MATH COMPREHENSIVE EXAM NOTES

ALEXANDER LEE

Multivariable Calculus

Elementary Vector Analysis

Notation. The Cartesian coordinates: $(x, y) \in \mathbb{R}^2$ and $(x, y, z) \in \mathbb{R}^3$.

Notation. A vector $\vec{v}$ in $\mathbb{R}^2$ or $\mathbb{R}^3$ is often represented by a directed line segment. In terms of coordinates, we write $\vec{v} = \langle a_1, a_2 \rangle$ in $\mathbb{R}^2$ and $\vec{v} = \langle a_1, a_2, a_2 \rangle$ in $\mathbb{R}^3$.

Notation. The standard basis vectors $\vec{\imath} = \langle 1, 0 \rangle$, $\vec{\jmath} = \langle 1, 0 \rangle$ in $\mathbb{R}^2$ and $\vec{\imath} = \langle 1, 0, 0 \rangle$, $\vec{\jmath} = \langle 0, 1, 0 \rangle$, $\vec{k} = \langle 0, 0, 1 \rangle$ in $\mathbb{R}^3$.

Notation. A vector $\vec{v}$ has length $|\vec{v}|$, sometimes denoted $||\vec{v}||$.

Fact. Nonzero vectors $\vec{v}$ and $\vec{u}$ are parallel if and only if each is a constant multiple of the other.

Definition. A point P in $\mathbb{R}^2$ or $\mathbb{R}^3$ gives a vector from the origin to P, called the position vector of P. This allows us to regard points as vectors and vice versa.

Definition. The length of a n-dimensional vector $\vec{v} = \langle a_1, \ldots, a_n \rangle$ is

$$|\vec{v}| = \sqrt{{a_1}^2 + \cdots + {a_n}^2}$$

Definition. In $\mathbb{R}^2$, the dot (scalar) product of $\vec{u} = \langle a_1, a_2 \rangle$ and $\vec{v} = \langle b_1, b_2 \rangle$ is $\vec{u} \cdot \vec{v} = a_1 b_1 + a_2 b_2$, and similarly in $\mathbb{R}^3$, the dot product of $\vec{u} = \langle a_1, a_2, a_3, \rangle$ and $\vec{v} = \langle b_1, b_2, b_3 \rangle$ is $\vec{u} \cdot \vec{v} = a_1 b_1 + a_2 b_2 + a_3 b_3$.

Facts. The linearity properties of the dot product:

(1) $\vec{u} \cdot \vec{u} = |\vec{u}|^2$.
(2) $\vec{u} \cdot \vec{v} = \vec{v} \cdot \vec{u}$.
(3) $\vec{u} \cdot (\vec{v} + \vec{w}) = \vec{u} \cdot \vec{v} + \vec{u} \cdot \vec{w}$.
(4) $(c\vec{u}) \cdot \vec{v} = c(\vec{u} \cdot \vec{v}) = \vec{v} \cdot (c\vec{v})$.
(5) $\vec{0} \cdot \vec{u} = 0$.

Additional properties:

(1) $\vec{u} \cdot \vec{v} = |\vec{u}||\vec{v}| \cos\theta$, where θ is the angle between $\vec{u}$ and $\vec{v}$.
(2) $\vec{u} \cdot \vec{v} = 0$ if and only if $\vec{u}$ and $\vec{v}$ are perpendicular (orthogonal).

Definition. Given $\vec{u} = \langle a_1, a_2, a_3 \rangle$ and $\vec{v} = \langle b_1, b_2, b_3 \rangle$ in $\mathbb{R}^3$, their cross (vector) product is

$$\vec{u} \times \vec{v} = \det \begin{pmatrix} \vec{\imath} & \vec{\jmath} & \vec{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix} = \det \begin{pmatrix} a_2 & a_3 \\ b_2 & b_3 \end{pmatrix} \vec{\imath} - \det \begin{pmatrix} a_1 & a_3 \\ b_1 & b_3 \end{pmatrix} \vec{\jmath} + \det \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \vec{k}.$$

Facts. The linearity properties of the cross product:

(1) $\vec{u} \times \vec{v} = -\vec{v} \times \vec{u}$.
(2) $(c\vec{u}) \times \vec{v} = c(\vec{u} \times \vec{v}) = \vec{u} \times (c\vec{v})$.
(3) $\vec{u} \times (\vec{v} + \vec{w}) = \vec{u} \times \vec{v} + \vec{u} \times \vec{w}$.
(4) $(\vec{u} + \vec{v}) \times \vec{w} = \vec{u} \times \vec{w} + \vec{v} \times \vec{w}$.
(5) $\vec{u} \cdot (\vec{v} \times \vec{w}) = (\vec{u} \times \vec{v}) \cdot \vec{w}$.
(6) $\vec{u} \times (\vec{v} \times \vec{w}) = (\vec{u} \cdot \vec{w})\vec{v} - (\vec{u} \cdot \vec{v})\vec{w}$.

Additional properties:

(1) $|\vec{u} \times \vec{v}| = |\vec{u}||\vec{v}| \sin\theta$, where θ is the angle between $\vec{u}$ and $\vec{v}$.
(2) $\vec{u} \times \vec{v} = \vec{0}$ if and only if $\vec{u}$ and $\vec{v}$ are parallel.
(3) $\vec{u} \times \vec{v}$ is perpendicular to both $\vec{u}$ and $\vec{v}$.

Definition. In $\mathbb{R}^2$ or $\mathbb{R}^3$, a point $\vec{r}_0$ and a nonzero vector $\vec{v}$ determine the line parametrized by

$$\vec{r}(t) = \vec{r}_0 + t\vec{v}.$$

The vector $\vec{v}$ is called a direction vector of the line. The parametric equations of a line for the coordinates $(x, y, z) \in \mathbb{R}^3$ are

$$x = x_0 + at \quad y = y_0 + bt \quad z = z_0 + ct,$$

where $\vec{v} = \langle a, b, c\rangle$, $\vec{r}_0 = \langle x_0, y_0, z_0\rangle$, and $t \in \mathbb{R}$. For $\mathbb{R}^2$, omit z.

Definition. A plan in $\mathbb{R}^3$ is defined by an equation of the form $ax + by + cz = d$ where $\langle a, b, c\rangle \neq \langle 0, 0, 0\rangle$. A more geometric way to write the equation uses a nonzero vector $\vec{n}$ perpendicular to the plane and point (x_0, y_0, z_0) in the plan. Then:

$$\begin{aligned}(x, y, z) \text{ is in the plane } &\iff \vec{n} \text{ is perpendicular to the vector from } (x, y, z) \text{ to } (x_0, y_0, z_0)\\ &\iff \vec{n} \cdot \langle x - x_0, y - y_0, z - z_0\rangle = 0.\end{aligned}$$

The vector $\vec{n}$ is called a normal vector to the plane. For a plane defined by $ax + by + cz = d$, a normal vector is given by $\vec{n} = \langle a, b, c\rangle$.

Definition. Given a curve parameterization $\vec{r}(t) = (x(t), y(t))$ in the plane, the tangent vector to the curve at the point $\vec{r}(t)$ is

$$\vec{r'}(t) = \langle x'(t), y'(t)\rangle.$$

The situation is similar on $\mathbb{R}^3$.

Functions of Several Variables

Definition. If f is a function of two variables, its partial derivatives are the functions f_x and f_y defined by

$$f_x(x, y) = \lim_{h \to 0} \frac{f(x + h, y) - f(x, y)}{h}$$
$$f_y(x, y) = \lim_{h \to 0} \frac{f(x, y + h) - f(x, y)}{h}$$

If f is a function of three variables x, y, and z, then its partial derivative with respect to x is defined as

$$f_x(x, y, z) = \lim_{h \to 0} \frac{f(x + h, y, z) - f(x, y, z)}{h}$$

Notation. The standard notation for the partial derivatives: $\frac{\partial f}{\partial x} = f_x(x, y)$, $\frac{\partial f}{\partial y} = f_y(x, y)$, $\frac{\partial^2 f}{\partial^2 x} = f_{xx}(x, y)$, $\frac{\partial^2 f}{\partial x \partial y} = f_{yx}(x, y)$, $\frac{\partial^2 f}{\partial^2 y} = f_{yy}(x, y)$ for $f(x, y)$, and similarly for $f(x, y, z)$.

Interpretation. If $z = f(x, y)$, then $\partial z/\partial x$ represents the rate of change of z with respect to x when y is fixed. Similarly, $\partial z/\partial y$ represents the rate of change of z with respect to y when x is fixed.

If $w = f(x, y, z)$, then $f_x = \partial w/\partial x$ can be interpreted as the rate of change of w with respect to x when y and z are held fixed.

Fact. Rule for find partial derivatives of $z = f(x, y)$.

(1) To find f_x, regard y as a constant and differentiate $f(x, y)$ with respect to x.
(2) To find f_y, regard x as a constant and differentiate $f(x, y)$ with respect to y.

Definition. A unit vector is a vector whose length is 1. In general, if $\vec{v} \neq \vec{0}$, then the unit vector that has the same direction as $\vec{v}$ is

$$\vec{u} = \frac{\vec{v}}{|\vec{v}|}.$$

Definition. The directional derivative of $f(x, y)$ in the direction of a unit vector $\vec{u} = \langle u_1, u_2 \rangle$ at the point (a, b) is

$$D_{\vec{u}} f(a, b) = \lim_{h \to 0} \frac{f(a + hu_1, b + hu_2) - f(a, b)}{h}$$

if this limit exists.

The directional derivative of $f(x, y, z)$ in the direction of a unit vector $\vec{u} = \langle u_1, u_2, u_3 \rangle$ at the point (a, b, c) is

$$D_{\vec{u}} f(a, b, c) = \lim_{h \to 0} \frac{f(a + hu_1, b + hu_2, c + hu_3) - f(a, b, c)}{h}$$

if this limit exists.

Interpretation. The directional derivative is the rate of change of a function of two or more variables in any direction.

Definition. The gradient of $f(x, y)$ at (a, b) is the vector

$$\nabla f(a, b) = \frac{\partial f}{\partial x}(a, b)\vec{\imath} + \frac{\partial f}{\partial y}(a, b)\vec{\jmath} = \left\langle \frac{\partial f}{\partial x}(a, b), \frac{\partial f}{\partial y}(a, b) \right\rangle$$

and similarly for $f(x, y, z)$.

Fact. $\nabla f(a, b)$ is perpendicular to the level curve $f(x, y) = f(a, b)$ at the point (a, b). Similarly, $\nabla f(a, b, c)$ is perpendicular to the level surface $f(x, y, z) = f(a, b, c)$ at (a, b, c).

Theorem. If $f(a, b)$ is differentiable at (a, b) and $\vec{u}$ is a unit vector, then

$$D_{\vec{u}} f(a, b) = \nabla f(a, b) \cdot \vec{u},$$

and similarly for $f(x, y, z)$.

Theorem. When $\nabla f(a, b) \neq \vec{0}$, the unit vector $\nabla f(a, b)/|\nabla f(a, b)|$ gives the direction in which $f(x, y)$ is increasing most rapidly. Furthermore, the maximum rate of increase is $|\nabla f(a, b)|$. Similar results hold for $f(x, y, z)$.

Facts. Tangent planes arise in two situations:

- If $f(x, y)$ is differentiable at (x_0, y_0), then the tangent plane to the graph $z = f(x, y)$ at the point $(x_0, y_0, f(x_0, y_0))$ is defined by

$$z - f(x_0, y_0) = f_x(x_0, y_0)(x - x_0) + f_y(x_0, y_0)(y - y_0). \tag{1}$$

- If $F(x,y,z)$ is differentiable at (x_0,y_0,z_0), then (x_0,y_0,z_0) lies on the level surface $F(x,y,z)=F(x_0,y_0,z_0)$, and the equation of the tangent plane to the surface at this point is defined by

$$\nabla F(x_0,y_0,z_0)\cdot(x-x_0,y-y_0,z-z_0)=0, \tag{2}$$

provided that the gradient $\nabla F(x_0,y_0,z_0)$ is nonzero. Written out, this is the equation

$$F_x(x_0,y_0,z_0)(x-x_0)+F_y(x_0,y_0,z_0)(y-y_0)+F_z(x_0,y_0,z_0)(z-z_0)=0.$$

The two situations are related since the graph $z=f(x,y)$ is the level surface $F(x,y,z)=f(x,y)-z=0$. Since $\nabla F=f_x\vec{\imath}+f_y\vec{\jmath}-\vec{k}$, equation (2) reduces to equation (1) in this case.

Maxima and Minima of Functions of Several Variables

Definition. In two dimensions (a,b) is a critical point of $f(x,y)$ provided

$$f_x(a,b)=f_y(a,b)=0.$$

Definition. A function of two variables has a local maximum at (a,b) if $f(x,y)\leq f(a,b)$ when (x,y) is near (a,b). [This means that $f(x,y)\leq f(a,b)$ for all points (x,y) in soem disk with center (a,b).] The number $f(a,b)$ is called a local maximum value. If $f(x,y)\geq f(a,b)$ when (x,y) is near (a,b), then f has a local minimum at (a,b) and $f(a,b)$ is a local minimum value.

Fact. If f has a local maximum or minimum at (a,b) and the first-order partial derivatives of f exist there, then (a,b) is a critical point of f.

Definition. Let (a,b) be a critical point of f. (a,b) is called a saddle point of f if $f(a,b)$ is not a local maximum or minimum.

Fact. For a suitably nice function $f(x,y)$, the second derivative test goes as follows. Let (a,b) be a critical point of f, and define

$$D=\det\begin{pmatrix} f_{xx} & f_{xy} \\ f_{xy} & f_{yy}\end{pmatrix}.$$

Then:

- If $D(a,b)>0$ and $f_{xx}(a,b)>0$, then f has a local minimum at (a,b).
- If $D(a,b)>0$ and $f_{xx}(a,b)<0$, then f has a local maximum at (a,b).
- If $D(a,b)<0$, then f has a saddle point at (a,b).

The second derivative test is inconclusive in all other cases.

Fact. In a constrained optimization problem, you want to find the maximum or minimum of a function subject to a constraint. Such problems occur in two and three dimensions and use the method of Lagrange multipliers. We assume that the function and constraint are differentiable.

- To maximize or minimize $f(x,y)$ subject to the constraint $g(x,y)=0$, solve

$$\nabla f(x,y)=\lambda\nabla g(x,y),\quad g(x,y)=0,$$

or equivalently,

$$f_x(x,y)=\lambda g_x(x,y),\quad f_y(x,y)=\lambda g_y(x,y),\quad g(x,y)=0.$$

- To maximize or minimize $f(x,y,z)$ subject to the constraint $g(x,y,z)=0$, solve
$$\nabla f(x,y,z) = \lambda \nabla g(x,y,z), \quad g(x,y,z)=0,$$
or equivalently,

$$f_x(x,y,z)=\lambda g_x(x,y,z), \quad f_y(x,y,z)=\lambda g_y(x,y,z), \quad f_z(x,y,z)=\lambda g_z(x,y,z), \quad g(x,y,z)=0.$$

It is customary to call λ the Lagrange multiplier.

Fact. A problem may ask for the maximum and minimum values (also called extreme values) of a differentiable function $f(x,y)$ on a closed and bounded region in the plane. Extreme values are known to exist in this situation. They can occur in one of two places:

- In the interior of the region, where they occur among the critical points of f.
- On the boundary of th region, where you use Lagrange multipliers. The constraint is the defining equation of the boundary.

Note that when you find the critical points in the interior, you do *not* need to apply the second derivative test (which would only tell you about local maxima or minima).

Double Integrals

Definition. When the region R has a nice description in Cartesian coordinates, the double integral can be expressed as an iterated integral in two ways:

- The first way is
$$\iint_R f(x,y)\,dA = \int_a^b \int_{g_1(x)}^{g_2(x)} f(x,y)\,dy\,dx$$
when R consists of all points (x,y) where $a \le x \le b$, and for x in this range, $g_1(x) \le y \le g_2(x)$. So $y=g_2(x)$ is the top of R, $y=g_1(x)$ is the bottom, and $x=a$, $x=b$ are the sides. When doing the inner integral $\int_{g_1(x)}^{g_2(x)} f(x,y)\,dy$, you should treat x as a constant.
- The second way is
$$\iint_R f(x,y)\,dA = \int_c^d \int_{h_1(y)}^{h_2(y)} f(x,y)\,dx\,dy$$
when R consists of all points (x,y) where $c \le y \le d$, and for y in this range, $h_1(y) \le x \le h_2(y)$. From the point of view of someone on the y-axis, $x=h_2(y)$ is the "top" of R, $x=h_1(y)$ is the "bottom", and $y=c$, $y=d$ are the "sides". When doing the inner integral $\int_{h_1(y)}^{h_2(y)} f(x,y)\,dx$, treat y as a constant.

Fact. The polar coordinates (r,θ) of a point are related to the Cartesian coordinates (x,y) by the equations
$$r^2 = x^2+y^2 \quad x = r\cos\theta \quad y = r\sin\theta.$$

Definition. When the region R in a double integral $\iint_R f(x,y)\,dA$ has a nice description in polar coordinates, the integral can be expressed as the iterated integral
$$\iint_R f(x,y)\,dA = \int_\alpha^\beta \int_{h_1(\theta)}^{h_2(\theta)} f(r,\theta)\,r\,dr\,d\theta,$$
where R consists of all points with polar coordinates (r,θ) such that $\alpha \le \theta \le \beta$, and for θ in this range, $h_1(\theta) \le r \le h_2(\theta)$. When doing the inner integral $\int_{h_1(\theta)}^{h_2(\theta)} f(r,\theta)\,r\,dr$, you should treat θ as a constant.

Definition. The basic area interpretation of the double integral is $\iint_R 1\,dA = \text{Area}(R)$.

For volumes, there are two situations to consider:

- When $f(x,y) \geq 0$ on R, $\iint_R f(x,y)\,dA$ is the volume under the surface $z = f(x,y)$ for $(x,y) \in R$.
- More generally, suppose that a 3-dimensional region V in $\mathbb{R}^3$ consists of all points (x,y,z) such that $(x,y) \in R$ and $f_1(x,y) \leq z \leq f_2(x,y)$. Thus $z = f_2(x,y)$ is the top of V, $z = f_1(x,y)$ is the bottom, and the sides lie over the boundary of R. In this case, the volume of V is

$$\text{Vol}(V) = \iint_R (f_2(x,y) - f_1(x,y))\,dA.$$

Triple Integrals

Definition. Given a function $f(x,y,z)$ on a region R in $\mathbb{R}^3$, one can define the triple integral $\iiint_R f(x,y,z)\,dV$.

- Cartesian coordinates x, y, z, where $dV = dx\,dy\,dz$ or $dz\,dy\,dx$. Other orders are possible.
- Cylindrical coordinates r, θ, z, where $dV = r\,dz\,dr\,d\theta$.
  - To convert from cylindrical to Cartesian coordinates, we use these equations
  $$x = r\cos\theta \quad y = r\sin\theta \quad z = z.$$
  - To convert from Cartesian to cylindrical coordinates, we use these equations
  $$r^2 = x^2 + y^2 \quad \tan\theta = \frac{y}{x} \quad z = z.$$
- Spherical coordinates ρ, ϕ, θ, where $dV = \rho^2 \sin\phi\,d\rho\,d\phi\,d\theta$.
  - To convert from spherical to Cartesian coordinates, we use these equations
  $$x = \rho\sin\phi\cos\theta \quad y = \rho\sin\phi\sin\theta \quad z = \rho\cos\phi.$$
  - To convert from Cartesian to spherical coordinates, we use the equation
  $$\rho^2 = x^2 + y^2 + z^2.$$

Definition. The basic volume interpretation of the triple integral is $\iiint_R 1\,dV = \text{Vol}(R)$.

Linear Algebra

Vector Spaces and Subspaces

Definition. A (real) *vector space* is a set V (whose elements are called *vectors*) together with

(1) an operation called *vector addition*, which for each pair of vector $\vec{x}, \vec{y} \in V$ produces another vector in V denoted $\vec{x} + \vec{y}$, and
(2) an operation called *multiplication by a scalar* (a real number), which for each vector $\vec{x} \in V$, and each scalar $c \in \mathbb{R}$ produces another vector in V denoted $c\vec{x}$.

Furthermore, the two operations must satisfy the follow *axioms*:

(1) For all vectors $\vec{x}, \vec{y}$, and $\vec{z} \in V$, $(\vec{x} + \vec{y}) + \vec{z} = \vec{x} + (\vec{y} + \vec{z})$.
(2) For all vectors $\vec{x}$ and $\vec{y} \in V$, $\vec{x} + \vec{y} = \vec{y} + \vec{x}$.
(3) There exists a vector $\vec{0} \in V$ with the property that $\vec{x} + \vec{0} = \vec{x}$ for all vectors $\vec{x} \in V$.
(4) For each vector $\vec{x} \in V$, there exists a vector denoted $-\vec{x}$ with the property that $\vec{x} + -\vec{x} = \vec{0}$.

(5) For all vectors $\vec{x}$ and $\vec{y} \in V$ and all scalars $c \in \mathbb{R}$, $c(\vec{x} + \vec{y}) = c\vec{x} + c\vec{y}$.
(6) For all vectors $\vec{x} \in V$, and all scalars c and $d \in \mathbb{R}$, $(c + d)\vec{x} = c\vec{x} + d\vec{x}$.
(7) For all vectors $\vec{x} \in V$, and all scalars c and $d \in \mathbb{R}$, $(cd)\vec{x} = c(d\vec{x})$.
(8) For all vectors $\vec{x} \in V$, $1\vec{x} = \vec{x}$.

Examples. Some simple vector spaces:

- $\mathbb{R}^n$ is the vector space of ordered n-tuples of real numbers. Note: $\dim(\mathbb{R}^n) = n$.
- $P_n(\mathbb{R})$ is the vector space of polynomials of degree *less than or equal to* n. Note: $\dim(P_n(\mathbb{R})) = n + 1$.
- $M_{m\times n}(\mathbb{R})$ is the vector space of $m \times n$ matrices with real entries. Note: $\dim(M_{m\times n}(\mathbb{R})) = mn$.

Definition. Let V be a vector space and let $W \subseteq V$ be a subset. Then W is a (vector) *subspace* of V if W is a vector space itself under the operations of vector sum and scalar multiplication from V.

Notes. The empty set $\emptyset$ is not a vector space. Instead the smallest vector space is the trivial space, $\{\vec{0}\}$. Every vector space V has two obvious subspaces: the trivial subspace $\{\vec{0}\} \subseteq V$, and the improper subspace $V \subseteq V$.

Theorem (Subspace Theorem)**.** Let V be a vector space. A subset $W \subseteq V$ is a subspace if it satisfies the following properties:

(1) $W \neq \emptyset$
(2) For all $\vec{x}, \vec{y} \in W$ and all $c \in \mathbb{R}$, we have $c\vec{x} + \vec{y} \in W$.

Definition. Let V be a vector space, and let $S = \{\vec{v}_1, \ldots, \vec{v}_n\} \subseteq V$ be a finite set of vectors in V.

- A *linear combination* of elements of S is an expression $a_1\vec{v}_1 + \cdots + a_n\vec{v}_n$ for some scalars $a_1, \ldots, a_n \in \mathbb{R}$.
- The *span* of S, denoted $\text{Span}(S)$, is the set of all linear combinations of elements of S. That is,
$$\text{Span}(S) = \{a_1\vec{v}_1 + \cdots a_n\vec{v}_n \mid a_1, \ldots, a_n \in \mathbb{R}\}.$$
- We define $\text{Span}(\emptyset) = \{\vec{0}\}$.
- If $\text{Span}(S) = W$, we say that S spans W.

Fact. Let V be a vector space and let S be any subset of V. Then $\text{Span}(S)$ is a subspace of V.

Fact. If W is a subspace and $S \subseteq W$, then $\text{Span}(S) \subseteq W$.

Definition. The set S is *linearly dependent* if there exists scalars $a_1, \ldots, a_n \in \mathbb{R}$ that are not all zero such that $a_1\vec{v}_1 + \cdots + a_n\vec{v}_n = \vec{0}$. S is *linearly independent* if it is not linearly dependent. Equivalently, for any scalars $a_1, \ldots, a_n \in \mathbb{R}$ such that $a_1\vec{v}_1 + \cdots a_n\vec{v}_n = \vec{0}$, we must have $a_1 = \cdots = a_n = 0$.

Definition. The set $S \subseteq V$ is a basis for V if S is linearly independent and $\text{Span}(S) = V$.

Definition. The *dimension* of V is the number $\dim(V)$ of elements in a basis for V. If V has no finite basis, we say $\dim(V) = \infty$.

Theorem. Any two bases of V have the same number of elements.

Fact. The three kinds of row reduction steps are

(1) Switching two rows.
(2) Multiplying a row by a nonzero scalar.
(3) Adding a multiple of one row to another.

Definition. A matrix is in *echelon form* if it satisfies all of the following conditions:

(1) If a row is not a zero row (i.e., all entries of that row are zeros), then the first nonzero entry is a 1 (and called the *pivot*).
(2) If a column contains a pivot, then all other entries in that column are 0.
(3) If a row contains a pivot, then each row above contains a pivot further to the left. This also implies that zero rows, if any, appear at the bottom.

Variables corresponding to the pivots are called *pivot variables*. All other variables are called *free variables*.

Definition. A *homogeneous* system of linear equations is when all the linear combinations equal 0. A system is *inhomogeneous* otherwise.

Definition. The *nullspace* of a matrix A is the solution set of its corresponding homogeneous system of equations. The basis of the nullspace of A is the set of vectors that the free variables end up multiplied by in the solution.

Definition. The *column space* of a matrix A is the span of its columns. If B is the echelon form of A, then the columns of A corresponding to the columns of B with pivots form a basis of the column space.

Linear Transformations

Definition. Let V and W be vector spaces, and let $T : V \to W$ be a function. We say T is a *linear transformation* (or a *linear map*, or simply that T is *linear*) if for all $\vec{x}, \vec{y} \in V$ and all $c \in \mathbb{R}$, we have

$$T(c\vec{x} + \vec{y}) = cT(\vec{x}) + T(\vec{y}).$$

That is, T *respects addition* and *scalar multiplication*.

Corollary. When T is linear,

$$T(a_1\vec{v}_1 + \cdots + a_n\vec{v}_n) = a_1T(\vec{v}_1) + \cdots + a_nT(\vec{v}_n).$$

Theorem. Let $T : V \to W$ be a linear transformation. If $U : W \to X$ is another linear transformation, then the composition $U \circ T : V \to X$ is also linear. The composition $U \circ T$ is often denoted simply UT.

Theorem. If $A \in M_{m\times n}(\mathbb{R})$ is an $m \times n$ matrix, then the function $T : \mathbb{R}^n \to \mathbb{R}^m$ by $T(\vec{x}) = A\vec{x}$ is linear.

Theorem. If $T : \mathbb{R}^n \to \mathbb{R}^m$ is linear, then there is a matrix $A \in M_{m\times n}(\mathbb{R})$ so that T is given by $T(\vec{x}) = A\vec{x}$.

Definition. Let $T : V \to W$ be a linear transformation.

- The *kernel* or *nullspace* of T is

$$\{\vec{v} \in V \mid T(\vec{v}) = \vec{0}_W\} \subseteq V.$$

  It is usually denoted as $\text{Ker}(T)$ or $N(T)$. Its dimension $\dim(\text{Ker}(T))$ is called the *nullity* of T, sometimes denoted $\text{nullity}(T)$.

- The *image* or *range* of T is

$$\{T(\vec{v}) \mid \vec{v} \in V\} = \{\vec{w} \in W \mid \exists \vec{v} \in V \text{ s.t. } T(\vec{v}) = \vec{w}\} \subseteq W.$$

  It is usually denoted as $\text{Im}(T)$ or $R(T)$. Its dimension $\dim(\text{Im}(T))$ is called the *rank* of T, sometimes denoted $\text{rank}(T)$. If $T : \mathbb{R}^n \to \mathbb{R}^m$ is multiplication by a matrix A, the range of T is sometimes called the *column space* of A, because it is precisely the span of the columns of A.

Facts. Let $T : V \to W$ be a linear transformation.

- $N(T)$ is a subspace of V, and $R(T)$ is a subspace of W.
- T is one-to-one if and only if $N(T) = \{\vec{0}_V\}$, i.e., iff $N(T)$ is as small as possible, i.e., iff $\text{nullity}(T) = 0$.
- T is onto if and only if $R(T) = W$, i.e., iff $R(T)$ is as big as possible. If $\dim(W) < \infty$, this is equivalent to saying $\text{rank}(T) = \dim(W)$.
- If $T : \mathbb{R}^n \to \mathbb{R}^m$ is represented by a matrix A, then

$$N(T) = \{\vec{x} \in \mathbb{R}^n \mid A\vec{x} = \vec{0}\} \text{ and } R(T) = \text{column space of } A.$$

  Furthermore, after finding an echelon form of A via row reduction, $\text{rank}(T)$ is the number of columns *with* pivots (since the corresponding columns form a basis of $R(T)$), and $\text{nullity}(T)$ is the number of columns *without* pivots (since the vectors that give the general solution form a basis of $N(T)$).

Fact. If $X \subseteq V$ is a subspace, then $\dim(X) \leq \dim(V)$. Moreover, if $\dim(V) < \infty$, then $\dim(X) = \dim(V)$ if and only if $X = V$.

Fact. Let V be a vector space with $\dim(V) = n$, and let $S \subseteq V$ be a set of m distinct vectors in V.

- If $m < n$, then S cannot span V.
- If $m > n$, then S cannot be linearly independent.

Theorem. Let V be a vector space, and let $S \subseteq V$ be a set of n distinct vectors in V. If any two of the following conditions hold, then all three hold (and S is a basis for V):

(1) S is linearly independent.
(2) S spans V.
(3) $\dim(V) = n$.

Theorem. Let $T : V \to W$ be a linear transformation, and suppose that at least one of V, W is finite-dimensional. If any two of the following conditions hold, then all three hold:

(1) T is one-to-one.
(2) T is onto.
(3) $\dim(V) = \dim(W)$.

In this case, T is *invertible.*

Theorem (Rank-Nullity/Dimension Theorem)**.** Let $T : V \to W$ be a linear transformation. Then

$$\text{rank}(T) + \text{nullity}(T) = \dim(V).$$

Matrices

Facts. Some facts about matrices:

- Matrix addition is commutative and associative.
- Matrix multiplication is associative *but not commutative.*
- The $m \times n$ matrix of zeros (denoted 0 or O) is the additive identity: $A + O = O + A = A$.
- The $n \times n$ identity matrix I, sometimes denoted I_n, has 1's down the diagonal and 0's everywhere else.
- The distributive laws: $A(B + C) = AB + AC$ and $(A + B)C = AC + BC$.

If A is a *square* matrix (i.e., $n \times n$):

- A is a *diagonal matrix* if every entry not on the diagonal is 0.
- The *transpose* of A, denoted A^t or A^T, is the $n \times n$ matrix formed by reflecting A across the diagonal.
- The *determinant* of A, denoted $\det(A)$, is a real number given by a more complicated formula.
  - For a given $n \times n$ matrix A where $n \geq 1$,

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}),$$

    where a_{ij} is the entry in the ith row and jth column, and A_{ij} is the $(n-1) \times (n-1)$ matrix obtained by deleting the ith row and jth column of A.
  - $\det(AB) = \det(A)\det(B)$.
  - $\det(A) \neq 0$ if and only if A is invertible.
  - $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ means the same thing as $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, namely $ad - bc$.

Definition. Let V and W be finite-dimensional vector spaces with bases $\alpha = \{\vec{v}_1, \ldots, \vec{v}_n\}$ and $\beta = \{\vec{w}_1, \ldots, \vec{w}_m\}$, respectively, and let $T : V \to W$ be a linear transformation.

Find real numbers a_{ij}, for $q \leq i \leq m$ and $1 \leq j \leq n$, by computing $T(\vec{v}_1), \ldots, T(\vec{v}_n)$ and expressing each as a linear combination of $\vec{w}_1, \ldots, \vec{w}_m$. That is,

$$\begin{aligned} T(\vec{v}_1) &= a_{11}\vec{w}_1 + a_{21}\vec{w}_2 + \cdots + a_{m1}\vec{w}_m \\ T(\vec{v}_2) &= a_{12}\vec{w}_1 + a_{22}\vec{w}_2 + \cdots + a_{m2}\vec{w}_m \\ &\vdots \\ T(\vec{v}_n) &= a_{1n}\vec{w}_1 + a_{2n}\vec{w}_2 + \cdots + a_{mn}\vec{w}_m. \end{aligned}$$

Then, turning the grid of coefficients sideways, the $m \times n$ *matrix of* T *with respect to* α *and* β is

$$[T]_\alpha^\beta = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

Definition. Let V be a finite-dimensional vector space, and let $\alpha = \{\vec{v}_1, \ldots, \vec{v}_n\}$ be a basis for V. For any $\vec{v} \in V$, the *coordinate vector* of $\vec{v}$ with respect to α is the n-entry

column vector $[\vec{v}]_\alpha = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in \mathbb{R}^n$, where $a_1, \ldots, a_n \in \mathbb{R}$ are the unique scalars such that $\vec{v} = a_1\vec{v}_1 + \cdots + a_n\vec{v}_n$.

Fact. For any $\vec{v} \in V$, the coordinate vectors $[\vec{v}]_\alpha \in \mathbb{R}^n$ and $[T(\vec{v})]_\beta \in \mathbb{R}^m$ are related via the matrix $[T]_\alpha^\beta \in M_{m\times n}(\mathbb{R})$ by the equation

$$[T]_\alpha^\beta [\vec{v}]_\alpha = [T(\vec{v})]_\beta.$$

Fact. If X is another vector space, with basis $\gamma = \{\vec{x}_1, \ldots, \vec{x}_p\}$, and if $U : W \to X$ is linear, then the $m \times n$ matrix $[T]_\alpha^\beta$, the $n \times p$ matrix $[U]_\beta^\gamma$, and the $m \times p$ matrix $[UT]_\alpha^\gamma$ are related by matrix multiplication:

$$[UT]_\alpha^\beta = [U]_\beta^\gamma [T]_\alpha^\beta.$$

Definition. A linear transformation $T : V \to W$ is *invertible* if it has an *inverse*, i.e., if there is another linear map $T^{-1} : W \to V$ such that $T(T^{-1}(\vec{w})) = \vec{w}$ for all $\vec{w} \in W$, and $T^{-1}(T(\vec{v})) = \vec{v}$ for all $\vec{v} \in V$. The following are equivalent:

- T is invertible (i.e., T has an inverse $T^{-1} : W \to V$).
- T is one-to-one and onto.

Facts. Suppose $T : V \to W$ is invertible. Then:

- Its inverse T^{-1} is unique.
- Its inverse T^{-1} is also invertible, and $(T^{-1})^{-1} = T$.
- If $U : W \to X$ is also invertible, then $UT : V \to X$ is invertible, and $(UT)^{-1} = T^{-1}U^{-1}$.

Definition. A square matrix $A \in M_{n\times n}(\mathbb{R})$ is *invertible* if it has an *inverse*, i.e., if there is another matrix $B \in M_{n\times n}(\mathbb{R})$ such that $AB = I$ and $BA = I$. The following are equivalent:

- A is invertible.
- The columns of A are linearly independent.
- The rows of A are linearly independent.
- The columns of A together span $\mathbb{R}^n$.
- The rows of A together span $\mathbb{R}^n$.
- The column space (i.e., range or image) of A is all of R^n.
- The null space (i.e., kernel) of A is $\{\vec{0}\}$.
- $\text{rank}(A) = n$.
- $\text{nullity}(A) = 0$.
- $\det(A) \neq 0$.
- $\lambda = 0$ is not an eigenvalue of A.

Facts. Suppose $A \in M_{n\times n}(\mathbb{R})$ is invertible. Then:

- Its inverse A^{-1} is unique.
- Its inverse A^{-1} is also invertible, and $(A^{-1})^{-1} = A$.
- If $B \in M_{n\times n}(\mathbb{R})$ is invertible, then AB is invertible, and $(AB)^{-1} = B^{-1}A^{-1}$.

Facts. Computing inverse:

- $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible if and only if $ad-bc \neq 0$, in which case $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.
- For 3×3 and larger matrices, use the Gauss-Jordan method (row reduction).

Definition. Let V be a finite-dimensional vector space, and let $\alpha = \{\vec{v}_1, \dots, \vec{v}_n\}$ and $\beta = \{\vec{w}_1, \dots, \vec{w}_n\}$ both be bases for V. The *change-of-basis matrix* from the α-coordinate to β-coordinate is the $n \times n$ matrix $[I]_\alpha^\beta$, where $I : V \to V$ is the identity map $I(\vec{v}) = \vec{v}$. That is,

$$[I]_\alpha^\beta = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

where

$$\begin{aligned} \vec{v}_1 &= a_{11}\vec{w}_1 + a_{21}\vec{w}_2 + \cdots + a_{m1}\vec{w}_m \\ \vec{v}_2 &= a_{12}\vec{w}_1 + a_{22}\vec{w}_2 + \cdots + a_{m2}\vec{w}_m \\ &\vdots \\ \vec{v}_n &= a_{1n}\vec{w}_1 + a_{2n}\vec{w}_2 + \cdots + a_{mn}\vec{w}_m. \end{aligned}$$

As before, note that the grid of coefficients is flipped sideways to form the matrix.

Fact. For any $\vec{v} \in V$, recall that $[\vec{v}]_\alpha \in \mathbb{R}^n$ is the n-entry column vector of α-coordinates for $\vec{v}$. We can compute the β-coordinate vector for $\vec{v}$ via the formula $[\vec{v}]_\beta = [I]_\alpha^\beta [\vec{v}]_\alpha$.

Fact. The change of coordinates matrix to change coordinates the other way is the inverse: $[I]_\beta^\alpha = \left([I]_\alpha^\beta\right)^{-1}$.

Eigenvalues and Eigenvectors

Definition. Let A be an $n \times n$ matrix, let $\lambda \in \mathbb{R}$ be a scalar, and let $\vec{v} \in \mathbb{R}^n$. We say that $\vec{v}$ is an *eigenvector* with *eigenvalue* λ if $\vec{v} \neq 0$ and $A\vec{v} = \lambda\vec{v}$.

- To say "λ is an eigenvalue of A" means there exists $\vec{v} \in \mathbb{R}^n \setminus \{0\}$ such that $A\vec{v} = \lambda\vec{v}$.
- To say "$\vec{v}$ is an eigenvector of A" means that $\vec{v} \neq \vec{0}$ and there exists $\lambda \in \mathbb{R}$ such that $A\vec{v} = \lambda\vec{v}$.
- An eigenvalue λ can be 0.
- An eigenvector cannot be $\vec{0}$. (By definition.)

Definition. The *characteristic polynomial* of A is $\det(A - \lambda I)$; that is, subtract the variable λ from each diagonal entry and take the determinant. The result is a polynomial of degree n in the variable λ.

Fact. The roots of the characteristic polynomial of A are *precisely* the eigenvalues of A.

Definition. The number of times that a given scalar λ shows up as a root of the characteristic polynomial is called the *algebraic multiplicity* of λ, or sometimes simply the *multiplicity* of λ.

Definition. The *eigenspace* E_λ of an eigenvalue λ is the null space $N(A - \lambda I)$ of the matrix $A - \lambda I$. It consists of all the eigenvectors with eigenvalue λ, along with $\vec{0}$, which is not an eigenvector.

Definition. The eigenspace dimension $\dim(E_\lambda)$ is sometimes called the *geometric multiplicity* of λ.

Fact. For any eigenvalue λ of A, we have

$$1 \leq (\text{geometric multiplicity of } \lambda) \leq (\text{algebraic multiplicity of } \lambda).$$

Fact. To find the eigenvalues and eigenvectors of a matrix A:

(1) Compute the characteristic polynomial $\det(A - \lambda I)$.
(2) Find all roots of the characteristic polynomial; these are the eigenvalues.
(3) For each eigenvalue λ, use row reduction to find a basis for the eigenspace $E_\lambda = N(A - \lambda I)$.

Definition. We say an $n \times n$ matrix A is *diagonalizable* if there is an invertible matrix P and a diagonal matrix D such that $P^{-1}AP = D$. The following are equivalent:

- A is diagonalizable.
- There is a *basis* for $\mathbb{R}^n$ consisting of eigenvectors of A.
- All roots of the characteristic polynomial of A are real, and for each such root λ,

$$(\text{geometric multiplicity of } \lambda) = (\text{algebraic multiplicity of } \lambda).$$

In that case, the matrix P consists of n linearly independent eigenvectors down the columns, and the diagonal matrix D has the eigenvalues along the diagonal, *in the same order*.

Fact. If A has n *distinct* real eigenvalues, then A is certainly diagonalizable. (However, if A has repeated eigenvalues, it may or may not be diagonalizable.)

Abstract Algebra

Integers

Fact (The Division Algorithm)**.** If a and n are integers and n is positive, then there exists unique integers q and r such that $a = qn + r$ and $0 \leq r < n$.

Fact. If $\gcd(a, b) = d$, then there exists $m, n \in \mathbb{Z}$ such that $ma + nb = d$.

Groups

Definition. Suppose that:

(1) G is a set and $*$ is a binary operation on G,
(2) $*$ is associative,
(3) there exists an element e of G such that $\forall x \in G$

$$x * e = e * x = x \text{ (identity element)}$$

(4) for each $x \in G$, there exists an element $y \in G$ such that

$$x * y = y * x = e$$

Then G, together with the binary operation $*$, is called a *group* and denoted $(G, *)$.

Theorem. If $(G, *)$ is a group, then there is only one identity element in G.

Theorem. If $(G, *)$ is a group and $x \in G$, then x has only one inverse.

Definition. We say a group G is *abelian* if the group operation is commutative, i.e., if $xy = yx$ for all $x, y \in G$.

Notation. For $g \in G$ and $n \in \mathbb{Z}$, $g^n = g \cdot g \cdots g$ (n-times).

Notation. If the operation of G is called $+$, then we write ng instead of g^n.

Notation. When G is finite, its order $|G|$ is the number of elements in the group.

Notation. When $g \in G$ has finite order, its order $o(g)$ is the smallest integer $m > 0$ with $g^m = e$.

Notation. If $g^m = e$ for some $m \in \mathbb{Z}$, then $o(g) \mid m$.

Subgroups

Definition. Let $(G, *)$ be a group and $H \subseteq G$. H is a *subgroup* of G if the elements of H from a group under $*$. I.e. $(H, *)$ is a group.

Theorem. Let H be a nonempty subset of group G. Then, H is a subgroup of G if and only if

(1) $\forall a, b \in H$, $ab \in H$ and
(2) $\forall a \in H$, $a^{-1} \in H$.

Terminology: If H has property 1 we say it is closed under multiplication. If H has property 2 we say it is closed under inverses.

Definition. An element $g \in G$ generates the *cyclic* subgroup $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$.

Theorem. An element $g \in G$ has finite order if and only if $\langle g \rangle$ is finite, in which case $o(g) = |\langle g \rangle|$.

Theorem (Lagrange's Theorem)**.** If H is a subgroup of a finite group G, then $|H| \mid |G|$.

Corollary. If $|G|$ is prime, the G is cyclic.

Corollary. For all $g \in G$, we have $o(g) \mid |G|$.

Corollary. For all $g \in G$, we have $g^{|G|} = e$.

Cosets

Definition. If H is a subgroup of G, then by *right coset* of H in G we mean a subset of the form Hg, where $g \in G$ and

$$Hg = \{hg \mid h \in H\}.$$

Definition. If H is a subgroup of G, then by *left coset* of H in G we mean a subset of the form gH, where $g \in G$ and

$$gH = \{gh \mid h \in H\}.$$

Theorem. Two right cosets Hx and Hy are either the same set or disjoint sets. (That is, if they share even one element, they are exactly the same set.) The same holds for left cosets. (On the other hand, a right coset and a left coset can intersect each other without being the same set.)

Corollary (Right coset relation)**.** $Hx = Hy \iff xy^{-1} \in H \iff x \in Hy$.

Corollary (Left coset relation)**.** $xH = yH \iff y^{-1}x \in H \iff x \in yH$.

Corollary. $Hx = H \iff x \in H \iff xH = H$.

Notation. If G is abelian and the group operation is written as addition, then the left and right cosets of $H \subseteq G$ coincide and are written

$$H + a = \{h + a \mid h \in H\}.$$

Here, the coset relation becomes

$$H + a = H + b \iff a - b \in H \iff a \in H + b.$$

Definition. When a group G is a union of finitely many left cosets of a subgroup H, we say that H has finite index in G and the *index* of H in G is defined to be

$$[G : H] = \text{number of distinct left cosets of } H \text{ in } G.$$

The same holds for right cosets. When G is finite, $[G : H] = |G|/|H|$, since all cosets of H have the same number of elements.

Normal Subgroups

Theorem. Given a subgroup $H \subseteq G$, H being normal in G is equivalent to any of the following conditions:

- $gH = Hg$ for all $g \in G$.
- $gHg^{-1} = H$ for all $g \in G$.
- $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

Theorem. When $N \subseteq G$ is a normal subgroup, every left coset is a right coset, and vice versa. The set of all cosets of N in G forms a group and is denoted G/N. The group operation is defined by $Na \cdot Nb = Nab$, which is well-defined since N is normal. When G is finite, G/N is also finite and $|G/N| = [G : N] = |G|/|N|$.

Group Homomorphisms

Definition. Let G and H be groups and let $\phi : G \to H$ be a function. We say that ϕ is a *homomorphism* if for all $a, b \in G$,

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

Theorem. If $\phi : G \to H$ is a homomorphism, then

- $\phi(e_G) = e_H$.
- $\phi(g^n) = \phi(g)^n$ for all $g \in G$ and $n \in \mathbb{Z}$.

Definition. If $\phi : G \to H$ is a homomorphism, then

- The *kernel* of ϕ is $\text{Ker}(\phi) = \{g \in G \mid \phi(g) = e_H\} \subseteq G$.
- The *image* of ϕ is $\text{Im}(\phi) = \{\phi(g) \mid g \in G\} \subseteq H$.

Theorem. If $\phi : G \to H$ is a homomorphism, then $\text{Ker}(\phi)$ is a normal subgroup of G.

Theorem. If $\phi : G \to H$ is a homomorphism, then $\text{Im}(\phi)$ is a subgroup of H, but not necessarily normal.

Theorem. Given $\phi : G \to H$ is a homomorphism, ϕ is one-to-one if and only if $\text{Ker}(\phi) = \{e_G\}$.

Theorem. Given a group homomorphism $\phi : G \to H$, ϕ being an isomorphism is equivalent to

- ϕ is one-to-one and onto.
- ϕ has an inverse function $\phi^{-1} : H \to G$ that is a group homomorphism.

Theorem (The Fundamental Theorem of Group Homomorphisms)**.** If $\phi : G \to H$ is a group homomorphism, then there is a group isomorphism $\widetilde{\phi} : G/\text{Ker}(\phi) \simeq \text{Im}(\phi)$ defined by $\widetilde{\phi}(g\text{Ker}(\phi)) = \phi(g)$.

Permutations

Definition. If X is a nonempty set, then a one-to-one onto function $f : X \to X$ is called a *permutation*.

Definition. Let X be a nonempty set. The group $(S_X, \circ)$ is called the *symmetric group on* X. If X is a finite set, there is no harm in assuming that $X = \{1, 2, \ldots, n\}$. In this case, we denote the group $(S_X, \circ)$ by S_n.

Notation. If $\sigma \in S_n$, we can represent σ by an array

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

Fact. $|S_n| = n!$

Definition. Given distinct $i_1, \ldots, i_n$, the n-cycle $(i_1\ i_2 \cdots i_n)$ maps i_1 to i_2, i_2 to i_3, $\ldots$, i_n to i_1, and is the identity elsewhere.

Fact. The order of an n-cycle is its length n.

Definition. Two cycles $(i_1\ i_2 \cdots i_n)$ and $(j_1\ j_2 \cdots j_n)$ are *disjoint* if

$$\{i_1, \ldots, i_n\} \cap \{j_1, \ldots, j_n\} = \emptyset.$$

Fact. If $\sigma \in S_n$ is written as a product of disjoint cycles $\sigma = \sigma_1 \cdots \sigma_k$, then

$$o(\sigma) = \text{lcm}(\text{length } \sigma_1, \ldots, \text{length } \sigma_k).$$

Definition. "Transposition" is just another word for 2-cycle.

Fact. Every element of S_n can be written as a product of transpositions. A given $\sigma \in S_n$ can be written as a product of transpositions in many ways, this product is *not* a unique factorization.

Definition. A permutation is said to be *even* if it can be written as the product of an even number of transpositions. It is *odd* if it can be written as the product of an odd number of transpositions.

Definition. The alternating group A_n consists of all even permutations in S_n.

Fact. For $n \geq 2$, $|A_n| = \frac{n!}{2}$.

Fact. An n-cycle can be written as a product of $n - 1$ transpositions. In particular, every cycle of odd length has odd order but is an even permutation. Similarly, every cycle of even length has even order but is an odd permutation.

Rings

Definition. Suppose that R is a set and $+$ and $\cdot$ are two binary operations on R. Further suppose that:

(1) $(R, +)$ is an abelian group
(2) $\cdot$ is associative
(3) $\forall r_1, r_2, r_3 \in R$,

$$r_1(r_2 + r_3) = r_1 r_2 + r_1 r_3 \text{ and}$$
$$(r_2 + r_3) r_1 = r_2 r_1 + r_3 r_1.$$

Then, R together with $+$ and $\cdot$ is called a *ring*. We denote it by $(R, +, \cdot)$ or just R for short.

Definition. If $\cdot$ is commutative, then R is called a *commutative ring*.

Notation. The *additive* identity element of R is denoted by 0_R or just 0.

Definition. If $\cdot$ has a *multiplicative* identity element, it is unique and denoted 1_R or just 1. We call 1_R the *unity* of R if it exists. A ring with unity is called a *ring with unity*.

Definition. If R is a ring with unity, then any $x \in R$ that has a *multiplicative* inverse x^{-1} is called a *unit*. The set of all units of R is denoted $R^\times$ and forms a group under the multiplication operation, with identity element 1_R.

Definition. A ring R is called a *division ring* if R has a unity $1 \neq 0$ and every nonzero element of R is a unit. A commutative division ring is called a *field*.

Facts. Suppose R is a ring and $x \in R$.

- $0_R x = x 0_R = 0_R$.
- Since $(R, +)$ forms a group, for an integer n, we write nx to denote x added to itself n times (or subtracted, if n is negative; or 0_R if $n = 0$).
- For a *positive* integer n, we write x^n for x multiplied by itself n times. If R has unity, then $x^0 = 1_R$; if in addition x is a unit (i.e., if x has multiplicative inverse), then $x^{-n} = (x^{-1})^n$.

Definition. If R is a commutative ring, the *polynomial ring* $R[x]$ consists of all polynomials in x with coefficients in R.

Ideals

Definition. A subset $I \subseteq R$ is an *ideal* if it satisfies the following properties:

(1) $I \neq \emptyset$.
(2) For all $x, y \in I$, we have $x - y \in I$.
(3) For all $x \in I$ and $r \in R$, we have $rx \in I$ and $xr \in I$.

Properties 1 and 2 say that I is a subgroup under addition, and property 3 is sometimes informally called the "sticky" property.

Facts. Some facts about ideals.

- When the ring is commutative, we have $rx = xr$, so the sticky property simplifies to: For all $x \in I$ and $r \in R$, we have $rx \in I$.
- An ideal I always contains the zero element of the ring.
- Let R be a ring with unity 1, and let $I \subseteq R$ be an ideal. Then I contains 1 if and only if $I = R$.

Quotient Rings

Definition. Recall that an ideal $I \subseteq R$ is a group under addition, so the cosets of I are usually written

$$I + r = \{s + r \mid s \in I\},$$

although sometimes you see $r + I$ since addition is commutative. The definition of ideal guarantees that the set of cosets

$$R/I = \{I + r \mid r \in R\}$$

becomes a ring, called the quotient ring, under the following operations:

$$(I + a) + (I + b) = I + (a + b) \quad \text{and} \quad (I + a)(I + b) = I + ab.$$

Ring Homomorphisms

Definition. Let R and S be rings and let $\phi : R \to S$ be a function. Then, ϕ is a *ring homomorphism* if for all $x, y \in R$:

(1) $\phi(x+y) = \phi(x) + \phi(y)$.
(2) $\phi(xy) = \phi(x)\phi(y)$.

We define *isomorphism* just as before.

Facts. Some facts about ring homomorphisms.

- If $\phi : R \to s$ is a ring homomorphism, then $\phi(0_R) = 0_S$. [But even if both rings have 1, we might *not* have $\phi(1_R) = 1_S$!]
- If $\phi : R \to S$ is a ring homomorphism, then for all $x \in R$ and all $n \in \mathbb{Z}$, we have $\phi(nx) = n\phi(x)$.
- If $\phi : R \to S$ is a ring homomorphism, then for all $x \in R$ and all $n \in \mathbb{N}$, we have $\phi(x^n) = \phi(x)^n$.

Theorem. If $\phi : R \to S$ is a ring homomorphism, then $\mathrm{Ker}(\phi)$ is an ideal of R.

Theorem (The Fundamental Theorem of Ring Homomorphisms)**.** If $\phi : R \to S$ is a ring homomorphism, then there is a ring homomorphism $\widetilde{\phi} : R/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi)$ defined by $\widetilde{\phi}(\mathrm{Ker}(\phi) + r) = \phi(r)$.

Quotient Rings and Fields

Theorem. A commutative ring with unity is a field if and only if its only ideals are $\{0\}$ and the whole ring.

Definition. An ideal I of a ring R is called a *maximal ideal* if I is a proper ideal and there is no other proper ideal J such that $I \subsetneq J$.

Theorem. Let R be a commutative ring with unity. Ideal $M \subseteq R$ is maximal if and only if R/M is a field.

Polynomial Rings $k[x]$, for a Field k

Definition. A polynomial $f = f(x) \in k[x]$ is a symbolic object (x is just a symbol) in the ring $k[x]$. However, if we replace x with an element $a \in k$ (sometimes called "plugging in"), then we get an element $f(a) \in k$. This operation is compatible with addition and multiplication.

Theorem (The Division Algorithm)**.** Let k be a field and let $f(x), g(x) \in k[x]$. If $g(x) \neq 0$, then there exists $q(x), r(x) \in k[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

Definition. Let R be a commutative ring with unity and let $a \in R$. Define

$$aR = \{ar \mid r \in R\}$$

Then, aR is an ideal of R aR is called the *principal ideal generated by* a.