ABSTRACT ALGEBRA I-III

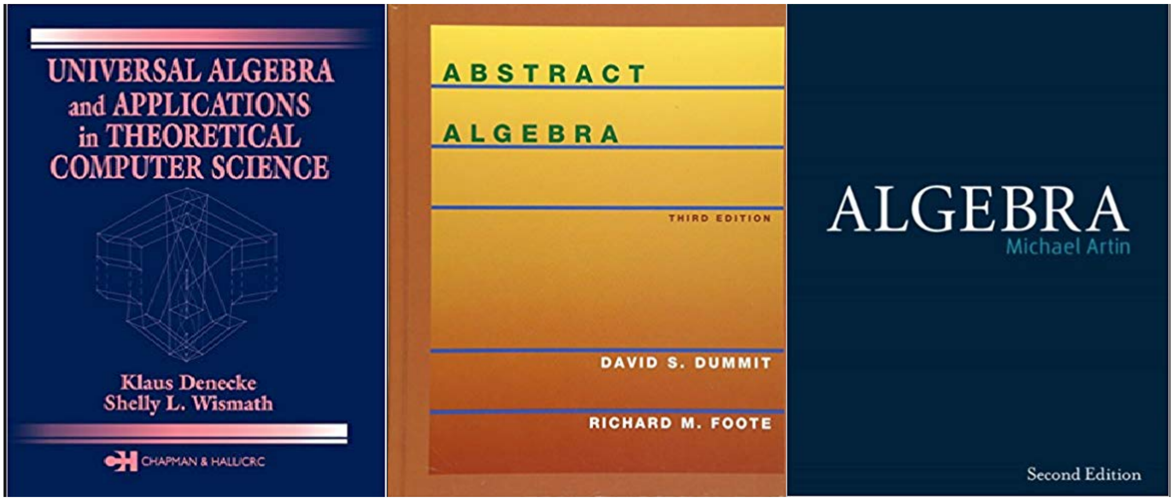
Definitions and Theorems

Collected By: Kevin Smith

Preface

This text is intended to be a brief, conceptual outline for a graduate sequence in Abstract Algebra.

The benefit to this list is that all the definitions are immediately stated and ready for use in problems. As well, the theory at the end is named and streamlined. The texts that I have referenced here consist of:



Lastly, I have included some navigation hyperlinks in the pdf, so any red headers and the / << / symbol you can click to navigate.

- Kevin

Table of Contents (Compressed)

Abstract Algebra I-III

Table of Contents (Expanded)

PART I

PART II

Specialized Structures:

PART III

<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>

PART I

1. Basic Structures

• Def. 1.1: An **algebraic structure** is a collection $\mathfrak{A} = \{A, (f_i)_{i\in I}, \tau\}$, where A is the underlying set or **universe**, the f_i are indexed **operations** with a corresponding indexed **arities** listed in the vector $\tau = (n_i)_{i\in I}$ called the **type**. Most examples just state explicitly the type instead of listing it.

• Def. 1.2: A **group** $G = \{G, \{*, 1\}, (2, 1)\}$ is a set together with a unary operation $1 : G \to G$; $1(g) = g$ (a.k.a. identity) and an associative binary operation $* : G \times G \to G$ (called product or composition), such that $\forall g \in G$, $\exists g^{-1} \in G$ for which $g * g^{-1} = g^{-1} * g = 1$.

A group is called **abelian** if $*$ is also commutative.

• Def. 1.3: A **ring with unit** $R = \{R, \{+, *, 0, 1\}, (2, 2, 1, 1)\}$ is an abelian group in $\{R, +, 0\}$ and a semigroup in $\{R, *, 1\}$ (that is, R is not closed under $*$ inverses) and for which distribution of $*$ over $+$ holds. A ring is commutative if $*$ is.

• Def. 1.4: A **field** $F = \{F, \{+, *, 0, 1\}, (2, 2, 1, 1)\}$ is an abelian group with respect to both pairs of operations as above.

• Def. 1.5: A **vector space over a field** $V \equiv V/F = \{V \cup F, \{+, *, 0, \tilde{+}, \tilde{*}, \tilde{0}, \tilde{1}\}, (2, 2, 1, 2, 2, 1, 1)\}$ is an abelian group in $\{V, +, 0\}$ together with an associative field action (binary operation) $* : F \times V \to V$ and distribution properties for $*/+$ and $*/\tilde{+}$. The tilde operations are for the field.

• Def. 1.6: An **R-module** or **module over a ring** $V \equiv V/R = \{V \cup R, \{+, *, 0, \tilde{+}, \tilde{*}, \tilde{0}, \tilde{1}\}, (2, 2, 1, 2, 2, 1, 1)\}$ is an abelian group in $\{V, +, 0\}$ together with an associative (left *or* right) ring action $* : R \times V \to V$ *or* $* : V \times R \to V$ with distribution properties for $*/+$ and $*/\tilde{+}$.

• Def. 1.7: A **(traditional) algebra over a field or ring** $A = \{A, \langle\cdot,\cdot\rangle, (2)\}$ is simply a vector space or a module A respectively, together with a *bilinear* operation $\langle\cdot,\cdot\rangle : A \times A \to A$.

Notice here in (1.7) we have shorthanded the mass of operations for the vector space and its field or ring. This is done in context with all algebras. Some "traditional" algebras we will see are *Euclidean* and *Hermitian spaces* with their *bilinear form* $<,>: A \times A \to A$ (Section II.6) and Group Rings (Section II.8).

• Def. 1.8: A **group ring**, **RG-module**, or **group algebra** is a traditional algebra generalized to the case of not necessarily commutative "additive" group.

We denote $RG \equiv R[G] = \{A, \langle\cdot,\cdot\rangle, (2)\}$, where $A = \{\sum\limits_{g\in G} \alpha_g g \mid \alpha_g \in R\}$ "formal linear combinations".

Addition $+$ is defined via $\sum\limits_{g\in G} \alpha_g g + \sum\limits_{g\in G} \beta_g g = \sum\limits_{g\in G} (\alpha_g \dot{+} \beta_g) g$, where we use $\dot{+}$ in the ring.

The *ring action* is given by $\alpha * \sum\limits_{g\in G} \alpha_g g = \sum\limits_{g\in G} (\alpha \dot{*} \alpha_g) g$.

And the *bilinear operation* is given by: $\Big\langle \sum\limits_{g\in G} \alpha_g g, \sum\limits_{g\in G} \beta_h h \Big\rangle = \sum\limits_{g,h\in G} (\alpha_g \dot{*} \beta_h) g * h.$

There are many other structures not listed here. See for example *lattices* or *boolean algebras*.

2. General Constructions

★ Quotients, Homomorphic Images, and Substructures

• Def. 2.1: In addition to typifying as we did in the previous section, abstract and explicit algebraic structures can be listed by **presentations**: $\langle S \mid R \rangle$ where S is some **generating set** and R is a **set of relations**. Relations are also known as *axioms* or *identities.*

• Def. 2.2: When no relations have been given, the structure is typically called a **free structure**. Otherwise it is called a **Non-free structure**.

• Def. 2.3: (Types of Relations)
An **n-ary relation** is a subset of the cartesian product $\underbrace{S \times ... \times S}_{n-\text{times}}$. Particularly, a **binary relation** on a set S is a subset $R \subseteq S \times S$. A **ternary relation** $R \subseteq S \times S \times S$, etc.

A binary relation is said to be:
1.) **Reflexive** if $\forall x \in S, (x, x) \in R$,
2.) **Symmetric** if $\forall x, y \in S, (x, y) \in R \leftrightarrow (y, x) \in R$,
3.) **Anti-symmetric** if $\forall x \neq y \in S, (x, y) \in R \rightarrow (y, x) \notin R$, and
4.) **Transitive** if $\forall x, y, z \in S, (x, y)$ and $(y, z) \in R \rightarrow (x, z) \in R$.

An **equivalence relation** is one that is *reflexive, symmetric, and transitive.* A **congruence relation** is an equivalence relation that is also compatible with all the operations of the algebraic structure.

A **partial order** is *reflexive, antisymmetric, and transitive*, a **total order** is a partial order under which every pair of elements are *comparable* i.e. either $(x, y) \in R$ or $(y, x) \in R$.

• Def. 2.4: The **Power Set** $\mathscr{P}(S)$ of a set S is the collection of all subsets of S. A **partition** of S is a subset $\mathscr{T} \subseteq \mathscr{P}(S)$ such that:

i.) $S = \bigcup_{A \in \mathscr{T}} A$ and

ii.) $\forall A, B \in \mathscr{T}, \quad A \cap B = \emptyset$ or $A = B$.

• Def. 2.5: Given a set S and a relation R, a **relationary class of an element** $x \in S$, which we'll call $[x] = \{y \in S \mid (x, y) \in R\}$. When R is an equivalence relation or congruence relation, $[x]$ becomes an **equivalence class** or **congruence class** respectively.

• Def. 2.6: Given an algebraic structure $\mathfrak{A}$ and a congruence relation R, the set of all congruence classes under the relation is called the **quotient structure** and can be denoted by $\mathfrak{B} = \mathfrak{A}/R = \{[x] \mid x \in A\}$. Alternatively, in structures with a notion of "shifting", $\mathfrak{A}/B$ denotes the set of all **cosets of $\boldsymbol{B}$** (shifted sets).

It is easy to show that the set of equivalence classes forms a partition of the underlying set $A \in \mathfrak{A}$. Similarly for congruence classes. [Proof: Definition pushing.]

• Def. 2.7: A map between algebraic structures of the same type who's image is compatible with the corresponding operations is called a **morphism** or **homomorphism**. Structures are **homomorphic** if there exists such a map between them. We can create "new" structures out of an existing one via sending it to a **homomorphic image**. (This covers group homs, ring homs, field homs, linear maps, etc.)

• Def. 2.8: Given two algebraic structures of the same type, $\mathfrak{A}$ and $\mathfrak{B}$, we say $\mathfrak{A}$ is **embedded** in $\mathfrak{B}$ if there exists an injective homomorphism between their universes. We usually denote the map by $\varphi : A \hookrightarrow B$.

• Def. 2.9: Given $\mathfrak{A} = \{A, (f_i)_{i\in I}, \tau\}$ and $\mathfrak{B} = \{B, (g_j)_{j\in J}, \sigma\}$, we say $\mathfrak{B}$ is a **substructure** of $\mathfrak{A}$ and denote $\mathfrak{B} \leq \mathfrak{A}$ if:

i.) $B \subseteq A$ and $(g_j)_{j\in J} \subseteq (f_i)_{i\in I}$,
ii.) $\forall j\ \exists i$ such that $g_j = f_i\big|_B$, and
iii.) perhaps redundantly, B is closed with respect to $(g_j)_{j\in J}$.

Note: This covers subgroups, subrings, subfields, subspaces, submodules, etc. There are in each case propositions that make substructure determination easy (e.g. *subgroup criterion*).

• Def. 2.10: A structure is said to be **generated** by a set X and specified operations, denoted $\mathfrak{X} \equiv \langle X\rangle$ if each element in $\mathfrak{X}$ is a "product" of elements in X. By product we mean of course the image of some operation. *Substructures* may be generated by subsets of a given universe along with the superstructure's operations, usually this is denoted $\langle X\rangle_{\mathfrak{A}}$ or just $\langle X\rangle$ when context is understood. The set X is called the **generating set**. If $\mathfrak{A}$ is generated by one element, it is called **cyclic**.

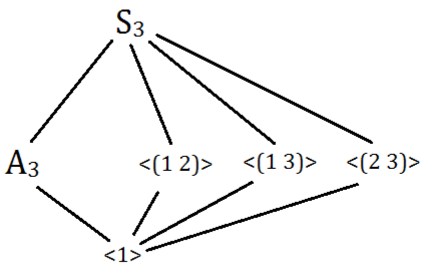
• Def. 2.11: If a substructure $\mathfrak{B} \leq \mathfrak{A}$ can be "shifted" in a superstructure via some operation to generate a quotient of A, we say $\mathfrak{B}$ is **normal**.

Notes: Shifting can take on various meanings depending on the operation used. Traditional examples include *normal subgroups* whereby one can shift a normal subgroup N with the group operation $g * N$ to generate a quotient; in ring theory, we use $r + N$ etc. In each case, one must of course check that the axioms of a congruence relation hold. It is exactly this process of checking that yields criteria for "normality".

• Def. 2.12: A structure is called **simple** if it has no proper normal substructures.

• Def. 2.13: We can take all the substructures and display them graphically, ordered vertically by the relation *"is a substructure of"*. We connect two such objects by a line if they are comparable. This can be done similarly with quotients as well. The results are called the **substructure lattice** and **quotient lattice** respectively.

Note: We avoid properly defining a lattice as an algebraic structure, but this can be looked up. Among other things, these lattices are good for visualizing global properties of a particular algebraic structure as well as aiding in combinatorial arguments. Here is an example picture for the subgroup lattice of S_3.



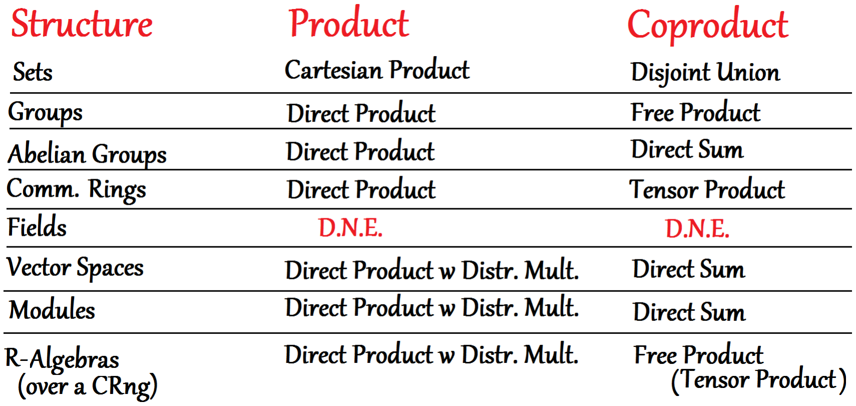
★ "Products" of Structures, Decomposability, and Extended Structures

In addition to quotients, homomorphic images, and substructures, we can combine existing ones to obtain larger structures of the same type. This concept has two *dual* notions according to category theory, called *product* and *coproduct.*

Briefly, a category can be thought of as a collection of algebraic structures of the same type together with all possible morphisms between them. In this language, we refer to "algebraic structures of the same type" as just "objects" in a particular category.

• Def. 2.14: The **product** of two objects A and B is a triple (C, p_1, p_2) where C is another object and each p_i is a projection morphism onto the components A and B respectively. Moreover, we require that this product is unique up to homomorphism by what's called a *universal property.* Dually, a **coproduct** is a triple (D, i_1, i_2) where the i_j are injection morphisms from A and B respectively, obeying a similar universal property.

The following is a prospective list compiled from wikipedia of *finite* products and coproducts:



Structure	Product	Coproduct
Sets	Cartesian Product	Disjoint Union
Groups	Direct Product	Free Product
Abelian Groups	Direct Product	Direct Sum
Comm. Rings	Direct Product	Tensor Product
Fields	D.N.E.	D.N.E.
Vector Spaces	Direct Product w Distr. Mult.	Direct Sum
Modules	Direct Product w Distr. Mult.	Direct Sum
R-Algebras (over a CRng)	Direct Product w Distr. Mult.	Free Product (Tensor Product)

Notes: *These constructions do not always exist or generalize to the infinite case. It seems as if direct product and free product are the way to go for all of these constructions, however it is not clear in the literature, nor is it clear the relationship between say direct sum and tensor product (since they may exist simultaneously) or whether or not semi-direct or sub-direct products etc can be characterized like this. The point is, we can sometimes create larger algebraic structures of the same type from 2 or more existing ones.*

• Def. 2.15: We call an object **decomposable** if it can be written as a product or coproduct of two sub-objects. In the instance of modules for example, a module is decomposable if it can be written as a direct sum of two sub-modules. We call objects **completely reducible** if they can be written as finite products or coproducts of all indecomposable sub-objects.

Lastly, we can make larger structures out of existing ones by appending sets of elements formally and extending linearly as the following shows:
• Def. 2.16: Let $\mathfrak{A}$ be given and let x be indeterminate. Denote the **extension algebra** $\boldsymbol{\mathfrak{A}[x] = \{\sum \alpha_n x^n \mid \alpha_n \in A, n \in} \mathbb{Z}\}$ together with operations from $\mathfrak{A}$ extended via linearity.

Note: If we let the powers range from 0 to $N \in \mathbb{Z}$, we obtain polynomial like structures. If we substitute $x \mapsto \alpha$ for particular $\alpha \notin A$ then we obtain things similar to complex numbers $\mathbb{C} = \mathbb{R}[i]$ (II.5).

3. Morhisms

• Def. 3.1: A map between two algebras of the same type, $\varphi : \mathfrak{A} \to \mathfrak{B}$, is called **structure preserving** if all the images of all of the operations are compatible with the operations in the range. That is, given an $n - ary$ operation and n elements of A, φ is structure preserving if $\varphi\big(* (a_1, ..., a_n)\big) = \tilde{*}\big(\varphi(a_1), ..., \varphi(a_n)\big)$. Note that this also includes 1-ary operations such as identities: $1(a) := a$.

• Def. 3.2: As special cases, we obtain **Group, Ring, and Field Homomorphisms** and **Vector Space/Module Homomorphisms (R-Linear Maps)** and for the case of RG modules, **R-Linear Homomorphisms**.

• Def. 3.3: **Composites of morphisms** are again morphisms. Morphisms on product algebras are known as **multi-homomorphisms**.

• Def. 3.4: The canonical map between an algebra and its quotient is called a **quotient homomorphism**. We also have **injection/embedding homomorphisms** as well as **projection homomorphisms** (from a product algebra).

• Def. 3.5: We have **isomorphisms** are bijective homomorphisms; **endomorphisms** are homomorphisms between an algebra and itself; an **automorphism** is a bijective endomorphism.

• Def. 3.6: Let f, g be morphisms such that $f : A \to B$ and $g : B \to A$ and $g \circ f = Id_A$. We say f is a **retraction** and g is a **coretraction** or **section**. These are relative terms and depend what set is designated as the focal point. For example, vector fields are considered sections of a vector bundle, relative to the vector bundles projection map that takes a vector at a point to its base point: $\pi : (v, p) \to p$ and $X(p) = (v, p), \forall p, \forall v$. Here the focal point is the underlying manifold (not the vector bundle). To retract means more or less to bring back. Section means roughly, cross-section? Lousy terminology...

• Def. 3.7: A **monomorphism** is a morphism that is **left-cancellative**, that is: for any two morphisms $g, h : X \to A$ and $f : A \to B$, we have: $f \circ g = f \circ h \implies g = h$. Similarly, an **epimorphism** is a **right-cancellative** morphism. Mono is meant to mimick 1-1 and it just so happens that these are generalizations of 1-1 and onto respectively.

• Def. 3.8: The **kernel** of a morphism is the domain set that maps to the zero element of the image (assuming that algebra has one). In the more general case, the kernel is defined as
$ker(\varphi) = \{a \in A \mid \varphi(a) = \varphi(b)\}$ - that is, the set of congruence classes of elements with the same images. The **cokernel** of a morphism $\varphi : A \to B$ is given by: $cok(\varphi) = B/Im(\varphi)$. That is, the set of all cosets of the image. This definition applies more generally to algebras with a notion of "shifting" as discussed in Def 2.11 above.

4. Other Mappings

• <u>Def. 4.1:</u> An **action** (of a group) on a set is a map $\theta : G \times S \to S$ such that $\theta\big(g, \theta(h, s)\big) = \theta(gh, s)$ and $\theta(1, s) = s$. One may generalize to any **algebraic action** by replacing G with A with appropriate compatibility conditions. It should be noted that a ring acting on itself generates an R-module [see Section II.7].

• <u>Def. 4.2:</u> Homomorphic images can be used to represent groups with different labeling. For example given any group G, the **linear representation** of G is just the image of a homomorphism: $\rho : G \to GL_n(V)$, where $GL_n(V)$ is the group of $n \times n$ matrices. If we use elements of G as the basis for an arbitrary vector space over some field F, the map $\rho : G \to GL_n(G \backslash F)$ provides us with the **regular representation**. Now if we use for an arbitrary vector space, $\rho : G \to Aut(V)$ we get the **permutation representation**.

In general, a **representation of an algebra** is a particular homomorphic image of the algebra in a familiar structure. [For more on representation theory, see Section II.8 and III.1.6]

• <u>Def. 4.3:</u> A **category** is a pair of classes $\mathbf{C} = (Ob(\mathbf{C}), Hom(\mathbf{C}))$ respectively, the objects and the morphisms of $\mathbf{C}$, subject to a set of rules. The rules are for every object there exists an identity morphism and morphisms are associative in their composition. **Functors** are bi-maps that take objects and morphisms from one category to another. **Natural transformations** are morphisms between Functors (we can consider the category of all Functors, with objects being functors and the morphisms being natural transformations.

• <u>Def. 4.4:</u> A **Galois-connection** between sets A and B is a pair (σ, τ) of mappings between power sets $\mathscr{P}(A)$ and $\mathscr{P}(B)$,
$\sigma : \mathscr{P}(A) \to \mathscr{P}(B)$ and $\tau : \mathscr{P}(B) \to \mathscr{P}(A)$, such that $\forall X, X' \subseteq A$ and $\forall Y, Y' \subseteq B$ the following conditions are satisfied:
1.) $X \subseteq X' \implies \sigma(X') \subseteq (X)$, and $Y \subseteq (Y') \implies \tau(Y') \subseteq \tau(Y)$;
2.) $X \subseteq \tau\sigma(X)$, and $Y \subseteq \sigma\tau(Y)$. [Denecke (pg. 40)].

In other words, a connection is a pair of quasi-inverse set mappings taking subsets to subsets with inclusions reversed in each image. Quasi-inverse because it is not necessarily the case that $\tau\sigma = Id_A$. See the traditional Galois connection in Section II.5.

PART II

Specialized Structures

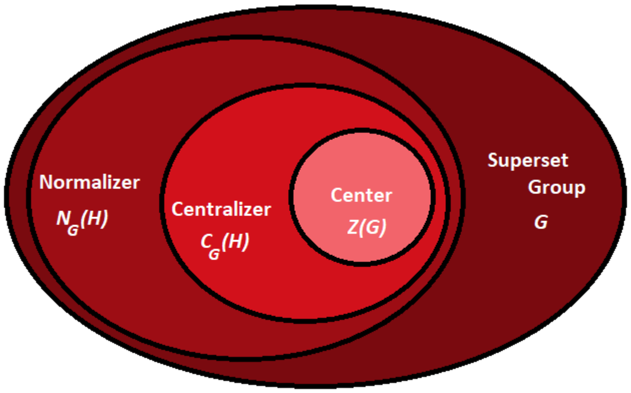
1. Groups (See: Results)

- Def. 1.1: Given a subset $H \subseteq G$, the **centralizer of H in G** denoted $\boldsymbol{C_G(H) = \{g \in G \mid gh = hg, \forall h \in H\}}$, that is, the set of elements that commute with every element of H.

- Def. 1.2: The **center** of a group G is just the subset $\boldsymbol{Z(G) := C_G(G)}$.

- Def. 1.3: The **normalizer of $H \subseteq G$** is $\boldsymbol{N_G(H) = \{g \in G \mid gH = Hg\}}$.

- Def. 1.4: A subgroup $H \leq G$ is **normal**, denoted $H \lhd G$ if it is invariant under conjugation by all elements of G. That is, $\forall g \in G, gH = Hg$. In other words $G = N_G(H)$. The **normal closure** of a subset H is the subgroup given by: $\langle\langle H \rangle\rangle = \bigcup\limits_{g \in G} gHg^{-1}$.



$$\boldsymbol{Z(G) \subseteq C_G(H) \subseteq N_G(H) \subseteq G}.$$

Note: **Zi-Ca-N-Gee** is the acronym for the inclusion chain. An easy way to think of the order is in terms of conjugation and invariance. That is: the normalizer of a subset H is the set of elements in G for which H is invariant under conjugation, whereas the centralizer of H is the set of elements of G that make all elements $h \in H$ individually invariant under conjugation.

- Def. 1.5: The **conjugacy class** of an element $g \in G$, denoted $\boldsymbol{C(g) = \{h \in G \mid h = kgk^{-1}}$, **for** $\boldsymbol{k \in G\}}$.

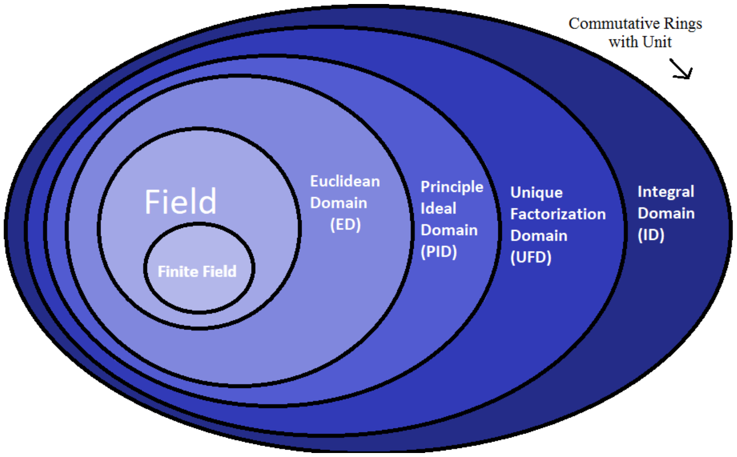
Conjugacy classes show up in a few places, one of which being similar matrices (more on this in Section II.6).

- Def. 1.6: Given a set A and a group action $* : G \times A \to A$, the **stabilizer of $x \in A$**, denoted $\boldsymbol{G_x = \{g \in G \mid gx = x\}}$. Similarly we have G_S for $S \subseteq A$.

We will see later as well (Section II.6) an example of a linear operator action on a vector space that is an element of the space's stabilizer. We think from the side of the invariant space getting acted on usually.

- Def 1.7: Given a set and a group action as before, we have the **orbit of $x \in A$**, denoted $\boldsymbol{O_x = G * x = \{y \in A \mid y = gx, g \in G\}}$.

2. Rings (See: Results)


Commutative Rings with Unit
Field
Finite Field
Euclidean Domain (ED)
Principle Ideal Domain (PID)
Unique Factorization Domain (UFD)
Integral Domain (ID)

The following lists instances of *commutative rings with units* along with their own additional structures. The order of entries designates set inclusion as in the figure above. The acronym being **FEPUI**. Starting with the most general we have:

• Def 2.1: An **Integral Domain** is a commutative ring $\{R, +, *, 0, 1\}$ with unit that does not contain any **zero divisors** – elements defined by the property that $a, b \neq 0$ but $a * b = 0$.

• Def. 2.2: A **Unique Factorization Domain (UFD)** is an integral domain in which every element $r \neq 0, 1$ has the following properties:

1. r can be written as a finite product of prime elements $p_i \in R$: $\quad r = p_1^{k_1} \cdot ... \cdot p_n^{k_n}$.
2. This decomposition is unique up to ordering of the p_i's.

• Def. 2.3: Given a ring R, an **ideal** $I \subseteq R$ is a subring $\{I, +, *, 0, 1\}$ which is closed under multiplication in R. That is, $\forall r \in R$, $\forall i \in I$, $ri, ir \in I$.

• Def. 2.4: A **Principle Ideal Domain (PID)** is an integral domain in which every ideal is *principle* (that is, every ideal is generated by a single element).

• Def. 2.5: An integral domain is called a **Euclidean Domain (ED)** if it possesses a **division algorithm**. I.e. if there exists a function $N : R \to \mathbb{Z}^{\geq 0}$ with $N(0) = 0$ such that $\forall a, b \in R$ $(b \neq 0)$, $\exists q, r \in R$ such that $a = qb + r$, with either $r = 0$ or $N(r) < N(b)$. N is referred to as a **Euclidean function**.

• Def. 2.6: A **Field** is a commutative ring with unit which is closed under element inversion. That is, $\forall a, \exists a^{-1}$.

• Def. 2.7: A **Finite Field** is a field with finitely many elements.

There are other types of rings existing within these like *GCD Domains* and *Bezout Domains* etc. not listed here.

3. Subrings and Other Related Notions

• Def. 3.1: Recall that an **ideal** $I \leq R$ is simply a subring closed under R-multiplication. We define the **Unit Ideal** and the **Zero Ideal** to be respectively (1) and (0). That is, the principle ideals generated by elements 1 and 0. Any other ideal is called **proper**.

• Def. 3.2: A **maximal ideal** is any proper ideal that is not contained in any other proper ideal. A **prime ideal** $P \neq AB = \{ab | a \in A, b \in B\}$ for any two proper ideals A, B.

• Def. 3.3: A ring is **Noetherian** if all ascending chains of ideals stabilize (also known as the **ascending chain condition**). In other words, given any chain of left or right ideals:

$$I_1 \subseteq ... \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq ...\ I_n = I_{n+1} = ... \qquad \text{for some } n.$$

Similarly a ring is called **Artinian** or is said to satisfy the **descending chain condition** if every descending chain of ideals stabilizes.

• Def. 3.4: A **unit** of a ring is any element that has a "multiplicative" inverse. A pair of elements $a, b \in R$ are called **associates** if $\exists u$ (unit) such that either $au = b$ or $a = bu$.

• Def. 3.5: An element of a ring is **irreducible** if it is non-zero and non-unital and there is no "multiplicative" factorization into two or more *non-unit* elements.

• Def. 3.6: An element p of an ring is **prime** if it is non-zero and non-unital and whenever $p|ab$ either $p|a$ or $p|b$.

It should be noted that *prime does not mean irreducible* in general. If R is an integral domain, prime implies irreducible. If R is not UFD, it may fail to be the case that irreducible implies prime.

• Def. 3.7: A **nilpotent** element is one such that there exists $n \in \mathbb{N}$ with $x^n = 0$. The set of all nilpotents in a commutative ring forms a subring called the **nilradical**, denoted $\mathfrak{N}(R)$.

• Def. 3.8: In a ring, an **idempotent** is an element x such that $x^2 = x$. Two idempotents are **orthogonal** if $xy = yx = 0$. A **primitive idempotent** is one that is not a sum of two commuting orthogonal idempotents. An idempotent is **central** if it is contained in the center of the ring $Z(R)$ (i.e. the center of the multiplicative *monoid*).

• Def. 3.9: A ring satisfying any and hence all the conditions in *Wedderburn's Theorem* is called **semisimple**. See Section III results on Module Theory.

Another relevant definition for Wedderburn (FG-module classification theorem) is the definition of a *division ring.*

• Def. 3.10: A **division ring** is a field with the commutivity of $*$ dropped.

4. Fields (See: Results)

⋆ Def. 4.1: The three most important classes of fields are as follows:
1.) A **number field** K is a subfield of $\mathbb{C}$.
2.) A **finite field** $\mathbb{F}_q$ is a field with finitely many elements.
3.) **Function fields** are extensions of the field $F = \mathbb{C}(t)$ of rational functions.

• Def. 4.2: Given a pair of fields $F \subseteq K$, we say K is a **field extension of $\boldsymbol{F}$** or an **extension field**. We indicate this relationship by $K \backslash F$. Some fields may be extensions by finite amounts of elements, while others may extend infinitely. In the finite case, we may also refer to the extension field as an **adjunction field**.

• Def. 4.3: $K \backslash F$. $\alpha \in K$ is **algebraic over $\boldsymbol{F}$** if it is the root of a **monic polynomial with coefficients in $\boldsymbol{F}$**, say $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ with $a_i \in F$ and $f(\alpha) = 0$. Otherwise, if no such poly exists, we call α **transcendental over $\boldsymbol{F}$**. (Take for example the transcendental element π over $\mathbb{Q}$.)

Adjunction rings for single elements look like this: $F[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n \mid a_i \in F\}$. The adjunction field is then just the **field of fractions** for $F[\alpha]$. That is, $F(\alpha)$ is the set of all linear combinations of elements in F with powers of α (both positive and negative).

• Def. 4.4: Given $F(\alpha)$, we call α the **primitive element** of the field.

• Def. 4.5: The **minimal polynomial for $\boldsymbol{\alpha}$** is the lowest degree monic poly with the above properties. The **degree of $\boldsymbol{\alpha}$** is the degree of its minimal polynomial.

• Def. 4.6: When we regard $K \backslash F$ as a vector space, the **degree of $\boldsymbol{K \backslash F}$** is denoted by $[K : F]$. A **quadratic field** has $[K : F] = 2$, a cubic field $= 3$, etc.

• Def. 4.7: A set of elements to be adjoined to a field are called **algebraically dependent** if there exists a polynomial representation of any one in terms of the others. That same set, if independent becomes a basis for the corresponding vector field. If the basis consists of all transcendental elements and they are all algebraically independent, the basis is called **purely transcendental**.

• Def. 4.8 A poly $f \in F[x]$ **splits completely in a field** K if it factors into linear factors in K, that is in terms of the form $(x - \alpha)$ etc. In this case, K is called a **splitting field** for f. The minimal extension field for which this happens is the **adjunction field** $F(\alpha_1, ..., \alpha_n)[x]$, where α_i's are the roots of f.

Take for example $f(x) = x^2 + 1 = (x + i)(x - i) \in \mathbb{R}[i][x] \cong \mathbb{C}[x]$.

• Def. 4.9: A field is **algebraically closed** if every poly of positive degree with coefficients in F has a root in F. Ex: $\mathbb{C}$. In other words, the splitting field for all elements in $F[x]$ is $F[x]$.

5. Groups, Rings, and Fields in Galois Theory (See: Results)

- Def. 5.1: We define the **univariate polynomial ring** $R[x]$ as the adjunction ring with formal powers of x and coefficients in R. The **multivariate polynomial ring** is similarly defined as $R[x_1, ..., x_n]$ for all mixed products of x_i's and coefficients in R. The corresponding **fraction fields** can be thought of as the sets of rational functions in x_i.

- Def. 5.2: We define the **formal (univariate) power series ring** as $R[[x]] = \{\sum_{i=1}^{\infty} c_i x^i \mid c_i \in R\}$.

- Def. 5.3: Let K and K' be extensions of the same field F. An isomorphism $\varphi : K \to K'$ such that $\varphi|_F = Id_F$ is called an ***F*-isomorphism** or an **isomorphism of field extensions**. If $\exists$ an F-isomorphism between K and K', we say the two are ***F*-isomorphic**.

- Def. 5.4: A permutation σ operates on polys by permuting the variables. In this way, σ also serves as an **automorphism** on $R[u_1, ..., u_n] \equiv R[u]$. In particular, since it restricts to the identity on R we call it an ***R*-automorphism**. We define this for any ring R. Especially when $R = F$ a field.

- Def. 5.5: A poly is **symmetric** if it is invariant under all such R-automorphisms.

- Def. 5.6: The F-automorphisms of a finite extension K form a group called the **Galois group of *K***.
  $\boldsymbol{Gal(K \backslash F) = \{Aut(F(u_1, ..., u_n)), \circ, Id_F\}}$.
A finite extension $K \backslash F$ is a **Galois extension** if the order of its Galois group $|G(K \backslash F)| = [K : F]$.

- Def. 5.7: Let H be a group of automorphisms of a field K. The **fixed field of *H***, denoted K^H, is the set of elements of K that are fixed by every group element.
  $\boldsymbol{K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha, \forall \alpha \in H\}}$. $\quad$ **$K^H \leq K$ and $H \leq G(K \backslash K^H)$.

- Def. 5.8: If K is an extension field of F, an **intermediate field** L is a field such that $F \subseteq L \subseteq K$. Of course we include the term *proper* if it is neither F or K.

We have the following correspondances:

$$\begin{tikzcd}
K \arrow[r, dash] \arrow[d, dash] & 1 \arrow[d, dash] \\
K^H \arrow[r, dash] \arrow[d, dash] & H \arrow[d, dash] \\
F \arrow[r, dash] & G
\end{tikzcd}$$

We can see now that the pair $\{K/F, Gal(K/F)\}$ together with the above correspondence between substructures forms a *Galois connection* (as in I.4.5).

- Def. 5.9: Let F be a subfield of $\mathbb{C}$. TFAE: and α is called **solvable** over F if it satisfies either:
  $\exists$ a chain of subfields $F = F_0 \subseteq F_1 \subseteq ... \subseteq F_r = K$ of $\mathbb{C}$ such that $\alpha \in K$ and
  1.) for $j = 1, ..., r$, $F_j = F_{j-1}(\beta_j^{1/n_j})$, $\beta_j \in F_{j-1}$ $\quad$ or
  2.) for $j = 1, ..., r$, F_{j+1} is a Galois extension of F_j of prime degree.

- Def. 5.10: A finite group G is **solvable** if $\exists$ a sequence $1 \lhd G_0 \lhd G_1 \lhd ... \lhd G_r = G$ such that $G_i \backslash G_{i-1}$ is abelian (or cyclic or prime order).

6. Vector Spaces, Operators, and Forms (See: Results)

• Def. 6.1: Recall that a **vector space** is an abelian group $\mathbf{V} = \{V, +\}$ equipped with a distributive field action (scalar multiplication). As a general algebriac structure, a vector space is listed as: $\boldsymbol{\mathfrak{V} = \{F \cup V, \{+, *, 0, 1\}, (2, 2, 1, 1)\}}$ together with the specifics of the operations such as compatibility. Or just a set of vectors with scalar multiplication and some axioms defining compatibility (first one is usually the best).

• Def. 6.2: A **linear map** or **linear transformation** $T : V \to W$ is a vector space homomorphism. A **linear operator** however, is a vector space endomorphism $T : V \to V$. When we say linear we mean symbolically $T(\lambda v + w) = \lambda T(v) + T(w)$. Scalars may be applied to the second vector but it is redundant in the definition. To every linear transformation (linear map for short), we have an **associated matrix** given with respect to two bases (one for **domain** (β) and **codomain** (γ)). We write: $[T]_\beta^\gamma = \Bigg[[T(\beta_1)]_\gamma \;\cdots\; [T(\beta_n)]_\gamma \Bigg] = A \in GL_n(V/F)$. The latter notation denotes the coordinate vectors for the images of the basis vectors from the domain.

If T is complex, the **adjoint operator** $T^* : W \to V$ is defined via the **adjoint matrix** $A^* = \overline{A^t}$.

• Def. 6.3: Given a vector space V/F. We define a **bilinear form** to be a map $B : V \times V \to F$ such that it is linear in both vector variables. That is:

$$B(\lambda u + v, w) = \lambda B(u, w) + B(v, w) \text{ and } B(u, \lambda v + w) = B(u, w) + \lambda B(v, w).$$

A **Euclidean form** is a real bilinear form (i.e. $B : V \times V \to \mathbb{R}$) that is also *symmetric* and *positive definite* (to be defined). A **Euclidean Space** is a real vector space equipped with a Euclidean form: $\{V/\mathbb{R}, B_{Eucl}\}$.

A **Hermitian form** is a complex bilinear form ($B : V \times V \to \mathbb{C}$) that is **conjugate linear** in the first variable $\big(B(\lambda u + v, w) = \overline{\lambda} B(u, w) + B(v, w)\big)$, linear in the second, and *Hermitian symmetric* (to be defined). A **Hermitian Space** is a complex vector space equipped with a *positive definite* Hermitian form: $\{V/\mathbb{C}, B_{Herm}\}$.

We have the **associated matrix to a bilinear form** given by the array enumerating pairs of basis vectors from V. That is, $A = (a_{ij})_{1 \le i,j \le n}$, where $a_{ij} = B(\beta_1, \beta_2)$. We define the bilinear form by its action on vectors using the matrix: $B(v, w) = X^t A Y$, where $X = [v]_\beta$ and $Y = [w]_\beta$.

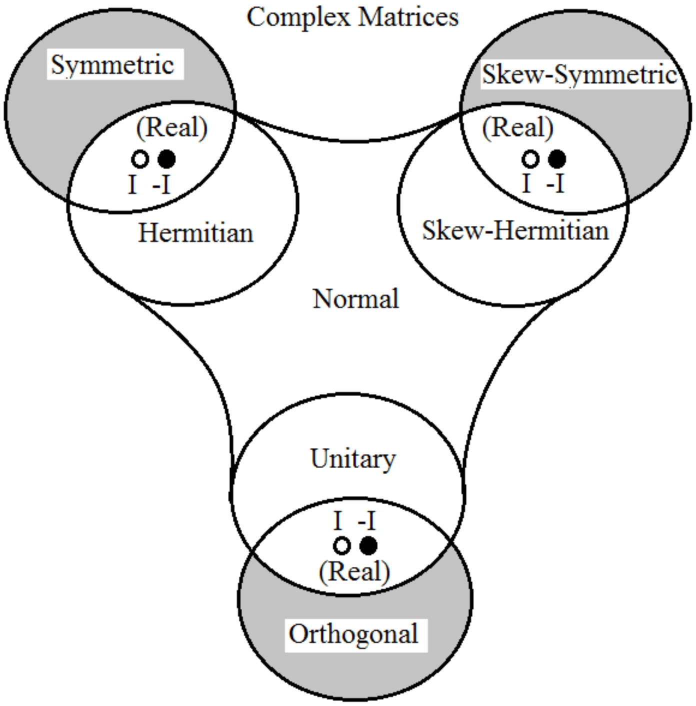
• Def. 6.4: A bilinear form is said to be **positive definite** if $\forall v,\ B(v, v) > 0$. Similarly, **negative definite** if $\forall v, B(v, v) < 0$. It is **positive or negative semi-definite** if $\forall v, B(v, v) \ge 0, \le 0$ respectively. And we say B is indefinite if it is neither positive or negative definite.

• Def. 6.5: A bilinear form is **symmetric** if $\forall v, w, B(v, w) = B(w, v)$,
skew-symmetric if $B(v, w) = -B(w, v)$,
Hermitian symmetric if $\overline{B(v, w)} = B(w, v)$, and
Hermitian skew-symmetric if $\overline{B(v, w)} = -B(w, v)$.

• Def. 6.6: A bilinear form is **degenerate** if its associated matrix has nontrivial **nullspace** (kernel). It is **nondegenerate** otherwise. A **null vector** is one such that $B(v, v) = 0$.

• Def. 6.7: Given a Euclidean form or Hermitian form, two vectors are **orthogonal** if $B(v, w) = 0$. Given such a form, we may decompose a vector space into a direct sum of the span of a basis and the span of its **orthogonal complement**. This is called the **orthogonal direct sum** and denoted: $V = S \oplus S^{\perp}$. Recall that the direct sum is defined as: $V \oplus W = \{v + w \mid v \in V \text{ and } w \in W, \text{ but } V \cap W = \{0\}\}$. *In the finite case, direct sum is equivalent to direct product.*

⋆ Def. 6.8: The following are properties of matrices and their corresponding bilinear forms. A matrix is said to be **normal** if it commutes with its adjoint: $AA^* = A^*A$, it is said to be **Hermitian** if $A^* = A$, **symmetric** if $A^t = A$ (for skew's add a minus sign), **unitary** if $A^*A = I$, and **orthogonal** if $A^tA = I$.



• Def. 6.9: **Conjugate matrices** are of the form BAB^{-1} and yield the same information since $det(BAB^{-1}) = det(A)$. For the special case of bilinear forms, conjugate matrices are of the form B^tAB (that is, $B^tB = I$). *Conjugating in either case assumes a basis is already in place that represents the operator or form as a matrix "A", if we forget about the original basis, representing the operator or form in the new basis needs no conjugation. One uses the new basis as the matrix "B" to conjugate. We get the same results.*

• Def. 6.10: Given a linear operator $T : V \to V$, a subspace $S \subseteq V$ is said to be ***T*-invariant** if $T(S) \subseteq S$. We may take advantage of T-invariant subspaces by using their bases to *conjugate* and **diagonalize** or quasi-diagonalize the operator's matrix.

A matrix is **diagonal** if its only nonzero elements are on the diagonal, it is "quasi" if it is diagonal except for elements on either the super- or sub-diagonal line. A matrix is *diagonalizable* if it is **similar** to a diagonal matrix (think conjugacy class).

A special case of T-invariance is given by **eigenvectors** $T(x) = \lambda x$, with corresponding **eigenvalue** λ. Clearly $S = \{\mu x \mid \mu \in F\}$ is invariant. So in terms of diagonalization, if we take $V = S \oplus W$, and a basis $\beta = \{x, w_1, ...w_{n-1}\}$, the matrix of T is of the form: $[T]_\beta^\beta = \begin{pmatrix}\lambda & 0 \\ 0 & A\end{pmatrix}$, for A and 0 blocks. This diagonalizes the matrix if all λ are distinct. In this event too $S = E_\lambda$ (see below).

• Def. 6.11: Given the matrix of an operator, the **characteristic equation** is given by $\boldsymbol{det(A-\lambda I)=0}$. The **minimal polynomial** for a matrix is the one of lowest degree such that $\boldsymbol{p(A)=0}$. Note that these may be different.

The nontrivial solutions to the characteristic equation are the eigenvalues and the corresponding eigenvectors are found by solving the system $(A-\lambda I)v=0$. The nullspace of the $A-\lambda I$ is the **eigenspace**. For repeated eigenvalues, we have **generalized eigenspaces** found by solving for the nullspaces of $(A-\lambda I)^k$ for progressively larger increments of k. We denote these by $\boldsymbol{E^k_\lambda}$. A **generalized eigenvector** is such that for some $k>0$, $(A-\lambda I)^k x=0$. The smallest such k is called the **exponent** of x.

The **algebraic multiplicity** of an eigenvalue is the power of the linear term it corresponds to in the characteristic equation (such as $(x-\lambda)^m$). The **geometric multiplicity** is the dimension of its first eigenspace $E^1_\lambda \equiv E_\lambda$.

We may represent any matrix in **Jordan canonical form**, that is in terms of ordered **Jordan blocks** corresponding to each invariant subspace. They are of the form: (λ), $\begin{pmatrix}\lambda & 0\\ 1 & \lambda\end{pmatrix}$, $\begin{pmatrix}\lambda & 0 & 0\\ 1 & \lambda & 0\\ 0 & 1 & \lambda\end{pmatrix}$, etc.

Generalized Eigen-Problem Diagonalization Outline:

We can decompose $V=S_1\oplus ... \oplus S_n$, where n is the number of distinct eigenvalues which may or may not equal $dim(V)$ and S_i is the corresponding total eigenspace for each value. Choosing an arbitrary basis for each one of the S_i's yields a

block diagonal form: $$[T]_\beta = \begin{pmatrix} A & & & \\ & B & & \\ & & \ddots & \\ & & & C \end{pmatrix}.$$

Consider a generalized e-vector of exponent k and the basis:
$\boldsymbol{\beta_\lambda = \{x, (T-\lambda I)x, ..., (T-\lambda I)^{k-1}x\}}$.

Since $(T-\lambda I)^{i+1} = (T-\lambda I)*(T-\lambda I)^i = T(T-\lambda I)^i - \lambda I(T-\lambda I)^i$
We have: $T(T-\lambda I)^i = (T-\lambda I)^{i+1} + \lambda(T-\lambda I)^i$.

$$\begin{aligned}\implies T\beta_\lambda &= \{T(T-\lambda I)^0x, T(T-\lambda I)^1x, ..., T(T-\lambda I)^{k-1}x\}\\ &= \{(T-\lambda I)x+\lambda x, (T-\lambda I)^2x+\lambda(T-\lambda I)x, ..., \lambda(T-\lambda I)^{k-1}x\},\end{aligned}$$
which in terms of the basis β_λ is just:

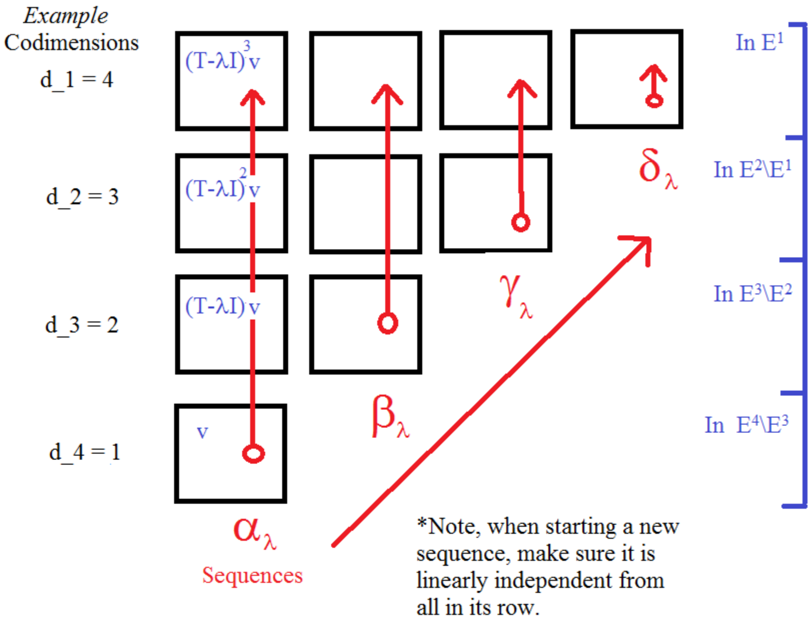
$$[T\beta_\lambda]_{\beta_\lambda} = \left\{\begin{pmatrix}\lambda\\1\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\\lambda\\1\\\vdots\\0\end{pmatrix}, ..., \begin{pmatrix}0\\\vdots\\0\\0\\\lambda\end{pmatrix}\right\}.$$

Now, consider the fact that we have: $E^1_\lambda \subseteq E^2_\lambda \subseteq ... \subseteq E^k_\lambda$. We may construct a basis concentrically as follows. Let $d_1 = dim(E^1)$,

$$\begin{aligned} d_2 &= dim(E^2) - dim(E^1),\\ d_3 &= dim(E^3) - dim(E^2),\\ &\vdots\\ d_k &= dim(E^k) - dim(E^{k-1}).\end{aligned}$$

Then for each i, we need d_i amount of elements from the complement $E^i \backslash E^{i-1}$. Appending the results will obtain a basis. One can see that the basis β_λ contains a sequence of vectors that descends the chain of inclusions from $x \in E^k$ to $(T - \lambda I)^{k-1}x \in E^1$. To keep the same sequence formatting, we wish to start with another linearly independent vector at the top of the list (either in E^k or the next highest) and then proceed down the chain. This process will terminate and the results will complete the corresponding Jordan form.

To reiterate: 1.) Compute the dimensions of all the generalized eigenspaces for a given eigenvalue, 2.) Find the list of codimensions d_i, 3.) Start at the top (E^k) and find linearly independent generators for sequences $\alpha_\lambda, \beta_\lambda, \gamma_\lambda$, etc. until the process terminates. The sequences constitute the bases for each block and appending all such sequences for all such eigenvalues gives the conjugation matrix that yields the Jordan normal form via $J = X^{-1}AX$. As well, it gives the new basis for which $J = [T]^\beta_\beta$.



*Note, when starting a new sequence, make sure it is linearly independent from all in its row.

Fig: Finding Basis Sequences for Jordan Blocks

⋆ Note that we may skip writing down the conjugation matrix or basis if we construct the diagram and observe: d_1 is the number of Jordan blocks, and the size of each block is the height of each column. From this information, we can just place the eigenvalue on the diagonal the algebraic multiplicity number of times and then place 1's below according to the block sizes □.

- Def. 6.12: In relation to solving systems of D.E.'s, a useful tool is the **matrix exponential**, which is defined as a **matrix series**: $e^A = \sum_{i=1}^{\infty} \frac{1}{k!} A^k$. We won't digress further here other than saying it is used in conjunction with diagonalization.

7. Modules (See: Results)

• Def. 7.1: Recall that a **module over a ring** is a *vector space over a ring* instead of a field. Strictly speaking, a module is an abelian group in $\{M, +\}$ together with a (left or right) distributive R-action. The sidedness stems from the ring's commutivity (or lack thereof). If R is commutative, the two are the same. From a structural standpoint, a module $\mathfrak{M} = \big\{R \cup V, \{+, *, 0\}, (2,2,1)\big\}$ together with compatibility conditions and most of the time unit 1.

Note that letting R act on itself defines an R-module since $\{R, +\}$ is an abelian group and any left or right action of R on itself is distributive by definition (see Definition I.1.3.). Hence *all rings can be considered modules*. Same goes for product rings: $R^n = \underbrace{R \times ... \times R}_{n-times}$. However, not all modules are rings.

• Def. 7.2: A **Free module** $\mathfrak{M}$ is characterized by the fact that there exists an R-isomorphism: $\varphi : R^n \to \mathfrak{M}$. The terminology stems from the fact that there are no relations defined on the elements in the domain (hence in the image by isomorphism).

• Def. 7.3: Given a **free module homomorphism** $T : \mathfrak{M} \to \mathfrak{N}$ we have: $A : R^n \to R^m$. Where $A = \varphi_2 \circ T \circ \varphi_1^{-1}$ since $\varphi_1 : R^n \to \mathfrak{M}$ and $\varphi_2 : R^m \to \mathfrak{N}$. A is a familiar R-matrix associated with T.

Since $A(R^n) \equiv AR^n \subseteq R^m$, we may find the quotient module $R^m \backslash AR^n$ (a.k.a. *cokernel* of A).

• Def. 7.4: **Non-free modules** are characterized by existence of an isomorphism $\varphi : R^m \backslash AR^n \to \mathfrak{M}$. Here the elements of the domain *are* constrained by a relation ($(y, 0) \in \mathscr{R}$ iff $\exists x$, such that $y = Ax$).

In this definition, A, n, and m are variables given by an arbitrary free module hom. If we freeze m and vary A and n, we may cover the set of all congruence relations defined on R^m. An arbitrary R-matrix $A : R^n \to R^m$ has m rows and n columns and may have rank anywhere between $0 \leq r \leq min\{m, n\}$. Particularly, the image may constitute any subspace of R^m. "Subspace" defines a congruence relation: two vectors are in the same subspace if they are generated by linear combinations of the same basis elements. Linear subspaces are the only possible congruences to define on a finite free module. Thus, this characterization of non-free modules as the isomorphism class of such quotients is admissible.

However, one may take products of quotient structures such as this as well as direct sums $\bigoplus_{i \in I} R^{m_i} \backslash A_i R^{n_i}$ (off to infinity especially), so this terminology is not all encompassing.

• Def. 7.5: In the above simple case, the matrix A is called the module's **presentation matrix**. The module AR^n is called the **module of relations**. It is generated by a basis for R^n and the matrix elements via: $\boldsymbol{y_j = a_{ij} x_j}$. We call these the **"relations"**. Lastly, one may speak of **generators** of the module. These would be elements of R^m for which the R-linear closure is $\mathfrak{M}$.

Notes:

1.) To find the presentation matrix, simply take the set of relations $b_{ij} v_j = 0$ where v_j are the generators, and extract the matrix $B = b_{ij}$. The presentation matrix is the matrix $A = B^t$. One can reduce it from there using a theorem in (Part III) below (Module Theory). Reasoning behind the transpose can be looked up in Artin's book or online.

2.) Modules are determined up to isomorphism class (similarity or conjugacy class) of matrix. Thus many matrices may describe the same module, but the module they describe is unique in the sense that one matrix doesn't describe two modules.

Some Related Notions for Modules

• Def. 7.6: A **Noetherian module** is one such that every ascending chain of submodules stabilizes. Similarly for **Artinian modules** with "descending chains of submodules".

• Def. 7.7: Recall at the end of Section I.2, we defined **decomposable** and **completely reducible** structures. This covers the cases for modules as well. **Simplicity** however is given by the absence of proper ideals (analogous to the case of no proper normal subgroups for simple groups).

• Def. 7.8: Observe the following diagrams:

$$\begin{tikzcd}
& F \arrow[dl, dashed, "!g"'] \arrow[d, "f"] \\
A \arrow[r, two heads, "\varphi"'] & B
\end{tikzcd}$$

Free

$$\begin{tikzcd}
& P \arrow[dl, dashed, "g"'] \arrow[d, "f"] \\
A \arrow[r, two heads, "\varphi"'] & B
\end{tikzcd}$$

Projective

$$\begin{tikzcd}
& I \\
A \arrow[ur, dashed, "g"] & B \arrow[l, hook', "\varphi"] \arrow[u, "f"']
\end{tikzcd}$$

Injective

A module is **free** if it satisfies the universal property given by the diagram, a module is **projective** if there exists such a g making the diagram commute. Likewise for **injective** modules. Except in the latter two, these aren't universal properties. Projective and Injective are dual notions, with free being an instance of projective.

• Def. 7.9: A **flat module** over a ring R is an R-module M such that taking the tensor product over R with M preserves exact sequences.

• Def. 7.10: A **torsion-free module** is a module over a ring such that 0 is the only element annihilated by a regular element (non zero-divisor) of the ring.

It turns out that we have the following relationship:

Free ⇒ **Projective** ⇒ **Flat** ⇒ **Torsion-Free**

8. Group Rings and Representation Theory (See: Results)

There is a correspondence between FG-modules and vector spaces with representations afforded to them, so we will start by defining both of those terms. Then the invariant information about representations is contained in their characters, so that is next.

• Def. 8.1: Recall from Section I.1, that a **group ring** or **RG-module** is the set of all formal linear combinations $\{\sum_{g\in G} \alpha_g g \mid \alpha_g \in R\}$ with contrived operations $\{+, *, \langle,\rangle\}$ defined to make it work as a traditional algebra. By FG-module here, we simply mean R is a field F.

• Def. 8.2: As in Section I.4, a **linear group representation** is just a homomorphism $\rho : G \to GL(V)$. It has an associated **matrix representation** given by $\psi : G \to GL_n(F)$, whenever we decide to specify a basis. The **degree** of a representation is the dimension of the vector space it maps into. A representation is called **faithful** if it is injective.

• Def. 8.3: A subspace W of an FG-module V is called **G-invariant** or **G-stable** if $\forall g \in G$, $[\varphi(g)](W) \subseteq W$, for some **afforded** representation φ given in the first correspondence:

Correspondences: (See III.1.6)

$$\left\{\text{V an FG-module}\right\} \longleftrightarrow \left\{\begin{matrix}\text{V an F-v.s. with a fin. dim.} \\ \text{linear rep. } \varphi : \text{G} \longrightarrow \text{GL(V)}\end{matrix}\right\}$$

$$\left\{\text{FG-submodules}\right\} \longleftrightarrow \left\{\text{G-invariant subspaces}\right\}$$

• Def. 8.3: Two linear representations $\varphi : G \to GL(V/F)$ and $\psi : G \to GL(W/F)$ are **equivalent** if the FG-modules V and W affording them are isomorphic (which requires a bijective linear map, compatible with the group action T). From this we get the relation: φ is equivalent to ψ iff there exists an isomorphism of FG-modules such that: $\boldsymbol{\varphi = T^{-1} \circ \psi \circ T}$.

Notes: Once a basis is chosen, this says the matrix representations differ by a change of basis. Since we are talking about change of basis applied to every representation of group elements in G, this is known as a **simultaneous change of basis**. In this event, φ and ψ are also said to be **intertwined**.

• Def. 8.4: The terms of **simplicity, reducibility, and decomposability** all carry over to representations from the modules that afford them. That is, a representation φ is irreducible iff the FG-module V affording it is irreducible.

• Def. 8.5: The **character** of a linear representation is a group homomorphism given by the traces of all the corresponding matrices. We denote this $\chi_\rho : G \to F$ such that $\chi_\rho(g) = tr(\rho(g))$. Depending on the ability to do so, we write out all the images into a vector known as the **character vector**.

A result about characters is that they are constant on conjugacy classes and so are said to be **class functions**, which in the full generality form a normed vector space (in which we find the **norm** and **inner products** between character vectors).

• Def. 8.6: **Character tables** are made listing components of irreducible characters.

PART III

Important Theorems

I have named all the Theorems below, these are not their standard names unless indicated in blue. Also, unless otherwise stated, all maps refer to morphisms.

Group Theory (See: Definitions)

1 • Lagrange's Theorem: $H \leq G \implies |G| = |H| \cdot |G\backslash H|$. (Subgroup orders divide group order.)

2 • Sylow Theorem 1: $|G| = n = p^k \cdot m \implies \forall i \in \{1, ...k\} \exists H \leq G$ and $|H| = p^i$.

3 • Sylow Thm 2: $|G| = p^k m$, then:
1.) $(H \leq G$ and $|H| = p^i) \implies \exists x, H = C(x)$ and
2.) Sylow p-subgroups are all conjugate to eachother.

4 • Sylow Thm 3: $|G| = p^k m$. $S =$ number of sylow p-subgroups, then $S|m$ and $S \equiv 1(mod - p)$.

5 • First Isomorphism Thm: $\varphi : G \to G'$ (surjective) $\implies \tilde{\varphi} : G\backslash ker(\varphi) \to G'$ is an iso.

6 • Third Iso Thm: $N \lhd K \lhd G$, then $G/H \cong (G/K)/(K/H)$ with $K/H \lhd G/K$.

7 • Correspondence Theorem (4th Iso): If $N \lhd G$, $\mathscr{X}$ is the set of all subgroups containing N and $\mathscr{Y}$ is the set of subgroups of the quotient $G\backslash N$, then $\exists$ a bijective map $\varphi : \mathscr{X} \to \mathscr{Y}$; $\varphi(A) = A\backslash N$.

8 • Counting Formulas: Given an action of G onto itself, we have $\boldsymbol{|G| = |G_x| \cdot |O_x|}$. (Stabilizer/Orbit)
Hence for the left actions on an element or subgroup or conjugation on an element or subgroup:
$\theta_L(g, x) = g * x$, $\tilde{\theta}_L(g, X) = gX$, $\theta_C(g, x) = gxg^{-1}$, and $\tilde{\theta}_C(g, X) = gXg^{-1}$:

1.) $|G| = | <1> | \cdot |G|$ (Uninteresting)
2.) $|G| = |X| \cdot |G\backslash X|$ (Repeat)
3.) $|G| = |Z(x)| \cdot |C(x)|$ (Centralizer/Conjugacy Class)
4.) $|G| = |N(X)| \cdot |C(X)|$ (Normalizer/Conjugacy Class)

9 • Another Counting Formula Thm: Given $\varphi : G \to G'$, $|G| = |ker\varphi| \cdot |Im\varphi|$.

10 • Class Equation: $|G| = \sum\limits_{x \in G} |C(x)| = |C_1| + ... + |C_k|$ for conjugacy classes in G.

11 • Cayley's Theorem: Every group is iso to a subgroup of a permutation group. That is,
$\forall G\ \exists H, \quad G \cong H$ and $H \leq S_n$ for some $n \in \mathbb{N}$.

12 • Structure Theorem for Finite Abelian Groups:
Every finitely generated abelian group $V \cong C_{d_1} \oplus ... \oplus C_{d_k} \oplus L$, where C_{d_i} are cyclic subgroups of order d_i, L is a free abelian group of order r distinct from the others, and $\forall i(d_i > 1$ and $d_i | d_{i+1})$.

13 • Coprimal Decomposition Thm:
G cyclic and $|G| = r \cdot s$. Then there exists cyclic groups A and B of respective orders r and s such that $G \cong A \oplus B \leftrightarrow gcd(r, s) = 1$.

Note that this allows us to further split up the structure theorem into prime order decompositions.

14 • Equivalent Conditions For Normality:
1.) $N \lhd G$
2.) $N_G(N) = G$
3.) $\forall g \in G, gNg^{-1} \subseteq N$ (or $Ng = gN, \forall g$)
4.) $\{gN\}$ forms a group
5.) $N = \bigcup_i \kappa_i$ (union of conjugacy classes)
6.) $N = ker\varphi$, φ is a homomorphism
7.) N is a Sylow p-subgroup with $n_p = 1$.

15 • Smallest Prime Dividing Order Implies Normality of Certain Subgroups:
If $|G| < \infty$ and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.

16 • The Flower Inequality: (Very useful in arguing for normality of a sylow subgroup)
Suppose $|G| = p^\alpha q^\beta \cdot ... \cdot r^\gamma$, then $|G| \geq n_p(p^\alpha - 1) + n_q(q^\beta - 1) + ... + n_r(r^\gamma - 1) + 1$

17 • Permutation Representation on Subgroups:
Suppose $H \lhd N_G(H)$ for any $H \leq G$. Then: $N_G(H)/C_G(H) \cong K \leq Aut(H)$.

18 • Recognition Theorem For Direct Products of Groups:
Suppose $H, K \leq G$ both of which are normal and disjoint except for 1. Then $HK \cong H \times K$.

19 • Recognition Theorem For Semi-Direct Products of Groups: Suppose $H, K \leq G$, disjoint except for 1, but only one of H or K is normal in G, then $HK \cong H \rtimes K$.

Ring Theory (See: Definitions)

1 • Mapping Property of Quotient Rings:
Let $\varphi : R \to R'$, $K = ker\varphi$, $I \leq R$, $\pi : R \to R\backslash I$. Then:
1.) $I \subseteq K$, $\exists! \tilde{\varphi} : R\backslash I \to R'$ such that $\tilde{\varphi} \circ \pi = \varphi$.
2.) φ surjective, $I = K \implies \tilde{\varphi}$ iso. (First Iso Thm).

2 • Correspondence Thm: $\varphi : R \to R'$ surjective ring hom, $K = ker\varphi$. Then $\{$ideals in R containing $K\} \leftrightarrow \{$ideals of $R'\}$.

3 • Ideal Type Theorem: An ideal $I \leq R$ is:
1.) maximal iff $R\backslash I$ is a field.
2.) It is prime iff $R\backslash I$ is an integral domain.

4 • Ideals and Fields: The only ideals in a field are (0) and (1).
If a ring has only two ideals, it is a field.

5 • Prime Ideal Thm: Let P be a prime ideal, then:
1.) $R\backslash P$ is an integral domain,
2.) $P \neq R$ and $a, b \in R$ such that $ab \in P$, then either $a \in P$ or $b \in P$.
3.) $P \neq R$ and $A, B \leq R$ (ideals), $AB \subseteq P$, then A or $B \subseteq P$.
Cor: A maximal ideal of R is prime. (α) is a prime ideal iff α is a prime element.

6 • Chinese Remainder Theorem: Let $I_1, ..., I_k$ be the two-sided ideals of a ring R that are pairwise coprime and $I = \bigcap_{i=1}^{k} I_i$. Then we have the isomorphism:
$R\backslash I = R\backslash I_1 \times ... \times R\backslash I_k$; $x(mod\ I) \mapsto (x(mod\ I_1), ..., x(mod\ I_k))$.

7 • Irreducibility vs. Primality Theorem:
1.) In a PID, a,b relatively prime implies there exists r,s such that $ra + sb = 1$.
2.) In a PID, an element of R is irreducible iff it is a prime element.
3.) In a PID, maximal ideals of R are the principle ideals generated by irreducible elements.
4.) In an ID, prime elements *are* irreducible elements.

8 • Chains and Factoring in I.D.'s: Factoring terminates iff all principle ideal inclusion chains are finite.

9 • Ideals of $\mathbb{Z}$: The integers form a PID. Maximal Ideals of $\mathbb{Z}$ are principle ideals generated by primes.

10 • Hilbert's Zero Places Theorem (Ideals of $\mathbb{C}[\boldsymbol{x_i}]$):
Maximal Ideals of $\mathbb{C}[x_1, ..., x_n]$ are in bijective correspondence with points of $\mathbb{C}^n$.

11 • Gauss' Lemma: Product of primitive polys is primitive.

12 • Eisenstein Criterion: Let $f(x) = a_n x^n + ... + a_0$ be an integer poly and let p be a prime integer such that:
1.) $p \nmid a_n$,
2.) $p | a_i$, $\forall i \in \{1, ..., n-1\}$, and
3.) $p^2 \nmid a_0$,
then f is irreducible in $\mathbb{Q}[x]$.

13 • Ideals of $F[[x]]$: (t^a) are maximal ideals in $F[[x]]$, a is the smallest degree of the nonzero terms.
(p, f) is a maximal ideal in $\mathbb{Z}[x]$, for p prime and f is primitive integer poly irreducible mod p.

Field/Galois Theory (See: Definitions)

1 • Main Theorem: There is a bijective correspondence between {subgroups of $G(K/F)$} and {intermediate fields of K/F} if K is a galois extension of F. Futhermore, $H \mapsto K^H$ and $L \mapsto G(K/L)$ are inverse functions.

2 • Computing the Galois Group: Let $K = F(\alpha_1, ...\alpha_n)$ be a splitting field for f over F. Suppose $g \in F[x]$ is irreducible over F and that $g|f$. Then any F-automorphism for K fixes g.

Cor: When computing the Galois group of f, it suffices to consider only automorphisms fixing irreducible polys that divide f.

⋆ Example: $f(x) = x^5 + x^3 - x^2 - 1 = (x - i)(x + i)(x - 1)(x + \frac{1}{2}(1 - \sqrt{3}))(x + \frac{1}{2}(1 + \sqrt{3}))$
Hence irreducible divisors over $\mathbb{Q}$ are $x^2 + 1$, $x - 1$, and $x^2 + x + 1$. Hence the only automorphisms are: $\sigma_1 : i \to -i$, $\sigma_2 : 1 \to 1$, and $\sigma_3 : \sqrt{3} \to -\sqrt{3}$. Labeling the roots in order of appearance then and rewriting the autos: $\sigma_1 = (12)$, $\sigma_2 = (3) = (1)$, and $\sigma_3 = (45)$. So that $G(K/F) = \langle (12), (45) \rangle \leq S_5$.

3 • Characteristic Properties of Galois Extensions: The following are equivalent:
1.) K/F is a galois extension,
2.) $K^G = F$, and
3.) K is a splitting field over F.

4 • Galois Subgroups Thm 1: K/F is galois, $H \leq G(K/F)$. Then K^H/F is galois iff $H \lhd G(K/F)$. If so, $G(K^H/F) \cong G(K/F)/H$ (the quotient of G over H).

5 • Galois Subgroups Thm 2 (a.k.a. Fixed Field Thm):
If H finite group of autos for K/F then $H = Gal(K/K^H)$ and $[K : K^H] = |H|$.

6 • Abstract Extensions Thm: Let F be a field, f irreducible in $F[x]$, then $K = F[x]\backslash(f)$ is an extension of F and $x(mod\ f)$ is a root of f in K.

7 • Finding the Min Poly for a Transcendental Element: Write out a few powers of α and look for a relation.

8 • Algebraic Extensions of Extensions Thm: Algebraic extensions of algebraic extensions are algebraic. That is, let $F \subseteq K \subseteq L$ and α algebraic over F and β algebraic over k, then β is algebraic over F.

9 • Algebraic Elements and Iso Extensions:
α, β algebraic over F implies $F(\alpha) \cong F(\beta)$ iff α, β have the same minimum poly over F.

10 • Algebraic Closures Thm: Every field has an algebraic closure. If a field has multiple, they are iso.
11 • Splitting Theorem: If K is a splitting field for f and an irreducible $g \in F[x]$ has one root in K, then g splits completely.

12 • Orbit of a Superelement and its Splitting Poly: $H \leq G(K/F)$, $|H| < \infty$. Let $\beta_1 \in K$, $\{\beta_i\}_{i=1}^n$ its H-orbit, then:
1.) Irreducible poly for β_1 over K^H is $g(x) = (x - \beta_1) \cdot ... \cdot (x - \beta_n)$ and
2.) β_1 is algebraic over K^H and $deg(\beta_1) = |H\text{-orbit}|$.

13 • Multiple Roots and Derivative: $f \in F[x]$, $\alpha \in K/F$, then α is a multiple root of f iff α is a root of both f and its derivative.
14 • Primitive Element Theorem: Every K/F finite with $char K = 0$ has a primitive element.

Vector Space/Operator/Form Theory (See: Definitions)

1 • Spectral Theorem for Normal Operators:
1.) Let T be a normal operator on Hermitian Space. Then $\exists$ an o.n. basis consisting of e-vectors of T.
2.) Let A be a normal matrix. There is a unitary matrix P such that P^*AP is diagonal.

2 • Cayley-Hamilton Theorem: Any matrix satisfies its own characteristic poly: $p_{char}(A) = 0$.

3 ⋆ Min Poly vs. Char Poly: If A has a degenerative eigenspace, then $p_{min}(x) \neq p_{char}(x)$, but $p_{min}(x)\big|p_{char}(x)$. Particularly, linear terms in $p_{min}(x)$ occur with multiplicity equal to the size of the largest Jordan block for each particular e-value.

4 • Commuting Matrices Preserve E-spaces: If $AB = BA$ and $Av = \lambda v$, then:
$A(Bv) = (AB)v = (BA)v = B(Av) = B(\lambda v) = \lambda(Bv)$. Furthermore, if both A and B are diagonalizable or quasi-diagonalizable, then they are so simultaneously, since the T invariant decomposition (w.r.t. A) is preserved by B, it can be further decomposed according to S-invariant subspaces (w.r.t. B), yielding an appended basis of simultaneous eigenvectors (and vice versa).

5 • Poly Expression for Commuting Matrices: If A diagonalizable and $AB = BA$, then $\exists n$ such that $B = a_nA^n + ... + a_1A + a_0$.

6 • Transitivity of the Commutator $[A, B]$: For any three matrices, it is not true in general that if $AB = BA$ and $AC = CA$ that $BC = CB$. If however, any one matrix is diagonalizable (i.e. $p_{char}(x) = p_{min}(x)$), then the transitivity holds.

Proof: Suppose A is diagonalizable and there exists two matrices B and C that commute with A. Then we can write $B = f(A) = a_nA^n + ... + a_0$ for some n. Then $BC = (a_nA^n + ... + a_0)C = C(a_nA^n + ... + a_0) = CB$, by associativity and linearity.■

7 • Eigenspaces and Adjoint Operators: λ eigen for $T \implies \bar{\lambda}$ eigen for T^*, moreover $v_\lambda = v_{\bar{\lambda}}$.

8 • Change of Bases for Bilinear Forms: If we change bases for a vector space, the associated matrix to a bilinear form changes as follows: Q^tAQ, for some invertible Q. (or Q^*AQ).
Cor1: Matrices that represent the same form are all ones in the orthogonal conjugacy class.
Cor2: A is symmetric and positive definite $\leftrightarrow$ A represents dot product $\leftrightarrow$ $A = P^tP$.

9 • Form Degeneracy and Invertability of Associated Matrices:
$<, >$ is nondegenerate iff $A \in GL_n(\mathbb{R}$ or $\mathbb{C})$.

10 • Symmetric Forms and Signature Diagonal Matrix Representations:
$<, >$ symmetric $\implies$ $\exists$ an othogonal basis for V. Moreover, $<, >$ Euclidean or Hermitian implies there exists a basis for which the associated matrix is **signature diagonal**. That is,
B^tAB or $B^*AB = diag\{I_p, -I_m, O_z\}$, where (p, m, z) is the number of pluses, minuses, and zeros in the signature.

11 • Decomposition of Vector Spaces by Forms: Let $<, >$ or $<, >_H$, $W \leq V$.
1.) $<, >$ nondegenerate on W iff $V = W \oplus W^\perp$.
2.) $<, >$ nondegenerate on V and $W \implies$ nondegenerate on $W^\perp$.

Module Theory (See: Definitions)

1 • Mapping Property: $f : V \to V'$ be a module hom whose kernel contains a submodule W. Then $\exists! \tilde{f} : V \backslash kerf \to V'$ such that $f = \tilde{f} \circ \pi$, where π is a surjective projection hom.

2 • First Isomorphism Thm: If f above is surjective and $W = kerf$ then $\tilde{f}$ is an isomorphism onto V'.

3 • Correspondence Thm: Let $f : V \to V'$ be a surjective module hom with $kerf = W$. Then there is a bijective correspondence between submodules of V containing W and submodules of V'. Two corresponding submodules have isomorphic quotients.

4 • Structure Theorem for F.G R-Modules over a P.I.D.:
If R is a P.I.D. and $\mathfrak{M}$ is finitely generated then $\exists (d_1), ..., (d_k) \leq R$ and an integer l such that
$\mathfrak{M} \cong R\backslash(d_1) \oplus ... \oplus R\backslash(d_k) \oplus R^l$. (Follows from Structure Theorem for Abelian Groups.)

5 • Diagonalization in Euclidean Domains: Let R be an E.D.. Then there exists products Q and P of elementary matrices such that an R-matrix A is diagonalizable of the form: $A' = Q^{-1}AP = diag(d_1, ..., d_k, 0, ..., 0)$ with $d_1 | d_2 | ... | d_k$ and all $d_i > 0$. Moreover, d_1 is the gcd of all elements in A and the product $(d_1 \cdot ... \cdot d_i)$, $i \leq k$ is the gcd of the determinants of all $(i \times i)$ minors of A.

6 • Condition for Free Submodules over E.D.:
Let R be E.D., $\mathfrak{M}$ an f.g. free R-module. Suppose N is a finitely generated submodule, then N is free.

7 • On Noetherian Modules:
1.) $\mathfrak{M}$ noetherian $\implies$ every submodule and quotient module are noetherian.
2.) $\mathfrak{M}$ an f.g. module over noetherian ring implies $\mathfrak{M}$ is noetherian.
3.) R noetherian implies $R[x]$ is noetherian implies $R[x_1, ..., x_n]$ is noetherian. (Hilbert Basis Theorem)

8 • Invertability of R-Matrices: Let $R \neq \{0\}$. A square R-matrix is invertible iff it has either a left or right inverse iff det$A$ is a unit of the ring. An invertible R-matrix is square.

9 ⋆ Simplifying Presentation Matrices: If we can reduce A by elementary row operations to the form:
$A' = \begin{pmatrix} 1 & \\ & B \end{pmatrix}$, then B also presents the module. Moreover if $A' = \begin{pmatrix} 0 & \\ \vdots & B \\ 0 & \end{pmatrix}$, then B presents the module.
This is because $v_i = 0$ is useless as a generator in the relation module and the other relations don't depend on it and in the second case, the column represents the trivial relation $0 = 0$ which is also useless. Other than that left or right multiplying by any invertible matrix yields a presentation matrix of the same module.

10 • Presentation and Generation Finiteness:
Finitely presented modules are finitely generated. But a finitely generated module is finitely presented only if it is noetherian.

11 • Application to Linear Operators: Given a finite dimensional vector space V/F with linear operator $T : V \to V$, V becomes an $F[t]$-module via the action $* : F[t] \times V \to V; \quad (f(t), v) \mapsto [f(T)](v)$. Conversely, given an $F[t]$-module, we may define a linear operator on the vector space via:
$T : V \to V; Tv = t \cdot v$.

We have the following line by line correspondence:

$F[t]$-module:	Linear Operator T:
○ Multiply by t	○ Operation of T
○ Free module of rank 1	○ Shift operator
○ Submodule	○ T-invariant subspace
○ Direct sum of submodules	○ Direct sum of T-invariant subspaces
○ Cyclic module generated by W	○ Subspace spanned by $\{w, T(w), T^2(w), ...\}$.

12 • Artin-Wedderburn Theorem (Classification of Semi-Simple Rings):
Let R be a nonzero ring with unit (not necessarily commutative). TFAE:
1.) Every R-module is projective
2.) Every R-module is injective
3.) Every R-module is completely reducible
4.) R considered as a left R-module is completely reducible as:

$R = L_1 \oplus ... \oplus L_n$ where $L_i = Re_i$ are simple modules formed by idempotents satisfying:

i.) $e_i e_j = 0 \ \forall i \neq j$ [Orthogonality]
ii.) $\sum e_i = 1$ [Partition of Unity-esque Property].

5.) As rings, $R \cong R_1 \times ... \times R_r$ (direct product) of matrix rings over division rings. $R = \Pi_{i=1}^{n} M_{n_i}(\Delta_i)$.
[R_i is a two sided ideal of R iso to the ring of all $n_i \times n_i$-matrices with entries in a division ring Δ_i which up to iso are completely determined by R.]

Representation Theory (See: Definitions)

1 • Main Theorem:
1.) The irreducible characters of group G are orthonormal.
2.) Isomorphism classes of irreducible representations correspond to conjugacy classes in the group.
3.) If $\rho_1, ..., \rho_r$ represent the isomorphism classes of irreducible representations of G and $\chi_1, ..., \chi_r$ their characters. The dimension d_i of ρ_i (or of χ_i) divides the order $|G|$ of the group, and $|G| = \sum d_i^2$.

2 • Corollaries of Main Theorem:
Let $\rho_1, ..., \rho_r$ represent iso classes with χ_i etc. Let ρ be any representation with χ.
1.) $\chi = n_1\chi_1 + ... + n_r\chi_r$.
2.) ρ is iso to $\bigoplus_{i=1}^{r} n_i\rho_i$.
3.) Two reps of a finite group are iso iff their characters are equal.

3 • Maschke's Theorem: Every representation of a finite group G on a nonzero, finite-dimensional complex vector space is a direct sum of irreducible representations.

4 • Unitary Rep. Decomposition: Every unitary representation $\rho : G \to GL(V)$ on a Hermitian space is an orthogonal sum of irreducible reps.

Particularly, if ρ is a unitary representation of G on a Hermitian space V, and if W is a G-invariant subspace. Then $W^{\perp}$ is also G-invariant. Moreover, ρ is the direct sum of its restrictions to the Hermitian spaces W and $W^{\perp}$. These restrictions are unitary representations as well.

5 • Reps. of Finite Groups: G a finite group and $\chi = tr(\rho(\cdot))$.
1.) $\chi(1)$ is the dimension of χ since $\chi(1) := tr(\rho(1)) = tr(I_n) = n$.
2.) The character is constant on conjugacy classes. $g' = hgh^{-1} \implies \chi(g') = \chi(g)$.
3.) $g^k = 1 \implies$ the roots of the characteristic poly of ρ_g are powers of the k^{th} root of unitary ζ_k.
If ρ has dimension d, then $\chi(g)$ is the sum of d such powers.
4.) Isomorphic representations of G have the same character.

6 • Reps. of Finite (Abelian) Groups: G a finite abelian group.
1.) Every irreducible character of G is one dimensional. The number of irr. characters equals $|G|$.
2.) Every matrix representation R of G is diagonalizable.

7 • Schur's Lemma:
1.) Let ρ and ρ' be irreducible representations of G on V, V' let $T : V' \to V$ be a G-invariant transformation. Either T is an isomorphism or $T = 0$.
2.) Let ρ be an irreducible representation of G on V and let $T : V \to V$ be a G-invariant linear operator. Then T is multiplication by a scalar.

8 • Representations, G-Invariance, and Forms: Let $\rho : G \to GL(V)$ be a rep of a finite group on a vector space V. Then there exists G-invariant, positive definite hermitian form on V. $< v, w >= \frac{1}{|G|} \sum\limits_{g} \{gv, gw\}$.

9 • Correspondence Theorem:

$$\left\{ \text{V an FG-module} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{V an F-v.s. with a fin. dim.} \\ \text{linear rep. } \varphi : G \longrightarrow GL(V) \end{matrix} \right\}$$

The correspondence is given by defining the representation in terms of the ring action and the ring action in terms of representation extended via linearity: $\boldsymbol{g * v :=: [\varphi(g)]v}$

Selected Examples

1 • Dihedral Group:
The dihedral group is the group of symmetries of a regular polygon (n-gon), which includes rotations and reflections (wiki). $D_n = \langle r, s \mid r^n = 1, s^2 = 1, \text{ and } srs = r^{-1} \rangle$

2 • Primitive Roots of Unity:
The roots of unity are complex nth roots of 1. Recall from complex analysis that this means: $G = \{\zeta_n^k \mid \zeta_n^k = e^{\frac{2\pi k}{n} i}, k = 0, ..., n-1\}$. It is easy to see that this forms an abelian group via the power addition law. The field extension $\mathbb{Q}[\zeta_n]$ is important in Galois theory.

3 • Symmetric Groups (Permutation Groups):
The symmetric groups $S_n = \big\{\sigma \mid \sigma \text{ is a permutation of the elements } \{1, ..., n\}\big\}$.

We have that $|S_n| = n!$ and any σ can be written in **cyclic notation**:
where $u \to v \to u, x \to y \to z \to x \equiv (xyz) \circ (uv)$

Example: $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ where each respective σ takes the set $\{1, 2, 3\}$ to $\left\{\begin{array}{l} \{1,2,3\} \\ \{2,1,3\} \\ \{3,2,1\} \\ \{1,3,2\} \\ \{2,3,1\} \\ \{3,1,2\} \end{array}\right.$

It should be noted that $(1) = (k)$ is the identity map, (mn) is a **2-cycle** and $(1...n)$ is an ***n*-cycle**. 2-cycles commute with everything. A two cycle and an n-cycle generate the entire group S_n. And each permutation has a **signature** "sgn σ"($= 1$ or -1) which refers to it being either an *even* or *odd* number of **transpositions**. The subgroup of all even permutations is called the **Alternating Group A_n**.

4 • Cyclic Groups:
These are groups generated by single elements, for example in $(\mathbb{Z}, *)$, we have $< 2 >= \{$ multiples of 2$\}$. The p**-Groups** or **Sylow groups** are prime ordered cyclic groups. The familiar $\mathbb{Z} \backslash n\mathbb{Z} \equiv \mathbb{Z}_n = \{[x]_{mod-n}\}$ are cyclic if n is prime.

5 • Gauss Integers
The Gauss Integers consist of the set $\mathbb{Z}[i]$. They form a Euclidean domain with respect to the complex norm and are considered a *quadratic number field.*

6 • Matrix Groups
The set of $n \times n$ matrices with elements in a field form a group under matrix multiplication. We denote this by the General Linear: $GL_n(F)$. There are many important subgroups of this group. To name a few: $O(n) = \{$orthogonal matrices$\}$, $SO(n) = \{$orthogonal matrices with unit determinant$\}$ (special orthogonal), $U(n) = \{$unitary matrices$\}$, $SU(n) = \{$special unitary$\}$, etc. There are many more.

⋆ ⋆ ⋆