Modern Algebra II

Orthogonal Transformations and Rotations

Definition. A real $n \times n$ matrix is orthogonal if $A^T = A^{-1}$. The group of orthogonal matrices is O_n, the orthogonal group.

Definition. The subgroup of the orthogonal group in which determinants are +1 is called the special orthogonal group, SO_2.

Theorem. A matrix represents a rotation in $\mathbf{R}^2$ or $\mathbf{R}^3$ if and only if it is in SO_2 or SO_3.

Proposition. The following conditions on an $n \times n$ matrix are equivalent:

- A is orthogonal
- Multiplication by A preserves dot products – $<A\mathbf{x}, A\mathbf{y}> = <\mathbf{x}, \mathbf{y}>$.
- The columns of A are mutually orthogonal unit vectors.

Proposition. Let m: $\mathbf{R}^n \to \mathbf{R}^n$. The followins are equivalent:

- m is a rigid motion which preserves the origin
- m preserves dot products
- m is left multiplication by an orthogonal matrix

Corollary. A rigid motion which fixes the origin is a linear operator.

Proposition. Every rigid motion is the composition of a linear operator and a translation. That is, $m(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$, for an orthogonal matirx A and some vector **b**.

Definition. An orthogonal operator is orientation-preserving if its determinat is +1 and oritentaion-reversing if its determinant is –1.

Theorem. We may classify the rigid motions of the plane as:

- Orientation-preserving motions:
  - Translation: parallel motion of the plane by a vector **a**: $\mathbf{p} \to \mathbf{p} + \mathbf{a}$
  - Rotation: Rotates the plane by an angle about some point
- Orientation-reversing motions:
  - Reflection about a line l
  - Glide Reflection: Reflecting about a line l and then translating by a nonzero vector **a** parallel to l

Lemma. Every rigid motion can be written as $m = t_a\rho_\theta$ or $m = t_a\rho_\theta r$, where t_a is translation by a vector a, ρ_θ is rotation by θ is r is reflection. This expression is unique.

Note. The rules for computing with these rigid motions are:

- $t_a t_b = t_{a+b}$
- $\rho_\theta \rho_\eta = \rho_{\theta+\eta}$
- $rr = 1$
- $\rho_\theta t_a = t_{a'}\rho_\theta$, where $a' = \rho_\theta(a)$
- $rt_a = t_{a'}r$, where $a' = r(a)$
- $r\rho_\theta = \rho_{-\theta}r$

Proposition. The subgroup of motions fixing **p** is $O' = t_p O t_p^{-1}$.

Theorem (Fixed Point Theorem). Let G be a finite subgroup of the group of motions M. There is a point p in the plane which is left fixed by every element of G; that is, $g(p) = p$ for all $g \in G$.

Theorem. Let G be a subgroup of the O (rigid motions which fix the origin). Then G is either C_n, the cyclic group of order n (generated by a rotation), or G is D_n, the dihedral group (generated by a rotation and reflection).

Definition. The dihedral group, D_n, is generated by the elements x and y subject to the relations $x^n = 1$, $y^2 = 1$, and $yx=x^{-1}y$.
Definition. A subgroup G of M is discrete if it does not contain arbitrarily small rotations or rotations.
Definition. Let G be a group of rigid motions. The translation group, L_G, of G is the set of vectors, **a**, such that $t_a \in G$.
Proposition. Every discrete subgroup L of $\mathbf{R}^2$ is of the form:

- $L = \{0\}$
- $L = \{m\mathbf{a} \mid m \in \mathbf{Z}\}$
- $L = \{m\mathbf{a} + n\mathbf{b} \mid m, n \in \mathbf{Z}\}$

Definition. Let G be a group of rigid motions. The point group, G-bar, of G is the image of G in O. If G is discrete, so is its point group.
Proposition. Let G be a discrete subgroup of M, with translation group L_G and point group G-bar. The elements of G-bar carry L_G to itself.
Proposition. Let $H \subset O$ be a finite subgroup of the group of symmetries of a lattice, L. Then every rotation in H has order 1, 2, 3, 4, or 6, so $H = C_n$ or D_n, with n = 1, 2, 3, 4, or 6.
Definition. An element $\mathbf{v} \in L$ is primitive if it is not an integer multiple of another vector in L.
Corollary. Let L be a lattice and **v** a primitive element of L. There is an element $\mathbf{w} \in L$ so that (**v**, **w**) is a lattice basis.
Theorem. Every finite subgroup of SO_3 is one of the following:

- C_k: the cyclic group of rotations by $2\pi/k$ about a fixed line
- D_k: the symmetries of a regular k-gon
- T: the tetrahedral group (12 rotations which carry a tetrahedron to itself)
- O: the octahedral group (24 rotations which carry either a cube or an octahedron to itself)
- I: the icosahedral group (60 rotations which carry either a regular dodecahdron or a regular icosahedron to itself)

Abstract Group Operations

Definition. Let G be a group and S a set. An operation of G on S is a rule for combining elements $g \in G$ and $s \in S$ so that $gs \in S$, such that 1s = s for all s, and (gg')s = g(g's) for all g, g', and s. With this operation, S is called a G-set.
Definition. Let $s \in S$, with S a G-set. The orbit of s is the set $O_s = \{s' \in S \mid s' = gs$ for some $g \in G\}$.
Proposition. S is a union of disjoint orbits.
Definition. If S consists of a single orbit, G operates transitively on S.
Definition. The stabilizer of $s \in S$ is the subgroup $G_s = \{g \in G \mid gs = s\}$.
Proposition. $xs = ys \Leftrightarrow x^{-1}y \in G_s$.
Definition. Let H be a subgroup of a group G. The set of left cosets, aH, of G is called the coset space, and may be written G/H. G/H is a G-set, under the operation g(aH) = (ga)H.
Proposition. Let S be a G-set. Let $s \in S$. Let H be the stabilizer of s and O_s the orbit of s. Then $\varphi: G/H \rightarrow O_s$ given by $\varphi(aH) = as$ is bijective.

Proposition. Let S be a G-set. Let $s \in S$. Let s' = as. Then, the set of elements of such that gs = s' is the left coset aG_s. $G_{s'} = aG_sa^{-1}$.

Proposition (Counting Formula). Let $s \in S$. Then, $|G| = |G_s|\,|O_s|$ = (order of stabilizer) (order of orbit). Equivalently, $|O_s| = [G: G_s]$. Because the orbits partition S, we find $|S| = |O_1| + \ldots + |O_n|$, where each summand divides $|G|$.

Proposition. Let H and K be subgroups of a group G. Then, $[H : H \cap K] \leq [G : K]$.

Definition. A <u>permutation representation</u> of a group G is a homomorphism $\varphi: G \rightarrow S_n$.

Proposition. There is a bijective correspondence between operations of G on S and homomorphisms from G to the group of permutations of S. We define $\varphi(g)$ as left multiplication by g.

Definition. If $\varphi: G \rightarrow \text{Perm}(S)$ is injective then we say the operation of G on S is <u>faithful</u>.

Proposition. $GL_2(\mathbf{Z}_2)$ is isomorphic to S_3.

Proposition. The map f: $S_3 \rightarrow \text{Aut}(S_3)$ defined by f(g) = conjugation by g is bijective.

Proposition. The group of automorphisms of the cyclic group of order p is isomorphic to the multiplicative group, $\mathbf{Z}_p^*$.

More Group Theory

Theorem (Cayley's Theorem). Every finite group is isomorphic to a subgroup of a permutation group. In particular, if |G| = n, then G is isomorphic to a subgroup of S_n.

Definition. The stabilizer of an element $x \in G$ under conjugation is called the <u>centralizer</u> of x: $Z(x) = \{g \in G \mid gx = xg\}$.

Definition. The orbit of an element under conjugation is called its <u>conjugacy class</u>.

Theorem (Class Equation). $|G| = |C_1| + \ldots + |C_n|$ where each $|C_i|$ is a distinct conjugacy class. Each summand divides |G| and at least one (the one of the identity) is exactly 1.

Proposition. A element is in the center of a group if and only if its centralizer Z(x) is the whole group.

Definition. Let G be a group where $|G| = p^k$, $k > 0$. Then G is called a <u>p-group</u>.

Proposition. The center of a p-group G has order greater than 1.

Proposition. Let G be a p-group. Let S be a finite G-set. If p does not divide the order of S, then there is a fixed point for the action of G (that is, an element whose stabilizer is G).

Proposition. Every group of order p^2 is abelian.

Corollary. Every group of order p^2 is isomorphic to either $\mathbf{Z}_{pp}$ or $\mathbf{Z}_p \times \mathbf{Z}_p$.

Lemma. If a normal subgroup of G contains an element x, it contains the conjugacy class of x. Thus every normal subgroup is the union of conjugacy classes and its size is the sum of the orders of these conjugacy classes.

Theorem. The icosahedral group is simple (and isomorphic to A_5).

Definition. Let S be a G-set. If $U \subset S$, then $gU = \{gu \mid u \in U\}$.

Proposition. Let S be an H-set. Let $U \subset S$. H stabilizes U if and only if U is the union of H-orbits.

Proposition. Let U be a subset of a group G. The order of Stab(U) under the operation of left multiplication divides the order of U. (Since U is a union of right cosets.)

Definition. The stabilizer of a subgroup H of G under conjugation is the <u>normalizer</u> of H, $N(H) = \{g \in G \mid gHg^{-1} = H\}$.

Note. N(H) is the largest subgroup containing H as a normal subgroup.

Corollary. If H is any subgroup of G, |G| = |N(H)| |conjugate subgroups of H|.

Theorem (First Sylow Theorem). Let G be a group, $|G| = p^e m$, $(m, p) = 1$. There is a subgroup of G whose order is p^e.

Corollary (Cauchy's Theorem). If a prime p divides the order of G, then G contains an element of order p.

Corollary. The only groups of order 6 are C_6 and D_3.

Definition. Let G be a group of order $p^e m$ (p prime, p not dividing m, $e \geq 1$). The subgroups H of G of order p^e are called <u>Sylow p-subgroups</u>.

Theorem (Second Sylow Theorem). Let K be a subgroup of G whose order is divisible by p. Het H be a Sylow p-subgroup of G. There is a conjugate subgroup $h' = gHg^{-1}$ such that $K \cap H'$ is a Sylow subgroup of K.

Corollary. If K is any subgroup of G which is a p-group, then K is contained in a Sylow p-subgroup of G.

Corollary. All the Sylow p-subgroups are conjugate.

Theorem (Third Sylow Theorem). Let $|G| = p^e m$. Let s be the number of Sylow p-subgroups. Then $s \mid m$, and $s \equiv 1 \pmod{p}$.

Example. Every group of order 15 is cyclic. (Show that both the 5- and 3-subgroups must be normal.)

Example. There are two isomorphism classes of groups of order 21 (The other one comes from having 7 conjugate Sylow 3-subgroups. Then, $x^7 = y^3 = 1$, and $yxy^{-1} = x^i$ for some i, since the 7-subgroup is normal and thus conjugates to itself.)

Example. A group of order 12 must be of the form:

- $C_3 \times C_4$
- $C_2 \times C_2 \times C_3$
- A_4 (the alternating group)
- D_6
- the group generated by x and y with $x^4 = y^3 = 1$, $xy = y^2x$.

Proposition. Let σ, τ be permutations which act on disjoint sets of indices. Then $\sigma\tau = \tau\sigma$.

Proposition. Every permutation which is not the identity is a product of disjoint cyclic permutations; these cyclic permutations are unique up to order.

Proposition. Let σ be the cyclic permutation $(i_1 \ldots i_k)$. Let q be any permutation. Let $q(i_r) = j_r$. Then $q\sigma q^{-1} = (j_1 \ldots j_k)$. If $p = \sigma_1 \ldots \sigma_n$ is the product of disjoint cycles, then $qpq^{-1} = (q\sigma_1 q^{-1}) \ldots (q\sigma_n q^{-1})$ is the product of disjoint cycles.

Corollary. Two permutations are conjugate elements of the symmetric group if and only if their disjoint cycle decompositions have the same order.

Theorem. Let p be prime. Let H be a subgroup of the symmetric group S_p whose order is divisible by p. If the Sylow p-subgroup of H is normal, then the elements of H can be relabeled so that H is contained in the group of operators of the form $f(x) = cx+a$, in the field $\mathbf{Z}_p$.

Bilinear Forms

Definition. Let V be a vector space over a field F. A <u>bilinear form</u> on V is a function of two variables, $<,>: V \times V \rightarrow F$, such that:

- $<v_1 + v_2, w> = <v_1, w> + <v_2, w>$
- $<cv, w> = c<v, w> = <v, cw>$

- $<v, w_1 + w_2> = <v, w_1> + <v, w_2>$

Definition. A form $<,>$ is symmetric if $<v, w> = <w, v>$ for all v and w.

Definition. A form $<,>$ is skew-symmetric if $<v, v> = 0$ for all v. (Equivalently, $<v, w> = - <w, v>$ for all v and w, if the field is not characteristic 2.)

Definition. Let A be an $n \times n$ matrix in F. Then $<X, Y> = X^T AY$ is a bilinear form.

Proposition. $<X, Y> = X^T AY$ is symmetric if and only if A is a symmetric matrix.

Proposition. Let A be the matrix of a bilinear form with respect to a basis. The matrices A' which represent the same form with respect to a different basis are $A' = QAQ^T$ where $Q \in GL_n(F)$.

Corollary. The matrices A which represent a form equivalent to a dot product (in some basis) are $A = P^T P$ where P is invertible.

Definition. A form is positive definite if $<X, X> > 0$ for all X.

Theorem. The following properties of a real $n \times n$ matrix, A, are equivalent:

- A represents dot product with respect to some basis of $\mathbf{R}^n$.
- There is an invertible matrix $P \in GL_n(\mathbf{R})$ such that $A = P^T P$.
- A is symmetric and positive definite.

Definition. Vectors v and w are orthogonal with respect to a symmetric form if $<v, w> = 0$.

Definition. A basis $\mathbf{B} = (v_1, \ldots, v_n)$ is an orthonormal basis with respect to a form $<,>$ if $<v_i, v_j> = 0$ when $i \neq j$ and $<v_i, v_i> = 1$ for all i.

Theorem. Let $<,>$ be a positive definite symmetric form on a finite-dimensional vector space V. There exists an orthonormal basis for V.

Proof. Use the Gram-Schmidt algorithm.

Theorem. Let A_i be the upper left $i \times i$ submatrix of a real symmetric $n \times n$ matrix A. A is positive definite if and only if det A_i is positive for each $i = 1, \ldots, n$.

Definition. A form $<,>$ is indefinite if $<v, v>$ can be positive or negative.

Proposition. Suppose $<,>$ is not identically zero. Then there is a vector, v, such that $<v, v> \neq 0$.

Definition. Let W be a subspace of V. The orthogonal complement of W is given by $W^\perp = \{v \in V \mid <v, W> = 0\}$, which is the set of vectors orthogonal to every vector in W.

Definition. A vector $v \in V$ is a null vector if $<v, w> = 0$ for every $w \in V$. The null space of the form is the set of all null vectors. A form is non-degenerate if the null space is $\{0\}$.

Proposition. Let A be the matrix of a symmetric form with respect to a basis. The null space of this form is the set of solutions to $AX = 0$. Thus, the form is nondegenerate if and only if A is non-singular.

Proposition. Let W be a subspace of V. If $<,>$ if nondegenerate on W, the $V = W \oplus W^\perp$. That is, $W \cap W^\perp = \{0\}$ and W and $W^\perp$ span V.

Definition. An orthogonal basis $\mathbf{B} = (v_1, \ldots, v_n)$ for V with respect to a form $<,>$ is a basis such that $<v_i, v_j> = 0$ whenever $i \neq j$.

Corollary. The matrix of a form is diagonal if and only if the basis is orthogonal.

Theorem. Let $<,>$ be a symmetric form on a real vector space V. There is a basis for V, $(v_1, \ldots, v_n)$ such that $<v_i, v_j> = 0$ when $i \neq j$ and $<v_i, v_i>$ is 0, 1 or –1. In matrix form, for any real symmetric matrix, there is a matrix $Q \in GL_n(\mathbf{R})$ such that QAQ^T is a diagonal matrix with diagonal entries 0, 1 or –1.

Theorem (Sylvester's Law of Inertia). The number +1, -1, and 0's in the diagonal matrix of a form are unique. (So we call (p, m) = (# of 1's, # of –1's) the <u>signature</u> of the form.)

Definition. Let $\langle , \rangle$ be a real symmetric positive definite form. The vector space together with this form is called a <u>Euclidean space</u>. The <u>length</u> of a vector is given by $\sqrt{\langle v, v\rangle} = |v|$.

Definition. Let W be a subspace of a Euclidean space. Then $V = W \oplus W^{\perp}$. Then the expression $v = w + w'$, with $w \in W$ and $\langle w, w'\rangle = 0$. The <u>orthogonal projection</u>, $\pi: V \rightarrow W$, is given by $\pi(w + w') = w$.

Proposition. Let $(w_1, \ldots, w_r)$ be an orthonormal basis of a subspace W. Let $v \in V$. The orthogonal projection $\pi(v)$ of v onto W is the vector $\pi(v) = \langle v, w_1\rangle w_1 + \ldots + \langle v, w_r\rangle w_r$.

Corollary. Let $B = (b_1, \ldots, b_n)$ be an orthonormal basis for a Euclidean space. Then, $v = \langle v, v_1\rangle v_1 + \ldots + \langle v, v_n\rangle v_n$. That is, the coordinate vector is $(\langle v, v_1\rangle, \ldots, \langle v, v_n\rangle)^T$.

Definition. If V is a complex vector space, a <u>hermitian form</u> on V is a function $\langle , \rangle: V \times V \rightarrow \mathbf{C}$ that satisfies the following properties:

- Linearity in the second variable: $\langle X, cY\rangle = c\langle X, Y\rangle$, $\langle X, Y_1 + Y_2\rangle = \langle X, Y_1\rangle + \langle X, Y_2\rangle$
- Conjugate linearity in the first variable: $\langle cX, Y\rangle = \overline{c}\langle X, Y\rangle$, $\langle X_1 + X_2, Y\rangle = \langle X_1, Y\rangle + \langle X_2, Y\rangle$
- Hermitian symmetry: $\langle Y, X\rangle = \overline{\langle X,Y\rangle}$ (conjugate)

Note. Let A be a complex matrix. Then A defines a form: $\langle X, Y\rangle = \overline{X}^T AY$.

Definition. The <u>adjoint</u> of a matrix A is $A^* = \overline{A}^T$ (A-conjugate^T). A matrix is <u>hermitian</u> or <u>self-adjoint</u> if $A = A^*$.

Corollary. A real matrix is symmetric if and only if it is hermitian.

Corollary. Let A be the matrix of a hermitian form. The matrices which represent the same form with respect to a different basis are those of the form $A' = QAQ^*$, $Q \in GL_n(\mathbf{C})$.

Definition. A matrix P is <u>unitary</u> if $P^*P = I$, or $P^* = P^{-1}$.

Definition. The set of all unitary matrices is the <u>unitary group</u>, U_n.

Corollary. A change of basis preserves the standard hermitian product – that is, $X^*Y = X'^*Y'$ – if and only if the matrix change of basis is unitary.

Proposition. Let T be a linear operator on a hermitian spacwe V. Let M be the matrix of T with respect to an orthonormal basis. The matrix M is hermititan if and only if $\langle v, Tw\rangle = \langle Tv, w\rangle$ for all $v, w \in V$. Then, T is called a <u>hermitian operator</u>. The matrix M is unitary if and only if $\langle v, w\rangle = \langle Tv, Tw\rangle$ for all $v, w \in V$. Then T is called a <u>unitary operator</u>.

Proposition. Let M be the matrix of a real operator T with respect to an orthonormal basis. The matrix M is symmetric if and only if $\langle v, Tw\rangle = \langle Tv, w\rangle$ for all $v, w \in V$. If so, T is called a <u>symmetric operator</u>. The matrix M is orthogonal if and only if $\langle v, w\rangle = \langle Tv, Tw\rangle$ for all $v, w \in V$. If so, T is called an <u>orthogonal operator</u>.

Theorem (Spectral Theorem). Let T be a hermitian operator on a hermitian vector space V. There is an orthonormal basis of V consisting of eigenvectors of T. If M is the matrix of T, there is a unitary matrix P such that $PMP^*$is a real diagonal matrix.

Theorem (Spectral Theorem – real case). Let T be asymmetric operator on a real vector space V with a positive definite biliear form. There is an orthonormal basis of eigenvectors of T. If M is the matrix of T, there is an orthogonal matric $P \in O_n$® such that PMP^T is diagonal.

Proposition. The eigenvalues of a hermitian operator T are real numbers.

Corollary. The eigenvalues of a real symmetric matrix are real.

Definition. A <u>conic</u> if a locus of points in $\mathbf{R}^2$ defined by a quadratic equation in two variables: $f(x, y) = a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + b_1x + b_2y + c = 0$. This locus is an ellipse, a hyperbola, a parabola, or degenerate (a pair of lines, a single line, a point, and empty).

Definition. A <u>quadratic form</u> in n variables $x_1, \ldots, x_n$ is a polynomial each of whose terms has degree two in the varibles.

Note. Every quadratic form is of the form $q(x_1, \ldots, x_n) = (x_1, \ldots, x_n) A(x_1, \ldots, x_n)^T$, where A is symmetric. (a_{ii} is the coefficient on x_i^2, a_{ij} is half the coefficient on x_ix_j.)

Theorem. The congruence classes of non-degenerate conics in $\mathbf{R}^2$ are:

- Ellipse: $a_{11}x_1^2 + a_{22}x_2^2 - 1 = 0$
- Hyperbola: $a_{11}x_1^2 - a_{22}x_2^2 - 1 = 0$
- Parabola: $a_{11}x_1^2 - x_2 = 0$

Proof. Diagonalize the matrix of the quadratic part and then translate to remove som of the linear and constant terms.

Theorem. The congruence classes of non-degenerate conics in $\mathbf{R}^3$ are:

- Ellipsoids: $a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 - 1 = 0$
- 1-sheeted hyperboloids: $a_{11}x_1^2 + a_{22}x_2^2 - a_{33}x_3^2 - 1 = 0$
- 2-sheeted hyperboloids: $a_{11}x_1^2 - a_{22}x_2^2 - a_{33}x_3^2 - 1 = 0$
- Elliptic Paraboloids: $a_{11}x_1^2 + a_{22}x_2^2 - x_3 = 0$
- Hyperbolic Paraboloids: $a_{11}x_1^2 - a_{22}x_2^2 - x_3 = 0$.

Definition. A matrix M is called <u>normal</u> if $MM^* = M^*M$.

Lemma. If M is normal and P is unitary, then $M' = PMP^*$ is normal.

definition. A <u>normal operator</u>, $T: V \rightarrow V$ is a linear operator whose matrix M is normal.

Theorem. A complex matrix is normal if and only if there is a unitary matrix such that PMP^* is diagonal.

Corollary. Every conjugacy class in the unitary group contains a diagonal matrix.

Theorem. Let V be a vector space of dimension m over a field F. Let <,> be a non-degenerate skew-symmetric form on V. The m is an even integer and tehre is a basis of V such that the matrix A is of the form:

$$J_{2n} = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$$

where 0 and I are $m/2 \times m/2$ matrices. Let A be a non-singular skew-symmetric $m \times m$ matrix. Then m is even and there is a matrix $Q \in GL_m(F)$ such that QAQ^T is the matrix J_{2n}.

Modules

Definition. Let R be a commutative ring with identity. An <u>r-module</u> V is an abelian group with law of composition +, together with a scalar multiplication $R \times V \rightarrow V$, satisfying the following axioms:

- $1v = v$
- $(rs)v = r(sv)$
- $(r + s)v = rv + sv$
- $r(v + v') = rv + rv'$

Definition. Let R^n be the set ofg R-vectors of length n. This is a mdule and is called a free module.
Example. Any abelian group (with composition written additively) is a **Z**-modulewith the scalar multiplication: nv = V + … + v (n times. Thus, any **Z**-module is an abelian group, if we ignore its scalar multiplication.
Definition. A submodule of an R-module V is a nonempty subset of V which is closed under addition and scalar multiplication.
Proposition. The submodules of the R-module R^1 are the ideals of R.
Definition. A homomorphism, $\varphi: V \rightarrow W$ of R-modules is a function that satisfies $\varphi(v + v') = \varphi(v) + \varphi(v')$ and $\varphi(rv) = r\varphi(v)$. A bijective homomorphism is an isomorphism.
Note. If $\varphi: V \rightarrow W$ is a homomorphism, the kernel of φ is a submodule of V and the image of φ is a submodule of W.
Definition. Let W be a submodule of an R-module V. The quotient V/W is the additive group of coset, [v] = v + W. This is an R-modlule if we deine r[v] = [rv].
Proposition. The definition of a quotient module is well-defined and creates an R-module. The canonical map, $\pi: V \rightarrow V/W$, $\pi(v) = [v]$ is a surjective homomorphis, of R-modules with kernel W.
Proposition (Mapping Property). Let $f: V \rightarrow V'$ be a homomorphism of R modules whose kernel contains W. There is a unique homomorphism $f': V/W \rightarrow V'$ such that $f = f'\pi$.
Theorem (First Isomorphism Theorem). If ker f = W, then $f': V/W \rightarrow V'$ is an isomorphism from V/W to Im f.
Theorem (Correspondence Theorem). There is a bijective correspondence between submodules S/W of V/W and the submodules S of V that contain W, defined by $S = \pi^{-1}(S/W)$ and $S/W = \pi(S)$. (V/W)/(S/W) = (V/S).
Proposition. The invertible $n \times n$ matrices with entries in a ring R are those matrices whose determinant is a unit. They form a group $GL_n(R)$, called the general linear group over R.
Definition. An ordered set $(v_1, \ldots, v_k)$ of elements of a module V generates V if every $v \in V$ can be written as $v = r_1v_1 + \ldots + r_kv_k$, $r_i \in R$. Then, the v_i are called generators. A module V is finitely generated if there exists a finite set of generators.
Definition. A finitely generated module is free if there is an isomorphism $\varphi: R^n \rightarrow V$. A free **Z**-module is also called a free abelian group.
Definition. A set of elements $(v_1, \ldots, v_n)$ of a module V is independent if no nontrivial linear combination of them is 0; that is, if $r_1v_1 + \ldots + r_nv_n = 0$ then $r_i = 0$ for all i.
Definition. A set of elements is a basis if it is independent and a generating set.
Proposition. A module has a basis if and only if it is free.
Theorem. Let R be a commutative ring. Any two bases of a free R-module have the same cardinality.
Definition. An elementary integer matrix corresponds to adding an integer multiple of a row/column to another row/column, interchanging two rows/columns, or multiplying a row/column by a unit.
Theorem. Let A be an $m \times n$ integer matrix. There exist Q and P, which are products of elementary integer matrices, such that QAP^{-1} is diagonal, where the diagonal entries d_{ii} are nonnegative and $d_i \mid d_{i+1}$ for all i.

Theorem. Let R be a Euclidean domain. Let A be an $m \times n$ matrix with entries in R. There are products Q and P of elementary R-matrices such that QAP^{-1} is diagonal and each diagonal entry divides the next.

Theorem. Let $\varphi: V \to W$ be a homomorphism of free abelian groups. There exists bases of V and W such that the matrix of the homomorphism has diagonal form.

Thorem. Let S be a subgroup of a free abelian group W of rank m. There is a basis $(w_1, \ldots, w_m)$ of W and a basis $(s_1, \ldots, s_n)$ of S such that $n \leq m$, for each $j \leq n$ there is a positive integer d_j such that $u_j = d_j w_j$, and $d_i \mid d_{i+1}$ for $i \leq n-1$.

Corollary. Every subgroup of a free abelian group of rank m is free and its rank is at most m.

Definition. If $(v_1, \ldots, v_m)$ are generators of an R-module V, equations of the form $a_1v_1 + \ldots + a_mv_m = 0$ are relations among the elements. The R-vector $(a_1, \ldots, a_m)^T$ is called a relation vector. A complete set of relations is a set fo relation vectors such that any other relation vector is a linear combination of the relation vectors in the set.

Definition. Let $\varphi: W \to W'$ be a homomorphism of R-modules. The cokernel of φ is the quotient module $W'/(\text{Im } \varphi)$.

Definition. Let $\varphi: R^n \to R^m$ be the homomorphism that is left multiplication by A. the cokernel of φ is presented by the matrix A.

Corollary. If A is an $m \times n$ presentation matrix, the module it presents is isomorphic to R^m/AR^n.

Proposition. Let A be an $m \times n$ presentation matrix for a module V. The following matrices present the same module V:

- QAP^{-1}, where $Q \in GL_m(R)$ and $P \in GL_n(R)$
- the matrix obtained by deleting a column of zeros (that relation tells us nothing)
- the matrix obtained by deleting the i^{th} row and j^{th} column, if the j^{th} column has a 1 in the i^{th} place and a 0 everywhere else (that generator must always be 0).

Proposition. Let V be an R-module. Every submodule W of V is finitely generated if and only if there is no infinite strictly increasing chain of submodules $W_1 < W_2 < \ldots$ of V (this is the ascending chain condition).

Lemma. Let $\varphi: V \to W$ be a homomorphism of R-modules. If the kernel and image of φ are finitely generated modules, so it V. If V is finitely generated and φ is surjective, W is finitely generated. In fact, if $(v_1, \ldots, v_n)$ generates V, then $(\varphi(v_1), \ldots, \varphi(v_n))$ generates W.

Corollary. Let W be a submodule of an R-module V. If both W and V/W are finitely generated, so is V.

Definition. A ring R is noetherian if every ideal of R is finitely generated.

Corollary. Let R be a noetherian ring. Every proper ideal of R is contained in a maximal ideal.

Proposition. Let V be a finitely generated model over a noetherian ring R. Then every submodule of V is finitely generated.

Theorem (Hilbert Basis Theorem). If a ring R is noetherian, so is R[x].

Proposition. Let R be a noetherian ring, and let I be an ideal of R. The quotient ring R/I is noetherian.

Lemma. The set of leading coefficients of the polynomials in an ideal of R[x], together with 0, is an ideal of R.

Lemma. Let P_n be the set of polynomials in R[x] with degree less than n, together with zero. Let $S_n = I \cap P_n$. Then S_n is an R-submodule of the R-module P_n.

Definition. Let $W_1, \ldots, W_k$ be submodules of a module V. V is the direct sum of the submodules W_i if each element $v \in V$ can be written uniquely in the form $w_1 + \ldots + w_k$, with $w_i \in W_i$. We then write $V = W_1 \oplus \ldots \oplus W_k$.

Theorem (Structure Theorem for Abelian Groups). Let V be a finitely generated abelian group. Then V is the direct sum of finite syclic subgroups $C_{d1}, \ldots, C_{dk}$ and a free abelian group L, where $d_i > 1$ and $d_1 \mid d_2 \mid d_3 \mid \ldots$

Proof. Write the group as a **Z**-module. Diagonalize the presentation matrix. This gives the necessary relations.

Corollary. Every finitely generated abelian group is the direct sum of cyclic groups of prime power orders and of a free abliean group.

Theorem. Suppose $V = C_{d1} \oplus \ldots \oplus C_{dk}$. Then the integers $d_1, \ldots, d_k$ are uniquely determined by V. (The same is true for the prime power orders.)

Theorem (Structure Theorem for modules over Euclidean domains). Let V be a finitely generated R-module, with R a Euclidean domain. The V is the direct sum of cyclic modules C_j and a free module L. Equivalently, there is an isomorphism from V to $R/(d_1) \times \ldots \times R/(d_k) \times R^r$.

Definition. Let T: V → V be a linear operator on a vector space over a field F. We make V a F[t]-module by $f(t)v = f(T)(v) = a_nT^n(V) + \ldots + a_1T(v) + a_0v$.

Definition. Suppose V is a F[t]-module. Define T: V → V be T(v) = tv. Then T is a linear operator on V.

Corollary. F[t]-modules are equivalent to linear operators on F-vector spaces.