $Z(G)$ of elements which commute with every element of G : $Z(G) = \{z \in G \mid xz = zx \forall x \in G\}$.

Section 2.5: Equivalence Relations and Partitions

Def: Let S be a set. A **partition** P of S is a subdivision of S into nonoverlapping subsets. An **equivalence relation** on S is a relation between certain elements ($a \sim b$) that is transitive, symmetric, and reflexive. The subset containing a and all elements b such that $a \sim b$ is called the **equivalence class** of a .

Def: The **inverse image** of a map $\varphi : S \rightarrow T$ is the subset $\varphi^{-1}(t) = \{s \in S \mid \varphi(s) = t\}$. These images are also called **fibres** of the map φ . The nonempty fibres form a partition of S . Elements in the same fibre are frequently referred to as **congruent**: $a \equiv b$ if $\varphi(a) = \varphi(b)$.

Prop: Let $\varphi : G \rightarrow G'$ be a group homomorphism with kernel N and let a, b be elements of G . Then $\varphi(a) = \varphi(b)$ if and only if $b = an$ for some element $n \in N$, or equivalently, if $a^{-1}b \in N$.

Def: The set of elements of the form an is denoted by aN and is called a **coset** of N in G : $aN = \{g \in G \mid g = an \text{ for some } n \in N, a \in G\}$. The congruence relation $a \equiv b$ partitions the group G into **congruence classes**, the cosets aN .

Cor: The group homomorphism $\varphi : G \rightarrow G'$ is injective if and only if its kernel is the trivial subgroup.

Section 2.6: Cosets

Def: For $H \leq G$, a **left coset** is a subset of the form $aH = ah \mid h \in H$.

Cor: The left cosets of a subgroup partition the group.

Note: $aH = bH$ if and only if $a \equiv b$. If aH and bH have an element in common, then they are equal.

Def: The number of left cosets of a subgroup $H \leq G$ is called the **index** of H in G , denoted $[G : H]$.

Thm (*Counting Formula*): $|G| = |H|[G : H]$.

Cor (*Lagrange's Theorem*): Let G be a finite group, and let H be a subgroup of G . The order of H divides the order of G .

Note: The order of an element divides the order of the group.

Cor: Suppose that a group G has p elements and that p is a prime integer. Let $a \in G$ be any element, not the identity. Then $\langle a \rangle$ is the cyclic group $\{1, a, \dots, a^{p-1}\}$ generated by a .

Cor: Let $\varphi : G \rightarrow G'$ be a homomorphism of finite groups. Then $|G'| = |\ker \varphi| |\text{im} \varphi|$. Thus $|\ker \varphi|$ divides $|G|$, and $|\text{im} \varphi|$ divides both $|G|$ and $|G'|$.

Def: The **right cosets** of a subgroup $H \leq G$ are the subsets $Ha = \{ha \mid h \in H\}$.

Prop: A subgroup H of a group G is normal if and only if every left coset is also a right coset. If H is normal, then $aH = Ha$ for every $a \in G$.

Section 2.7: Restriction of a Homomorphism to a Subgroup

Prop: The intersection $K \cap H$ of two subgroups is a subgroup of H . If K is a normal subgroup of G , then $K \cap H$ is a normal subgroup of H .

Prop: Let $\varphi : G \rightarrow G'$ be a homomorphism, and let H' be a subgroup of G' . Denote the inverse image $\varphi^{-1}(H') = \{x \in G \mid \varphi(x) \in H'\}$ by \tilde{H} . A. $\tilde{H} \leq G$. B. $H' \trianglelefteq G' \Rightarrow \tilde{H} \trianglelefteq G$. C. $\ker \varphi \subseteq \tilde{H}$. D. The restriction of φ to \tilde{H} defines a homomorphism $\tilde{H} \rightarrow H'$ whose kernel is $\ker \varphi$.

Section 2.8: Products of Groups

Prop (*The Mapping Property of Products*): Let H be any group. The homomorphism $\Phi : H \rightarrow G \times G'$ are in bijective correspondence with pairs (φ, φ') of homomorphisms $\varphi : H \rightarrow G$, $\varphi' : H \rightarrow G'$. $\ker \Phi = \ker \varphi \cap \ker \varphi'$.

Prop: Let r, s be integers with no common factor. A **cyclic** group of order rs is isomorphic to the product of a cyclic group of order r and a cyclic group of order s .

Prop: Let H and K be subgroups of a group G .

1. If $H \cap K = \{1\}$, the product map $p : H \times K \rightarrow G$ defined by $p(h, k) = hk$ is injective. $\text{im} p = HK \subseteq G$.
2. If either H or K is a normal subgroup of G then the product sets HK and KH are equal, and $HK \leq G$.
3. If H and K are both normal, $H \cap K = \{1\}$, and $HK = G$, then $G \cong H \times K$.

Section 2.9: Modular Arithmetic

Def: Two integers a, b are said to be **congruent modulo n** , written $a \equiv b \pmod{n}$ if $n \mid b - a$ or $b = a + nk$ for some integer k . This relation defines equivalence classes, called **congruence classes**.

Prop: There are n congruence classes modulo n , namely $\bar{0}, \bar{1}, \dots, \overline{n-1}$. Or, the index $[\mathbb{Z} : n\mathbb{Z}] = n$.

Lma: If $a' \equiv a \pmod{n}$ and $b' \equiv b \pmod{n}$, then $a' + b' \equiv a + b \pmod{n}$ and $a'b' \equiv ab \pmod{n}$.

Section 2.10: Quotient Groups

Lma: Let $N \trianglelefteq G$. Then the product of two cosets aN, bN is again a coset, in fact $(aN)(bN) = (ab)N$.

Thm: With the law of composition as composition of coset representatives, $\bar{G} = G/N$ is a group, and the map $\pi : G \rightarrow \bar{G}$ defined as $\pi(a) = aN$ is a homomorphism whose kernel is N . $|G/N| = [G : N]$.

Def: Groups of the form G/N are **quotient groups**.

Cor: Every normal subgroup of a group G is the kernel of a homomorphism.

Derrick Stolee – Algebra Study Guide

Lma: Let G be a bgroup, and let S be any set with a law of composition. Let $\varphi : G \rightarrow S$ be a surjective map which has the property $\varphi(a)\varphi(b) = \varphi(ab)$ for all $a, b \in G$. Then S is a group.

Thm (*First Isomorphism Theorem for Groups*): Let $\varphi : G \rightarrow G'$ be a group homomorphism. Then $G/\ker\varphi \cong \text{im}\varphi$ by the map $\bar{\varphi}(aN) = \varphi(a)$.