GRADUATE ALGEBRA NOTES

IMC

Abstract. These are some of the notes I took during my graduate algebra courses. They basics for cover Category Theory, Groups, Rings, Fields, Modules, and Bilinear Forms. They emphasizing the definitions, big theorems, and exercises for each theory.

Contents

1. Category Theory

Categories.

Definition. A **category** $\mathcal{C}$ consists of:

- a class $\text{obj}(\mathcal{C})$ of **objects**;
- to each pair of objects A, B, a class $\hom(A, B)$ of ***morphisms***, denoted $f\colon A \to B$;
- to each triple of objects A, B, C, a function
$$\circ\colon \hom(B, C) \times \hom(A, B) \to \hom(A, C)$$
defined by $(g, f) \mapsto g \circ f$ called the ***composite*** of f and g;

all subject to the associativity and identity axioms:

- for all morphisms $f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$, we have $h \circ (g \circ f) = (h \circ g) \circ f$;
- for all objects B in $\text{obj}(\mathcal{C})$ there is a morphism $\mathbb{1}_B\colon B \to B$ such that for any $f\colon A \to B$ and $g\colon B \to C$ we have $\mathbb{1}_B \circ f = f$ and $g \circ \mathbb{1}_B = g$.

Definition. A morphism $f\colon A \to B$ is an **equivalence** if there is a morphism $g\colon B \to A$ such that $g \circ f = \mathbb{1}_A$ and $f \circ g = \mathbb{1}_B$. The objects A and B are **equivalent**.

Definition. An object A in a category $\mathcal{C}$ is **universally attracting** (resp. universally repelling) if for every object $B \in \text{obj}(\mathcal{C})$ there is a unique morphism $B \to A$ (resp. $A \to B$).

► ***Exercise.*** *State which type of morphisms are equivalences in each of the categories below.*

► ***Exercise.*** *Show universally attracting (resp. repelling) elements are unique up to equivalence.*

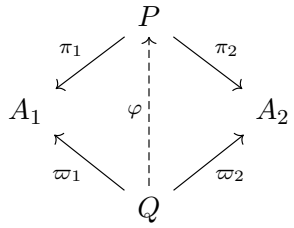
► ***Exercise.*** *Find the universally attracting and repelling objects in each of the categories below.*

Examples of Categories.

- The category Set whose objects are sets and whose morphisms are functions.
- The category Grp, Rng, or Mod_R whose objects are groups, rings, or R-modules and whose morphisms are group homomorphisms, ring homomorphisms, or R-linear maps.
- The category Top of topological spaces with continuous functions.
- The category hTop of topological spaces with continuous functions up to homotopy (note that the morphisms here are not functions, but equivalence classes of functions).

Products and Coproducts.

Definition. Let $\mathcal{C}$ be a category with $\{A_i\}_{i\in I}$ a family of objects. A **product** for the family is an object P together with a family of morphisms $\{\pi_i\colon P \to A_i\}_{i\in I}$ such that whenever an object Q has a family of morphisms $\{\varpi_i\colon Q \to A_i\}_{i\in I}$, there is a unique morphism $\varphi\colon Q \to P$ such that $\pi_i \circ \varphi = \pi_i$ for each $i \in I$.



Examples of (Co)Products.

- Let $\mathcal{C}$ be the category whose objects are the bounded subsets of the $\mathbb{R}$ and whose morphisms are inclusions $A \hookrightarrow B$ for bounded subsets A and B of $\mathbb{R}$ with $A \subseteq B$. The intersection of countably many objects in $\mathcal{C}$ forms a product in $\mathcal{C}$; there are no coproducts in $\mathcal{C}$.
- Let $\mathcal{D}$ be the category whose objects are positive integers and whose morphisms $p \to q$ exist iff p divides q. The greatest common divisor of countably many objects in $\mathcal{D}$ forms a product in $\mathcal{D}$; the least common multiple of countably many objects in $\mathcal{D}$ forms a coproduct.
- Let $\mathcal{E}$ be the category whose objects are finite groups. It is easy to see that the product of finitely many objects in $\mathcal{E}$ exists in $\mathcal{E}$, however, the coproducts are not necessarily contained in $\mathcal{E}$. If we restrict $\mathcal{E}$ to finite abelian groups, the coproduct exists, and is equal to the product.

► ***Exercise.*** *Show the (co)products in the above examples are indeed (co)products. If (co)products do not exist in the given category, then provide a counterexample.*

► ***Exercise.*** *Write out the definition for* ***coproducts*** *by switching all arrows in the definition for products. Draw a diagram similar to the one above.*

► ***Exercise.*** *Show that (co)products are unique up to equivalence.*

Functors.

Definition. A **covariant functor** T between categories $\mathcal{C}$ and $\mathcal{D}$ is a pair of functions assigning each object $A \in \mathrm{obj}(\mathcal{C})$ an object $T(A) \in \mathrm{obj}(\mathcal{D})$ and each morphism $f\colon A \to B$ in $\mathcal{C}$ a morphism $T(f)\colon T(A) \to T(B)$ in $\mathcal{D}$ such that

- $T(\mathbb{1}_A) = \mathbb{1}_{T(A)}$ for all objects A in $\mathcal{C}$;
- $T(g \circ f) = T(g) \circ T(f)$ for all morphisms f, g in $\mathcal{C}$ with $g \circ f$ defined.

By reversing all arrows, we obtain the definition for **contravariant functors**.

Definition. A functor $T\colon \mathcal{C} \to \mathcal{D}$ induces a function on the morphisms of $\mathcal{C}$ and $\mathcal{D}$, denoted

$$F_{XY}\colon \mathrm{Hom}(X, Y) \to \mathrm{Hom}(F(X), F(Y)).$$

If this map is injective, we say F is **faithful**. If it is surjective, we say F is **full**. A functor which is full and faithful is **fully faithful**.

Definition. A **concrete category** is a category with a faithful functor to the Set category.

Definition. Fix an object A in a category $\mathcal{C}$. Define $F_A\colon \mathcal{C} \to \mathrm{Set}$ by

$$F_A(C) = \hom(A, C), \quad F_A(f)\colon \hom(A, B) \to \hom(A, C)$$

where $F_A(g) = f \circ g$ for all $f\colon B \to C$. This is called the **covariant hom functor**.

Natural Transformations.

Definition. Given covariant functors F and G between categories $\mathcal{C}$ and $\mathcal{D}$, a **natural transformation** α from F to G is a family of morphisms $\{\alpha_C \colon F(C) \to G(C)\}_{C \in \mathrm{obj}(\mathcal{C})}$ in the category $\mathcal{D}$ making

$$\begin{array}{ccc} F(C) & \xrightarrow{\alpha_C} & G(C) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(D) & \xrightarrow{\alpha_D} & G(D) \end{array}$$

commute for each $f \in \hom(C, D)$. If each α_C is an equivalence, we say α is a **natural equivalence**.

Free Objects.

Definition. In a concrete category $\mathcal{C}$, an object $X \in \mathrm{obj}(\mathcal{C})$ is **free** if there is a subset $B \subset X$ such that any function from B to an object $Y \in \mathrm{obj}(\mathcal{C})$ extends uniquely to a morphism $X \to Y$.

$$\begin{array}{ccc} B & \hookrightarrow & X \\ & \searrow & \downarrow{\scriptstyle \exists!} \\ & & Y \end{array}$$

The set B is called a **basis** for X in $\mathcal{C}$. This extension property is called the **universal property** (succinctly, an object is free if it has a subset satisfying the universal property).

Examples of Free Objects.

- In the category of groups, the free objects are called free groups; we will construct them below.
- Restricting to abelian groups, the free objects are (up to isomorphism) direct products of $\mathbb{Z}$'s.
- The last example can be generalized to the category of R-modules, in which the free objects are (up to isomorphism) direct products of R's.

2. Groups

Normal Subgroups.

Conjugation.

Definition. Let G be a group with $a, b, x \in G$. The **conjugate** of a by x is the element ${}^x a = xax^{-1}$. We say that a and b are **conjugate elements** if ${}^x a = b$ for some $x \in G$.

Definition. The relation $a \sim b$ if a is conjugate to b forms an equivalence relation. We call the equivalence class containing a the **conjugacy class** of a, denoted $\overline{a}$.

Definition. The **automorphism group** of a group G, denoted $\mathrm{Aut}(G)$, is the set of all automorphisms of G. The set of all automorphisms which arise as conjugation by a fixed element form the **inner automorphism group** of G, denoted $\mathrm{Inn}(G)$.

- ***Exercise.*** *Prove the map $\alpha_x(a) = {}^x a$ is an automorphism.*
- ***Exercise.*** *Prove $Inn(G)$ is a normal subgroup of $Aut(G)$.*

Characteristic Subgroups.

Definition. The **center** of a group G, denoted $Z(G)$, is the set of all elements which commute with every element of G, i.e. $Z(G) = \{z \in G \mid zg = gz, \forall g \in G\}$.

Definition. Given a subset S of a group G, the **subgroup generated by S** is the smallest subgroup containing S, equivalently, the intersection of all subgroups containing S. The **normal subgroup generated by S** is the smallest normal subgroup containing S.

Definition. The **commutator subgroup** of a group G, denoted G' or $[G, G]$, is the subgroup generated by all **simple commutators** in the group, i.e. the elements $[a, b] = aba^{-1}b^{-1}$ such that $a, b \in G$. A product of simple commutators is simply called a **commutator**.

Definition. A subgroup $H < G$ is **characteristic** if $\alpha(H) = H$ for every automorphism α of G.

Definition. The quotient group G/G' is called the **abelianization** of G.

- ***Exercise.*** *Prove $[a, b]^{-1} = [b, a]$ and ${}^x[a, b] = [{}^x a, {}^x b]$.*
- ***Exercise.*** *Prove if $f\colon G \to H$ is a homomorphism, then $f([a, b]) = [f(a), f(b)]$.*
- ***Exercise.*** *Prove every characteristic subgroup is normal.*
- ***Exercise.*** *Prove G' and $Z(G)$ are characteristic, and therefore normal.*
- ***Exercise.*** *Prove G/N is abelian if and only if $G' \subseteq N$.*

Normalizer and Core.

Definition. The **normalizer** of a subgroup $H < G$ is a subgroup $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.

Definition. The **core** of a subgroup $H < G$ is the set $\bigcap_{x \in G} xHx^{-1}$.

- ***Exercise.*** *Prove every subgroup H is normal in $N_G(H)$.*
- ***Exercise.*** *Prove H is normal if and only if $N_G(H) = G$.*
- ***Exercise.*** *Prove the core of H is the largest normal subgroup in G contained in H.*

Simple Groups.

Definition. A group is **simple** if it has no proper, nontrivial normal subgroups.

Theorem. (Abel's Theorem) *The alternating group A_n is simple for all $n \neq 4$.*

Group Actions.

Definition. A **group action** of a group G on a set X is a function $G \times X \to X$ denoted $(g, x) \mapsto g \cdot x$ such that for all $x \in X$ and $g_1, g_2 \in G$ we have

$$1 \cdot x = x, \quad \text{and} \quad (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x).$$

We then say that G **acts on** X.

Definition. A **group action** of a group G on a set X is a homomorphism $\alpha \colon G \to \mathrm{Sym}(X)$.

Definition. A group action $\alpha \colon G \to \mathrm{Sym}(X)$ is **faithful** if it is injective.

Definition. The **orbit** of an element $x \in X$ is the subset $Gx = \{g \cdot x \mid g \in G\} \subset X$.

Definition. The **stabilizer** (**isotropy subgroup**) of $x \in X$ is a subgroup $G_x = \{g \mid g \cdot x = x\} < G$.

Definition. If $G_x = G$ then $Gx = \{x\}$, so x is a **fixed point**; conversely if $G_x = \{1\}$ then Gx is a **principal orbit**. The set of all fixed points is denoted X^G. If this set is trivial, the action is **fixed-point-free**. If all orbits are principal, the action is **free**.

- ***Exercise**. Prove the above definitions of a group action are equivalent.*
- ***Exercise**. Prove the map $\cdot \colon G \times G \to G$ given by $g \cdot x = {}^x g$ defines a group action of G on itself.*
- ***Exercise**. Show orbits partition X (i.e. $x \sim y$ iff $g \cdot x = y$ for some $g \in G$ is an equivalence).*
- ***Exercise**. Show the stabilizer of a group is generally not normal.*
- ***Exercise**. Prove stabilizers of elements in the same orbit are conjugate (i.e. $G_{g \cdot x} = {}^g G_x$).*
- ***Exercise**. Prove free implies fixed-point-free, but the converse dose not generally hold.*

Theorem. (Orbit Stabilizer Theorem) *Given a group action of a group G on a set X, the cardinality of each orbit is the index of the corresponding stabilizer, i.e. $|Gx| = [G : G_x]$ for all $x \in X$.*

- ***Exercise**. Prove this theorem (hint: consider $g \mapsto g \cdot x$).*

Corollary. (Class Equation) *For any group action of a finite group G on a finite set X, we have*

$$|X| = |X^G| + \sum [G : G_x],$$

where the sum is taken over a choice of elements representing each distinct, nontrivial orbit.

Examples of Group Actions. The most important actions in Sylow Theory are of a group G acting on some substructure of itself. In the following examples, let G be a group and H a subgroup.

(1) The *action of G on itself by translation* is defined by $g \cdot x = gx$. The action is faithful. The stabilizers are all trivial, so the orbits are all principle. Thus by definition, the action is free, and therefore fixed-point-free. The class equation says nothing illuminating.

(2) The *action of G on itself by conjugation* is defined by $g \cdot x = gxg^{-1}$. The orbits are $Gx = \overline{x}$, and the stabilizers are $G_x = Z(x)$. The fixed points form the center $Z(G)$. By the OST

$$|\overline{x}| = |G : Z(x)| \implies |\overline{x}| \text{ divides } |G|.$$

The class equation gives

$$|G| = |Z| + |G : Z_1| + |G : Z_2| + \dots$$

where $Z_1, Z_2, \dots$ are the centralizers of each of the nontrivial conjugacy classes of G.

(3) The *action of G on Sub(G) by conjugation* is defined by $g \cdot H = gHg^{-1}$. The orbits are $GH = \overline{H}$, and the stabilizers are $G_H = N_G(H)$. The fixed points are normal subgroups. By the Orbit Stabilizer Theorem
$$|\overline{H}| = |G : N_G(H)| \implies |\overline{H}| \text{ divides } |G|.$$
(4) The *action of $K < G$ on the cosets G/H by translation* is defined by $k \cdot gH = (kg)H$. Exercise: determine necessary and sufficient conditions for gH to be a fixed-point under this action. What does this imply when $K = G$? If $K = G$, the kernel of this action is given by
$$\{g \in G | g(xH) = xH \text{ for all } x \in G\} = \bigcap_{x \in G} xHx^{-1} =: \text{core}(H).$$
The core is the largest normal subgroup of G contained in H.

Theorem. *Let G be a group of order n, and let H be a subgroup of index ℓ. If ℓ is the smallest prime divisor of n, then $H \triangleleft G$. If n does not divide $\ell!$, then $\{1\} \neq core(H) \triangleleft G$.*

Sylow Theory.

Definition. A group G of order p^m for some prime p and some integer $m \geqslant 1$ is called a ***p*-group**. A p-group which is a subgroup of a finite group G is called a ***p*-subgroup**; in particular, if the subgroup has order the largest power of p that divides $|G|$, it is a **Sylow *p*-subgroup**. If p is a prime divisor of $|G| < \infty$, we denote the set of Sylow p-subgroups of G by $\text{Syl}_p(G)$. In addition, we denote $n_p(G) = |\text{Syl}_p(G)|$.

Theorem. (Sylow Theorems) *For a finite group G and a prime p,*
(I) *G has at least one Sylow p-subgroup P (i.e. $n_p \geqslant 1$);*
(II) *any two Sylow p-subgroups are conjugate (i.e. $Syl_p(G) = \overline{P}$);*
(III) *n_p divides $|G|$ and $n_p \equiv_p 1$ (i.e. $n_p \mid \ell$ where $|G| = p^m\ell$ with $p \nmid \ell$).*

► ***Exercise**. Show that $n_p = 1$ implies the Sylow p-subgroup is normal (hint: not* Sylow (II)).

Lemma. *If a finite p-group P acts on a finite set X, then $|X| \equiv_p |X^P|$.*

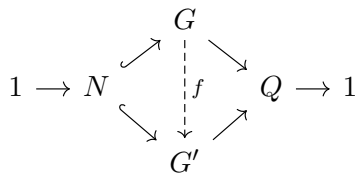
Corollary. (Burnside's Theorem) *Finite p-groups have nontrivial center.*

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

► ***Exercise**. Prove Burnside's Theorem. Use this and the Correspondence Theorem to show (by induction) that any p-group of order p^k contains subgroups of order p^m for all $0 \leqslant m \leqslant k$.*

Definition. If N and Q are groups, a group G satisfying
$$1 \to N \hookrightarrow G \to Q \to 1$$
is called an ***extension*** of Q by N.

► ***Exercise**. Two extensions G and G' of Q by N are **equivalent** if there is a homomorphism $f : G \to G'$ such that the diagram below commutes. Show such an f is an isomorphism.*



► ***Exercise**. Relate simple groups with the extension question: when does an extension G of Q by N exist? (hint: consider a group which is not simple first).*

Theorem. *The following six propositions hold:*

(1) A finite abelian group G is simple if and only if it has prime order.
Proof. Suppose first that G has prime order. Then the only subgroups are the trivial group and G, so G is simple. For the sufficiency, suppose $|G| = pn$ for some integer $n \geqslant 1$. By Cauchy's Theorem, there is an element of order p. The subgroup generated by this element is nontrivial, proper, and normal (from G abelian). Therefore, G is not simple. □

(2) If G is nonabelian of prime-power order, then G is not simple.
Proof. By Burnside's Theorem, the center is nontrivial. The center is also proper (since G is nonabelian) and normal. Thus, G is not simple. □

(3) If G is nonabelian and $|G| = pq$ for primes p and q, then G is not simple.
Proof. Without loss of generality, assume that $p < q$. Then by Sylow Theorem (III) we have $n_q | p$, meaning either n_q is 1 or p. However, $n_q \equiv_q 1$, so only $n_q = 1$ is possible. □

(4) If G is nonabelian and $|G| = p^2 q$ for primes p and q, then G is not simple.
Proof. Suppose first that $q < p$. Then by Sylow (III) we have $n_p | q$ and $n_p \equiv_p 1$. The only possibility is $n_p = 1$, as desired. Conversely, suppose that $p < q$. By Sylow (III) we have $n_q | p^2$. If $n_q = 1$, we are done. If $n_q = p$, then by Sylow (III) $q \equiv 1 (\mod p)$. So q divides $p - 1$, contradicting the assumption $p < q$. If $n_q = p^2$, then there are p^2-many subgroups of prime order q. Away from the identity, these subgroups are disjoint because the intersection of any pair of subgroups (itself a subgroup) has order which divides the order of either subgroup (which is prime). Furthermore, the nontrivial elements of these subgroups have order q because q is prime. Thus there are $p^2(q-1)$ many elements of order q in G, leaving only room for one Sylow p-subgroup, i.e. $n_p = 1$. □

(5) If G is nonabelian and $|G| = pqr$ for primes p, q, and r, then G is not simple.
Proof. Without loss of generality, suppose $p < q < r$. We utilize the "counting elements" technique. Consider n_r, which is any of 1, p, q, or pq. Since $n_r \equiv 1 (\mod r)$, either $n_r = 1$ or $n_r = pq$. If $n_r = 1$, we are done, so assume $n_r = pq$. As in (4.) above, there must be $pq(r-1)$ many elements of order r in the group. Consider next n_q, which is any of 1, p, r, or pr. Since $n_q \equiv 1 (\mod q)$, the case $n_q = p$ is omitted. If $n_q = 1$, we are done. So n_q is either pr or r. Assume first that $n_q = pr$. Then there are $pr(q-1)$ many elements of order q. In total, the group contains

$$pq(r-1) + pr(q-1) = pqr + (pqr - pr - pq) = pqr + p(qr - r - q)$$

many elements of order q or r, which exceeds the order of the group. So assume $n_q = r$. Then there are $r(q-1)$ many elements of order q. Note that this is not sufficiently many to surpass the number of elements in the group, so consider n_p, which is any of 1, q, r, or qr. If $n_p = 1$, we are done. In any of the remaining cases, $n_p \geqslant q$, so there are at least $q(p-1)$ many elements of order p in the group. In total, there are

$$\begin{aligned} pq(r-1) + r(q-1) + q(p-1) &= pqr - pq + qr - r + pq - q \\ &= pqr + qr - r - q \end{aligned}$$

many elements of order p, q, or r, which again exceeds the order of the group. We conclude that one of n_p, n_q, or n_r must have been 1, implying that G is not simple. □

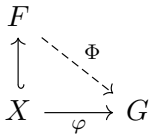
(6) If $|G| = n$ has prime divisor $1 < p < n$ and $n \nmid n_p!$, then G is not simple.
Proof. Let $X = \mathrm{Syl}_p(G)$, and consider the kernel of the group action $\alpha \colon G \to \mathrm{Sym}(X)$ given by conjugation of X by G. If $\ker(\alpha)$ is trivial, then G is isomorphic to a subgroup of $\mathrm{Sym}(X)$, contradicting the assumed orders. If $\ker(\alpha) = G$, then each $P \in X$ is normal ($P = gPg^{-1}$ for all $g \in G$), nontrivial, and proper ($p < n$). Otherwise, $\ker(\alpha)$ is a normal, nontrivial, proper subgroup of G. In either case, G is not simple. □

► ***Exercise.*** *Prove the following 6 propositions on your own.*

- ***Exercise.*** *Classify all simple, finite, abelian groups (answer: cyclic of prime order).*
- ***Exercise.*** *Classify all simple, finite, nonabelian groups of order below 60.*
- ***Exercise.*** *Prove for a prime p, any group of order p^2 is abelian.*
- ***Exercise.*** *If $|G| = p^n q$, with $p > q$ primes, G contains a unique normal subgroup of index q.*
- ***Exercise.*** *Prove every group of order 12, 28, 56, and 200 must contain a normal Sylow subgroup, and is consequently not simple.*

Free Groups.

Definition. Let F be a group and X a subset of F. We say F is a **free group on X** if every function $\varphi\colon X \to G$ to a group G extends uniquely to a homomorphism $\Phi\colon F \to G$.



A group F is **free** if it is free on some subset X, called a **basis** for F.

Theorem. *Free groups exist.*

Proof. Let X be a set. Define $X^{-1} = \{x^{-1} \mid x \in X\}$, where the exponent is (for now) only symbolic. The elements of $X \sqcup X^{-1}$ are ***letters***. A ***word*** ω on X is a finite string of letters

$$\omega = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n},$$

where $x_i \in X$ and $\varepsilon_i = \pm 1$. The value $n \geqslant 0$ is called the ***length of the word***. The ***empty word*** is the word with length 0. Let $\Omega(X)$ be the set of all words on X. We ***multiply*** words by juxtaposition, and ***invert*** by running backwards with inverse letters (i.e. sign of the exponent changes). A ***subword*** is a connected substring $x_i^{\varepsilon_i} x_{i+1}^{\varepsilon_{i+1}} \dots x_j^{\varepsilon_j}$, where $0 \leqslant i \leqslant j \leqslant n$. We say a word is ***reduced*** if it has no subwords xx^{-1} or $x^{-1}x$ for some $x \in X$. Define an ***elementary operation*** on a word ω by inserting/deleting a subword of the form xx^{-1} or $x^{-1}x$ in ω. Two words are ***related*** if they differ by finitely many elementary operations. This defines an equivalence relation $\sim$ on $\Omega(X)$. We define the **free group on X** to be the set

$$F(X) = \Omega(X)/\sim$$

under the operation $[\omega][\eta] = [\omega\eta]$. □

- ***Exercise.*** *Prove multiplication is well defined by showing (1) every word ω is equivalent to a unique reduced word $\overline{\omega}$, and (2) $\overline{\omega\eta} = \overline{\omega}\ \overline{\eta}$.*

Theorem. *The group $F(X)$ defined above is free on X.*

- ***Exercise.*** *Prove this theorem by showing (1) $F(X)$ is indeed a group, and (2) any function $X \to G$ extends (linearly) to a homomorphism $F(X) \to G$.*
- ***Exercise.*** *Show that $F(X)$ is free and nonabelian if $|X| \geqslant 2$.*

Theorem. *Every group G is isomorphic to the quotient of a free group.*

- ***Exercise.*** *Prove this by considering a generating set X for G along with its inclusion into G.*

Group Presentations.

Definition. Given a subset S of a group G, the **subgroup generated by S** is the smallest subgroup (S) containing S. Similarly, the **normal subgroup generated by S** is the smallest subgroup $\langle S \rangle$ containing S. If S is finite, we say the subgroup is **finitely generated**.

Definition. A group G is **finitely presented** if there exists a finite set X and a finitely generated, normally generated subgroup N of $F(X)$ for which $G \cong F(X)/N$. The elements of X are called **generators**, and the elements of N are called **relations**.

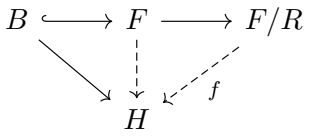
Definition. Suppose G is finitely presented with generators $x_1, \dots, x_p$ relations $r_1, \dots, r_q$. We write

$$G = \langle x_1, \dots, x_p \mid r_1, \dots, r_q \rangle$$

meaning $G \cong F(x_1, \dots, x_p)/\langle r_1, \dots, r_q \rangle$, and call this a (finite) **presentation** of G.

Note that the presentation of a group is not unique. Moreover, it is impossible to construct an algorithm which determines whether or not a presentation determines the trivial group (one can further reason there is no classification of four manifolds)! However, this is theoretically possible, as the following Theorems indicate.

Theorem. (von Dyck's Theorem) *If $G = \langle x_1, x_2, \dots | r_1, r_2, \dots \rangle$ and H is a group with generators $y_1, y_2, \dots$ such that $r_i(y_1, y_2, \dots) = 1 \in H$, there exists an epimorphism $G \twoheadrightarrow H$ with $f(x_i) = y_i$.*



► ***Exercise**. Prove this theorem using the Universal Property of Free Groups and the Characteristic Property of Quotient Groups.*

Theorem. (Tietze's Theorem) *If G has two different finite presentations $\langle x_1, \dots, x_p \mid r_1, \dots, r_q \rangle$ and $\langle y_1, \dots, y_m \mid s_1, \dots, s_n \rangle$, then one can pass from one to the other by **elementary Tietze operations**: add/remove generator; add/remove relation which are consequence of remaining ones.*

► ***Exercise**. Show that $G = \langle x, y \mid x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$ is isomorphic to Q_8 (Hint: Use van Dyck's Theorem, and prove the group has order 8 by arguing each element can be written $a^n b^m$ for restricted values of m, n).*

Miscellany.

Lemma. (Product Recognition) *If $H, K \triangleleft G$ with $H \cap K = \{1\}$ and $HK = G$, then $G \cong H \times K$.*

Proposition. *If $S, T < G$, then $ST < G$ if and only if $ST = TS$ setwise. Moreover, if S and T are normal, then ST is normal, as well.*

Proposition. *If $S, T < G$ and $ST < G$, then $|ST| = |S||T|/|S \cap T|$.*

3. Rings

Basics.

Definition. A **ring** is a set R with two operations $+$ and $\cdot$ satisfying

(a) $(R, +)$ is an abelian group;
(b) $(R, \cdot)$ is a semi-group (i.e. a set with an associative binary operation);
(c) $\cdot$ distributes over $+$ on both sides (e.g. $a \cdot (b + c) = a \cdot b + a \cdot c$).

We often simplify the notation $a \cdot b = ab$. If the operation $\cdot$ is commutative, we say R is a **commutative ring**. When one exists, we call the identity in $(R, \cdot)$ a **unity**. Elements with inverses in $(R, \cdot)$ are called **units**. A commutative ring with unity is a **field** if every nonzero element is a unit.

Definition. A subset S of a ring R is a **subring** if itself forms a ring under the inherited operations. A subring I is an **ideal** (written $I \triangleleft R$) if $ab \in I$ for all $a \in R$, $b \in I$. Each element $a \in R$ generates an ideal $\langle a \rangle = \{ra, ar \in R \mid r \in R\}$ called the **principal ideal generated by a**.

Definition. A **ring homomorphism** is a map between rings $f \colon R \to S$ for which $f(rs) = f(r)f(s)$ and $f(r + s) = f(r) + f(s)$ for all $r, s \in R$.

- ***Exercise**. Prove the kernel of a ring homomorphism is an ideal.*
- ***Exercise**. Prove analogous isomorphism theorems and the Correspondence Theorem for rings.*
- ***Exercise**. Prove that a ring is a field if and only if it has no nontrivial, proper ideals (hint: Correspondence Theorem).*

Definition. If $I, J < R$, the sets $I + J$ and IJ are defined by

$$I + J = \{a + b \mid a \in I, b \in J\}$$
$$IJ = \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in A, b_i \in B, n \in \mathbb{N}\}.$$

- ***Exercise**. Prove that if $I, J \triangleleft R$, then the sets $I \cap J$, $I + J$, and IJ are also ideals in R. Moreover,*
  (a) *$I + J$ is the smallest ideal containing both I and J;*
  (b) *$IJ \subset I \cap J$, and if $R = I + J$ is commutative with identity, $IJ = I \cap J$.*

Definition. An element $r \in R$ is **nilpotent** if $r^n = 0$ for some $n \in \mathbb{N}$.

- ***Exercise**. Let $\mathcal{N}$ be the set of nilpotent elements in a ring R.*
  (a) *Prove that if R is commutative, $\mathcal{N}$ is an ideal in R contained in any prime ideal of R (hint: use binomial theorem to show closure under addition);*
  (b) *show that $\mathcal{N}$ need be not be an ideal if R is not commutative (hint: use matrices);*
  (c) *show that if R is commutative with unity, then any sum $u + x$ of a unit u with a nilpotent x is a unit (hint: first show that $1 - x$ is a unit by factoring $1 - x^n$ for suitable n).*

Definition. An ideal $I \triangleleft R$ is **maximal** if there are no ideals properly contained between I and R (i.e. whenever J is an ideal of R satisfying $I \subseteq J \subseteq R$, either $I = J$ or $J = R$). An ideal is **prime** if $ab \in I$ implies either $a \in I$ or $b \in I$.

Definition. Given an ideal $I \triangleleft R$, the **quotient ring** of R by I is the set $R/I = \{a + I | a \in R\}$ under the operations

$$(a + I) + (b + I) = (a + b) + I \qquad (a + I)(b + I) = (ab) + I.$$

These operations are well defined because I is an ideal.

Fields, EDs, PIDs, and UFDs.

Definition. A **zero divisor** of $a \in R$ is a nonzero element $b \in R$ such that $ab = 0$. A ring with no zero divisors is called a (integral) **domain**.

- ***Exercise.*** *Prove that R is a domain if and only if $\{0\}$ is a prime ideal.*
- ***Exercise.*** *Prove a proper ideal $I \triangleleft R$ is prime if and only if R/I is a domain, and is maximal if and only if R/I is a field.*
- ***Exercise.*** *Prove every finite integral domain R is a field (hint: for any $r \neq 0$ consider $x \mapsto xr$).*

Definition. A **Euclidean function** on a ring R is a function $f\colon R \setminus 0 \to \mathbb{N}_{>0}$ such that for any pair of nonzero $a, b \in R$, there exist unique $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $f(r) < f(q)$. A ring R is a **Euclidean domain** (ED) if it has a Euclidean function.

Definition. A **principal ideal domain** (PID) is a a ring in which all ideals are principal.

- ***Exercise.*** *Prove that every field is an ED. Show the converse need not hold.*
- ***Exercise.*** *Prove that every ED is an PID. Show the converse need not hold.*

Definition. A nonzero element p in a domain R is **irreducible** if $ab = p$ implies a or b is a unit. Moreover, p is **prime** if $ab|p$ implies $a|p$ or $b|p$.

- ***Exercise.*** *Define what it means for one element to divide another, i.e. $a|b$ for $a, b \in R$. Provide equivalent definitions of divides, irreducible, and prime using ideals.*
- ***Exercise.*** *Prove in a domain, prime elements are irreducible. Show the converse need not hold.*
- ***Exercise.*** *Prove that a nonzero ideal is prime iff maximal in a PID.*

Definition. A **unique factorization domain** is a ring R for which every nonzero, nonunit element $r \in R$ there exist unique (up to associates) irreducibles $p_1, \ldots, p_n$ such that $r = p_1 \cdots p_n$.

- ***Exercise.*** *Prove every PID is a UFD. Show the converse need not hold.*
- ***Exercise.*** *Show $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but not prime. Show that $\mathbb{Z}[\sqrt{-5}]$ is nat a UFD.*
- ***Exercise.*** *Show that $\mathbb{Z}[i]$ is a UFD, and explain why $2 \cdot 5 = 10 = (3-i)(3+i)$ does not contradict this.*
- ***Exercise.*** *Show that if F is a field, $F[x]$ is an ED.*
- ***Exercise.*** *Let F be a field. Show that irreducible and prime are the same for polynomials in $F[x]$. Prove that for $f \in F[x]$, the quotient $F[x]/\langle f \rangle$ is a field if and only if f is irreducible.*
- ***Exercise.*** *Let R be a commutative ring with unity and f a nonzero polynomial in $R[x]$ of degree n. Show $c \in R$ is a root of f if and only if $(x - c)|f$. Moreover, if R is a domain, f has at most n roots in R.*

Theorem. *If R is a UFD, then $R[x]$ is a UFD.*

Theorem. (Cubic Criterion) *If R is a domain and f is a primitive polynomial in $R[x]$ of degree no more than 3, then f is irreducible over R if and only if it has a root in $F(R)$.*

- ***Exercise.*** *Show $x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$. Then construct a field of order 9. Write down its multiplication table.*
- ***Exercise.*** *Show that $x^3 + 6x + 12$ is irreducible in $\mathbb{Z}[x]$.*

Theorem. (Eisenstein's Criterion) *Let $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ be primitive. If there is a prime p for which $p|a_0, \ldots, a_{n-1}$ but $p \nmid a_n$ and $p^2 \nmid a_0$, then f is irreducible.*

- ***Exercise.*** *Prove that $x^3 + 6x + 12$ and $x^4 + x^3 + x^2 + x + 1$ are irreducible in $\mathbb{Z}[x]$.*

4. Fields

Definition. Let L be a field with $K \subseteq L$ a subfield. We call L a **field extension** of K, written L/K. For $u \in L \setminus K$, the field extension $K(u)/K$ is called a **simple extension** of K.

Definition. Given a field extension L/K, we can consider L as a K-vector space; the dimension of this vector space is called the **degree** of the field extension and is denoted $[L:K]$. According to the cardinality of this number, we say the extension of L over K is (in)finite.

Properties:
- the degree of an extension L/K is 1 if and only if $L = K$;
- given fields $K \subset L \subset M$, we have $[M:K] = [M:L][L:K]$.

Definition. Let L/K be a field extension. An element in $L \setminus K$ is **algebraic** over K if it is a zero of some nonzero polynomial in $K[x]$; otherwise, it is **transcendental**. A simple extension $K(u)$ is an **algebraic extension** if u is algebraic over K; otherwise it is a **transcendental extension**.

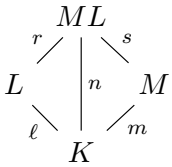
Definition. A field F is **algebraically closed** if

Theorem. *Let L/K be a field extension and $u \in L$. Then:*
- *if u is transcendental over K, then $K[u] \cong K[x]$ and $K(u) \cong K(x)$;*
- *if u is algebraic over K, then there exists a unique, monic, irreducible polynomial $m_u \in K[x]$ such that each $f \in K[x]$ with $f(u) = 0$ is a multiple of m_u and $K[u] \cong K(u)$.*

Corollary. *Transcendental extensions are infinite; finite extensions are algebraic.*

Definition. Let M and L be fields containing a field K. Then $LM = L(M) = M(L)$ is a field extension over K and L and M.

Theorem. *Consider extensions ML/K, M/K, and L/K having degrees n, m, and ℓ.*



Then $n \leqslant m\ell$, or equivalently $s \leqslant \ell$, or equivalently $r \leqslant m$.

Definition. For a field extension M/K, the **Galois group** of N over K is the group $\mathrm{Gal}(M:K)$ of automorphisms that leave every element of K fixed. The **fixer** of an intermediate field L is the set $L' \subseteq G$ of automorphisms in $\mathrm{Gal}(M:K)$ which fix L pointwise. Conversely, the **fixed field** of the subgroup $H < G$ is the subset $H' \subset M$ of elements fixed by each element in H.

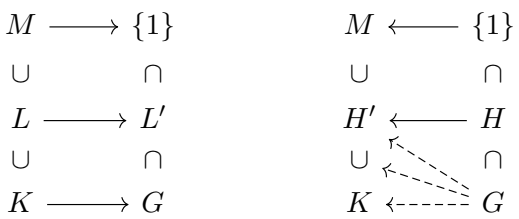


Figure 1. The extreme cases of the correspondence, which are for the most part as desired.

Definition. The **closure** of an intermediate object is its double prime. An intermediate object is **closed** if it is equivalent to its closure. We say M is **normal** over K if $\mathrm{Gal}(M:K)' = K$.

Properties:
- let L and M be intermediate fields of N/K with $[M:L] = n$, then $[L':M'] \leqslant n$;
- let $H \subset J$ be subgroups of $G = \mathrm{Gal}(N:K)$ with $[H:J] = n$, then $[J':H'] \leqslant n$;
- if L is closed, then also M is closed; moreover, $[L':M'] = n$;
- if H is closed, then also J is closed; moreover, $[H':J'] = n$;
- all finite subgroups of G are closed;
- if M is normal over K, then M is normal over any intermediate field L with $[L:K]$ finite.

Theorem. (Fundamental Theorem of Galois Theory) *Let M be a normal, finite-dimensional extension of K, and let $G = Gal(M:K)$. There is a one-to-one correspondence between the subgroups of G and the intermediate fields of M and K, implemented by the priming operation. Moreover, the relative degrees are preserved, and in particular, $[M:K] = |G|$.*

Theorem. *Given a finite group G of automorphisms of a field M, the field extension of M over the fixed field of G is normal, finite-dimensional, and has Galois group G.*

Definition. For fields $K \subset M \subset L$, we say that L is **stable** relative to K and M if every automorphism of M/K sends L into (and consequently onto) itself.

Properties:
- stable intermediate fields correspond to normal subgroups;
- the closure of a normal subgroup is normal; the closure of a stable intermediate field is stable;
- if M is normal over K and L is stable relative to K and M, then L is normal over K;
- if M is normal over K and $f \in K[x]$ is irreducible with root $u \in M$, then f factors over M into distinct linear factors;
- if L is normal and algebraic over K, then L is stable (relative to any extension $M \supset L$);
- if L is a stable intermediate field of M/K, then G/L' is isomorphic to the group of all automorphisms of L/K that are extendible to M, where $G = \mathrm{Gal}(M:K)$.

Theorem. (Fundamental Theorem of Galois Theory, cont'd) *In the correspondence, a field L is normal over K if and only if the corresponding subgroup is normal in $G = Gal(M:K)$, and in this case, G/H is the Galois group of L/K.*

Theorem. *Let f be irreducible in $K[x]$. Then there exists a field containing K and a root of f. This field is unique up to isomorphism of K.*

Definition. Let $f \in K[x]$. We say that M is a **splitting field** of f over K if f factors completely in M and $M = K(u_1, \ldots, u_n)$, where u's are the roots of f. We say M is a splitting field over K if there exists a polynomial f for which M is a splitting field of f over K.

Definition. The **formal derivative** of a polynomial $f = \sum a_i x^i$ is a polynomial $f' = \sum i a_i x^{i-1}$.

Properties:
- each $f \in K[x]$ has a splitting field, which is unique up to isomorphism of the base field;
- if $f \in K[x]$ and $a \in K$, then $(x-a)^2$ divides f if and only if $x - a$ divides f and f';

Definition. An irreducible polynomial f in $K[x]$ is **separable** if, in some splitting field over K, it factors into distinct linear factors. An element u that is algebraic over K is said to be **separable** over K if its irreducible polynomial is separable over K. A field L that is algebraic over K is **separable** over K if every element is separable over K.

Properties:

- if f is irreducible in $K[x]$, the following are equivalent:
  - in every splitting field if f over K, f factors into distinct linear factors;
  - f is separable;
  - $f' \neq 0$;
- if M is a finite extension of K, the following are equivalent:
  - M is normal over K;
  - M is separable over K and M is a splitting field over K;
  - M is a splitting field over K of a polynomial whose irreducible factors are separable;
- if L is a finite extension of K, the following are equivalent:
  - L is a splitting field over K;
  - whenever an irreducible polynomial over K has a root in L it factors completely in L;

Definition. Let $K \subset L \subset M$ with L/K finite. We say M is the **split closure** of L if it is the smallest splitting field over K containing L. If L is separable, we say M is the **normal closure**.

Theorem. *Every finite extension has a split closure, which is unique up to isomorphism fixing L. If L is separable, M is normal over K.*

Properties:

- for characteristic 0, normal is the same as splitting field;
- for characteristic p, normal is splitting field plus separability.

5. Modules

Basics.

Definition. An R-module M is a vector space whose scalars have been replaced by a ring R.

- ***Exercise.*** *A module is* ***simple*** *if its only submodules are M and $\{0\}$. Classify the simple $\mathbb{Z}$-submodules.*

Definition. An ***R*-linear map** or ***R*-module homomorphism** is a function $f\colon M \to N$ satisfying $f(rm+n) = rf(m) + f(n)$ for every $m, n \in M$ and $r \in R$. The set of all R-linear maps from M to N is denoted $\mathrm{Hom}_R MN$; in the case $M = N$, we write $\mathrm{End}_R M$ for endomorphism.

Definition. The **quotient *R*-module** of an R-module M by a submodule N is the module of cosets of N in M under the operations

$$(a+N)+(b+N) = (a+b)+N \text{ and } r(a+N) = ra+N,$$

for all $a, b \in M$ and $r \in R$.

- ***Exercise.*** *Show that the kernel of an R-linear map $f\colon M \to N$ is an R-submodule of M, and if this submodule is trivial, then f is injective.*
- ***Exercise.*** *Find a positive integer k such that $Hom_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) \cong \mathbb{Z}_k$.*
- ***Exercise.*** *Show the analogous isomorphism theorems hold for quotients of R modules.*

Definition. The **direct sum** of R-modules M and N is the module $M \oplus N = \{(m,n) | m \in M, n \in N\}$ with pointwise operations. We often write $M^n = M \oplus \cdots \oplus M$ for n-many copies of M.

Definition. An element m of an R-module M is **torsion** if there exists a nonzero $r \in R$ such that $rm = 0$. An R-module M is a **torsion module** if each of its elements are torsion.

Definition. An R-module M is **free** if there exists a subset B of M, called a **basis**, such that every element in M can be written uniquely as a finite linear combination of elements in B.

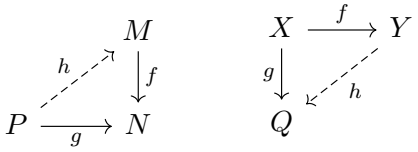
Definition. For a subset S of an R-module M, the **submodule $\langle S \rangle$ generated by *S*** is the smallest submodule of M containing S (equivalently, the intersection of all submodules containing S), or constructively

$$\langle S \rangle = \Big\{ \sum r_i s_i \;\Big|\; r_i \in R, s_i \in S \Big\}.$$

If $S = \{s\}$, then $M = \langle s \rangle$ is a **cyclic *R*-module**. If S is a finite set, then M is **finitely generated**.

- ***Exercise.*** *Prove an R-module M is free on $B \subset M$ if and only if M is isomorphic to $R^{|B|}$.*
- ***Exercise.*** *Prove an R-module M is free on $B \subset M$ if and only if any function from B to an R-module N extends uniquely to an R-linear map $M \to N$.*
- ***Exercise.*** *Prove an R-module M is cyclic if and only if $M \cong R/J$ for some $J \lhd R$.*
- ***Exercise.*** *Find an example and a counterexample of a free module and a torsion module.*
- ***Exercise.*** *Prove Schur's Lemma: Let M and N be simple R-modules and $f\colon M \to N$ be a nonzero R-linear map. Then f is an isomorphism. Moreover, if $M = N$ and R is commutative, then f is multiplication by a scalar (i.e. there is some $r \in R$ such that $f(x) = rx$ for all $x \in M$.*

Definition. An R-module P is **projective** if for every surjective module homomorphism $f\colon M \to N$ and every module homomorphism $g\colon P \to N$, there exists a module homomorphism $h\colon P \to M$ such that $fh = g$. Similarly, an R-module Q is **injective** if for every injective module homomorphism $f\colon X \to Y$ and every module homomorphism $g\colon X \to Q$ there is a module homomorphism $h\colon Y \to Q$ such that $hf = g$. That is, the following commutative diagrams commute, respectively.



- ***Exercise**. Show that P is a projective R-module if and only if every short exact sequence of the form $0 \to M \to N \to P \to 0$ splits.*
- ***Exercise**. Show that Q is an injective R-module if and only if every short exact sequence of the form $0 \to Q \to M \to N \to 0$ splits.*

Modules over a PID.

Theorem. (Invariant Structure Theorem) *If R is a PID and M is a finitely-generated R-module, then there is a unique nonnegative integer r and a unique sequence $J_i < R$ of nested, nonzero proper ideals such that*

$$M \cong R/J_1 \oplus \cdots \oplus R/J_k \oplus R^r.$$

*The integer r is called the **rank** of M, and the ideals are called the **invariant factors** of M.*

Theorem. (Primary Structure Theorem) *If R is a PID and M is a finitely-generated R-module, then there exist finitely many prime elements $p_i \in F[t]$ and nonzero integers n_i such that*

$$M \cong R/\langle p_1^{n_1}\rangle \oplus \cdots \oplus R/\langle p_k^{n_k}\rangle.$$

*The prime elements p^n are called the **elementary divisors** of M.*

- ***Exercise**. Prove the rank of a torsion module is 0.*
- ***Exercise**. Prove all finitely generated abelian groups can be characterized by setting $R = \mathbb{Z}$.*

The Vector Transformation Module.

Definition. Let V be an F-vector space, and let $T\colon V \to V$ an endomorphism. We define $\boldsymbol{V_T}$ to be the $F[t]$-module whose additive structure is inherited from V, and whose ring is $F[t]$, where scalar multiplication is given by $f(t) \cdot v = f(T)v$.

Properties:

- if V is finite dimensional, then V_T is torsion – since $\mathrm{End}(V) \cong M_n(F)$ is n^2 dimensional, there are $a_i \in F$ such that $\sum_{i=1}^{n^2} a_i T^i = 0$;
- by the Invariant Structure Theorem, $V_T \cong F[t]/\langle f_1\rangle \oplus \cdots \oplus F[t]/\langle f_k\rangle$;
- in this module, we reconstruct T as multiplication by the scalar $g(t) = t$, acting in each summand (i.e. $Tv = t \cdot v$); to understand T, we can understand this multiplication;
- for $f = \sum_{i=0}^{n+1} a_i t^i$, the module $F[t]/\langle f\rangle$ has basis $B = \{\overline{1}, \overline{t}, \overline{t}^2, \ldots, \overline{t}^n\}$, so multiplication by $\overline{t}$ can be represented by the **companion matrix**

$$C_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_n \end{pmatrix}.$$

- carrying the basis B to V_T by the isomorphism given above, it follows that there is a basis C for V such that $T_C = C_{f_1} \oplus \cdots \oplus C_{f_k}$, where $\oplus$ denotes the block sum of matrices.

Definition. A matrix is said to be in **rational canonical form** if it can be written as $C_{f_1} \oplus \cdots \oplus C_{f_k}$ for monic polynomials $f_1, \ldots, f_k$ with $f_1 | \ldots | f_k$.

Corollary. *Every $T \in End_F(V)$ has a coordinate matrix in rational canonical form, uniquely determined by T and F, which we denote by R_T (or $R_{T/F}$ to denote over which field).*

Corollary. *If F is a field, any $A \in M_n(F)$ is similar over F to a unique matrix R_A (i.e. there is an invertible $P \in M_n(F)$ such that $PAP^{-1} = R_A$). It follows that two matrices are similar if and only if they have the same Rational Canonical Form.*

Definition. Note that $\{f \in F[t] : f(T) = 0\}$ is an ideal of $F[t]$, which is a PID. The unique, monic generator $m_T(t)$ is called the **minimal polynomial** of T.

Properties:
- $m_T(T) = 0$ (just a nice reminder);
- the minimal polynomial is the larges (last) invariant factor of T;
- the characteristic polynomial c_T is equal to the product of the invariant factors of T;
- (Cayley-Hamilton) m_T divides c_T and the roots of c_T are roots of m_T;

Corollary. *If $F \subseteq E$ are fields, then two matrices $A, B \in M_n(F)$ are similar over F if and only if they are similar over E.*

- ***Exercise**. Prove properties 1-4 of characteristic/minimal polynomials.*
- ***Exercise**. Use 1-4 to compute the characteristic and minimal polynomials of the endomorphism T on $\mathbb{R}^3$ given by the matrix with 1's in each corner and 0's elsewhere. Then find the invariant factors of T.*
- ***Exercise**. Find all possible RCFs for matrices over $\mathbb{Q}$ and $\mathbb{C}$ with characteristic polynomial $(t^4-1)(t^2+1)$.*
- ***Exercise**. Prove the preceding corollary.*

Definition. Suppose the characteristic polynomial of an endomorphism T factors into linear terms: $c_T = (t-\lambda_1)^{n_1}\dots(t-\lambda_k)^{n_k}$. Each λ_i is an **eigenvalue** of T.

Definition. The multiplication of $(t-\lambda)^n$ by t can be written as an $n \times n$ matrix $J_{\lambda,n}$ called a **Jordan block**. Noting that

$$(t-\lambda)(t-\lambda)^n = (t-\lambda)^{n+1} \implies t(t-\lambda)^n = \lambda(t-\lambda)^n + (t-\lambda)^{n+1},$$

each Jordan block can be written as

$$\begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 \\ 1 & \lambda & 0 & \cdots & 0 \\ 0 & 1 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & \lambda \end{pmatrix}$$

Any matrix which is a block sum of Jordan blocks is in **Jordan canonical form**. Therefore, by the Structure Theorem (Primary Form):

Corollary. *Every $T \in End_F(V)$ whose characteristic polynomial factors into linear terms is similar over F to a matrix J_T in Jordan canonical form (unique up to permutation of blocks). The total number of appearances of each eigenvalue λ is its multiplicity in c_T, and the size of the largest associated Jordan block is the multiplicity of λ as a root of m_T.*

- ***Exercise**. Find all Jordan canonical forms for rational and complex matrices T with characteristic polynomial $c_T = (t^4-1)(t^2+1)$.*
- ***Exercise**. Show that any square matrix over any subfield of $\mathbb{C}$ is similar to its transpose.*
- ***Exercise**. Let F be any field. Show that $A \in M_n(F)$ is diagonalizable (i.e. similar to a diagonal matrix) if and only if m_A is a product of linear factors.*

Tensor Products.

Definition. Let $M_1, \dots, M_k, N$ be R-modules. A map $F\colon M_1 \times \cdots \times M_n \to N$ is **multilinear** if

$$F(m_1, \dots, m_j + rm_j', \dots m_k) = F(m_1, \dots, m_j, \dots, m_n) + rf(m_1, \dots, m_j', \dots, m_k)$$

for all scalars $r \in R$ and all $1 \leqslant j \leqslant k$. Denote the space of all multilinear maps $M_1 \times \cdots \times M_k \to N$ by $L(M_1, \dots, M_k; N)$.

Definition. For any set S and ring R, a **formal linear combination** of elements of S is a function $f\colon S \to R$ with $f(s) = 0$ for all but finitely many $s \in S$. The **free module generated by S**, denoted $\mathcal{F}(S)$, is the set of all formal linear combinations of elements of S. One can think of elements of $f \in \mathcal{F}(S)$ as finite formal sums $\sum_i a_i x_i$ where $x_i \in S$ and $a_i = f(x_i) \in R$.

Definition. Let $M_1, \ldots, M_k$ be R-modules. We define the **tensor product** $M_1 \bigotimes \ldots \bigotimes M_k$ to be the R-module

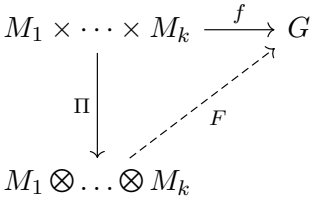
$$M_1 \bigotimes \ldots \bigotimes M_k = \mathcal{F}(M_1 \times \cdots \times M_k)/\mathcal{R},$$

where $\mathcal{R}$ is the submodule of $M_1 \times \cdots \times M_k$ containing all elements of the form

$$(m_1, \ldots, rm_i, \ldots, m_k) - r(m_1, \ldots, m_i, \ldots m_k)$$
$$(m_1, \ldots, m_i + m_i', \ldots, m_k) - (m_1, \ldots, m_i, \ldots, m_k) - (m_1, \ldots, m_i', \ldots, m_j)$$

with $m_i, m_i' \in M_i$, $i \in \{1, \ldots, k\}$, and $r \in R$.

Proposition. (Characteristic Property of Tensor Products) *Let $M_1, \ldots, M_k$ be R-modules and G an abelian group. If $f\colon M_1 \times \cdots \times M_k \to G$ is any multilinear, then there is a unique homomorphism map $F\colon M_1 \bigotimes \ldots \bigotimes M_k \to G$ making the following diagram commute:*



- ***Exercise.*** *Prove that $M \bigotimes R \cong M$ for any R-module M.*
- ***Exercise.*** *Let K be the field of fractions of a ring R, and let M be an R-module. Prove that $M \bigotimes K$ is trivial if M is torsion, and nontrivial otherwise.*
- ***Exercise.*** *Compute $\mathbb{Z} \bigotimes \mathbb{Z}$, $\mathbb{Z} \bigotimes Z_n$, and $\mathbb{Z}_m \bigotimes \mathbb{Z}_n$.*