Grad Algebra Notes

Pramana Saldin

Fall 2024 and Spring 2025

These are the combined notes of the two first-year graduate algebra courses.

MATH 741: Groups, structure of abelian groups, Sylow's theorems, category theory, representation theory and linear algebra. Textbooks: [Art18] and [Hun12].

MATH 742: Continuation of MATH 741. Commutative algebra: prime and maximal ideals, modules, tensor products, the Yoneda lemma, exact sequences, localization, Cayley-Hamilton, PID structure theorem. Field theory: field extensions, splitting fields, algebraic closure, Galois theory, solvability of polynomials over $\mathbb{Q}$, finite fields, infinite Galois theory. Textbooks: [AK12] (for commutative algebra) and [Mil22] (for field theory).

Professor: Dima Arinkin.

Contents

1. Groups

1.1. Basics

September 04, 2024

Groups are related to the symmetries of objects.

Example 1.1 (Familiar groups) –

1. Symmetry groups:
$$S_n \coloneqq \{\text{bijections } \{1,\dots,n\} \to \{1,\dots,n\}\}.$$
2. Dihedral groups: D_n.
3. Cyclic groups: $\mathbb{Z}/n\mathbb{Z}$.
4. General linear groups: $GL_n(\mathbb{R})$, $GL_n(\mathbb{C})$; invertible $n \times n$ matrices.

1.1.1. Subgroups

Given a group G and a subset S, the **subgroup generated by S** is (1) the smallest subgroup containing S, or (equivalently, but requiring a proof) (2) the intersection of all subgroups containing S. We denote the subgroup generated by S as $\langle S\rangle$.

Example 1.2 – In S_5 consider the elements $a = (12345)$ and $b = (12)$. What is $\langle a, b\rangle$?

To compute the subgroup, we can't really use the definitions. We just need to take products of a and b (loosely, $\langle a, b\rangle = \left\{a^{\alpha_1}b^{\beta_1}\cdots a^{\alpha_n}b^{\beta_n} \mid \alpha_i, \beta_i \in \mathbb{Z}, n \geq 0\right\}$). It's still hard to get the answer (S_5) in practice.

Example 1.3 – In S_5 consider the elements $a = (12345)$ and $b = (12)(35)$. What is $\langle a, b\rangle$?

Here, we can draw a picture of a pentagon and imagine what the element a and b do to the vertices. We notice that they represent a reflection and a rotation, so we know the subgroup is isomorphic to D_{10}.

1.1.2. Cosets and quotients

Let G be a group and $H \leq G$. G/H is the **quotient** of H in G. We define
$$G/H \coloneqq \{\text{cosets of } H \text{ in } G\}.$$

Recall that a **(left) coset** of H in G is $gH \coloneqq \{gh \mid h \in H\} \subseteq G$. A right coset is defined by $Hg \coloneqq \{hg \mid h \in H\}$.[1] So G can be either split into left or right cosets, with (at least) H as a left and right coset.

If H is **normal**, i.e. $gHg^{-1} = H$ for all $g \in G$, then G/H is actually a group.

Proposition 1.1

There are the same number of left and right cosets.

[1] Another way to define left (resp. right) is by the equivalence relation $a \sim b$ if $a^{-1}b \in H$ (resp. $a \sim b$ if $ba^{-1} \in H$).

Proof. This follows from the fact that $(gH)^{-1} = Hg^{-1}$. We are essentially taking the bijective anti-homomorphism[1] $x \mapsto x^{-1}$ and showing it descends to a bijection between the left and right cosets:

$$\begin{tikzcd} G \arrow[r, "x\mapsto x^{-1}"] \arrow[d, two heads] & G \arrow[d, two heads] \\ G/H \arrow[r, "\text{bij.}"'] & H\backslash G \end{tikzcd}$$

□

[1] A function between groups $\varphi\colon G \to H$ is an **anti-homomorphism** if $\varphi(ab) = \varphi(b)\varphi(a)$.

The **index** of H in G, denoted $[G : H]$, is the number of (left/right) cosets of H in G, i.e. $|G/H|$.

September 06, 2024

Proposition 1.2
The following are equivalent:

1. $H \trianglelefteq G$,
2. left and right cosets coincide,
3. $(g_1, g_2) \mapsto g_1 g_2$ is a well-defined map from $G/H \times G/H$ to G/H.

Remark 1.3 ("French style"). The last statement is equivalent to the existence of a unique homomorphism on the bottom of the following diagram that makes it commute

$$\begin{tikzcd} G \times G \arrow[r, "(g_1,g_2)\mapsto g_1g_2"] \arrow[d, two heads] & G \arrow[d, two heads] \\ G/H \times G/H \arrow[r, dashed, "?"'] & G/H \end{tikzcd}$$

1.2. Quotients and homomorphisms

If $\varphi\colon G \to H$ is a group homomorphism, let $\ker \varphi = \{g \in G : \varphi(g) = e\}$.

Theorem 1.4 (First isomorphism theorem)
Let $\varphi\colon G \to H$ be a group homomorphism. Then

$$\varphi(G) \cong G/\ker \varphi.$$

Remark 1.5. We implicitly assumed that (1) $\varphi(G)$ is a group, (2) $\ker \varphi$ is a normal subgroup, and (3) φ induces an isomorphism between the two sides.

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d] & H \arrow[d, phantom, "\cup"] \\ G/\ker \varphi \arrow[r, "\sim"] & \varphi(G) \end{tikzcd}$$

Example 1.4 (Simple application of Theorem 1.4) – If $|G|$ and $|H|$ are coprime, then the only homomorphism $\varphi\colon G \to H$ is $\varphi \equiv e$.

Theorem 1.6 (Second isomorphism theorem)
Let G be a group and let N be a normal subgroup and K a subgroup. Then

$$KN/N \cong K/(K \cap N).$$

Remark 1.7. We have more implicit assumptions here: (1) $K \cap N$ is normal, (2) $KN = \{ab \mid a \in K, b \in N\}$ is a subgroup, (3) N is normal in KN (4) how we define the isomorphism.

(1) is easy to show. (2) is because $KNKN = KKNN = KN$ (using normal subgroup properties). Note that $KN = NK = \langle K \cup N \rangle =: K \vee N$.

Proof of Theorem 1.6 (sketch). We check that the group homomorphism $K \to G/N\colon a \mapsto a \cdot N$ has kernel $K \cap N$, and then prove that KN/N is the image. Then we apply Theorem 1.4 to finish. □

Theorem 1.8 (Third isomorphism theorem)
Given $H, K \trianglelefteq G$ and $K \subseteq H$,

$$G/H \cong (G/K)/(H/K).$$

Theorem 1.9 (Fourth isomorphism theorem)
Given $K \trianglelefteq G$, there is a bijection preserving normality

$$\begin{Bmatrix}\text{subgroups of}\\ G/K\end{Bmatrix} \xrightarrow{\sim} \begin{Bmatrix}\text{subgroups of}\\ G\text{ containing }K\end{Bmatrix}$$

$$\widetilde{H} \mapsto \pi^{-1}(\widetilde{H})$$

$$\pi(H) = H/K \leftarrow\!\shortmid H$$

Remark 1.10. Now that we are talking about isomorphisms, it is worth explaining that these notes will write "=" for isomorphism. Whenever this happens, we mean that there it is "natural" in some sense.

The idea is that these equalities will not require a choice of elements in the group (or rings, modules, etc. later). We could also explain this via the categorical language of natural transformations later.

1.3. Symmetric groups

September 09, 2024

Let $n \in \mathbb{N}$. The **symmetric group** S_n (or Σ_n) consists of all **permutations** $(f\colon \{1, \dots, n\} \to \{1, \dots, n\}$ such that f is bijective). A **cycle** of length k $(i_1 i_2 \cdots i_k)$ is a permutation such that $i_j \mapsto i_{j+1 \pmod k}$. A **transposition** is a cycle of length 2. Note that $|S_n| = n!$.

Lemma 1.11
Any $\sigma \in S_n$ can be written as the product of transpositions.

Definition 1.1

A permutation $\sigma \in S_n$ is called **even** if it can be written as a product of an even number of transpositions, and **odd** otherwise.

Theorem 1.12 (Even/odd is well defined)

Every permutation is even or odd, but not both.

If we assume the theorem is true, then we may define

$$\operatorname{sgn}(\sigma) := \begin{cases} -1 & \text{if } \sigma \text{ is odd,} \\ +1 & \text{if } \sigma \text{ is even.} \end{cases}$$

The map $\operatorname{sgn}\colon S_n \to (\{-1,+1\}, \cdot\,) \cong \mathbb{Z}/2$ is a group homomorphism. When $n > 1$, there are odd permutations, so sgn is surjective. Define

$$A_n := \ker(\operatorname{sgn}) \trianglelefteq S_n,$$

which we call the **alternating group**.

Given a permutation $\sigma \in S_n$, it will be helpful to use the following quantity: $\Delta(\sigma) = \prod_{j<k}(i_j - i_k)$. For example,

$$\Delta\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (2-1)(2-3)(1-3) = 2,$$

$$\Delta\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (2-3)(2-1)(3-1) = -2.$$

Proof of Theorem 1.12. Let

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$

Notice that for all $\sigma \in S_n$, $\Delta(\sigma)$ will be $\pm k$ for some fixed k (in particular, it is nonzero).

Claim 1.1. If δ is the transposition (cd) (with $c < d$), then

$$\Delta(\delta\sigma) = -\Delta(\sigma).$$

If we prove this claim, then we are done because $\Delta(\sigma) \neq 0$ and if σ were both even and odd, then we could write

$$\sigma = \tau_1 \cdots \tau_k = \tau'_1 \cdots \tau'_\ell$$

for k even and ℓ odd, then

$$\Delta(\sigma) = (-1)^k \Delta(\mathrm{id}), \qquad \Delta(\sigma) = (-1)^\ell \Delta(\mathrm{id}).$$

But this means $\Delta(\mathrm{id}) = -\Delta(\mathrm{id})$, which means $\Delta(\mathrm{id}) = 0$, which is a contradiction.

Proof of Claim 1.1. We have

$$\sigma\delta = \begin{pmatrix} 1 & \cdots & c & \cdots & d & \cdots & n \\ i_1 & \cdots & i_d & \cdots & i_c & \cdots & i_n \end{pmatrix}.$$

So

$$\Delta(\sigma) = \underbrace{\left(\prod_{\substack{j=c\\k=d}} (i_j - i_k)\right)}_{H} \underbrace{\left(\prod_{\substack{j\neq c\\k\neq d}} (i_j - i_k)\right)}_{A} \underbrace{\left(\prod_{\substack{j<c\\k=d}} (i_j - i_d)\right)}_{B} \underbrace{\left(\prod_{\substack{c<j<d\\k=d}} (i_j - i_d)\right)}_{C} \underbrace{\left(\prod_{\substack{j=c\\c<k<d}} (i_c - i_k)\right)}_{D}$$

$$\underbrace{\left(\prod_{\substack{j=c\\d<k}} (i_c - i_k)\right)}_{E} \underbrace{\left(\prod_{\substack{k=c\\j<k}} (i_j - i_c)\right)}_{F} \underbrace{\left(\prod_{\substack{j=d\\j<k}} (i_j - i_k)\right)}_{G}$$

$$= (-H)(A)(F)(1)^{d-c-1}D(-1)^{d-c-1}CGBE$$

$$= -ABCDEFGH.$$ ■

So we are finished. □

September 11, 2024 Another way to calculate $\operatorname{sgn}(\sigma)$ is to find the number of **inversions**:

$$\#\left\{(j,k) \mid j < k, i_j > i_k\right\}.$$

Then $\operatorname{sgn}(\sigma) = (-1)^{\#\{(j,k) \mid j<k, i_j>i_k\}}$.

Example 1.5 (Conjugation in S_n) – In the symmetric group, conjugation is something like "re-indexing." For example, considering $r = (25)(34)$ and $s = (12345)$ in S_5, we have that

$$rsr^{-1} = (15432),$$

because we changed $2 \to 5$, $3 \to 4$ in the labelling or s. This is because we expect rsr^{-1} to have the same properties as s.

Proposition 1.13

If $\sigma = (i_1 \cdots i_r) \in S_n$ and $\tau \in S_n$, then $\tau\sigma\tau^{-1}$ is the cycle

$$\begin{pmatrix} \tau(i_1) & \tau(i_2) & \cdots & \tau(i_n) \end{pmatrix}.$$

Definition 1.2

A group is **simple** if it has no non-trivial ($\{e\}$ and the group itself) normal subgroups.

Theorem 1.14

A_n is a simple group $\iff n \neq 4$.

1.4. Product of groups

We know what a product is, but it is worth getting an alternate perspective through the lens of abstract nonsense. In this case, we define the **product** $A \times B$ of sets to be a set with two **projection maps** $\pi_A : A \times B \to A$, $\pi_B : A \times B \to B$ satisfying the following **universal property**: given a set C and maps $f : C \to A$ and $g : C \to B$, there exists a unique map $h : C \to A \times B$ such that the following diagram commutes:

$$\begin{tikzcd}
C \arrow[rrd, bend left, "f"] \arrow[rd, dashed, "\exists ! h"] \arrow[rdd, bend right, "g"'] & & \\
& A \times B \arrow[r, "\pi_A"] \arrow[d, "\pi_B"] & A \\
& B &
\end{tikzcd}$$

We can use this same universal property to define the product of groups: $G \times H$. Instead of functions of sets, we use functions of groups: $G \times H$ is a group combined with projection homomorphisms $\pi_G : G \times H \times G$, $\pi_H : G \times H \to H$ such that for any group L with homomorphisms $f : L \to G$ and $g : L \to H$, there exists a unique homomorphism $k : L \to G \times H$ making the following diagram commute:

$$\begin{tikzcd}
L \arrow[rrd, bend left, "f"] \arrow[rd, dashed, "\exists ! k"] \arrow[rdd, bend right, "g"'] & & \\
& G \times H \arrow[r, "\pi_G"] \arrow[d, "\pi_H"] & G \\
& H &
\end{tikzcd}$$

We know how to explicitly construct $G \times H$: we let its underlying set be the set-theoretic product $G \times H$ with operation

$$(g, h)(g', h') = (gg', hh').$$

Exercise 1.1. Prove that $G \times H$ is a group (easy) and that $G \times H$ satisfies the universal property described above (slightly harder).

Exercise 1.2. Show that the product is unique up to isomorphism (in sets and groups). [Hint: Show that the proposed isomorphism h composed with its proposed inverse k satisfies $h \circ k = \mathrm{id}$ and $k \circ h = \mathrm{id}$. Use universal properties! If this is confusing now, it might become more clear in subsection 3.1]

Remark 1.15. Let $\mathcal{A}$ be an arbitrary (possibly uncountably infinite) indexing set. Recall that the arbitrary products of sets can be thought of as functions with a special property:

$$\prod_{\alpha \in \mathcal{A}} A_\alpha = \left\{ f : \mathcal{A} \to \bigcup_{\alpha \in \mathcal{A}} A_\alpha \mid f(\alpha) \in A_\alpha \right\}.$$

We can use universal properties to describe the arbitrary product of groups: $\prod_{\alpha \in \mathcal{A}} G_\alpha$.

1.5. Free groups

A "free" object conceptually represents an object without any relations (other than those given by the axioms of the object).

Let X be a set. A group F with a map (of sets) $X \to F$ is said to be a **free group on X** if[2], given any other group H with a map of sets $X \to H$, then there exists a unique homomorphism $F \to H$ such that the following diagram commutes:

$$\begin{tikzcd} X \arrow[r] \arrow[dr] & F \arrow[d, dashed, "\exists!"] \\ & H \end{tikzcd}$$

> **Example 1.6** (Free group on 1 element) – Let $X = \{1\}$. We claim the free group on X is $\mathbb{Z}$ with the map $X \to (\mathbb{Z}, +)$: $1 \mapsto 1$. We will prove it is universal. Suppose we have a group H with a map $\{1\} \to H$: $1 \mapsto h$. By constructing a map $\mathbb{Z} \to H$, we are forced to have $0 \mapsto 0_H$ and $1 \mapsto h$, $2 \mapsto h^2$, etc.

1.5.1. Explicit construction

September 16, 2024

Elements of the free group on a set X, $F = F(X)$ are strings (or **words**) of the form

$$g_1 \cdots g_n, \quad n \geq 0, g_i \in \{x \mid x \in X\} \cup \left\{x^{-1} \mid x \in X\right\}.$$[3]

$n = 0$ gives you the identity in F. If we want a unique representation for every word, we need **reduced words**, which never have x and x^{-1} adjacent. The group operation is concatenation:

$$(g_1 \cdots g_n) \cdot (g_1' \cdots g_m') = g_1 \cdots g_n g_1' \cdots g_m',$$

followed by reduction.

We have a second construction:

$$F = \left\{\text{strings } x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid x_i \in X, x_i \neq x_{i+1}, n \geq 0, \alpha_i \in \mathbb{Z} \setminus \{0\}\right\}.$$

> **Example 1.7** (Free group on 2 elements) – While $F(\{1\})$ was easy, F on a 2 element set is harder. Let $X = \{g, h\}$. Then
>
> $$F = \left\{\text{strings } x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \mid x_i \in X, x_i \neq x_{i+1}, n \geq 0, \alpha_i \in \mathbb{Z} \setminus \{0\}\right\}.$$

It's easy to check that this definition satisfies the group axioms, except associativity, because of the reduction after multiplication.

One can prove that F(X) satisfies the universal property we desired of the free group on X:

$$\begin{tikzcd} X \arrow[r, "\iota"] \arrow[dr, "f"'] & F(X) \arrow[d, dashed, "\overline{f}"] \\ & G \end{tikzcd}$$

We can imagine X goes into G to "represent" some elements of G. The elements in F(X) represent multiplying those elements of G together without the relationships between elements defined in G, and $\overline{f}$ means "adding" the relations in G.

Since the elements of X does not really matter, we may instead use the cardinality of X to describe a free group $F_{|X|}$, e.g., F_2.

[2] we could finish here by ending with "it is universal."

[3] x^{-1} is just a symbol (completely different from x) for now; it doesn't inherit and inverse structure from X if it was, e.g., a group.

Proposition 1.16
$\overline{f}$ is surjective $\iff \langle f(X) \rangle = G$.

Remark 1.17. It's worth noting the philosophy of the last two constructions: we started with a universal property of some sort and then created a set, group, etc. that satisfied this universal property. In the case of free groups, it was relatively easy to state the universal property, but hard to actually construct the group.

1.5.2. Relations

Example 1.8 – Let $X = \{A, B, C\}$, and $G = F(\{g, h\})$.

$$\begin{tikzcd} X \arrow[r] \arrow[dr, "f"] & F(X) \arrow[d, "\overline{f}"'] \\ & F(\{g,h\}) \end{tikzcd}$$

Suppose we send $A \mapsto ghg$, $B \mapsto g^2h^2g^2$, $C \mapsto g^3h^3g^3$. Then

$$\overline{f}(F(X)) = \left\langle ghg, g^2h^2g^2, \dots \right\rangle.$$

It turns out that $\ker \overline{f} = \{e\}$. This is counterintuitive because we have shown there is a copy of F_2 as a subgroup of F_3, but also there is a copy of F_3 as a subgroup of F_2. Moreover, one can show they are not isomorphic.

The relations on G leads to an isomorphism

$$G \cong F(X)/N,$$

for some normal subgroup N. Informally, N is "adding the relations" to $F(X)$.

Example 1.9 (Symmetric group) – Let $S_n = \langle (12), (12 \cdots n) \rangle$. Then we can think of some isomorphism

$$F_2/\text{some normal subgroup} \xrightarrow{\sim} S_2.$$

We know $(12)(12) = \text{id}$, so we would expect $(12)^2$ to be in the normal subgroup above.

September 18, 2024

Example 1.10 (Dihedral group) – Suppose $s, r \in D_{2n}$ represent $\frac{2\pi}{n}$ rotation and reflection respectively. D_{2n} is defined by the **defining relations** $s^n = e$, $r^2 = e$, $rsr = s^{-1}$. Let $Y = \left\{s^n = e, r^2 = e, rsr^{-1} = s^{-1}\right\}$. In this case, we get a quotient of the free group on s and r as

$$F(\{s, r\}) / \langle Y \rangle.$$

But $\langle Y \rangle$ is not necessarily normal. So instead we consider the **normal subgroup generated by** Y, which consists of conjugation of every element of Y by $g \in F(\{s, r\})$:

$$Y' := \left\langle gYg^{-1} \mid g \in F(\{s, r\}) \right\rangle.$$

Now let's prove that $F(\{s, r\})/Y'$ is isomorphic to D_n. It's easy to check that D_n is generated by $\{s, r\}$, and that the relations hold. But this doesn't show an isomorphism yet.

We know that we have a map

$$F(\{s,r\}) \to D_n$$

by the universal property of the free group. It's clear that the kernel of this map contains Y'. To show the other direction, we want to show that any relation in D_n between r and s is built out of relations in Y. This is more technical. To do this, we will show that there is a canonical form of elements in $F(\{s,r\})/Y'$ (note that $D_{2n} = \left\{r^\alpha s^\beta \mid \alpha = 0,1, \beta = 0,1,\dots,n-1\right\}$).

Consider an arbitrary element

$$r^{\alpha_1}s^{\beta_1}\cdots r^{\alpha_m}s^{\beta_m} \in F(\{s,r\}).$$

With $rs = s^{-1}r$, we can bring the r's to the left and get an element of the form

$$r^\alpha s^\beta.$$

Then we can use s^n and r^2 to show $\alpha = 0,1$ and $\beta = 0,1,\dots,n-1$.

Definition 1.3

Given a set X of **generators** and $Y \subseteq F(X)$ of **defining relations**, we may define a group

$$G = F(X)/\left\langle gYg^{-1} \mid g \in F(X)\right\rangle =: \langle X \mid Y\rangle .$$

September 20, 2024

Example 1.11 – Let $X = \{s_1,\dots,s_{n-1}\}$, where $s_i^2 = e$, $s_is_j = s_js_i$ unless $|i-j| = 1$, and $s_is_{i+1}s_i = s_{i+1}s_is_{i+1}$. It turns out this defines S_n by letting $s_i \mapsto \begin{pmatrix} i & i+1 \end{pmatrix}$. The first two properties are easy to check. The last property, the *braid relation*, is a little harder to check, but is still true.

Dropping the $s_i^2 = e$ relation, we get the *braid group*.

Theorem 1.18 (Universal property)

Given $X, Y \subseteq F(X)$, a group H, and a map $f\colon X \to H$ such that the relations Y are satisfied[1]. Then there exists a unique homomorphism $\bar{f}\colon F(X)/\left\langle gYg^{-1} \mid g \in F(X)\right\rangle \to H$ such that $\bar{f}(x) = f(x)$.

[1] Notice that f induces a map $F(X) \to H$. Then we say that the relations Y are satisfied if $Y \subseteq F(X)$ gets sent to the identity by this map.

Remark 1.19. Universal mapping properties determine a group (up to isomorphism). Details later.

1.6. Free products of groups

We would like to create a free group, but instead of a generating set X, we want it to be some groups, and allowing elements of the same group to interact as normal.

Theorem 1.20 (Universal property of free groups)
Let $\{G_i \mid i \in I\}$ be a family of groups. Let F be a group with a family of homomorphisms $\iota_i \colon G_i \to F$. Consider a family of homomorphisms $\psi_i \colon G_i \to H$ to some group H, then there exists a unique homomorphism $\psi \colon F \to H$ such that the following diagram commutes

$$\begin{tikzcd}
 & H \\
G_i \arrow[ur, "\psi_i"] \arrow[r, "\iota_i"'] & F \arrow[u, dashed, "\exists!\psi"']
\end{tikzcd}$$

for all $i \in I$. In other words, F is the coproduct in the category Grp.

For example, with two groups G and H, we have the following diagram:

$$\begin{tikzcd}
 & K & \\
G \arrow[ur, "\psi_1"] \arrow[r, "\iota_1"'] & F \arrow[u, dashed, "\exists!\psi"'] & H \arrow[ul, "\psi_2"'] \arrow[l, "\iota_2"]
\end{tikzcd}$$

This group F describes this "free group formed out of groups" structure we wanted at the beginning of this section.

Definition 1.4
Given two groups G, H, we have an operation called the **free product** $G * H$. We define it as

$$G * H = \{g_1h_1 \cdots g_nh_n \mid g_i \in G, h_i \in H, g_1, h_n \text{ can be } e, \text{the rest cannot}, n \geq 1\}.$$

Another way to think about $G * H$ is as the free group on $G \sqcup H$ mod the relations given by the group G and H. We also have

$$\langle X_1 \mid Y_1 \rangle * \langle X_2 \mid Y_2 \rangle = \langle X_1 \sqcup X_2 \mid Y_1 \cup Y_2 \rangle .$$

Compared to the direct product $G \times H$, $G * H$ would need to add the relations $gh = hg$ for $g \in G, h \in H$, so it is "larger."

2. Structure of groups

2.1. Structure of abelian groups

For general groups, there is a difference between *images* and *kernels* of maps. They correspond to subgroups and normal subgroups. A similar property happens for rings, giving us subrings and ideals. Importantly, in abelian groups, these concepts coincide, because all subgroups are normal.

Definition 2.1

The **free abelian group on X** is

$$F(X)^{ab} \coloneqq F(X)/\left\langle\left\langle xyx^{-1}y^{-1}\right\rangle\right\rangle.$$

$$F(X)^{ab} = \left\{\sum_{x\in X} a_x x \mid \text{all but finitely many}/\textit{almost all } a_x \text{ are } 0\right\} \subseteq \mathbb{Z}^X = \prod_{x\in X} \mathbb{Z}\cdot x.$$

Another way to write the second set above is with the **direct sum** instead of the direct product:

$$\bigoplus_{x\in X} \mathbb{Z}\cdot x = \mathbb{Z}^{\oplus X}.$$

Every abelian group G is isomorphic to

$$F(X)^{ab}/\text{some subgroup}.$$

This is a presentation by generators and relations.

Theorem 2.1 (Structure theorem of finitely generated abelian groups)

If G be a finitely generated abelian group, then

$$G \cong \mathbb{Z}^n/\left(\bigoplus_{i=1}^{n} r_i\mathbb{Z}\right), \qquad r_i \in \mathbb{Z}.$$

2.1.1. Subgroups of free abelian groups (of finite rank)

September 25, 2024

For the remainder of this section, “free group” refers to free *abelian* group. If G is any finitely generated abelian group, then choosing some finite set of generators $X \subseteq G$, we have a surjective homomorphism $\mathbb{Z}^{\oplus X} \twoheadrightarrow G$. This induces an isomorphism $\mathbb{Z}^{\oplus X}/H \xrightarrow{\sim} G$.

Theorem 2.2

For any subgroup $H \subseteq \mathbb{Z}^r$, there exists a basis of $\mathbb{Z}^r$, call it $(e_1, \dots, e_r)$ such that $H = \langle d_1e_1, \dots, d_re_r\rangle$, where $d_i \in \mathbb{Z}$, $d_i \geq 0$, and $d_1 \mid d_2 \mid \cdots \mid d_r$.

Corollary 2.3

With $H \leq \mathbb{Z}^r$ with the $d_1 \mid \cdots \mid d_r$ given by Theorem 2.2, we have

$$\mathbb{Z}^r/H \cong (\mathbb{Z}^{\oplus r})/(d_1\mathbb{Z} \oplus \cdots \oplus d_r\mathbb{Z}) \cong (\mathbb{Z}/d_1) \oplus \cdots \oplus (\mathbb{Z}/d_r).$$

Some of the d_k's can be zero (these will be at the end), in which case the last theorem has $\mathbb{Z}/0 \cong \mathbb{Z}$. Some of the d_k's can be 1 (these will be at the beginning), then we have $\mathbb{Z}/1 \cong \{e\}$.

Corollary 2.4

Any finitely generated abelian group is isomorphic to the product of cyclic groups.

Remark 2.5. Theorem 2.2 generalizes to finitely generated modules over a PID, so its proof should belong to the modules section.

We have by the Chinese remainder theorem, e.g., $\mathbb{Z}/2 \oplus \mathbb{Z}/3 \cong \mathbb{Z}/6$. So we can change the form given by Corollary 2.3.

Theorem 2.6

Any finitely generated abelian group is isomorphic to

1. (*invariant factors*) $(\mathbb{Z}/d_1) \oplus \cdots \oplus (\mathbb{Z}/d_k) \oplus \mathbb{Z}^f$. The first k parts of the sum are the *torsion group*, and $\mathbb{Z}^f$ is the *free* part. These are unique given $d_1 \mid \cdots \mid d_k$ and $d_i > 1$.
2. (*elementary divisors*) $\mathbb{Z}/p_1^{\alpha_1} \oplus \mathbb{Z}/p_2^{\alpha_2} \oplus \cdots \oplus \mathbb{Z}/p_m^{\alpha_m} \oplus \mathbb{Z}^f$, where p_i's are prime and $\alpha_i \geq 1$. This is unique up to reordering the $p_i^{\alpha_i}$'s.

September 27, 2024

Before we prove Theorem 2.2, we use the following fact:

Fact 2.7. Any basis of $\mathbb{Z}^r$ has r elements.

Corollary 2.8

Any subgroup of $\mathbb{Z}^r$ is free.

Proof of Theorem 2.2.

Lemma 2.9

Suppose $x \in \mathbb{Z}^r$ is primitive.[1] Then $\mathbb{Z}^r$ has a basis $\widetilde{e_1}, \dots, \widetilde{e_r}$ with $\widetilde{e_1} = x$.

[1] i.e. if $x = (a_1, \dots, a_r)$, then $\gcd(a_1, \dots, a_r) = 1$. Equivalently, $x \notin d \cdot \mathbb{Z}^r$ for any $d > 1$

Proof. Start with $x = \sum_i a_i e_i$, where e_i is the standard basis of $\mathbb{Z}^r$. Consider the operations (1) $e_i \mapsto -e_i$, and (2) given $i \neq j$, $e_i \mapsto e_i + e_j$.

In terms of coefficients, (1) sends $a_i \mapsto -a_i$, and (2) sends $a_j \mapsto a_j - a_i$. Algorithmically, we can subtract smaller numbers from larger numbers until all but one a_i vanish. Since x is primitive, $a_1 = 1, a_2 = \cdots = a_n = 0$. ■

Note that any $x = (a_1, \dots, a_r)$ can be written as $d \cdot x'$, where $d = \gcd(a_1, \dots, a_r)$ and x' is primitive.

Lemma 2.10

Suppose $x = d \cdot x'$ for $d > 0$, x' primitive. Given $y \notin d\mathbb{Z}^r$. Then there exists $a, b \in \mathbb{Z}$ and $z = ax + by$ such that $z = \widetilde{d} \cdot z'$ for a primitive z', and $0 < \widetilde{d} < d$.

Proof. Use Lemma 2.9 to change the basis so that $x' = (1, 0, \ldots, 0)$ and $x = d \cdot x' = (d, 0, \ldots, 0)$. Hence, there exists $a \in \mathbb{Z}$ such that $y + ax = (z_1, \ldots, z_r)$ for $z_1 \in \{1, \ldots, d\}$. We have

$$\gcd(z_1, \ldots, z_r) \leq z_1 \leq d.$$

If $z_1 \neq d$, we are done. If $z_1 = d$, then since $y \notin d\mathbb{Z}^r$, there is some entry that makes $\gcd(z_1, \ldots, z_r) \neq d$. ■

Take $x \in H \setminus \{0\}$. Write it as $x = d \cdot x'$ for primitive x'. Either $H \subseteq d\mathbb{Z}^r$, or, by Lemma 2.10, there exists $\widetilde{x} \in H \setminus \{0\}$ where $\widetilde{x} = \widetilde{d} \cdot \widetilde{x}'$ for primitive $\widetilde{x}'$ and $\widetilde{d} < d$. Repeat this until we find $x = d \cdot x'$ such that $H \subseteq d\mathbb{Z}^r$. Form a basis $e_1 = x', e_2, \ldots, e_r$ of $\mathbb{Z}^r$ by Lemma 2.9. In this basis, $H \ni (d, 0, \ldots, 0) = x$. Every element of H is of the form

$$ax + d(0, b_2, \ldots, b_r).$$

Consider

$$\{(b_2, \ldots, b_r) \mid (0, db_2, \ldots, db_r) \in H\} \subseteq \mathbb{Z}^{r-1}$$

and continue inductively.[2] □

[2] What we did here was show that $H = d\mathbb{Z} \oplus H'$, where H' is some subgroup of $\mathbb{Z}^{r-1}$.

2.2. Group actions on a set

We now pivot to arbitrary finite groups. The main tool we will use is group actions.

Definition 2.2

September 30, 2024

Let G be a group. A **(left) action** of G on a set X is a map

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

satisfying

$$\begin{aligned} e \cdot x &= x \\ (g_1 g_2) \cdot x &= g_1 \cdot (g_2 \cdot x). \end{aligned}$$

We write $G \curvearrowright X$. A set that G acts on is called a **G-set**.[1]

[1] G-sets are to a group G as R-modules are to a ring R.

Example 2.1 –

1. G acts on itself: $X = G$ and $g \cdot x = gx$.
2. G acts on any set trivially: $g \cdot x = x$ for all $g \in G$ and $x \in X$
3. G acts on itself on the right:

$$g \cdot x = xg^{-1}$$

(we need the inverse for this to remain as an action).

4. $G \times G$ acts on G with a *two-sided action*:
$$(g,h) \cdot x = gxh^{-1}.$$

5. G acts on itself by conjugation:
$$g \cdot x = gxg^{-1}.$$
This action is special because it preserves the group operations: $(gxg^{-1})(gyg^{-1}) = gxyg^{-1}$.

6. $S_n \curvearrowright \{1, \ldots, n\}$ by permuting the set. This example is particularly useful to think about because it says that any action of a group on a set can also be viewed as an action of the symmetric group on that set.

7. $GL_n(k) \curvearrowright k^n$ by applying matrices in $GL_n(k)$ to vectors in k^n.

Here are some equivalent ways to view group actions. Given $G \times X \to X$, consider $\alpha_g \colon X \to X \colon x \mapsto g \cdot x$, where $g \in G$ is fixed. We may rewrite the definition of a group action as $\alpha_e = \mathrm{id}_X$ and $\alpha_{g_1} \circ \alpha_{g_2} = \alpha_{g_1 g_2}$. These two properties implies $\alpha_{g^{-1}} = (\alpha_g)^{-1}$, which implies that all α_g are bijective.

Given a set X, consider
$$\mathrm{Aut}(X) = \{\varphi \colon X \to X \mid \varphi \text{ is bijective}\},$$
which is a group under composition.

Example 2.2 – If $X = \{1, \ldots, n\}$, then $\mathrm{Aut}(X)$ is the symmetric group.

Then an action $G \curvearrowright X$ is equivalent to a homomorphism
$$\begin{aligned} \alpha_\bullet \colon G &\to \mathrm{Aut}(X) \\ \colon g &\mapsto \alpha_g. \end{aligned}$$

It follows that $\mathrm{Aut}(X)$ is the "universal group," that acts on X; any other group that acts on X must factor through $\mathrm{Aut}(X)$'s action on X.

Given $G \curvearrowright X$, define a relation $\sim$ on X by $x_1 \sim x_2$ if there exists a $g \in G$ such that $g \cdot x_1 = x_2$. We call the equivalence classes **G-orbits**, and let $X/\sim$ be X/G (or $G \backslash X$ if we want to make it clear that $G \curvearrowright X$ is a left action).

Example 2.3 –

1. Let $H \leq G$ act on G on the right. Then G/H is the set of right cosets.

2. $k^n/GL_n(k)$ by the action described in the last example has two orbits: the orbit of any nonzero vector, and the orbit of the zero vector.

Given $G \curvearrowright X$, fix $x \in X$ and consider the map
$$\varphi_x \colon G \to X \colon g \mapsto g \cdot x.$$

Notice that $\varphi_x(G) = G \cdot x$ is the orbit of x. Moreover, $\varphi^{-1}(x) = \{g \in G \mid g \cdot x = x\}$ are the group elements that fix x, and this is a subgroup of G. We call it the **stabilizer** of x, and we denote it $G_x = \mathrm{Stab}_G(x)$.

More generally, it only makes sense to look at $\varphi^{-1}(x')$ for $x' \in G \cdot x$.

Claim 2.1. $\varphi^{-1}(x') = gG_x$ for some $g \in G$. In other words, $G \cdot x \cong G/G_x$.

Example 2.4 – Let $S_n \curvearrowright \{1, \ldots, n\}$ by permutation. Let $x = n$. Then the orbit of x is $\{1, \ldots, n\}$ (if this holds for all x, then the action is **transitive**). We can identify the stabilizer of x with S_{n-1} (permuting everything except n). Then the above claim says that

$$S_n/S_{n-1} = \{1, \ldots, n\}.$$

October 2, 2024

Example 2.5 – Let $n = n_1 + \cdots + n_k$ with $n_i > 0$. We may identify $S_{n_1} \times \cdots \times S_{n_k}$ with a subgroup of S_n that permutes the first n_1 elements, then the next n_2 elements, and so on. Then taking the quotient of this action

$$S_n/S_{n_1} \times \cdots \times S_{n_k}$$

makes sense. This is identified with all partitions of $\{1, \ldots, n\}$ into subsets of size $n_1, n_2, \ldots, n_k$.

Example 2.6 – The subgroup $H \le GL_2(\mathbb{R})$ of upper triangular matrices fix the x-axis. Any other matrix changes the x-axis to another line that passes through the origin.

2.3. Sylow's theorems

For this section, let p be a prime. Sylow's theorems are about the existence of p-subgroups of a group G. Recall that a **p-(sub)group** is a group where all elements have order p^k for $k \ge 0$.

Lemma 2.11

If $|G| = p^n$ and $G \curvearrowright X$ for some $|X| < \infty$, then

$$\left|X^G\right| \equiv |X| \pmod p,$$

where $X^G := \{x \in X \mid g \cdot x = x, \forall g \in G\}$ is the set of **fixed points** of the action.

Proof. Let $G \cdot x_1, \ldots, G \cdot x_k$ be the orbits of the action. We may write

$$X = \bigsqcup_{i=1}^{k} G \cdot x_i.$$

Notice that $G \cdot x_i = \{x_i\}$ is equivalent to x_i being a fixed point. So we may rewrite this disjoint union as

$$X = X^G \sqcup \bigsqcup_{i=1}^{\ell} G \cdot x_i',$$

where x_i' are orbit representatives such that $|G \cdot x_i'| > 1$. Since $|G \cdot x_i'| = [G : G_{x_i'}] > 1$ and

$|G| = p^n$, $|G \cdot x_i'|$ is a positive power of p. So

$$|X| = |X^G| + \sum_{i=1}^{\ell} |G \cdot x_i'| \equiv |X^G| \pmod{p}. \qquad \blacksquare$$

We may rewrite the equation

$$|X| = |X^G| + \sum_{i=1}^{\ell} |G \cdot x_i'|$$

as

$$|X| = |X^G| + \sum_{i=1}^{\ell} [G : G_{x_i'}]. \tag{2.1}$$

Proposition 2.12

If $|G| = p^n$ and $G \neq \{e\}$, then the center of G is nontrivial.

Proof (sketch). Use the class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{\ell} [G : C_G(x_i)],$$

where x_i are representatives for the conjugacy classes of G (this is derived from letting $G \curvearrowright G$ by conjugation and plugging things into Equation 2.1). Then reduce modulo p. □

October 07, 2024

Corollary 2.13

If $|G| = p^n$, then for every $k = 0, \ldots, n$, there exists $H \trianglelefteq G$ such that $|H| = p^k$.

Proof. $Z(G)$ is abelian, so the structure theorem gives us that it has a subgroup H of order p. Consider G/H (since $H \subseteq Z(G)$ it is normal in G). It has order p^{n-1}, so we may find another subgroup of order p. Suppose it is generated by xH. Then $|\langle x, H\rangle| = p^2$. Continue this process inductively to finish the proof. □

Theorem 2.14 (Cauchy)

If $p \mid |G|$, there exists $x \in G$ such that $x^p = e$ and $x \neq e$.

Remark 2.15. The converse to Lagrange's theorem (every element of a finite group has order dividing the order of a group) is not generally true, but Cauchy's theorem gives a partial converse.

Proof of Theorem 2.14. Consider $X = \{(x_1, \ldots, x_p) \in G^p \mid x_1 \cdots x_p = e\}$. Notice that

$$x_1 \cdots x_p = e \implies x_1^{-1} x_1 \cdots x_p x_1 = x_2 \cdots x_p x_1 = x_1^{-1} x_1 = e,$$

so our set is closed under cyclic permutations. So $\mathbb{Z}/p \curvearrowright X$, which means $|X^{\mathbb{Z}/p}| \equiv |X|$

(mod p). Hence, $X^{\mathbb{Z}/p} = \{x \mid x^p = e\}$, and $|X| = |G|^{p-1}$ (we choose $x_1, \ldots, x_{p-1}$ and then x_p is forced). This implies that $X^{\mathbb{Z}/p}$ contains more than just e. □

Corollary 2.16

A finite group is a p-group if and only if the order of any element is a power of p.

Definition 2.3

Let G be a finite group. Suppose $|G| = p^k m$, where $p \nmid m$. A **Sylow p-subgroup** of G is a subgroup of order p^k (equivalently, a p-subgroup such that p does not divide its index in G).

Theorem 2.17 (First Sylow theorem)

Sylow's p-subgroups of G exist (where $p \mid |G|$). Moreover, if $H \leq G$ and H is a p group that is not maximal, i.e. $p \mid [G : H]$, then there exists $H' \trianglerighteq H$ such that $|H'| = p|H|$.

Proof. Start with $H \leq G$ such that $|H| = p$ (this is by Theorem 2.14).

Claim 2.2. If $H \leq G$ is a p-subgroup and $p \mid [G : H]$, then there exists a larger p-subgroup H' strictly containing H that is also a p-subgroup.

Consider $H \curvearrowright G/H$ by left multiplication. Since p divides the order of both H and G/H,

$$\left|(G/H)^H\right| \equiv 0 \pmod{p}.$$

Let $N_G(H) = \{g \mid gHg^{-1} = H\}$. We have that $(G/H)^H = N_G(H)/H$. So $p \mid [N_G(H) : H]$. $N_G(H)/H$ is a group by construction, and Theorem 2.14 gives us an element $x \in N_G(H)/H$ with order p, which corresponds to a subgroup H' of $N_G(H)$ that is larger than H. □

In this proof, we also showed that

$$[G : H] = [N_G(H) : H] \pmod{p}.$$

Theorem 2.18 (Second Sylow theorem)

All Sylow p-subgroups of G are conjugate. In particular, they are all isomorphic to each other. If $H \leq G$ is a Sylow p-subgroup and $H' \leq G$ is any p-subgroup, then there exists $g \in G$ such that $gH'g^{-1} \subseteq H$.

Proof. Let $H' \curvearrowright G/H$ by $h' \cdot gH = h'gH$. Then

$$\left|(G/H)^{H'}\right| \equiv |G/H| \pmod{p}.$$

Since $p \nmid [G : H]$,

$$(G/H)^{H'} \neq \varnothing,$$

i.e., there exists $g \in G$ such that $H'gH \subseteq gH \implies H'g \subseteq gH \implies H' \subseteq gHg^{-1} \implies$

$g^{-1}H'g \subseteq H$. □

Theorem 2.19 (Third Sylow theorem)
Let S be the number of Sylow p-subgroups in G. Then

1. $S \mid |G|$,
2. $S \equiv 1 \pmod p$.

October 9, 2024 **Example 2.7** (All groups of order 15 are cyclic) – Let $|G| = 15$. By Theorem 2.17, there exist subgroups H_3 and H_5 of order 3 and 5 respectively. Suppose they are generated by a and b respectively (since they are both cyclic). Theorem 2.19 gives that H_3 and H_5 are the only Sylow subgroups in G. Theorem 2.18 gives that H_3 and H_5 are normal.

Recall that if $H, H' \trianglelefteq G$ satisfy $H \cap H' = \{e\}$ and $HH' = G$, then $G \cong H \times H'$. So $G \cong \mathbb{Z}/3 \times \mathbb{Z}/5$.

2.4. Semidirect products

Let $N, H \subseteq G$ such that $N \cap H = \{e\}$ and $NH = G$, where N is normal and H is any subgroup. The condition $NH = G$ gives that each coset in G/N has a representative in H. The condition $N \cap H = \{e\}$ gives that this representative is unique. So we may write any $g \in G$ uniquely as nh for $n \in N$, $h \in H$. We define the product as

$$(n_1h_1)(n_2h_2) = n_1(h_1n_1h_1^{-1})h_1h_2,$$

so the product is known once we know how H acts on N by conjugation.

G acts on N by conjugation, so we have a homomorphism

$$\varphi\colon G \to \operatorname{Aut}(N),$$

which we may restrict to H by

$$\begin{aligned}\varphi\big|_H\colon H \hookrightarrow G &\to \operatorname{Aut}(N)\colon\\ h &\mapsto \left[n \mapsto hnh^{-1}\right].\end{aligned}$$

This determines G because we may rewrite the previous product as

$$(n_1h_1)(n_2h_2) = n_1(\varphi(h_1)(n_2))h_1h_2.$$

This is the **semidirect product** of H and N. The former construction was the *inner* semidirect product, and the latter was the *outer* semidirect product. We denote this as $G \cong H \ltimes_\varphi N$.

October 11, 2024 In the language of free groups,

$$H \ltimes_\varphi N \cong H * N / \left\{\text{normal subgroup generated by } h_2^{-1}h_2^{-1}(\varphi(h_1)(n_2))h_1\right\}$$

2.5. Structure of finite groups

Recall that a non-trivial group G is *simple* if its only normal subgroups are G and $\{e\}$.

Example 2.8 – If G is abelian, G is simple if and only if $G \cong \mathbb{Z}/p$ for prime p.

Theorem 2.20
Finite simple groups are classified.

- There are 18 infinite collections of groups, e.g.,
  - $\mathbb{Z}/p$ where p is prime,
  - A_n, where $n \geq 5$.
- There are 26 *sporadic groups* that don't fit into these 18 collections.

We'll introduce two theorems useful for working with finite groups, the *Jordan-Hölder theorem* and the *Krull-Schmidt theorem*, but we will not prove them.

Definition 2.4
Let G be a finite group. A **composition series** of G is a chain

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_k = \{e\}$$

such that G_{i+1} is normal in G_i (recall that "is a normal subgroup of" is not transitive, so when we write $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_k = \{e\}$, it only says that G_{i+1} is normal in G_i) and G_i/G_{i+1} is simple. We call the quotients $G_0/G_1, G_1/G_2, \ldots, G_{k-1}/G_k$ the **simple factors** of G.

Fact 2.21. For any finite group G, a composition series exists.

Theorem 2.22 (Jordan-Hölder)
Any two composition series of the same group G have isomorphic simple factors (up to reordering).

In particular, if all G_i/G_{i+1} in the composition series of G are abelian, then G is **solvable**.

October 14, 2024

Definition 2.5
A group G is **indecomposable** if whenever $G \cong G_1 \times G_2$ for some groups G_1, G_2, either $G_1 = \{e\}$ or $G_2 = \{e\}$.

Example 2.9 – The indecomposable abelian groups are $\mathbb{Z}/p^n\mathbb{Z}$ for prime p and $n \geq 1$.

Fact 2.23. Any finite group G can be written as the product $G \cong G_1 \times \cdots \times G_\ell$ for indecomposable groups G_i.

Theorem 2.24 (Krull-Schmidt)
Any two such presentations have the same number of indecomposable groups and the groups are unique up to permutation (and isomorphism).

Remark 2.25. Theorem 2.22 and Theorem 2.24 hold for weaker conditions; namely that G need not be finite, it just needs to satisfy the *ascending* and *descending chain conditions*. These are statements about the finiteness of a series. The descending chain condition is that for $\{G_i \mid G_i \trianglelefteq G\}$,

$$G_1 \trianglerighteq G_2 \trianglerighteq \cdots$$

eventually has $G_i = G_{i+1}$ for all $i \geq n$ (*stabilizes*). The ascending chain condition is the same but for

$$G_1 \trianglelefteq G_2 \trianglelefteq \cdots$$

We'll see more about this in 742.

Example 2.10 – $\mathbb{Z}$ satisfies the ascending chain condition but not the descending chain condition.

3. Category theory

Definition 3.1

A **category** $\mathscr{C}$ consists of

1. A class of **objects** $\mathrm{Ob}(\mathscr{C})$.
2. For any objects $A, B \in \mathrm{Ob}(\mathscr{C})$, there is a set $\mathrm{Mor}_{\mathscr{C}}(A, B)$ of **morphisms** from A to B.
3. For any $A, B, C \in \mathrm{Ob}(\mathscr{C})$, there is an operation of **composition**

$$\begin{aligned} \circ\colon \mathrm{Mor}_{\mathscr{C}}(B, C) \times \mathrm{Mor}_{\mathscr{C}}(A, B) &\to \mathrm{Mor}_{\mathscr{C}}(A, C) \\ (\varphi, \psi) &\mapsto \varphi \circ \psi. \end{aligned}$$

The composition operation must satisfy

a) For all $A \in \mathrm{Ob}(\mathscr{C})$, there exists an **identity morphism** $\mathrm{id}_A \in \mathrm{Mor}_{\mathscr{C}}(A, A)$ such that $\varphi \circ \mathrm{id}_A = \varphi$ and $\mathrm{id}_A \circ \psi = \psi$ (φ and ψ are chosen so that these compositions make sense).

b) Given φ, ψ, θ (whose compositions below make sense), we have

$$(\varphi \circ \psi) \circ \theta = \varphi \circ (\psi \circ \theta).$$

October 16, 2024

Example 3.1 – Groups form a category, where objects are groups and morphisms are group homomorphisms with composition being defined as expected.

Moreover, abelian groups, rings, and sets form a group with morphisms being the usual homomorphisms.

When a category's objects are sets (possibly with extra structure) and $\mathrm{Mor}(A, B) \subseteq \mathrm{Mor}_{\mathsf{Set}}(A, B)$, i.e. morphisms happen to be set-theoretic functions, we say the category is **concrete**.

For every $X \in \mathscr{C}$ (this means $X \in \mathrm{Ob}(\mathscr{C})$), $\mathrm{id}_X \in \mathrm{Mor}_{\mathscr{C}}(X, X)$ is unique.

Definition 3.2

$\varphi \in \mathrm{Mor}_{\mathscr{C}}(X, Y)$ is an **isomorphism** if there exists $\psi \in \mathrm{Mor}_{\mathscr{C}}(Y, X)$ such that $\psi \circ \varphi = \mathrm{id}_X$ and $\varphi \circ \psi = \mathrm{id}_Y$.

3.1. Universal properties

October 18, 2024

Example 3.2 – Let $A, B \in \mathscr{C}$. Given $C \in \mathscr{C}$ and two morphisms $p_1\colon C \to A$ and $p_2\colon C \to B$, we say that C (along with the morphisms p_1 and p_2) is the **(direct) product** of A and B if the following *universal property* holds: given any $C' \in \mathscr{C}$ and any $p_1'\colon C' \to A$ and $p_2'\colon C' \to B$, there exists a unique morphism $\varphi\colon C' \to C$ such that $p_1' = p_1 \circ \varphi$, $p_2' = p_2 \circ \varphi$.

In a picture:

$$\begin{tikzcd}
C' \arrow[drr, bend left, "p_1'"] \arrow[dr, dashed, "\exists!\varphi"'] \arrow[ddr, bend right, "p_2'"'] & & \\
& C \arrow[r, "p_1"'] \arrow[d, "p_2"] & A \\
& B &
\end{tikzcd}$$

The black part is a direct product if for any given orange part, there is a unique blue part making the diagram commute.

Definition 3.3

Let $\mathcal{C}$ be a category and $\{A_i\}_{i \in I}$ be a family of objects. Their **product** is an object $C \in \mathcal{C}$ equipped with maps $p_i \colon C \to A_i$ (for all $i \in I$) such that for any $C' \in \mathcal{C}$ and any maps $p_i' \colon C' \to A_i$, there exists a unique $\varphi \colon C' \to C$ such that $p_i' = p_i \circ \varphi$ for all i.

Theorem 3.1

In any category $\mathscr{C}$ if a product exists, it is unique up to unique isomorphism.

Because of this, we write $C = \prod_{i \in I} A_i$.
We can take the "dual" of the product by reversing the arrows in the category.

Example 3.3 – Let $A, B \in \mathscr{C}$. Given $C \in \mathscr{C}$ and two morphisms $i_1 : A \to C$ and $i_2 : B \to C$, we say that C (along with the morphisms i_1 and i_2) is the **(direct) coproduct** A and B if the following universal property holds: given any $C' \in \mathscr{C}$ and any $i_1' : A \to C'$ and $i_2' : B \to C'$, there exists a unique morphism $\varphi \colon C \to C'$ such that $i_1' = \varphi \circ i_1, i_2' = \varphi \circ i_2$.
In a picture:

$$\begin{tikzcd}
C' & & \\
& C \arrow[ul, dashed, "\exists!\varphi"'] & A \arrow[l, "i_1"'] \arrow[ull, bend right, "i_1'"'] \\
& B \arrow[u, "i_2"] \arrow[uul, bend left, "i_2'"] &
\end{tikzcd}$$

Definition 3.4

Let $\mathcal{C}$ be a category and $\{A_i\}_{i \in I}$ be a family of objects. Their **coproduct** is an object $C \in \mathcal{C}$ equipped with maps $i_j \colon A_j \to C$ (for all $j \in I$) such that for any $C' \in \mathcal{C}$ and any maps $i_j' \colon A_j \to C'$, there exists a unique $\varphi \colon C \to C'$ such that $i_j' = \varphi \circ i_j$ for all i.

Theorem 3.2

In any category $\mathscr{C}$ if a coproduct exists, it is unique up to unique isomorphism.

Because of this, we write $C = \coprod_{i \in I} A_i$.

Example 3.4 – In Set, the product of sets A, B is the usual cartesian product $A \times B$. The coproduct is the disjoint union $A \sqcup B$.

In Grp, the coproduct is the free product.

In AbGrp, the product and the coproduct are $A \times B$.

Definition 3.5

October 21, 2024

Given a category $\mathscr{C}$, we define the **opposite category**, denoted $\mathscr{C}^{\mathrm{op}}$ as $\mathscr{C}$ with arrows reversed. In other words, $\mathrm{Ob}(\mathscr{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathscr{C})$, $\mathrm{Mor}_{\mathscr{C}^{\mathrm{op}}}(A, B) = \mathrm{Mor}_{\mathscr{C}}(B, A)$. We compose morphisms as follows: given $\varphi \in \mathrm{Mor}_{\mathscr{C}^{\mathrm{op}}}(A, B)$ and $\psi \in \mathrm{Mor}_{\mathscr{C}^{\mathrm{op}}}(B, C)$, we define $\psi \circ \varphi \in \mathrm{Mor}_{\mathscr{C}}(C, A) = \mathrm{Mor}_{\mathscr{C}^{\mathrm{op}}}(A, C)$

So we can say that if some object is a product in the opposite category, then it is the coproduct in the original category, since the arrows in the diagram would be reversed.

3.2. Functors

Definition 3.6

Given categories $\mathscr{C}$ and $\mathscr{D}$, a **functor** $F \colon \mathscr{C} \to \mathscr{D}$ is

1. A map $F \colon \mathrm{Ob}(\mathscr{C}) \to \mathrm{Ob}(\mathscr{D}) \colon A \mapsto F(A)$,
2. For all $A, B \in \mathscr{C}$ and $\varphi \in \mathrm{Mor}_{\mathscr{C}}(A, B)$, we have corresponding morphism $F(\varphi) \in \mathrm{Mor}_{\mathscr{D}}(F(A), F(B))$. In other words we have a map $\mathrm{Mor}_{\mathscr{C}}(A, B) \to \mathrm{Mor}_{\mathscr{D}}(F(A), F(B))$. F needs to satisfy
   a) $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$,
   b) $F(\varphi \circ \psi) = F(\varphi) \circ F(\psi)$.

Example 3.5 –

- We have the identity functor $\mathrm{id}_{\mathscr{C}} \colon \mathscr{C} \to \mathscr{C}$.
- Another functor is $\mathrm{id} \colon \mathrm{AbGrp} \to \mathrm{Grp}$, since abelian groups and their homomorphisms are, in particular, groups and group homomorphisms respectively. This example is saying that AbGrp is a **subcategory** of Grp.
- Consider a functor $\mathrm{Tors} \colon \mathrm{AbGrp} \to \mathrm{AbGrp}$ given by sending A to its torsion subgroup, $A^{\mathrm{tors}} := \{x \in A \mid x^n = 1 \text{ for some } n < \infty\}$. The functor sends a morphism from $A \to B$ to its restriction $A^{\mathrm{tors}} \to B^{\mathrm{tors}}$ (it's easy to check this is a well-defined map).
- In general, the torsion elements of a general group do not form a group. But we still have a functor $\mathrm{Tors} \colon \mathrm{Grp} \to \mathrm{Set}$.

Example 3.6 (Free and forgetful functors) –

- The **free functor** $F \colon \mathrm{Set} \to \mathrm{Grp}$ that sends a set X to the free group on X, $F(X)$.
- The **forgetful functor** $G \colon \mathrm{Grp} \to \mathrm{Set}$ that sends a group H to its underlying set, and homomorphisms to set-theoretic maps.

October 23, 2024 A more interesting thing we would want to define as a functor is how, say, group homomorphisms

$$G_1 \to G_1', \quad G_2 \to G_2'$$

induce a homomorphism $G_1 \times G_2 \to G_1' \times G_2'$. But functors don't take in two inputs. We can resolve this easily.

Definition 3.7

Given categories $\mathscr{C}, \mathscr{D}$, define the **product category**, $\mathscr{C} \times \mathscr{D}$ where

1. $\mathrm{Ob}(\mathscr{C} \times \mathscr{D}) = \mathrm{Ob}(\mathscr{C}) \times \mathrm{Ob}(\mathscr{D})$.
2. For $(C_1, D_1), (C_2, D_2) \in \mathscr{C} \times \mathscr{D}$, let

$$\mathrm{Mor}_{\mathscr{C} \times \mathscr{D}}((C_1, D_1), (C_2, D_2)) \coloneqq \mathrm{Mor}_{\mathscr{C}}(C_1, C_2) \times \mathrm{Mor}_{\mathscr{D}}(D_1, D_2).$$

3. Composition is given by composition in each category (i.e., $(\varphi_1, \psi_1) \circ (\varphi_2, \psi_2) = (\varphi_1 \circ \varphi_2, \psi_1 \circ \psi_2)$).

Example 3.7 – Now our product operation defined before is the same as a functor

$$F\colon \mathsf{Grp} \times \mathsf{Grp} \to \mathsf{Grp}.$$

Example 3.8 (Quotients by subgroups) – For any group G and any subgroup $H \leq G$, we have a quotient G/H, which is a set. Let's represent this operation as a functor.

The starting category will be SubGrp, whose objects are pairs $(G \supseteq H)$, where G is a group and H is a subgroup of G. The morphisms $(G_1 \supseteq H_1) \to (G_2 \supseteq H_2)$ are given by

$$\mathrm{Mor}_{\mathsf{SubGrp}}((G_1 \supseteq H_1), (G_2 \supseteq H_2)) \coloneqq \{\varphi\colon G_1 \to G_2 \mid \varphi(H_1) \subseteq H_2\}.$$

We then have a functor

$$Q\colon \mathsf{SubGrp} \to \mathsf{Set}$$

that sends $(G \supseteq H)$ to G/H (and morphisms are the induced ones).

October 25, 2024 **Example 3.9** – Consider a direct sum functor $F\colon \mathsf{AbGrp} \times \mathsf{AbGrp} \to \mathsf{AbGrp}$ that sends (A, B) to $A \oplus B$ (with the obvious morphisms), and another direct sum functor $G\colon \mathsf{AbGrp} \times \mathsf{AbGrp} \to \mathsf{AbGrp}$ that sends (A, B) to $B \oplus A$. Then F is naturally isomorphic to G.

4. Representation theory

November 20, 2024

Definition 4.1

Given a group G and a vector space V over a field k, a **representation of G** on V is a **linear action** of G on V, i.e., $G \times V \to V\colon (g, v) \mapsto g \cdot v$ is a group action, and $g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2$, $g \cdot (cv) = c(g \cdot v)$.

If V is finite-dimensional, we can choose a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V. For each $g \in G$, we have a map $\rho(g)\colon V \to V\colon v \mapsto g \cdot v$, which corresponds to a matrix $R_g := \mathcal{M}^{\mathcal{B}}_{\mathcal{B}}(\rho(g))$.

Because $G \curvearrowright V$ is an action, R_g is invertible for all $g \in G$, and $R_{g_1} R_{g_2} = R_{g_1 g_2}$, $R_e = I$. So we have a homomorphism

$$\rho\colon G \to GL_n(k),$$

which we call a **matrix representation of G**.

Example 4.1 – D_n is the symmetries of a regular n-gon, so we can think of its representation $D_n \to GL_2(\mathbb{R})$. The matrix representation of the generators of D_n are

$$r \mapsto \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}, \qquad s \mapsto \begin{bmatrix} -1 & \\ & 1 \end{bmatrix}.$$

November 22, 2024

Example 4.2 – If $G \curvearrowright X$, we can form a representation of G by letting $V = \langle X \rangle$ be the free vector space on X.[1] Since $g \in G$ permutes the elements of X, we can create a corresponding automorphism of V by permuting the basis elements in the same way. This corresponds to a linear transformation. If X is finite, the matrix representation is written as a permutation matrix.

Let's consider $S_n \curvearrowright \{1, \dots, n\}$. Then

$$\underbrace{\rho(\sigma)}_{\in GL_n}(a_1, \dots, a_n) = (a_{\sigma^{-1}(1)}, \dots, a_{\sigma^{-1}(n)}).$$

[1] This means the vector space where we make X a basis.

Here's an equivalent formulation. Let X be a set with a group action $G \curvearrowright X$, and $V = \{f\colon X \to k\}$, a k-vector space. Then a representation is a group homomorphism $\rho\colon G \to GL(V)$ such that

$$(\rho(g)f)(x) = f(g^{-1} \cdot x).$$

The inverse is here to make sure $\rho(g_1)\rho(g_2) = \rho(g_1 g_2)$.

Remark 4.1. A representation of G on V is also a homomorphism $\rho\colon G \to \mathrm{Aut}_{\mathsf{Vect}_k}(V)$. More functorially, if we create the category BG with one object $*$ and $\mathrm{Hom}_{BG}(*, *) = G$ (with composition given by group multiplication), a representation is a functor $F\colon BG \to \mathsf{Vect}_k$. The example given above was a *contravariant* functor $\mathsf{Sets} \to \mathsf{Vect}_k\colon X \mapsto \{f\colon X \to k\}$, where

$$[\varphi\colon X \to Y] \mapsto [\varphi^*\colon \{g\colon Y \to k\} \to \{\varphi^* g = g \circ \varphi\colon X \to k\}].$$

If X is infinite, then $\langle X \rangle$ can be strictly "smaller than" $X^* := \{f\colon X \to k\}$, because $\langle X \rangle$ corresponds to $\bigoplus_{x \in X} k$ and X^* corresponds to $\prod_{x \in X} k$.

4.1. Structure of representations

November 25, 2024 Let V be a representation of G. If G has a **G-invariant subspace** $W \subseteq V$, i.e. $GW \subseteq W$, then we induce a **sub-representation** of G on the subspace W. Further, we induce a **quotient representation** of G on the space V/W given by $g \cdot (v + W) = g \cdot v + W$.

If V_1 and V_2 are G-representations, then $V_1 \oplus V_2$ (the outer direct sum) is a G representation by letting G act on each entry: $g \cdot (v_1, v_2) = (g \cdot v_1, g \cdot v_2)$. If $W_1, W_2 \subseteq V$ are sub-representations and $W_1 \oplus W_2 = V$ (the inner direct sum), then we can also define a representation on $W_1 \oplus W_2$.

Example 4.3 – Let $G = S_2$ have a representation on $\mathbb{R}^2$ by permuting basis vectors. Then $\langle(1,1)\rangle$ and $\langle(1,-1)\rangle$ are both G-invariant. Let these become sub-representations as V_1 and V_2. Then $\mathbb{R}^2 = V_1 \oplus V_2$ is a decomposition of $\mathbb{R}^2$ into G-invariant subspaces.

We also claim these are the *only* (non-trivial) G-invariant subspaces. Suppose the permutation $\begin{pmatrix}1 & 2\end{pmatrix} \in S_2$ satisfies

$$\begin{pmatrix}1 & 2\end{pmatrix} \cdot (a,b) = (b,a) \in W$$

for all $(a,b) \in W$. If (a,b) and (b,a) are linearly independent, then $W = \mathbb{R}^2$. Otherwise, $(a,b) = \pm(b,a)$, which means $W \supseteq \langle(1,1)\rangle$ or $W \supseteq \langle(1,-1)\rangle$, which implies the result.

Definition 4.2

A representation $V \neq 0$ of G is **irreducible (simple)** if the only invariant subspaces are 0 and V. A representation V is **completely reducible (semisimple)** if $V \cong \bigoplus_\alpha V_\alpha$ for irreducible V_α (we can also think of this as an inner direct sum by letting V_α be irreducible sub-representations).

Example 4.4 – Irreducible representations of $G = \{e\}$ are one-dimensional vector spaces.

$\mathbb{Z}/2 \curvearrowright \mathbb{R}$ by multiplying by -1, so we have an action of $\mathbb{Z}/2$ on $\mathbb{R}^{\mathbb{R}}$ (the set of functions $f\colon \mathbb{R} \to \mathbb{R}$) by $[1] \cdot f(x) = f(-x)$. A small irreducible subspace can be formed by taking the function $f \in \mathbb{R}^{\mathbb{R}}$ and considering the subspace $\langle f(x), f(-x)\rangle$, which is an irreducible sub-representation. In particular, if f is even or odd, then this is a one-dimensional space. We now prove that $\mathbb{R}^{\mathbb{R}}$ is completely reducible. Recall that every function can be uniquely decomposed as the sum of an even and odd function. In other words,

$$\mathbb{R}^{\mathbb{R}} = (\mathbb{R}^{\mathbb{R}})^{\text{even}} \oplus (\mathbb{R}^{\mathbb{R}})^{\text{odd}}.$$

We further decompose these subspaces using the facts above to show that $\mathbb{R}^{\mathbb{R}}$ is completely reducible.

December 02, 2024 **Example 4.5** – If $\operatorname{char}(k) \neq 2$ and $\rho\colon S_2 \to V$ is a representation where V is a vector space over $\mathbb{R}$, then we have a decomposition

$$V = V^+ \oplus V^-,$$

where

$$V^+ = \{v : \rho(\sigma)v = v\}, \qquad V^- = \{v : \rho(\sigma)v = -v\}.$$

4.2. Morphisms of representations

We want to define morphisms in the category of represenations.

Definition 4.3

Suppose V, W are two representations of G. A **morphism of representations (homomorphism)** is a k-linear map $\varphi\colon V \to W$ which is also a map of G-sets:

$$\varphi(g \cdot v) = g \cdot \varphi(v), \qquad \forall v \in V, g \in G$$

(the second condition is called **G-equivariance**). This defines a category of G representations over k.

Remark 4.2. Given two representations V, W, we can just consider them as vector spaces and look at the vector space of linear maps $\mathrm{Mor}_k(V, W)$. Consider the action $G \curvearrowright \mathrm{Hom}_k(V, W)$ given by

$$\varphi^g(v) \coloneqq g \cdot \varphi(g^{-1} \cdot v).$$

Then $\varphi \in \mathrm{Hom}_{G\text{-Rep}}(V, W) \iff \varphi^g = \varphi$ for all $g \in G$.

4.3. Decomposing representations: Maschke's theorem

Theorem 4.3 (Maschke's theorem)

Any representation V of a finite group G is completely reducible provided that $\operatorname{char} k \nmid |G|$.

We'll reduce the theorem to the problem of finding complementary subspaces.

Lemma 4.4

A representation V is completely reducible $\iff$ every sub-representation $W \subseteq V$ has a complementary subspace (i.e. $W^\perp \subseteq V$ with $V = W \oplus W^\perp$).

Proof. ($\impliedby$) If V is reducible, there exists a sub-representation $W \subseteq V$ with $W \neq 0, V$. So there exists $U \subseteq V$ such that $V = U \oplus W$. To iterate, we need to show that the assumption holds for W. If $W' \subseteq W$ is a sub-representation, there is a U' such that $V = U' \oplus W'$. Then $W = (U' \cap W) \oplus W'$.

This works if $\dim V < \infty$, but extends to the infinite case with Zorn's lemma.

($\implies$) Suppose $V = \bigoplus_i V_i \supseteq W$, where V_i are irreducible. $W = V$ is trivial. $W \subset V$ implies $V_i \not\subseteq W$ for some i. For each such i, $V_i \cap W \subset V_i$, so $V_i \cap W = 0$, hence $V_i \oplus W \subseteq V$. We iterate, i.e., find $V_j \not\subseteq V_i \oplus W$ and continue. □

There's a natural way to find a complementary subspace of, say $W \subseteq \mathbb{R}^n$: use an inner product $\langle \cdot, \cdot \rangle$ on $\mathbb{R}^n$ and consider the orthogonal complement

$$W^\perp = \{u : \langle u, w \rangle = 0, \forall w \in W\}$$

We'll need to adapt this to work with the G action.

If V is a finite-dimensional, real/complex vector space, then it has an inner product $\langle \cdot, \cdot \rangle$. We then define a new inner product that is G-invariant (i.e., $\langle g \cdot v, g \cdot w \rangle = \langle v, w \rangle$) by using an "averaging" technique:

$$\langle v, w \rangle_G \coloneqq \frac{1}{|G|} \sum_{g \in G} \langle g \cdot v, g \cdot w \rangle .$$

Then we can decompose as in the case of the normal inner product.

The caveat with this proof is that it only works for finite-dimensional representations over $\mathbb{R}$ or $\mathbb{C}$. We can still extend this idea of creating a G-invariant complementary subspace out of some complementary subspace though.

Proof of Theorem 4.3 (sketch). Let $W \subseteq V$ and consider any complementary subspace U, which may not be G-invariant. We have a natural isomorphism

$$U \overset{\iota}{\hookrightarrow} V \overset{\pi}{\twoheadrightarrow} V/W,$$

so U corresponds to a (linear) section $s \colon V/W \to V$ (i.e. $\pi s = \mathrm{id}_{V/W}$), and conversely, any section corresponds to a complementary space.

Now take any section $s \colon V/W \to V$. Consider

$$\tilde{s}(x) := \frac{1}{|G|} \sum_{g \in G} s^g(x) = \frac{1}{|G|} \sum_{g \in G} g \cdot s(g^{-1} \cdot x),$$

(c.f. Remark 4.2). We first claim this is a section. Indeed,

$$\begin{aligned} \pi\left(\frac{1}{|G|} \sum_{g \in G} g \cdot s(g^{-1} \cdot x)\right) &= \frac{1}{|G|} \sum_{g \in G} \pi\left(g \cdot s(g^{-1} \cdot x)\right) \\ &= \frac{1}{|G|} \sum_{g \in G} g \cdot \pi s(g^{-1} \cdot x) \\ &= \frac{1}{|G|} \sum_{g \in G} e \cdot x \\ &= x. \end{aligned}$$

We now let $\tilde{U} := \tilde{s}(V/W)$ be the corresponding complementary subspace. This subspace is g invariant, since multiplication by $g \in G$ is a bijeciton of G to itself.

We then finish by applying Lemma 4.4. □

Example 4.6 – Before, we showed that we can decompose a representation V of $G = S_2$ into two irreducible subspaces over $\mathbb{R}$.

On the other hand, if $k = \mathbb{F}_2$, then if we let

$$\rho(\sigma) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

then there is only one irreducible subspace, $\langle(1, 0)\rangle$.

Schur's lemma tells us that the homomorphisms of G-representations are easy to describe over algebraically closed fields.

December 06, 2024

Theorem 4.5 (Schur's lemma)
Let V, W be irreducible, finite-dimensional representations of G over an algebraically closed field k. Then

1. if $V \not\cong W$, then $\operatorname{Hom}_{G\text{-rep}}(V, W) = 0$,
2. if $V \cong W$, then $\operatorname{Hom}_{G\text{-rep}}(V, W) = \operatorname{End}_{G\text{-rep}}(V) = k$.

Proof. Use the definition of irreducible to get that any morphism $\varphi \colon V \to W$ is either the zero map, or an isomorphism.

Now we show that, in the case of an isomorphism, it is a scalar. Since $\dim V < \infty$ and k is algebraically closed, we have a root of the minimal polynomial, λ (eigenvalue). By the first paragraph, either $\varphi - \lambda I = 0$ or $\varphi - \lambda I$ is an isomorphism, but the latter cannot happen, since an eigenvector corresponding to λ is in the kernel of this map. □

Given an irreducible representation V and any finite dimensional representation W, we can use Maschke's theorem (4.3) to decompose $W = \bigoplus_{i=1}^{n} W_i$ into irreducible representations, and then

$$\operatorname{Hom}_{G\text{-rep}}(V, W) \cong \bigoplus_{i=1}^{n} \operatorname{Hom}_{G\text{-rep}}(V, W_i).$$

Corollary 4.6
Let $V \cong \bigoplus_i V_i^{m_i}$, $W \cong \bigoplus_j V_i^{n_i}$, where V_i are irreducible, non-isomorphic representations. Then

$$\dim \operatorname{Hom}_{G\text{-rep}}(V, W) = \sum_i m_i n_i.$$

December 09, 2024

Corollary 4.7
Let V be an irreducible representation of a group G over an algebraically closed field k. Let $g \in Z(G)$, so $\rho(g) \colon V \to V$ is a homomorphism. Then $\rho(g) \in k$ (i.e. it represents scalar multiplication).

If G is abelian, then G acts by scalars ($\rho \colon G \to K^{\times}$), so $\dim V = 1$.

Non-Example 4.1 – Let $G = SO(2)$ (which is abelian, because it's isomorphic to $\mathbb{R}/(2\pi\mathbb{Z})$) and let it act on $\mathbb{R}^2$ in the natural way.

4.4. Some character theory

The overall goal is to find $\dim_{\mathbb{C}} \operatorname{Hom}_{G-\text{rep}}(V, W)$ for V and W G-representations over $\mathbb{C}$. A smaller goal s to find $\dim V^G$, where $V^G = \{v \in V : G \cdot v = v\}$.

Exercise 4.1.

(a) Let V be a linear space and $P \colon V \to V$ be a linear operator such that $P^2 = P$. Show that $V = \ker P \oplus \operatorname{im} P$. Operators having this property are called **projectors**.

(b) Suppose further that $\dim V = n$. Prove that there exists a basis of V such that the matrix P is a diagonal matrix with some number of 1's on the diagonal and 0's elsewhere.

Consider the operator

$$\begin{aligned} A_V &: V \to V, \\ &: v \mapsto \frac{1}{|G|} \sum_{g \in G} \rho(g) v. \end{aligned}$$

We have that $A_V(V) \subseteq V^G$, and $A_V|_{V^G} = \mathrm{id}_{V^G}$. This makes A_V a *projector*, so $V = \mathrm{im}(A_V) \oplus \ker(A_V) = V^G \oplus \ker(A_V)$. Recall that we can choose a basis so that the matrix of A_V is $\mathrm{diag}(1, \dots, 1, 0, \dots, 0)$, where the basis vectors that get mapped to themselves span $\mathrm{im}(A_V)$.

Notice that this gives a "fast" way of computing $\dim \mathrm{im}(A_V) = \dim V^G$: by taking $\mathrm{Tr}(A_V)$. So

$$\dim V^G = \mathrm{Tr}\, A_V = \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(\rho(g)).$$

Example 4.7 – Let $S_3 \curvearrowright \mathbb{C}^3$ by the permutation matrices. We compute the trace of each representation for $\sigma \in S^3$ and we have

$$\dim V^G = \frac{1}{|S^3|} \sum_{\sigma \in S^3} \mathrm{Tr}(\rho(\sigma)) = \frac{3+1+1+1}{6} = 1.$$

December 11, 2024

Definition 4.4

If (V, ρ) is a finite-dimensional representation of a group G over k, its **character** is a map $\chi_V \colon G \to k \colon g \mapsto \mathrm{Tr}(\rho_V(g))$.

Proposition 4.8 (Properties of characters)

1. $\chi_V(hgh^{-1}) = \chi_V(g)$ for $g, h \in G$. So χ_V is constant on conjugacy classes (the fancy name for a function with this property is a **class function**).
2. If $V_1, \dots, V_k$ representations of G over k, $\chi_{V_1^{n_1} \oplus \cdots \oplus V_k^{n_k}} = n_1 \chi_{V_1} + \cdots + n_k \chi_{V_k}$.
3. If $W \subseteq V$ is a subrepresentation, $\chi_V = \chi_W + \chi_{V/W}$.

Proposition 4.9 (Properties of characters of $\mathbb{C}$-representations of finite groups)

1. If G is finite and V is an n-dimensional representation of G over $\mathbb{C}$, $\rho(g)$ has n eigenvalues (in fact, $\rho(g)$ is diagonalizable), and $\chi_V(g)$ is the sum of those eigenvalues.[1]
2. The eigenvalues are roots of unity, and $|\chi_V(g)| \leq n$.
3. $\chi_V(g^{-1}) = \overline{\chi_V(g)}$.

[1] Further $\chi_V(g^k)$ is the sum of the kth powers of eigenvalues, which we could use to recover the actual eigenvalues.

Example 4.8 – In S_n the conjugacy classes are determined by cycle type. Further, g^{-1} is conjugate to g in S_n for all $g \in S_n$. So all characters of S_n are real.

Let's return to the original question: computing the dimension of $\mathrm{Hom}_{G\text{-rep}}(V, W)$. We have an action $G \curvearrowright \mathrm{Hom}_{G\text{-rep}}(V, W)$ by $g \cdot \varphi = \rho_V(g)\varphi\rho_W(g)^{-1}$. We also showed that $\mathrm{Hom}_{G\text{-rep}}(V, W) = \mathrm{Hom}_{\mathbb{C}}(V, W)^G$. Therefore, the dimension is equal to $\chi_{\mathrm{Hom}_{\mathbb{C}}(V,W)}$.

Lemma 4.10

Fix n, m and consider $A \in \mathrm{Mat}_{n\times n}(k)$, $B \in \mathrm{Mat}_{m\times m}(k)$. Consider the map

$$\begin{aligned} \Phi\colon \mathrm{Mat}_{n\times m}(k) &\to \mathrm{Mat}_{n\times m}(k) \\ M &\mapsto AMB. \end{aligned}$$

Then $\mathrm{Tr}(\Phi) = \sum_{i,j} A_{ii}B_{jj} = \mathrm{Tr}(A)\,\mathrm{Tr}(B)$.

Proof.

$$[M_{ij}] \overset{\Phi}{\mapsto} \left[\sum_{k,\ell} A_{ik}M_{k\ell}B_{\ell j}\right].$$

Looking at where it sends the matrix E_{ij}, which is 1 in the ijth entry and zero is everywhere else, we have $\Phi(E_{ij})_{ij} = A_{ii}B_{jj}$. This gives us the formula. □

Hence,

$$\chi_{\mathrm{Hom}_{\mathbb{C}}(V,W)}(g) = \mathrm{Tr}(\rho_V(g))\,\mathrm{Tr}(\rho_W(g^{-1})) = \chi_V(g)\chi_W(g^{-1}) = \chi_V(g)\overline{\chi_W(g)}.$$

Theorem 4.11 (Orthogonality relation)

$$\langle \chi_V, \chi_W \rangle \coloneqq \dim \mathrm{Hom}_{G\text{-rep}}(V, W) = \frac{1}{|G|}\sum_{g\in G} \chi_V(g)\overline{\chi_W(g)}.$$

If V and W are irreducible,

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 0 & \text{if } V \neq W, \\ 1 & \text{if } V \cong W. \end{cases}$$

Example 4.9 – Let $G = S_3$. We've computed characters already for two representations:

Representation\Character of Cycle Type	$\chi(e)$	$\chi(12)$	$\chi(123)$
$\mathbb{C}$ (trivial)	1	1	1
$V = \mathbb{C}^3$ (permuting basis)	3	1	0

We compute that

$$\langle \chi_V, \mathrm{id}_{\mathbb{C}} \rangle = \frac{1\cdot 3 + 3\cdot 1\cdot 1 + 2\cdot 1\cdot 0}{6} = 1.$$

So there exists a representation W such that $\chi_W = \chi_V - 1$ (this gives us $\chi_W(e) = 3 - 1 =$

> $2, \chi_W(12) = 0, \chi_W(123) = -1$ by additivity of characters). We compute
>
> $$\langle \chi_W, \chi_W \rangle = \frac{2 \cdot 2 + 0 + -1 \cdot -1 \cdot 2}{6} = 1.$$

Theorem 4.12

χ_V span the space of class functions (i.e. the number of irreducible representations is the number of conjugacy classes).

5. Commutative algebra

January 22, 2025 This is the beginning of 2nd semester (MATH 742).

For this section, assume all rings are associative (i.e. multiplication is associative) and unital ($1 \in R$). Rings are (usually) commutative. We'll now try to build a category of such rings. The objects will be rings as above. A **homomorphism** between rings R, S preserves addition and multiplication, and also sends 1_R to 1_S. Denote the category of rings as Ring.

Example 5.1 (Zero ring) – We have $1 = 0$ in $R \iff R = \{0\}$ is the zero ring.

Example 5.2 – The only homomorphism $\varphi\colon \mathbb{Z} \to \mathbb{Z}$ is the identity. Further, there is only one homomorphism $\varphi\colon \mathbb{Z} \to R$, where R is any ring.

In other words, $\mathbb{Z}$ is the *initial object* (for every $R \in \mathsf{Ring}$, there exists a unique homomorphism $\varphi\colon \mathbb{Z} \to R$) in Ring.

Further, 0 is the *final object* (for every $R \in \mathsf{Ring}$, there exists a unique homomorphism $\varphi\colon R \to 0$) in Ring.

5.1. Ideals

Definition 5.1

A **ideal** I is a(n additive) subgroup of R such that $R \cdot I = I$. A **subring** S is a(n additive) subgroup of R such that $S \cdot S \subseteq S$ and $1 \in S$.

We have operations on ideals:

$$I + J, I \cap J, I \cdot J.$$

The last one is subtle: $I \cdot J = \left\{\sum_{\text{finite}} x_i y_i : x_i \in I, y_j \in J\right\}$. Given an infinite collection of ideals $\{I_\lambda\}$, $\bigcap_\lambda I_\lambda$ and $\sum_\lambda I_\lambda$ are both ideals, where the latter is defined by finite sums of elements of $\{I_\lambda\}$.

Theorem 5.1

Let $\varphi\colon R \to S$ be a homomorphism. Then

1. $\ker \varphi$ is an ideal.
2. There is an isomorphism $R/\ker\varphi \xrightarrow{\sim} \varphi(R)$ induced by φ.

Remark 5.2 (Universal mapping property of the quotient). R/I is the unique object in Ring such that $\varphi\colon R \to S$ uniquely factors through R/I when $\varphi|_I = 0$.

Example 5.3 – Following the ideas of the above remark, since $\mathbb{Z}$ is initial, the unique map $\mathbb{Z} \to R$ factors through $\mathbb{Z}/3$ only when the ideal $3\mathbb{Z}$ gets sent to 0. In other words, this map factoring is equivalent to $0 = 3$ in R.

Example 5.4 – Further, if $\varphi\colon \mathbb{R}[x, y] \to S$ is a ring homomorphism, it is entirely determined by $\varphi|_{\mathbb{R}}\colon \mathbb{R} \to S$ and $\varphi(x)$, $\varphi(y)$. We can imagine polynomial rings as the "free objects" of Ring, and the universal mapping property of the quotient is the same as adding "relations".

5.2. Algebras

January 24, 2025

Definition 5.2

Let R be a ring. An **R-algebra** is a ring S together with a ring homomorphism $i\colon R \to S$.

Example 5.5 –

1. Any ring S that contains R as a subring.
2. $R = \mathbb{R}$, $S = \{\mathbb{R}\text{-valued functions on a "space" } X\}$, and $i\colon \mathbb{R} \to S$ sends a to the constant function that is always a.
3. $S = R[x_1, \ldots, x_n]$, where $i\colon R \to S$ is the obvious identity map.
4. Any ring is a $\mathbb{Z}$-algebra because $\mathbb{Z}$ is initial.

Here's the motivation for homomorphisms of algebras: suppose we wanted to classify all ring homomorphisms $\varphi\colon \mathbb{R}[x] \to \mathbb{C}$. The "obvious" candidates are evaluation maps over some $z \in \mathbb{C}$. However, we only know where 1 gets sent to, but perhaps irrational numbers (π, e, $\sqrt{2}$) could get mapped somewhere unexpected, so the space of such φ is much larger than it seems. However, once $\varphi|_{\mathbb{R}}$ is determined, all we need is $\varphi(x)$ to get the whole homomorphism. To recover this issue with $\varphi|_{\mathbb{R}}$, we define an *algebra homomorphism*.

Definition 5.3

Given two algebras S_1, S_2 over R is an **algebra homomorphism** $\varphi\colon S_1 \to S_2$ is a homomorphism such that the diagram

$$\begin{tikzcd} & S_1 \arrow[dd, "\varphi"] \\ R \arrow[ur, "i_1"] \arrow[dr, "i_2"'] & \\ & S_2 \end{tikzcd}$$

commutes.

Consider the two $\mathbb{R}$-algebras $\mathbb{R}[x]$ and $\mathbb{C}$ with structure maps $i_1 : \mathbb{R} \to \mathbb{R}[x]$ and $i_2 : \mathbb{R} \to \mathbb{C}$, respectively as the obvious inclusion maps. Then the algebra homomorphisms $\varphi\colon \mathbb{R}[x] \to \mathbb{C}$ are precisely the evaluation maps. This generalizes.

Proposition 5.3

Let S be an R-algebra. Then

$$\mathrm{Hom}_{R\text{-alg}}(R[x], S) = \{\mathrm{ev}_\alpha \colon \alpha \in S\},$$

where ev_α is the evaluation map.

Corollary 5.4

Let $p_1, \dots, p_k \in R[x]$. Then

$$\mathrm{Hom}_{R\text{-alg}}(R[x]/(p_1(x), \dots, p_k(x)), S) = \{ev_\alpha : \alpha \in Z(p_1, \dots, p_k)\}.$$

Remark 5.5. What this says: $R[x]/(p_1(x), \dots, p_k(x))$ has all the "data" of solutions to $p_1(\alpha) = \cdots = p_k(\alpha) = 0$. If we want to check solutions over some R-algebra S, then we look at the above Hom set.

5.3. Chinese remainder theorem and idempotents

January 27, 2025

Definition 5.4

Two ideals $I_1, I_2 \subseteq R$ are **comaximal** if $I_1 + I_2 = R$.

Theorem 5.6 (Chinese remainder theorem)

If I_1 and I_2 are comaximal, the natural map $R \to R/I_1 \times R/I_2$ is surjective, hence $R/I_1 \cap I_2 \cong R/I_1 \times R/I_2$. Also, $I_1 \cdot I_2 = I_1 \cap I_2$.

Theorem 5.7

There is a 1-1 correspondence between

1. Isomorphisms $R \xrightarrow{\sim} R_1 \times R_2$,
2. pairs of ideals $I_1, I_2 \subseteq R$ that are comaximal and $I_1 \cap I_2 = 0$.

Proof. ((2) $\implies$ (1)) Set $R_j = R/I_j$ for $j = 1, 2$ and use CRT.
((1) $\implies$ (2)) Set $I_1 = \{0\} \times R_2$ and $I_2 = R_1 \times \{0\}$. □

Definition 5.5

$e \in R$ is an **idempotent** if $e^2 = e$.

The key example is that whenever $R \cong R_1 \times R_2$, then $(1, 0)$, $(0, 1)$ are idempotents. Hence, the identity $(1, 1)$ is a sum of idemptoents.

Proposition 5.8

There is also a 1-1 correspondence from objects in Theorem 5.7 and

3. idempotents $e \in R$.

Proof. ((1) $\implies$ (3)) was the above example, where $(1, 1) = (1, 0) + (0, 1)$.
((3) $\implies$ (1)) Given an idempotent e, set $I_1 = (1 - e)$, $I_2 = (e)$. We have $e + (1 - e) = 1 \in I_1 + I_2$, so $I_1 + I_2 = R$. To prove $I_1 \cap I_2 = 0$, recall that $I_1 \cdot I_2$ by CRT. Then $a_1(1 - e) \cdot a_2 e = a_1 a_2 (e - e^2) = 0$. □

5.4. Prime and maximal ideals

These are *proper* containments.

Definition 5.6

$\mathfrak{m} \subset R$ is **maximal** if $I \supset \mathfrak{m}$ implies $I = R$. $\mathfrak{p} \subset R$ is **prime** if $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Proposition 5.9

$\mathfrak{m} \subsetneq R$ (resp. $\mathfrak{p} \subsetneq R$) is maximal (resp. prime) $\iff$ $R/\mathfrak{m}$ is a field (resp. $R/\mathfrak{p}$ is a(n integral) domain).

Proposition 5.10

1. Any maximal ideal is prime.
2. Any ring $R \neq 0$ has maximal ideals.
3. Given an ideal I, there is a 1-1 correspondence between ideals of R/I and ideals of R containing I. In particular, any proper ideal $I \subset R$ is contained in a maximal ideal.

5.5. Extensions and contractions of ideals

January 29, 2025

Let $\varphi \colon R \to R'$ be a homomorphism. If $I' \subseteq R'$ is an ideal, $\varphi^{-1}(I') \subseteq R$ is an ideal. We write $(I')^c$ as the **contraction** of I'.

If $I \subseteq R$, $\varphi(I) \subseteq R'$ is not necessarily an ideal. Instead, we consider $(\varphi(I)) = R' \cdot \varphi(I) =: I^e$, which we call the **extension** of I.

Proposition 5.11

A contraction of a prime ideal is prime, but a contraction of a maximal ideal is not necessarily maximal.

Proof. Notice that we have an injective ring homomorphism $R/(I')^c \hookrightarrow R'/I'$ induced by φ. This identifies $R/(I')^c$ with a subring of a domain. The subring of a domain is a domain, so $(I')^c$ is prime. On the other hand, a subring of a field need not be a field. □

Remark 5.12. If $\varphi \colon R \to R'$ is surjective, then $R'/I' \cong R/(I')^c$, so contractions of maximal ideals are actually maximal.

5.6. Types of domains

Let R be a domain, i.e., R has no zero divisors and $1 \neq 0$. Then $a \mid b \iff b \in (a) \iff (b) \subseteq (a)$. We say a nonzero, non-unit element $x \in R$ is **irreducible** if $x = ab$ implies $a \in R^\times$ or $b \in R^\times$.

Definition 5.7

A domain R is a **unique factorization domain (UFD)** if every nonzero, non-unit element is a product of irreducibles uniquely (up to permutation).

Definition 5.8

A ring R is a **principal ideal domain (PID)** if every ideal is **principal**, i.e., generated by one element.

Proposition 5.13

Field $\implies$ PID $\implies$ UFD.

Proposition 5.14

If F is a field, then $F[x]$ is a PID.

The idea to prove this is to create a long division algorithm for polynomials.

Proposition 5.15

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

Proof (sketch). Let $F = \operatorname{Frac}(R)$ (R's **field of fractions**). The idea is to compare factorization in $R[x]$ and $F[x]$.

For example, if $R = \mathbb{Z}$, then $F = \mathbb{Q}$. Consider $\frac{1}{3}x^2 - 3x + \frac{1}{5}$, which is irreducible in $\mathbb{Q}[x]$. We can "clear denominators" to get $5x^2 - 45x + 3$ being irreducible in $\mathbb{Z}[x]$.

So we consider the set

$$\widetilde{R[x]} = \{a_n x^n + \cdots + a_0 \in R[x] : \gcd(a_0, \ldots, a_n) = 1\}.$$

Hence,

$$R[x] \setminus \{0\} = (R \setminus \{0\}) \cdot \widetilde{R[x]}.$$

In fact,

$$F[x] \setminus \{0\} = (F \setminus \{0\}) \cdot \widetilde{R[x]}.$$

Lemma 5.16 (Gauss' lemma)

$\widetilde{R[x]} \cdot \widetilde{R[x]} \subseteq \widetilde{R[x]}$.

As a consequence, if $aP(x) \in F[x]$, where $a \in F \setminus \{0\}$ and $P \in \widetilde{R[x]}$, then $aP(x)$ is irreducible in $F[x]$ if and only if $P(x)$ is irreducible in $R[x]$. □

Corollary 5.17

If F is a field $F[x_1, \ldots, x_n]$ is a UFD.

5.7. Radical ideals

January 31, 2025

Definition 5.9

For $I \subseteq R$ an ideal, the **radical of I** is the set

$$\sqrt{I} = \left\{x : x^k \in I, k \in \mathbb{N}\right\}.$$

Example 5.6 – If $I = (300) = (2^2 \cdot 3 \cdot 5^2) \subseteq \mathbb{Z}$, then $\sqrt{I} = (2 \cdot 3 \cdot 5) = (30)$.

Proposition 5.18 (Properties of the radical)

Let $I \subseteq R$ be an ideal.

(a) $\sqrt{I} \supseteq I$.

(b) $\sqrt{I}$ is an ideal.

(c) $\sqrt{\sqrt{I}} = \sqrt{I}$.

Proof. (a) is clear.

(b) if $a \in \sqrt{I}$ and $b \in R$, then $(ab)^k = \underbrace{a^k}_{\in I} b^k \in I$. If $a, b \in \sqrt{I}$ such that $a^n, b^m \in I$, then $(a+b)^{n+m-1} \in I$.

(c) if $a \in \sqrt{\sqrt{I}}$, then $a^k \in \sqrt{I}$, so $a^{km} \in I$, which means $a \in \sqrt{I}$. □

Example 5.7 – The radical ideals in $\mathbb{Z}$ are (a), where a is square-free or zero.

Definition 5.10

I is a **radical ideal** if $\sqrt{I} = I$.

$\sqrt{I}$ is the smallest radical ideal containing I.
Notice that prime ideals are radical.

Theorem 5.19 (Scheinnullstellensatz)

Let $I \subseteq R$ be an ideal. Then

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \supseteq I \\ \mathfrak{p} \text{ prime}}} \mathfrak{p}.$$

Proof. ($\subseteq$) Since $\sqrt{I}$ is the smallest radical ideal containing I and each $\mathfrak{p}$ is a prime (hence radical) ideal containing I, we are done.

($\supseteq$) Let $x \notin \sqrt{I}$, so $\left\{x^k : k \geq 0\right\} \cap I = \varnothing$. We'll construct a prime ideal J such that $J \supseteq I$ and $x \notin J$.

Let J be an ideal such that (1) $J \supseteq I$, (2) $\left\{x^k : k \geq 0\right\} \cap J = \varnothing$, (3) J is maximal amongst ideals satisfying (1) and (2).

We'll use Zorn's lemma. Consider the poset $(\mathcal{P}, \preceq)$ of all ideals satisfying (1) and (2), ordered by inclusion. The poset is non-empty because $I \in \mathcal{P}$. Now consider a chain of ideals $\{I_\alpha\}$. The upper bound $\bigcup_\alpha I_\alpha$ satisfies (1) and (2).

We prove J is prime. Let $a, b \notin J$. We have $J + (a) \supset J$, which means $J + (a)$ fails (1) or (2), but it clearly fails (2). Hence, there exists $n \geq 0$ such that $x^n \in J + (a)$. Similarly, there exists $m \geq 0$ such that $x^m \in J + (b)$. Then $x^{n+m} \in J + (ab)$, which means $ab \notin J$. □

Definition 5.11

Let R be a ring. Then $\operatorname{nil}(R) = \sqrt{(0)} = \left\{x : x^k = 0, k \geq 0\right\} = \{x : x \text{ is } \textbf{nilpotent}\}$ is called the **nilradical** of R.

Corollary 5.20

Let R be a ring. Then

$$\operatorname{nil}(R) = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}.$$

Example 5.8 –

1. If R is a domain, then $\operatorname{nil}(R) = 0$ (because (0) is prime in a domain).
2. $\operatorname{nil}(\mathbb{Z}/300) = \sqrt{(300)}/(300) = (30)/(300)$.
3. The last example hints at the fact that if $I \subseteq R$ is an ideal, then $\sqrt{I}$ corresponds to the ideal $\operatorname{nil}(R/I) = \sqrt{I}/I \subseteq R/I$ (using the correspondence between ideals (5.10)).
4. Consider $(x^2y^3) \subseteq \mathbb{C}[x, y]$. $\sqrt{(x^2y^3)} = (xy)$. Then the radical corresponds to $\operatorname{nil}\left(\mathbb{C}[x, y]/(x^2y^3)\right) = (xy)/(x^2y^3)$.

February 3, 2025 The prime ideals that contain (x^2y^3) are (x), (y), and the maximal ideals of the form $(x, y + b)$, $(x + a, y)$ for $a, b \in \mathbb{C}$ (the fact that these are the only maximal ideals is a deeper fact). Hence,

$$\sqrt{(x^2y^3)} = (xy) = (x) \cap (y) \cap \bigcap_{b \in \mathbb{C}} (x, y + b) \cap \bigcap_{a \in \mathbb{C}} (x + a, y).$$

The last two intersections are unnecessary, since each ideal is contained in either (x) or (y).

Definition 5.12

$\mathfrak{p} \supseteq I$ is called a **minimal prime** of I if

1. $\mathfrak{p}$ is prime,
2. there are no prime $\mathfrak{q}$ such that $\mathfrak{p} \supset \mathfrak{q} \supseteq I$.

By Zorn's lemma, given any prime $\mathfrak{p} \supseteq I$, there exists a minimal prime $\widetilde{\mathfrak{p}}$ such that $\mathfrak{p} \supseteq \widetilde{\mathfrak{p}} \supseteq I$.

Therefore, we can more efficiently write the radical of an ideal:

Theorem 5.21

Let $I \subseteq R$ be an ideal. Then

$$\sqrt{I} = \bigcap_{\widetilde{\mathfrak{p}} \text{ min'l prime of } I} \mathfrak{p}.$$

In particular,

$$\operatorname{nil}(R) = \bigcap_{\widetilde{\mathfrak{p}} \text{ min'l prime of } R} \mathfrak{p}.$$

5.8. Jacobson's radical

Definition 5.13

Given a ring R, define its **Jacobson radical** as

$$\operatorname{jac}(R) \coloneqq \operatorname{rad}(R) \coloneqq \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}.$$

Then $\operatorname{nil}(R) \subseteq \operatorname{rad}(R)$.

Proposition 5.22

Fix a unit $u \in R^\times$ (usually $u = 1$). Then $a \in \operatorname{rad}(R) \iff u + xa \in R^\times$ for all $x \in R$.

Proof. Suppose $a \notin \operatorname{rad}(R)$. Then there exists a maximal $\mathfrak{m}$ not containing a. So $a + \mathfrak{m}$ is nonzero (hence a unit) in $R/\mathfrak{m}$. So there exists x such that $x(a + \mathfrak{m}) + u = 0 + \mathfrak{m} \in R/\mathfrak{m}$. So $u + ax \in \mathfrak{m} \implies u + ax \notin R^\times$.

Conversely, suppose $u + ax \notin R^\times$. Then $(u + ax)$ is a proper ideal, so it is contained in some maximal ideal $\mathfrak{m}$. We have $u \notin \mathfrak{m} \implies ax \notin \mathfrak{m} \implies a \notin \mathfrak{m}$, so $a \notin \operatorname{rad}(R)$. □

Example 5.9 –

$$\operatorname{rad}(\mathbb{C}[x,y]/(x^2y^3)) = \left(\bigcap_{b \in \mathbb{C}} (x, y+b) \cap \bigcap_{a \in \mathbb{C}} (x+a, y) \right) / (x^2y^3).$$

It turns out this coincides with $\operatorname{nil}(\mathbb{C}[x,y]/(x^2y^3))$.

5.8.1. Special case: local rings

Definition 5.14

We say a ring $R \neq 0$ is **local** if there is only one maximal ideal, $\mathfrak{m}$.

Proposition 5.23

R is local with $\mathfrak{m} \subseteq R \iff$ any $x \notin \mathfrak{m}$ is a unit $\iff R \setminus R^\times$ is an ideal (and $\mathfrak{m} = R \setminus R^\times$).

Example 5.10 –

1. If R is a field, R is local because (0) is the only proper ideal.
2. Let k be a field, then define the **power series ring** as

$$k[[t]] \coloneqq \left\{ \sum_{i \geq 0} a_i t^i \mid a_i \in k \right\}.$$

We have the famous identity

$$(1 + t + t^2 + \cdots)(1 - t) = 1,$$

so $(1 - t) \in k[[t]]^\times$. This extends to show any $1 - tp(t)$ is a unit, which further extends to show that $a_0 + a_1 t + \cdots$ is a unit if $a_0 \neq 0$. Hence,

$$k[[t]] = k[[t]]^\times \sqcup (t),$$

so $k[[t]]$ is local with maximal ideal (t).

5.9. Modules

Definition 5.15

February 5, 2025

Let R be a ring. An **R-module** M is an abelian group plus a multiplication operation $\cdot \colon R \times M \to M$ that is (1) distributive (both kinds), (2) associative, (3) unitary $1 \cdot m = m$.

Example 5.11 –

1. If k is a field, k-modules are k-vector spaces.
2. $\mathbb{Z}$-modules are abelian groups (multiplication doesn't add any structure).

Example 5.12 – Let k be a field, V a vector space over k, and G a group. A representation $\rho \colon G \to GL(V)$ is a k-linear G-action.

Define the $R = k[G]$ (the **group algebra** of G) as linear combinations of group elements:

$$k[G] = \left\{ \sum_{\gamma \in G} c_\gamma \gamma : c_\gamma \in k, \text{finitely many } c_\gamma \text{ are nonzero} \right\}.$$

Define the product as

$$\gamma \cdot \gamma' \coloneqq \underbrace{\gamma\gamma'}_{\text{product in } G},$$

and extend to a bilinear map $\cdot \colon k[G] \times k[G] \to k[G]$ over k. The identity is e. In fact, $k \to k[G] \colon c \mapsto ce$ makes this a k-algebra.

Now, any representation of G/k is automatically a $k[G]$-module and any $k[G]$-module is a representation of G/k.

Note that $k[G]$ is commutative $\iff$ G is abelian.

Definition 5.16

Let M be an R-module. A **submodule** $N \subseteq M$ is a subgroup that is closed under multiplication, i.e., $R \cdot N \subseteq N$.

Given a submodule $N \subseteq M$, M/N is naturally an R-module.

Definition 5.17

Let M be an R-module. If $m \in M$, the **annihilator of m** is $\operatorname{Ann}(m) := \{x \in R : xm = 0\}$. The **annihilator of M** is $\operatorname{Ann}(M) := \{x \in R : xm = 0 \text{ for all } m \in M\}$.

Let's start defining the category.

Definition 5.18

A **module homomorphism** is an R-linear homomorphism of abelian groups.

Given $\varphi \colon M \to N$, $\ker(\varphi) \subseteq M$, $\operatorname{im}(\varphi) \subseteq N$ are submodules. The fundamental theorems (as with other algebraic structures) apply.[4]

Given R-modules $\{M_\alpha\}$, we have a product and direct sum. $\prod_\alpha M_\alpha \supseteq \bigoplus_\alpha M_\alpha$ (recall in a direct sum, all but finitely many entries are zero, whereas the product has no such restriction). Categorically, the product is a categorical product:

$$\begin{tikzcd}
 & M_\alpha \\
N \arrow[ur, "\varphi_\alpha"] \arrow[r, dashed, "\exists!"'] & \prod_\alpha M_\alpha \arrow[u, "\pi_\alpha"']
\end{tikzcd}$$

and the direct sum is a categorical coproduct:

$$\begin{tikzcd}
 & M_\alpha \arrow[dl, "\varphi_\alpha"'] \arrow[d, "\iota_\alpha"] \\
N & \bigoplus_\alpha M_\alpha \arrow[l, dashed, "\exists!"]
\end{tikzcd}$$

Suppose M, N are R-modules. If $\varphi, \psi \colon M \to N$ are R-module homomorphisms, then so is $r\varphi + s\psi$ for $r, s \in R$ (this only happens because R is commutative!). As a result, $\operatorname{Hom}_{R\text{-mod}}(M, N) =: \operatorname{Hom}_R(M, M)$ is an R-module.

In particular, we have that the **endomorphisms** of a module M, $\operatorname{End}_{R\text{-mod}}(M) := \operatorname{End}_R(M) := \operatorname{Hom}_R(M, M)$ form an R-module, but also carries a composition operation ($\circ$). So $(\operatorname{End}_R(M), +, \circ)$ is a ring with $1 = \mathrm{id}_M$. In addition, for $r \in R$, $r \cdot \mathrm{id}_M \in \operatorname{End}_R(M)$. We consider the map $r \mapsto r \cdot \mathrm{id}_M$. Then the R-module structure on $\operatorname{End}(M)$ can be viewed as setting $r \cdot \varphi := (r \cdot \mathrm{id}_M) \circ \varphi$.

Remark 5.24. Here's an equivalent definition of a module. Let M be an abelian group. Then $\operatorname{End}_{\mathbb{Z}}(M)$ is a ring. Under some ring map $R \to \operatorname{End}_{\mathbb{Z}}(M)$, we get an R-module structure.

February 7, 2025 To restate the result in the above remark, given an abelian group M, we have the correspondence

$$\left\{\begin{matrix}\text{R-module structues} \\ \text{on } M\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{ring homomorphisms} \\ R \to \operatorname{End}_{\mathbb{Z}}(M)\end{matrix}\right\}.$$

[4] One possible explanation is that the category of R-modules, R-Mod forms an **abelian category**.

Example 5.13 – We use this correspondence to describe R-modules for various rings. The main object of note will be $\mathrm{Hom}_{\mathsf{Ring}}(R, S)$ for an arbitrary ring S, which we will later specialize to $S = \mathrm{End}_{\mathbb{Z}}(M)$.

- If $R = \mathbb{Z}$, $\mathrm{Hom}_{\mathsf{Ring}}(R, S)$ always has a unique morphism for all rings S. With the correspondence, this means all abelian groups M are $\mathbb{Z}$-modules.
- If $R = \mathbb{Z}/n$, $\mathrm{Hom}_{\mathsf{Ring}}(R, S)$ has a unique morphism if $n = 0$ in S for some $n \in \mathbb{Z}$, and none exist if $n \neq 0$ for all n. The corresponding R-modules are abelian groups M with $n \cdot M = 0$.
- If $R = \mathbb{Q}$, a unique morphism in $\mathrm{Hom}_{\mathsf{Ring}}(R, S)$ exists when $n \cdot 1 \in S^{\times}$ when $n \in \mathbb{Z} \setminus \{0\}$. The corresponding R-modules are those such that the map $x \mapsto n \cdot x$ is bijective for all $n \neq 0$ (in other words, the group is *divisible* and *torsion-free*).
- If $R = \mathbb{Z}[x]$, any morphism in $\mathrm{Hom}_{\mathsf{Ring}}(R, S)$ is uniquely determined by the image of x. The corresponding R-modules are abelian groups M together with a map $A\colon M \to M$ which represents "multiplication by x."
- If $R = \mathbb{Z}[x, y]$, any morphism in $\mathrm{Hom}_{\mathsf{Ring}}(R, S)$ is uniquely determined by the image of x and y, say, α, β, but we also impose that α and β commute (recall, $\mathrm{End}_R(M)$ is not necessarily commutative!). The corresponding R-modules are abelian groups M together with commuting maps $A, B\colon M \to M$ representing "multiplication by x and y."
- If $R = \mathbb{R}[x]$, any morphism $\varphi \in \mathrm{Hom}_{\mathsf{Ring}}(R, S)$ is uniquely determined by the image of $\mathbb{R}$ and the image of x. However, we also need to impose that $\varphi(x)$ commutes with all of $\varphi(\mathbb{R}) \subseteq S$. The corresponding R-modules are abelian groups M that are $\mathbb{R}$-modules ($\mathbb{R}$-vector spaces) with a map $A\colon M \to M$ that commutes with "scaling" by $\mathbb{R}$ (i.e., A is $\mathbb{R}$-linear).

Exercise 5.1. What are the corresponding R-modules when $R = \mathbb{C}[x, y]/(x^2 + y^2 - 1)$?

5.10. Free modules

February 10, 2025

Definition 5.19

Let M be an R-module and consider a collection of elements $\{x_\alpha\}_{\alpha \in I} \subseteq M$. The **submodule generated by $\{x_\alpha\}$** is

$$\langle x_\alpha \rangle := \left\{ \sum_{\substack{\alpha \\ \text{finite}}} c_\alpha x_\alpha \right\}.$$

We say the x_α's are **linearly independent** if for every finite combination $\sum_{\substack{\alpha \\ \text{finite}}} c_\alpha x_\alpha = 0$ implies $c_\alpha = 0$ for all α.

We say the $\{x_\alpha\}$ forms a **basis** if they generate M and are linearly independent.

Definition 5.20

Given an indexing set I, the **free module** on I is the module

$$R^{\oplus I} := \{(c_\alpha) \mid \text{almost all } c_\alpha\text{'s are zero}\}.$$

"almost all" means all but finitely many.

Given any module M with a subset indexed by I, we have a map

$$\begin{aligned} \varphi\colon R^{\oplus I} &\to M \\ (c_\alpha) &\mapsto \sum_\alpha c_\alpha x_\alpha \end{aligned}$$

So M being generated by $\{x_\alpha\}$ is the same as φ being surjective, the x_α's being linearly independent is the same as φ being injective.

Definition 5.21

M is **free** R-submodule if a basis exists (equivalently, $M \cong R^{\oplus I}$ for some I using the map φ above).

M is **finitely generated (f.g.)** if there exists a finite set of generators (in other words, $M \cong R^n/N$ for some submodule $N \subseteq R^n$).

Non-Example 5.1 (Non-free modules) –

1. $\mathbb{Z}/2$ as a $\mathbb{Z}$-module.
2. $\mathbb{Q}$ as a $\mathbb{Z}$-module (you cannot find more than one linearly independent element).
3. Any non-principal ideal $I \subseteq \mathbb{C}[x,y]$ (e.g., (x,y)) as a $\mathbb{C}[x,y]$-module, since if we have $f, g \in I$, then $fg - gf = 0$.

Remark 5.25. $R^{\oplus I}$ has a universal mapping property. Let $e_\alpha \in R^{\oplus I}$ be the element that is 1 in the αth entry and 0 everywhere else. Given any M and $\{x_\alpha\} \subseteq M$, there exists a unique map

$$\varphi\colon R^{\oplus I} \to M$$

such that $\varphi(e_\alpha) = x_\alpha$.

Theorem 5.26

If R is a PID and M is a free R-module, any submodule $N \subseteq M$ is free.

Proof (sketch). Idea: Let $M \cong R^2$. Consider the intersection with the x-axis: $N \cap (R \times \{0\})$. Since R is a PID, this intersection is generated by $e_1 := (a, 0)$. Now project N onto the y-axis: $\pi_2(N) \subseteq R$, and let it be generated by b. Suppose $e_2 := (c, b) \in \pi_2^{-1}(N)$. Then prove e_1, e_2 for a basis for N (warning: if either a or b are zero, then omit the corresponding basis element).

General finite case: If $M \cong R^m$, consider the module R^k for $k \leq m$ embedded into R^m where the first k coordinates are in R, and the rest are zero (by abuse of notation, denote it R^k). Let

$$\pi_k\colon R^k \to R$$

give the kth coordinate. Consider $\pi_k(N \cap R^k) \subseteq R$. R is a PID, so it is generated by some (a_k). Let $e_k = (*, \dots, *, a_k, 0, \dots, 0) \in \pi_k^{-1}(a_k)$. Now prove that $\{e_k : a_k \neq 0\}$ forms a basis for N.

General case: See book. □

5.11. Exact sequences

Consider modules M_1, M_2, M_3 and morphisms such that

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3.$$

We say this is **exact** if $\operatorname{im} f = \ker g$. Note that if $\operatorname{im} f \subseteq \ker g$, $gf = 0$.

In general, for a sequence $\{M_i\}$ of modules are morphisms such that

$$\cdots \to M_{i-1} \to M_i \xrightarrow{f} M_{i+1} \xrightarrow{g} M_{i+2} \to M_{i+3} \to \cdots$$

we say it is **exact at M_{i+1}** if $\operatorname{im} f \subseteq \ker g$. The sequence is *exact* if it is exact at all M_i.

Example 5.14 (Important exact sequences) –

1. a) The exactness of $0 \to L \xrightarrow{\varphi} M$ is the same as φ being injective (L embeds into M).

   b) The exactness of $L \xrightarrow{\varphi} M \to 0$ is the same as φ being surjective.

   c) ...so the exactness of $0 \to L \xrightarrow{\varphi} M \to 0$ is the same as φ being an isomorphism.

2. a) The exactness of $0 \to L \to M \xrightarrow{\varphi} N$ means that the image of L in M is the kernel of φ.

   b) The exactness of $M \xrightarrow{\varphi} N \to P \to 0$ means that P is isomorphic to $N/\operatorname{im}\varphi$.

   If $\varphi\colon M \to N$ is a morphism, the **cokernel** is defined as $\operatorname{coker}\varphi := N/\operatorname{im}\varphi$.

   c) ...so since the kernel and image exist for any morphism $\varphi\colon M \to N$, we can include it into an exact sequence

$$0 \to \underbrace{L}_{\ker\varphi} \to M \xrightarrow{\varphi} N \to \underbrace{P}_{\operatorname{coker}\varphi} \to 0.$$

3. A **short exact sequence** is an exact sequence of the form

$$0 \to L \to M \to N \to 0.$$

   This is equivalent to:

   - $L \hookrightarrow M$ and N is its cokernel,
   - $M \twoheadrightarrow N$ and L is its kernel,
   - we can identify L as a subset of M and $N = M/L$.

In undergraduate algebra, we considered the kernel and cokernel as objects, but for the future, we will want to consider them as an object together with a morphism (representing inclusion and projection respectively): $i\colon \ker f \to M'$, $p\colon M'' \to \operatorname{coker} f$.

Proposition 5.27 (Universal mapping property of ker and coker)
The kernel of a map $f\colon M \to M''$ is a has the following universal mapping property: $fi = 0$, and if $M' \xrightarrow{\gamma} M \xrightarrow{f} M''$ satisfies $gf = 0$, then there exists a unique map $\varphi\colon M' \to \ker f$ such that $i\varphi = \gamma$.

$$\begin{tikzcd}
\ker f \arrow[r, "i"] \arrow[rr, bend left, "0"] & M \arrow[r, "f"] & M'' \\
& M' \arrow[ul, dashed, "\exists!\varphi"] \arrow[u, "\gamma"'] \arrow[ur, "0"'] &
\end{tikzcd}$$

The cokernel of the map $f\colon M' \to M$ has the following universal mapping property: $pf = 0$, and if $M' \xrightarrow{f} M \xrightarrow{\gamma} M''$ satisfies $gf = 0$, then there exists a unique map $\psi\colon \operatorname{coker} f \to M''$ such that $\psi p = g$.

$$\begin{tikzcd}
M' \arrow[r, "f"] \arrow[rr, bend left, "0"] \arrow[dr, "0"'] & M \arrow[r, "p"] \arrow[d, "\gamma"'] & \operatorname{coker} f \arrow[dl, dashed, "\exists!\psi"] \\
& M'' &
\end{tikzcd}$$

Remark 5.28. In an additive category, we take these universal properties to be the *definitions* of $\ker f$ and $\operatorname{coker} f$. In this abstract case, the kernel (resp. cokernel) is actually the map $i\colon \ker f \to M$ (resp. $p\colon M \to \operatorname{coker} f$).

Example 5.15 (Splitting) – Given modules L, N, we can form an exact sequence involving $L \oplus N$ by

$$0 \to L \xrightarrow{x \mapsto (x,0)} L \oplus N \xrightarrow{(x,y) \mapsto y} N \to 0.$$

This is called a **split short exact sequence**. We say a short exact sequence $0 \to L \to M \to N \to 0$ **splits** if there exists an isomorphism $M \xrightarrow{\sim} L \oplus N$ that is compatible with the given maps: $L \to M \xrightarrow{\sim} L \oplus N\colon x \mapsto (x, 0)$, $M \xrightarrow{\sim} L \oplus N \to N\colon (x, y) \mapsto y$. This is summarized succinctly by the following diagram commuting:

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d, equal] & M \arrow[r] \arrow[d, "\sim"] & N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & L \arrow[r] & L \oplus N \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

Not all short exact sequences split. In $\mathrm{Mod}_{\mathbb{Z}}$, the following sequences split

$$0 \to \mathbb{Z}/2 \to \mathbb{Z}/2 \oplus \mathbb{Z}/2 \to \mathbb{Z}/2 \to 0,$$

$$0 \to \mathbb{Z}/2 \xrightarrow{\times 2} \mathbb{Z}/4 \xrightarrow{\text{mod } 2} \mathbb{Z}/2 \to 0.$$

But $\mathbb{Z}/4 \not\cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$.

Theorem 5.29

The following are equivalent:

1. The exact sequence $0 \to L \to M \to N \to 0$ splits.
2. The map $g\colon M \to N$ admits a **section** $s\colon N \to M$ (i.e. $gs = 1_N$).
3. The map $f\colon L \to M$ admits a **retract** $r\colon M \to L$ (i.e., $rf = 1_M$).

Exercise 5.2. Use the above theorem to prove that every exact sequence of vector spaces splits.

Example 5.16 – Let M have generators $\{x_i\}_{i\in I}$. This is equivalent to a surjection $R^{\oplus I} \to M$, which is the same as $R^{\oplus I} \xrightarrow{\pi} M \to 0$ being exact. $\ker \pi$ is a module representing the relations. Choose a set of generators $y_j = (y_{ji})_{i\in I} \in R^{\oplus I}$, which we could consider the "defining relations." Then M is the cokernel of the map

$$R^{\oplus J} \xrightarrow{\phi} R^{\oplus I} \xrightarrow{\pi} M \to 0.$$

Definition 5.22

February 14, 2025

A **presentation** of an R-module M is an exact sequence of the form

$$G \to F \to M \to 0,$$

where G and F are free modules. F represents the **generators** of M. The image of G generates the space of **relations**.

A module M is **finitely generated** if there exists exact $G \to F \to M \to 0$ where F, G are finite rank free modules. We can write $M = R^n/AR^m$ for some $A \in \mathrm{Mat}_{n\times m}(R)$.

5.11.1. Exactness and Hom

Recall $\mathrm{Hom}_R(M, N)$ is a functor that is covariant in the N entry and contravariant in the M entry.

Theorem 5.30

1. If $M' \to M \to M'' \to 0$ is exact, then $0 \to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N)$ is exact.
2. If $0 \to N' \to N \to N''$ is exact, then $0 \to \mathrm{Hom}(M, N') \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'')$ is exact.

Proof. (1) Let α be the map from $M' \to M$. Then exactness is the same as $M'' \cong \operatorname{coker} \alpha = M/\operatorname{im} \alpha$. The UMP of the cokernel says that we have 1-1 correspondence

$$\mathrm{Hom}(\operatorname{coker} \alpha, N) \overset{1-1}{\leftrightarrow} \{f\colon M \to N \mid f\alpha = 0\}.$$

The this set is the kernel of $\mathrm{Hom}(\bullet, N)(\alpha) := \alpha^*$, where $\alpha^*\colon \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N)$. Thus, $\mathrm{Hom}(M'', N) \to \ker(\mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N))$ is an isomorphism. Therefore, $0 \to \mathrm{Hom}_R(M'', N) \xrightarrow{\alpha^*} \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N)$ is exact.

(2) This is a dual proof, so we give the main ideas. Let β be the map from $N' \to N$. Then use the UMP of the kernel:

$$\operatorname{Hom}(M, \ker\beta) \overset{1-1}{\leftrightarrow} \{f\colon M \to N \mid \beta f = 0\}. \qquad \square$$

Definition 5.23

A module P is **projective** if whenever we have a surjection $\beta\colon N \to N''$ and a map $\alpha\colon P \to N''$, there exists a map $\gamma\colon P \to N$ such that $\beta\gamma = \alpha$. In other words, the following diagram commutes:

$$\begin{tikzcd} P \arrow[d, dashed, "\gamma"'] \arrow[dr, "\alpha"] & \\ N \arrow[r, "\beta"'] & N'' \end{tikzcd}$$

Theorem 5.31

Let P be a module. The following are equivalent:

1. P is projective.
2. Every short exact sequence $0 \to K \to M \to P \to 0$ splits (i.e. we have a section $P \dashrightarrow M$).
3. P is a summand of free module. In other words, there exists a free module F so that $F \cong P \oplus Q$.
4. If $N' \to N \to N''$ is exact, then $\operatorname{Hom}(P, N') \to \operatorname{Hom}(P, N) \to \operatorname{Hom}(P, N'')$ is exact.
5. If $0 \to N' \to N \to N'' \to 0$ is exact, then
$$0 \to \operatorname{Hom}(P, N') \to \operatorname{Hom}(P, N) \to \operatorname{Hom}(P, N'') \to 0$$
is exact.
6. If $\beta\colon N \twoheadrightarrow N''$, then $\beta_*\colon \operatorname{Hom}(P, N) \to \operatorname{Hom}(P, N'')$ is surjective.

Proof. ((1) $\implies$ (2)) Let $0 \to K \to M \to P \to 0$ be exact. Consider the identity map $\mathrm{id}\colon P \to P$. Then there exists a $\beta\colon P \to M$ such that $\beta\gamma = \mathrm{id}_P$, which implies γ is our desired section that splits.

((2) $\implies$ (3)) Pick a set of generators for P. Then we have a short exact sequence $0 \to K \to F \to P \to 0$ with F a free module. $P \oplus K \cong F$ by (2).

((3) $\implies$ (4)) If $F = R^\Lambda$, then $\operatorname{Hom}(R^\Lambda, N) = \prod_{\lambda\in\Lambda} N$. Repeating for $\operatorname{Hom}(R^\Lambda, N')$, $\operatorname{Hom}(R^\Lambda, N'')$, we are asking for the exactness of

$$\prod_{\lambda\in\Lambda} N' \to \prod_{\lambda\in\Lambda} N \to \prod_{\lambda\in\Lambda} N'',$$

which follows from the exactness of $N' \to N \to N''$.

Since $\operatorname{Hom}(F, N') \to \operatorname{Hom}(F, N) \to \operatorname{Hom}(F, N'')$ is exact, $\operatorname{Hom}(P, N') \to \operatorname{Hom}(P, N) \to \operatorname{Hom}(P, N'')$ is exact.

((4) $\implies$ (5)) Apply (4) at each of the middle three terms.

((5) $\implies$ (6)) Let $\beta\colon N \twoheadrightarrow N''$. Then letting $N' = \ker\beta$ gives us that

$$0 \to N' \to N \to N'' \to 0$$

is exact. By (5),

$$0 \to \operatorname{Hom}(P, N') \to \operatorname{Hom}(P, N) \to \operatorname{Hom}(P, N'') \to 0$$

is exact, which implies $\beta_*\colon \operatorname{Hom}(P, N) \to \operatorname{Hom}(P, N'')$ is surjective.

((6) $\implies$ (1)) If $\beta\colon N \to N''$ is surjective, then $\beta_*\colon \operatorname{Hom}(P, N) \to \operatorname{Hom}(P, N'')$ is a surjection. Let $\alpha \in \operatorname{Hom}(P, N'')$. Then we can write $\beta\gamma = \alpha$ for some $\gamma \in \operatorname{Hom}(P, N)$ by the surjectivity of β_*. □

Example 5.17 –

1. Free modules are projective (use (3)).
2. If $R = A \times B$, where R, A, B are rings, then $R = (A \times 0) \oplus (0 \times B)$ as a module. Each $A \times 0$ and $0 \times B$ are projective, but not free if $A \neq 0$, $B \neq 0$.
3. From number theory, we have that $R = \mathbb{Z}[\sqrt{-5}]$ is not a UFD because, e.g. the ideals $I = (3, 1 + \sqrt{-5})$, $I' = (3, 1 - \sqrt{-5})$. I and I' (as R-modules) are projective but not free, which we will prove. One can show that I and I' are not principal. However, they are maximal because $R/I \cong R/I' \cong \mathbb{Z}/3$. We can check that $I \neq I'$, so I and I' are comaximal. By CRT, $I \cap I' = II'$, which turns out to be (3), a free R-module. So it fits into an exact sequence

$$0 \to \underbrace{I \cap I'}_{\cong R} \to I \oplus I' \to R \to 0,$$

hence $I \oplus I' \cong R \oplus R$, so each ideal is projective.

Remark 5.32. There is a "dual" notion of a projective module. An **injective module** is a module Q such that, given an exact sequence

$$0 \to M' \to M \to M'' \to 0,$$

the induced sequence

$$0 \to \operatorname{Hom}(Q, M') \to \operatorname{Hom}(Q, M) \to \operatorname{Hom}(Q, M'') \to 0$$

is exact.

5.12. Tensor products

Definition 5.24

February 17, 2025

Let R be a ring and M, N, P R-modules. $\beta\colon M \times N \to P$ is **bilinear** if $\beta(m + m', n) = \beta(m, n) + \beta(m', n)$, $\beta(m, n + n') = \beta(m, n) + \beta(m, n')$, $\beta(rm, n) = r\beta(m, n) = \beta(m, rn)$.

Definition 5.25

If M and N are R-modules, the **tensor product** $M \otimes_R N$ (also written $M \otimes N$ when the ring R is clear) is the quotient

$$M \otimes_R N := R^{M \times N}/A,$$

where

$$\begin{aligned} A = \langle &(m+m', n) - (m,n) - (m', n), (m, n+n') - (m,n) - (m,n'), \\ &(rm, n) - r(m,n), r(m,n) - (m, rn) : m, m' \in M, n, n' \in N, r \in R \rangle. \end{aligned}$$

Write $m \otimes n$ as the image of (m,n) in $M \otimes N$ under the above quotient.

Theorem 5.33 (Universal mapping property of $\otimes$)

If M, N, P are R-modules, then

$$\mathrm{Hom}_R(M \otimes N, P) \cong \mathrm{Bil}_R(M \times N, P),$$

where the RHS are bilinear maps from $M \times N$ to P.

Proof (sketch). Recall $\mathrm{Hom}(R^{M \times N}, P)$ is precisely (set) maps $M \times N \to P$. The quotient mapping property guarantees the only maps $\mathrm{Hom}(R^{M\times N}/A, P)$ are bilinear maps. □

The tensor product is commutative and associative. We have $M \otimes R \cong M$ (so $M \otimes R^{\oplus n} \cong M^{\oplus n}$). We also have "distributivity:"

$$M \otimes \left(\bigoplus_\alpha N_\alpha \right) \cong \bigoplus_\alpha M \otimes N_\alpha.$$

5.12.1. Hom-tensor adjunction

Proposition 5.34

We have a bijection

$$\mathrm{Bil}_R(M \times N, P) \xrightarrow{\sim} \mathrm{Hom}(M, \mathrm{Hom}(N, P))$$

given by the map $\beta \mapsto [m \mapsto \beta(m, -)]$.

We'll prove a more powerful version (5.35).

Definition 5.26

Let R, R' be rings. An **(R, R')-bimodule** N is an abelian group with R-module and R'-module structures that "play nicely" with each other:

$$r(r'n) = r'(rn)$$

for $r \in R$, $r' \in R'$, $n \in N$.

Example 5.18 –

1. If N is an R-module, then it is automatically an (R,R)-bimodule, where we have the same action for both rings.
2. If $f\colon R \to R'$ is a ring homomorphism, then R' is an (R,R')-bimodule, where the R-action comes from the R'-action using $f(r)$.

Theorem 5.35

Let R, R' be rings, M and R-module, N an (R,R')-bimodule, P an R'-module. Then

$$\mathrm{Hom}_{R'}(M \otimes_R N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_{R'}(N,P)).$$

Remark 5.36. We'll need to show $M \otimes_R N$ is an R'-module and $\mathrm{Hom}_{R'}(N,P)$ is an R-module.

Proof of Theorem 5.35. On the LHS, we have

$$\begin{aligned}\mathrm{Hom}_{R'}(M \otimes_R N, P) = \{\beta\colon M \times N \to P \mid \beta \text{ is biadditive},\\ \beta(m, rn) = \beta(rm, n), \beta(m, r'n) = r'\beta(m,n), r \in R, r' \in R'\}.\end{aligned}$$

On the RHS, assume that maps in $\mathrm{Hom}_R(M, \mathrm{Hom}_{R'}(N,P))$ can be written as $[m \mapsto \beta(m,-)]$, hence we can consider it as a single map $\beta\colon M \times N \to P$ (this is a general tehcnique called *currying*). One can verify that

$$\begin{aligned}\mathrm{Hom}_R(M, \mathrm{Hom}_{R'}(N,P)) = \{\beta\colon M \times N \to P \mid \beta \text{ is biadditive},\\ \beta(m, rn) = \beta(rm, n), \beta(m, r'n) = r'\beta(m,n), r \in R, r' \in R'\},\end{aligned}$$

which corresponds with what we wrote above. □

5.12.2. Exactness

Definition 5.27

A functor $F\colon \mathrm{Mod}_R \to \mathrm{Mod}_{R'}$ is **left exact** if it preserves kernels. M' is a kernel if and only if it fits into an exact sequence $0 \to M' \to M \to M''$. Then F being left exact is the same as $0 \to FM' \to FM \to FM''$ being exact.

F is **right exact** if it preserves cokernels. M'' is a cokernel if and only if it fits into an exact sequence $M' \to M \to M'' \to 0$. Then F being right exact is the same as $FM' \to FM \to FM'' \to 0$ being exact.

F is **exact** if it is both left and right exact. Equivalently, if $M' \to M \to M''$ is exact, then $FM' \to FM \to FM''$ is exact.

We showed before that Hom is left exact in both arguments (5.30).

Theorem 5.37 ($- \otimes N$ is right exact)

The tensor product is right exact both arguments: if $M' \to M \to M'' \to 0$ is exact, then so is $M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$.

Remark 5.38. Stating the theorem for the other argument is redundant since the tensor product is commutative.

Remark 5.39 (How to remember this theorem if you know category theory)**.** The tensor product and the cokernel are both colimits, and colimits commute.

Proof. Let M'' be the cokernel of a map $M' \to M$. In other words, it fits in an exact sequence

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

Using pullbacks, we can create a sequence

$$0 \to \mathrm{Hom}(M'', \mathrm{Hom}(N,P)) \xrightarrow{g^*} \mathrm{Hom}(M, \mathrm{Hom}(N,P)) \xrightarrow{f^*} \mathrm{Hom}(M', \mathrm{Hom}(N,P)).$$

By the Hom-tensor adjunction,

$$0 \to \mathrm{Hom}(M'' \otimes N, P) \to \mathrm{Hom}(M \otimes N, P) \to \mathrm{Hom}(M' \otimes N, P)$$

is also exact. This shows that $M'' \otimes N$ is the cokernel of $M \otimes N \to M' \otimes N$ using the universal mapping property of the cokernel again. □

5.12.3. Some special examples of tensor products

February 19, 2025

Example 5.19 – This right-exactness property is useful for actual computations. Let M be an R-module defined by $M = Re_1 \oplus Re_2 / \langle (r,s) \rangle$ for basis elements e_1, e_2 and $r, s \in R$. Then M belongs to the sequence

$$R \xrightarrow{f} R^{\oplus 2} \to M \to 0,$$

where $f(\alpha) = (r\alpha, s\alpha)$. Let N be any R-module. We wish to compute $M \otimes N$. Right exactness implies

$$N \xrightarrow{f \otimes \mathrm{id}_R} N^{\oplus 2} \to M \otimes N \to 0$$

is exact. The map $f \otimes \mathrm{id}_R$ sends $n \mapsto (rn, sn) = (re_1 + se_2)n$. Therefore, $M \otimes N$ "looks like" $(e_1 \otimes N) \otimes (e_2 \otimes N) / \langle re_1 \otimes n + se_2 \otimes n : n \in N \rangle$.

Example 5.20 – Consider $M \otimes_R (R/I)$. R/I fits into an exact sequence

$$I \to R \to R/I \to 0.$$

By right exactness of the tensor,

$$M \otimes I \to M \otimes R \to M \otimes (R/I) \to 0.$$

The elements of $M \otimes I$ are $m \otimes x$ for $x \in I$. These map to $m \otimes x \in M \otimes R$, which can be identified in M with xm. Hence, $M \otimes (R/I) \cong M/IM$.

February 21, 2025

Remark 5.40. The map $I \to R$ above is injective, but the tensor product is only right exact, so $M \otimes I \to M \otimes R$ is *not* generally injective, so we don't have $M \otimes I \cong IM$.

For example, if $R = \mathbb{Z}$ and $I = (2)$, then we have an exact sequence

$$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2 \to 0.$$

Then, tensoring with M, we have that

$$M \xrightarrow{\times 2} M \to M/2M \to 0$$

is exact. But $M \xrightarrow{\times 2} M$ my not be injective. (Such counterexamples hold for all n, as we will see (for the case of primes) in)

Let R' be an R-algebra. Then we can consider R' as an R-module. Let M be an R module and consider $M \otimes_R R'$. This has an R'-module structure by $s(m \otimes r') := m \otimes (sr')$, for $s, r' \in R'$, $m \in M$, and extending by linearity. We call this an **extension of scalars** from R to R'.

Example 5.21 – If $R = \mathbb{R}$, $R' = \mathbb{C}$, $M = \mathbb{R}^n$. Then

$$\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}^n.$$

Concretely, if $\mathbf{a} \in \mathbb{R}^n$ and $x + yi \in \mathbb{C}$, then

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \otimes (x + yi) = \begin{bmatrix} xa_1 \\ \vdots \\ xa_n \end{bmatrix} \otimes 1 + \begin{bmatrix} ya_1 \\ \vdots \\ ya_n \end{bmatrix} \otimes i.$$

So generally, $- \otimes_{\mathbb{R}} \mathbb{C}$ gives a functor

$$\mathsf{Vect}_{\mathbb{R}} \to \mathsf{Vect}_{\mathbb{C}},$$

which we call **complexification**. The nice thing about this compared to the undergraduate treatment is that this description is basis-free.

Example 5.22 (Tensor over rings) – If $R = \mathbb{Z}$, R' is any ring, and $M = \mathbb{Z}/n$, then

$$\mathbb{Z}/n \otimes_{\mathbb{Z}} R = R/nR.$$

For example, if $R' = \mathbb{Q}$,

$$\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Q} = 0.$$

Remark 5.41. If N is an (R, R')-bimodule, then $M \otimes_R N$ is an R'-module. In particular, R' is an (R, R')-bimodule, explaining why $M \otimes_R R'$ could be viewed as an R'-module.

Remark 5.42 (Cautionary tale; what goes wrong with infinity products)**.** Consider $\mathbb{R}^\infty \otimes_{\mathbb{R}} \mathbb{R}[x]$ (where $\mathbb{R}^\infty$ is the infinite direct product of $\mathbb{R}$'s). We claim this is *not* $(\mathbb{R}[x])^\infty$. Indeed, simple tensors in $\mathbb{R}^\infty \otimes_{\mathbb{R}} \mathbb{R}[x]$ are

$$(a_1, a_2, \dots) \otimes (c_0 + c_1 x + \cdots + c_k x^k) = (c_0 a_1, c_0 a_2, \dots) \otimes 1 + \cdots + (c_k a_1, c_k a_2, \dots) \otimes x^k.$$

Since elements of the tensor product of finite sums of such elements, the degree of each entry is "uniformly bounded". Hence, $\mathbb{R}^\infty \otimes_{\mathbb{R}} \mathbb{R}[x] \cong (\mathbb{R}^\infty)[x]$. An element not in this ring is $(1, x, x^2, \dots)$.

Remark 5.43 (Restriction of scalars)**.** $M \otimes_R R'$ has universal mapping property from $\otimes_R$. It has a different universal mapping property as an R' module: for M an R-module and N an R'-module, given R-linear $f \colon M \to N$, it uniquely factors through the surjective R'-linear map $M \otimes_R R' \to N$.

$$\begin{tikzcd}
M \arrow[r, dashed, "\exists!"] \arrow[dr, "f"'] & M \otimes_R R' \arrow[d] \\
& N
\end{tikzcd}$$

5.13. Interlude: category theory, limits, and colimits

February 24, 2025 Recall category theory from last semester. Here are some recent examples of functors:

Example 5.23 – The tensor product is a functor

$$- \otimes -\colon \mathsf{Mod}_R \times \mathsf{Mod}_R \to \mathsf{Mod}_R.$$

Extension of scalars is a functor

$$- \otimes_R R'\colon \mathsf{Mod}_R \to \mathsf{Mod}_{R'}$$

(implicitly, we need to show $M \to M'$ induces a map $M \otimes_R R' \to M' \otimes_R R'$ that is functorial).

The $\mathrm{Hom}_R(-,-)$ functor is contravariant in the first input and covariant in the second. In other words,

$$\mathrm{Hom}_R(-,-)\colon (\mathsf{Mod}_R)^{\mathrm{op}} \times \mathsf{Mod}_R \to \mathsf{Mod}_R.$$

Definition 5.28

Let $\mathscr{C}, \mathscr{D}$ be categories. Define $\mathsf{Fun}(\mathscr{C}, \mathscr{D})$ be a category where

- objects are functors $\mathscr{C} \to \mathscr{D}$,
- morphisms are natural transformations. Recall that given $F, G\colon \mathscr{C} \to \mathscr{D}$, a *natural transformation* $\eta\colon F \to G$ consists of morphisms $\eta(A)\colon FA \to GA$ such that the following diagram in $\mathscr{D}$ commutes

$$\begin{tikzcd} A \arrow[d, "\varphi"'] & FA \arrow[r, "\eta(A)"] \arrow[d, "F(\varphi)"'] & GA \arrow[d, "G(\varphi)"] \\ B & FB \arrow[r, "\eta(B)"'] & GB \end{tikzcd}$$

If each $\eta(A)$ is an isomorphism for $A \in \mathscr{C}$, then we say that η is a **natural isomorphism**, denoted $F \simeq G$.

Definition 5.29

A functor $F\colon \mathscr{C} \to \mathscr{D}$ is an **equivalence (of categories)** if there exists a functor $G\colon \mathscr{D} \to \mathscr{C}$ such that the functor $F \circ G$ is naturally isomorphic to $\mathrm{Id}_{\mathscr{D}}$ and the functor $G \circ F$ is naturally isomorphic to $\mathrm{Id}_{\mathscr{C}}$. We call G a **quasi-inverse** to F.

Example 5.24 – Let k be a field and $\mathsf{Vect}_k^{\mathrm{f.d.}}$ be the space of finite-dimensional k-vector spaces. Consider the dual functor

$$\bullet^{\vee}\colon \left(\mathsf{Vect}_k^{\mathrm{f.d.}}\right)^{\mathrm{op}} \to \mathsf{Vect}_k^{\mathrm{f.d.}}\colon V \mapsto V^{\vee} = \mathrm{Hom}(V, k).$$

We can take the double dual, which is a functor

$$\left(\bullet^{\vee}\right)^{\vee}\colon \mathsf{Vect}_k^{\mathrm{f.d.}} \to \mathsf{Vect}_k^{\mathrm{f.d.}}\colon V \mapsto (V^{\vee})^{\vee} = \mathrm{Hom}(V^{\vee}, k).$$

This turns out to be an equivalence of categories.

Example 5.25 (Idempotents) – Consider the category Idem where objects are pairs (R, e), where R is a ring and $e \in R$ is an idempotent. Morphisms $(R, e) \to (R', e')$ are morphisms $\varphi\colon R \to R'$ such that $\varphi(e) = e'$. Now consider the category $\mathsf{Ring} \times \mathsf{Ring}$.

There is an equivalence of categories given by the functors

$$F\colon (R, e) \mapsto (R/(e), R/(1-e)),$$

$$G\colon (R_1, R_2) \mapsto (R_1 \times R_2, (0, 1)),$$

(implicitly, we have to show these are indeed functors).

February 26, 2025

Theorem 5.44

A functor $F\colon \mathscr{C} \to \mathscr{D}$ is an equivalence of categories if and only if

1. F is **fully faithful**: for all $C, C' \in \mathscr{C}$, the induced map

$$\mathrm{Hom}_{\mathscr{C}}(C, C') \xrightarrow{F} \mathrm{Hom}_{\mathscr{D}}(FC, FC')$$

   is a bijection.

2. F is **essentially surjective**: for all $D \in \mathscr{D}$, there exists $C \in \mathscr{C}$ such that $FC \cong D$.

Proof sketch of $\Longleftarrow$. We construct the quasi-inverse functor $G\colon \mathscr{D} \to \mathscr{C}$. For each $D \in \mathscr{D}$, choose some $C \in \mathscr{C}$ and an isomorphism $\varphi_D\colon FC \xrightarrow{\sim} D$. Set $GD := C$. Now if we have a morphism $f \in \mathrm{Mor}(D, D')$, let $G(f) \in \mathrm{Hom}_{\mathscr{C}}(C, C')$ that is the preimage of the morphism $\tilde{f} := \varphi_{D'}^{-1} f \varphi_D \in \mathrm{Hom}_{\mathscr{D}}(FC, FC')$

$$\begin{tikzcd}
FC \arrow[r, "\sim"] \arrow[d, dashed, "\tilde{f}"'] & D \arrow[d, "f"] \\
FC' & D' \arrow[l, "\sim"]
\end{tikzcd}$$

To do after this: verify this is a functor, verify that G is a quasi-inverse. □

If we only make the fully faithful assumption, define the **essential image of F** as

$$\mathrm{Im}(F) := \{D \in \mathscr{D} : F(C) \cong D \text{ for some } C \in \mathscr{D}\}.$$

The essential image is a subcategory of $\mathscr{D}$ and F is an equivalence of categories between $\mathscr{C}$ and $\mathrm{Im}(F)$.

Definition 5.30

A **full subcategory** is a subcategory $\mathscr{C} \subseteq \mathscr{C}'$ such that $\mathrm{Hom}_{\mathscr{C}'}(A, B) = \mathrm{Hom}_{\mathscr{C}}(A, B)$ for all objects $A, B \in \mathscr{C}$.

Example 5.26 – $\mathsf{AbGp} \subseteq \mathsf{Grp}$ is a full subcategory.

Corollary 5.45

F is fully faithful if and only if it gives an equivalence between $\mathscr{C}$ and a full subcategory of $\mathscr{D}$.

We call F a **full embedding**.

Proverb. *The best things in life are equivalences of categories.*

Example 5.27 – Let X be path-connected and $x \in X$. Then there is an equivalence of categories

$$\mathsf{Cov}(X) \coloneqq \{\text{Covering spaces of } X\} \xrightarrow{\sim} G\mathsf{Set},$$

where $G = \pi_1(X, x)$.

5.13.1. The Yoneda lemma

Consider $h_A(-) \coloneqq \mathrm{Hom}_{\mathscr{C}}(A, -)$ as a functor $\mathscr{C} \to \mathsf{Set}$. We have a functor $h_\bullet \colon \mathscr{C}^{op} \to \mathsf{Fun}(\mathscr{C}, \mathsf{Set})$ given by $A \mapsto h_A(-)$ and $f \in \mathrm{Hom}(A, B)$ maps to the natural transformation $f^* \colon h_B(-) \to h_A(-)$, defined for $g \in \mathrm{Hom}(C, C')$ as

$$\begin{tikzcd}
\mathrm{Hom}(B,C) \arrow[r, "f^*(C)"] \arrow[d, "g_*(h_B)"'] & \mathrm{Hom}(A,C) \arrow[d, "g_*(h_A)"] \\
\mathrm{Hom}(B,C') \arrow[r, "f^*(C')"'] & \mathrm{Hom}(A,C')
\end{tikzcd}$$

where

$$\begin{tikzcd}
h \arrow[r, mapsto] \arrow[d, mapsto] & h \circ f \arrow[d, mapsto] \\
g \circ h \arrow[r, mapsto] & g \circ h \circ f
\end{tikzcd}$$

We call this the **Yoneda embedding**.

Theorem 5.46

The Yoneda embedding is fully faithful.

Dually, there is a functor $h^A(-) \coloneqq \mathrm{Hom}_{\mathscr{C}}(-, A)$, which gives us a functor $\mathscr{C} \to \mathsf{Fun}(\mathscr{C}^{op}, \mathsf{Set})$ given by $A \mapsto h^A(-)$. The same results follow.

To prove this, we prove the following stronger statement:

Theorem 5.47 (Yoneda lemma)

1. Given $A \in \mathscr{C}$ and $F \in \mathsf{Fun}(\mathscr{C}, \mathsf{Set})$, there is an isomorphism

$$\mathrm{Hom}_{\mathsf{Fun}(\mathscr{C},\mathsf{Set})}(h_A, F) \to FA$$
$$\varphi \mapsto \varphi(A)(\mathrm{id}_A).$$

2. If we view both sides of the equality as functors,

$$\mathscr{C} \times \mathsf{Fun}(\mathscr{C}, \mathsf{Set}) \to \mathsf{Set},$$

then this isomorphism is natural.

February 28, 2025

This theorem gives us a categorical framework for universal mapping properties, which we will now describe.

Definition 5.31

Given $F\colon \mathscr{C} \to \mathrm{Set}$, F is **representable** if there exists $A \in \mathscr{C}$ such that $F \simeq h_A$ (or $F \simeq h^A$). We say A **represents** the functor F.

Proposition 5.48

If F is representable, the representing object A is unique up to natural isomorphism.

Proof. If $h_A \simeq F$ and $h_B \simeq F$, then there is a natural isomorphism $h_A \simeq h_B$. Since the Yoneda embedding is fully faithful, this isomorphism comes from some isomorphism $A \cong B$. □

Example 5.28 (Tensor products via Yoneda) – Let $A, B \in \mathrm{Mod}_R$. We construct a functor $\mathrm{Mod}_R \to \mathrm{Set}$ as follows: given $X \in \mathrm{Mod}_R$, consider all bilinear maps $\mathrm{Bil}_R(A, B; X)$. For this to be a functor, we need to check composition (and identity, but that's okay). Given a homomorphism $X \to Y$, we have a map $\mathrm{Bil}_R(A, B; X) \to \mathrm{Bil}_R(A, B; Y)$ with this homomorphism.

$$\begin{tikzcd}
A \times B \arrow[r] \arrow[dr, dashed] & X \arrow[d] \\
 & Y
\end{tikzcd}$$

We now can give an alternative definition of the tensor product: $A \otimes_R B$ is the R-module representing the functor $\mathrm{Bil}_R(A, B; -)$. Once we verify that the functor is representable (by constructing the tensor product), we immediately get that the tensor product is unique up to isomorphism.

Example 5.29 (Extensions of scalars via Yoneda) – Let $R \to R'$ be a structure map and A an R-module. Consider the extension of scalars of A, which we denote $\mathrm{Ex}_R^{R'}(A) \in \mathrm{Mod}_{R'}$. Consider the functor

$$\begin{aligned}
\mathrm{Mod}_{R'} &\to \mathrm{Set} \\
X &\mapsto \mathrm{Hom}_R(A, X).
\end{aligned}$$

Then $\mathrm{Ex}_R^{R'}(A)$ is the representing object is the same as saying $\mathrm{Hom}_{R'}(\mathrm{Ex}_R^{R'}(A), X) = \mathrm{Hom}_R(A, X)$ for any $X \in \mathrm{Mod}_{R'}$.

Example 5.30 (Restriction of scalars and some adjoint functors) – Given $X \in \mathrm{Mod}_{R'}$, we have a restriction of scalars $\mathrm{Res}_R^{R'}\colon \mathrm{Mod}_{R'} \to \mathrm{Mod}_R$. We have that

$$\mathrm{Hom}_{R'}(\mathrm{Ex}_R^{R'}(A), X) = \mathrm{Hom}_R(A, \mathrm{Res}_R^{R'}(X)).$$

Something to note: if we knew how the extension of scalars functor $\mathrm{Ex}_R^{R'}$, then finding

$\mathrm{Res}_R^{R'}(X)$ is the same as finding the representing object (h^A this time, not h_A) of

$$\begin{aligned} \mathsf{Mod}_{R'} &\to \mathsf{Set} \\ A &\mapsto \mathrm{Hom}_{R'}(\mathrm{Ex}_R^{R'}(A), X). \end{aligned}$$

The pair $(\mathrm{Ex}_R^{R'}, \mathrm{Res}_R^{R'})$ is an example of a pair of left/right adjoint functors. Theorem 5.46 implies that if a left adjoint exists, then it is unique up to natural isomorphism. By applying the theorem to the opposite category, we have that if a right adjoint exists, then it is unique up to natural isomorphism.

Example 5.31 (Free-forgetful adjuction) – Let $G\colon \mathsf{Grp} \to \mathsf{Set}$ be the functor that "forgets" a group H is a group. We claim a left-adjoint exists. In other words, given $H \in \mathsf{Grp}$ and $X \in \mathsf{Set}$, we have

$$\mathrm{Hom}_{\mathsf{Grp}}(F(X), H) = \mathrm{Hom}_{\mathsf{Set}}(X, G(H)).$$

The left adjoint is precisely given by the free group functor $F\colon \mathsf{Set} \to \mathsf{Grp}$ that makes a free group on a set.

This is a common example of a left/right adjoint pair: the right adjoint is a forgetful functor and the left adjoint is "free," however we ask to define it.

We have a forgetful functor $\mathsf{Ring} \to \mathsf{AbGp}$. The associated free functor is

$$A \mapsto \underbrace{A^{\otimes 0}}_{\cong \mathbb{Z}} \oplus A \oplus A^{\otimes 2} \oplus \cdots \oplus A^{\otimes n} \oplus \cdots$$

Example 5.32 – The notion of currying, that is, $\mathrm{Hom}(X \times Y, Z) = \mathrm{Hom}(X, \mathrm{Hom}(Y, Z))$ by $f \mapsto [x \mapsto f(x, -)]$ in Set (or any other category that is "Set with extra structure") is the statement that $(- \times Y, \mathrm{Hom}(Y, -))$ is an adjoint pair.

March 03, 2025

Proof of Theorem 5.47 (1). We construct an explicit inverse. Let $x \in FA$. For $B \in \mathscr{C}$ and $f \in h_A(B) = \mathrm{Hom}(A, B)$, define

$$\widetilde{x}_B(f) := F(f)(x) \in FB.$$

Thus, $\widetilde{x}_B$ is a morphism $\mathrm{Hom}(A, B) \to FB$. We claim $\widetilde{x}_\bullet\colon h_A \to F$ is a natural transformation. Let $g \in \mathrm{Hom}(B', B)$. It suffices to show the following diagram commutes:

$$\begin{tikzcd} \mathrm{Hom}(A,B) \arrow[r, "g_*"] \arrow[d, "\widetilde{x}_B"'] & \mathrm{Hom}(A,B') \arrow[d, "\widetilde{x}_{B'}"] \\ FB \arrow[r, "F(g)"'] & FB' \end{tikzcd}$$

Let $f \in \mathrm{Hom}(A, B)$. Then

$$(\widetilde{x}_{B'} \circ g_*)(f) = \widetilde{x}_{B'}(g \circ f) = F(g \circ f)(x).$$

On the other hand,

$$(F(g) \circ \widetilde{x}_B)(f) = F(g)(F(f)(x)) = F(g \circ f)(x).$$

Now we show these operations are inverses. If $x \in FA$, then

$$\widetilde{x}_A(\mathrm{id}_A) = F(\mathrm{id}_A)(x) = x.$$

On the other hand, if $\varphi \in \mathrm{Hom}(h_A, F)$, then

$$(\varphi\widetilde{(A)(\mathrm{id}}_A))_B(f) = F(f)(\varphi(A)(\mathrm{id}_A)).$$

Since the following diagram

$$\begin{tikzcd} h_A(A) \arrow[r, "f_*"] \arrow[d, "\varphi(A)"'] & h_A(B) \arrow[d, "\varphi(B)"] \\ FA \arrow[r, "F(f)"'] & FB \end{tikzcd}$$

commutes,

$$\begin{aligned} F(f)(\varphi(A)(\mathrm{id}_A)) &= \varphi(B)(f_*(\mathrm{id}_A)) \\ &= \varphi(B)(f). \end{aligned}$$

It follows that $\varphi = \varphi\widetilde{(A)(\mathrm{id}}_A)$, as desired. □

Proof of Theorem 5.46. This follows from replacing F with h_B in the Yoneda lemma (5.47). □

5.14. Examples and applications of tensor products

Example 5.33 – Let $M \in \mathrm{Mod}_R$. Then $M^{\otimes n}$ represents the functor

$$X \mapsto \left\{ \begin{array}{c} \text{Multilinear maps} \\ M \times \cdots \times M \to X \end{array} \right\}.$$

Definition 5.32

A multilinear map $\mu\colon M \times \cdots \times M \to X$ is **symmetric** if $\mu(m_1, \ldots, m_n) = \mu(m_{\sigma(1)}, \ldots, m_{\sigma(n)})$ for all $\sigma \in S_n$.

Now consider the functor for $X \in \mathrm{Mod}_R$:

$$X \mapsto \left\{ \begin{array}{c} \text{Symmetric multilinear maps} \\ M \times \cdots \times M \to X \end{array} \right\}.$$

We claim this functor is representable. The representation is the 'obvious" choice by modding out by the extra relations that a multilinear map has if it is symmetric:

$$M^{\otimes n} / \left\langle m_1 \otimes \cdots \otimes m_n - m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(n)} : \sigma \in S_n \right\rangle.$$

We define this as the **nth symmetric power of M**, denoted $\mathrm{Sym}^n M$.

Definition 5.33

A multilinear map $\mu\colon M \times \cdots \times M \to X$ is **skew-symmetric/anti-symmetric** if $\mu(m_1, \ldots, m_n) = 0$ whenever $m_i = m_j$ for $i \neq j$.

If 2 is invertible in R, then this is equivalent to

$$\mu(m_1, \ldots, m_i, \ldots, m_j, \ldots, m_n) = -\mu(m_1, \ldots, m_j, \ldots, m_i, \ldots, m_n).$$

The functor

$$X \mapsto \left\{ \begin{array}{c} \text{Skew-symmetric multilinear maps} \\ M \times \cdots \times M \to X \end{array} \right\}$$

has a representation:

$$M^{\otimes n} / \langle m_1 \otimes \cdots \otimes m_n : m_i = m_j, i \neq j \rangle .$$

We define this as the **nth exterior power of M**, denoted $\bigwedge^n M$. The image of $m_1 \otimes \cdots \otimes m_n$ in $\bigwedge^n M$ is denoted $m_1 \wedge \cdots \wedge m_n$.

Example 5.34 (Powers of free modules) – Let $M = \bigoplus_{i=1}^n Re_i$ be a free module. Then

$$\begin{aligned} M^{\otimes d} &= \bigoplus_{1 \leq i_1, \ldots, i_d \leq n} R(e_{i_1} \otimes \cdots \otimes e_{i_n}), \\ \operatorname{Sym}^d M &= \bigoplus_{1 \leq i_1 \leq \cdots \leq i_d \leq n} R(e_{i_1} \cdots e_{i_n}), \\ \bigwedge^d M &= \bigoplus_{1 \leq i_1 < \cdots < i_d \leq n} R(e_{i_1} \wedge \cdots \wedge e_{i_n}). \end{aligned}$$

March 5, 2025

Example 5.35 – We have a decomposition

$$R[x_1, \ldots, x_n] = \bigoplus_{d=0}^{\infty} \operatorname{Sym}^d(Rx_1 \oplus \cdots \oplus Rx_n)$$

by rewriting polynomials as sums of homogeneous polynomials.

Example 5.36 (Determinants) – If $M = Re_1 \oplus \cdots Re_n$, then

$$\bigwedge^n M = R(e_1 \wedge \cdots \wedge e_n).$$

In fact, $\bigwedge^n M$ is a functor: given $\varphi \colon M \to M$, we have an induced map $\bigwedge^n \varphi \colon \bigwedge^n M \to \bigwedge^n M$ that does the map on each basis element (extended by linearity). Since $\bigwedge^n M$ is free of rank 1, $\bigwedge^n \varphi$ represents multiplication by an element of R. Define $\det \varphi := \bigwedge^n \varphi$.

Upshot: basis-free definition of the determinant! Moreover, since $\bigwedge^n M$ is a functor, for $\varphi, \psi \in \operatorname{Hom}(M, M)$ we have that $\det \varphi\psi = \det \varphi \cdot \det \psi$ by functoriality. This gives a fast proof of the determinant being multiplicative.

Let S_1, S_2 be R-modules, and consider $S_1 \otimes_R S_2$. This has a natural R-algebra structure: addition is as usual. Define the product on simple tensors as

$$(s_1 \otimes s_2)(s_1' \otimes s_2') = (s_1 s_1') \otimes (s_2 s_2'),$$

and extend by linearity. The structure map $R \to S_1 \otimes_R S_2$ is given by $r \mapsto r(1 \otimes 1) = (i_1(r) \otimes 1) = (1 \otimes i_2(r))$. Of course, you need to verify that this actually makes $S_1 \otimes_R S_2$ a ring.

Example 5.37 – Let $S_1 = R[x]$. Then S_1 is a free R-module with basis $\left\{x^i : i \geq 0\right\}$. Then if S_2 is another R-algebra, then

$$S_1 \otimes S_2 = S_2[x] = \bigoplus_{i=0}^{\infty} S_2 \cdot x^i.$$

In the category $R\text{-Alg}_{\text{comm}}$ of (commutative) R-algebras, $S_1 \times S_2$ is the product and $S_1 \otimes S_2$ is the coproduct.

Let R, S be rings and consider a (R, S)-bimodule M. Define

$$(r \otimes s)m := r(ms) = (rm)s.$$

Proposition 5.49

A (R, S)-bimodule is the same as a $(R \otimes_{\mathbb{Z}} S)$-module with scalar products defined as above.

Remark 5.50. If we don't require that R and S commute then a (R, S)-bimodule is the same as a $(R \otimes_{\mathbb{Z}} S^{\text{op}})$-module.

5.15. Flatness

March 7, 2025 Recall that $- \otimes_R N$ is right-exact. In other words, a short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

induces an exact sequence

$$M' \otimes N \to M \otimes N \to M'' \otimes N \to 0. \tag{5.1}$$

It not necessarily left-exact (see Remark 5.40). N being flat means we can extend (5.1) to a short exact sequence.

Definition 5.34

An R-module N is **flat** if $- \otimes_R N$ is exact (Equivalently: left-exact. Equivalently: if $M \hookrightarrow M'$, then $M \otimes N \hookrightarrow M' \otimes N$).

We've seen this idea before: $\text{Hom}(M, -)$ is a left-exact functor, but if M is projective, then it is also right-exact.

Example 5.38 –

1. 0 is flat.
2. R is flat (over R).
3. If M_1 and M_2 are flat, $M_1 \oplus M_2$ is flat because $(M_1 \oplus M_2) \otimes N = (M_1 \otimes N) \oplus (M_2 \otimes N)$ and direct sums of exact sequences are exact. Since tensor products commute with *arbitrary* direct sums, if $\{M_\alpha\}$ is a collection of flat modules, then $\bigoplus_\alpha M_\alpha$ is flat. This implies, e.g., all free modules are flat.

Fact 5.51. Given sequences

$$0 \to M' \to M \to M'' \to 0,$$

$$0 \to N' \to N \to N'' \to 0,$$

the induced sequence

$$0 \to M' \oplus N' \to M \oplus N \to M'' \oplus N'' \to 0$$

is exact if *and only if* the first two are.

4. As a consequence, projective modules are flat.

Example 5.39 (The rank of a $\mathbb{Z}$-module) **–** $\mathbb{Q}$, viewed as a $\mathbb{Z}$-module, is flat, but not projective (take the fact that $\mathbb{Q}$ is flat for granted, but you can prove $\mathbb{Q}$ is not projective).

Let

$$0 \to A' \to A \to A'' \to 0$$

be an exact sequence of $\mathbb{Z}$-modules (abelian groups). Then

$$0 \to A' \otimes_{\mathbb{Z}} \mathbb{Q} \to A \otimes_{\mathbb{Z}} \mathbb{Q} \to A'' \otimes_{\mathbb{Z}} \mathbb{Q} \to 0$$

is exact. But $- \otimes_{\mathbb{Z}} \mathbb{Q}$ is an extension of scalars, making each module a $\mathbb{Q}$-vector space. Let $r(A) = \dim_{\mathbb{Q}}(A \otimes_{\mathbb{Z}} \mathbb{Q})$. Using facts of vector spaces, we have that r is an **additive function** (in short exact sequences): if $0 \to A' \to A \to A'' \to 0$ is exact, then $r(A) = r(A') + r(A'')$.

Consider the module $A \otimes_{\mathbb{Z}} \mathbb{Q}$ explicitly. If A is finitely generated, let its decomposition be

$$A \cong \mathbb{Z}^{\oplus n} \oplus \bigoplus_i \mathbb{Z}/d_i.$$

Then

$$A \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\mathbb{Z} \otimes \mathbb{Q})^{\oplus n} \oplus \bigoplus_i \mathbb{Q}/d_i\mathbb{Q} \cong \mathbb{Q}^{\oplus n}.$$

So r coincides with the traditional notion of the **free rank** of an abelian group.

Remark 5.52. In $\mathsf{Mod}_{\mathbb{Z}}$, short exact sequences do not split. The above example extended by scalars to the category $\mathsf{Mod}_{\mathbb{Q}}$, where short exact sequences *do* split.

Proposition 5.53

If R is a domain, its field of fractions F is a flat R-module. As a result, $r(M) := \dim_F(M \otimes_R F)$ is an additive function (in short exact sequences).

To prove this, we will prove a stronger statement about localizations.

Non-Example 5.2 – $\mathbb{Z}/p$ is a $\mathbb{Z}$-module. Define the p-*rank*, r_p as

$$r_p(A) := \dim_{\mathbb{Z}/p} A \otimes_{\mathbb{Z}} \mathbb{Z}/p = \dim_{\mathbb{Z}/p} A/pA.$$

This function is not additive precisely because $\mathbb{Z}/p$ is not flat; e.g.,

$$0 \to \mathbb{Z} \xrightarrow{\times p} \mathbb{Z} \to \mathbb{Z}/p \to 0$$

does not become exact under $- \otimes_{\mathbb{Z}} \mathbb{Z}/p$.

5.16. Localization of rings

Slogan. *Localization forms rings of quotients with fewer restrictions.*

Definition 5.35

Let R be a ring and $S \subseteq R$ be a multiplicative subset (i.e., S forms a semigroup under $\cdot$). The **localization of R with respect to S** is the set of pairs $(r, s) \in R \times S$, often written $\frac{r}{s}$ (we will call these *fractions*), modulo an equivalence that tells us when fractions are the same (we define this below). Denote this set as $S^{-1}R$ or $R[S^{-1}]$.

To represent fractions that are equal, we may naively give a relation

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2} \iff r_1 s_2 = r_2 s_1.$$

Unfortunately, this relation is not transitive. Indeed, if $\frac{r_1}{s_1} \sim \frac{r_2}{s_2}, \frac{r_2}{s_2} \sim \frac{r_3}{s_3}$, then $r_1 s_2 = r_2 s_1$ and $r_2 s_3 = r_3 s_2$. This does not imply $r_1 s_3 = r_3 s_1$. However, this does imply that $r_1 s_2 s_3 = r_3 s_2 s_1$. This motivates the "correct" equivalence relation:

$$\frac{r_1}{s_1} \sim \frac{r_2}{s_2} \iff \text{there exists } s \in S \text{ such that } s r_1 s_2 = s r_2 s_1.$$

We give $R[S^{-1}]$ a ring structure by

$$\begin{aligned} \frac{r_1}{s_1} + \frac{r_2}{s_2} &= \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \\ \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} &= \frac{r_1 r_2}{s_1 s_2} \\ \frac{1}{1} &= 1_{R[S^{-1}]}. \end{aligned}$$

There exists a natural map

$$\begin{aligned} \lambda \colon R &\to R[S^{-1}], \\ r &\mapsto \frac{r}{1}. \end{aligned}$$

Example 5.40 –

1. If $S \subseteq R^\times$, then $\frac{r}{s} \sim \frac{rs^{-1}}{1}$. Therefore, λ is an isomorphism.
2. If R is a domain and $S = R - \{0\}$, then $R[S^{-1}]$ is the field of fractions.

3. If $0 \in S$, then $R[S^{-1}] = 0$.

Warning: λ is not necessarily injective. Suppose $\lambda(r_1) = \lambda(r_2)$ Then there exists $s \in S$ such that $s(r_1 - r_2) = 0$. This does not imply $r_1 = r_2$, since S may have zero divisors. In fact, λ is injective $\iff$ S has no zero divisors.

Localization comes with its own universal mapping property.

Theorem 5.54 (Universal mapping property of $R[S^{-1}]$)
Given a ring R, a multiplicative subset S, and a ring map $\varphi\colon R \to X$ such that $\varphi(S) \subseteq X^\times$. Then there exists a unique morphism $\widetilde{\varphi}\colon R[S^{-1}] \to X$ such that the following diagram commutes:

$$\begin{tikzcd}
R \arrow[r, "\lambda"] \arrow[dr, "\varphi"'] & R[S^{-1}] \arrow[d, dashed, "\exists!\widetilde{\varphi}"] \\
 & X
\end{tikzcd}$$

Stated more cleanly with representables:

Theorem 5.55
$R[S^{-1}]$ represents the functor

$$X \mapsto \left\{\varphi \in \mathrm{Hom}_{\mathsf{Ring}}(R, X) : \varphi(S) \subseteq S^\times\right\}.$$

These two theorems are essentially the same because of a homework problem:

Exercise 5.3. Let $F\colon \mathscr{C} \to \mathsf{Set}$ be a functor. Show that F is represented by $a \in \mathscr{C}$ if and only if there exists $\alpha \in F(a)$ such that for any $b \in \mathscr{C}$ and $\beta \in F(b)$, there exists a unique $f \in \mathrm{Mor}(a, b)$ such that $F(f)(\alpha) = \beta$.

Example 5.41 – Let $f \in R$. Consider the multiplicative subset $S = \left\{f^k : k \geq 0\right\}$. We consider $R[S^{-1}]$ (sometimes denoted $R[f^{-1}]$ or R_f).

Proposition 5.56
$R_f = R[t]/(tf - 1)$.

A direct way to prove this would be by the map $\frac{1}{f} \mapsto t$. We'll do a more fancy proof.

Proof. By the representability of $R[S^{-1}]$ (5.55), we can see easily that R_f represents the functor

$$X \mapsto \{\varphi \in \mathrm{Hom}_{\mathsf{Ring}}(R, X) : \varphi(f) \in X^\times\} \tag{5.2}$$

On the other hand, $R[t]$ represents the functor

$$X \mapsto \{(\varphi, \tau) \in \mathrm{Hom}_{\mathsf{Ring}}(R, X) \times X\}$$

(this makes sense: a map out of $R[t]$ is the same as saying where R goes and where t goes). $R[t]/(tf - 1)$ represents the functor

$$X \mapsto \{(\varphi, \tau) \in \mathrm{Hom}_{\mathsf{Ring}}(R, X) \times X : \tau\varphi(f) - 1 = 0\}. \tag{5.3}$$

But $t\varphi(f) = 1$ if and only if $\varphi(f)$ is invertible, so (5.2) and (5.3) are represented by the same object. □

Proposition 5.57

March 12, 2025

There is a bijection

$$\left\{\begin{array}{c}\text{prime ideals}\\ \text{of } R[S^{-1}]\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{prime ideals } \mathfrak{p} \subseteq R\\ \text{such that } \mathfrak{p} \cap S = \varnothing\end{array}\right\},$$

given by $\mathfrak{q} \mapsto \mathfrak{q}^c$ under the ring map $\lambda \colon R \to R[S^{-1}]$. The inverse operation is $\mathfrak{p} \mapsto \mathfrak{p}^e = R[S^{-1}]\lambda(\mathfrak{p})$.

Remark 5.58. Recall that $\mathfrak{p}^e = \left\{\sum_i a_i\lambda(p_i) : a_i \in R[S^{-1}], p_i \in \mathfrak{p}\right\}$. This looks like an extension of scalars. Indeed, this is the image of $R[S^{-1}] \otimes_R \mathfrak{p}$ in $R[S^{-1}]$ (the map is induced by the inclusion $\mathfrak{p} \hookrightarrow R$).

Proof sketch of Proposition 5.57. Here are the main claims and the steps:

1. $\underline{\mathfrak{q} \text{ prime} \implies \mathfrak{q}^c \text{ prime}}$. We have proven this before.
2. $\underline{\mathfrak{q}^c \cap S = \varnothing}$. If $\frac{s}{1} \in \mathfrak{q}$ for some $s \in S$, then $\mathfrak{q} = (1)$ (since it contains a unit).
3. $\underline{(\mathfrak{q}^c)^e = \mathfrak{q}}$. If $\frac{r}{s} \in \mathfrak{q}$, then $\frac{r}{1} \in \mathfrak{q}$, which means $r \in \mathfrak{q}^c$, which implies $\frac{r}{s} \in (\mathfrak{q}^c)^e$.
4. $\underline{\text{If } \mathfrak{p} \subseteq R \text{ prime with } \mathfrak{p} \cap S = \varnothing\text{, then } \mathfrak{p}^e \text{ prime and } (\mathfrak{p}^e)^c = \mathfrak{p}}$. Suppose $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{p}{s}$, where $p \in \mathfrak{p}$. Then there exists $s' \in S$ such that

$$s'a_1a_2a = ps_1s_2s'.$$

Since $\mathfrak{p} \cap S = \varnothing$, this implies a_1 or a_2 are in $\mathfrak{p}$, so $\frac{a_1}{s_1}$ or $\frac{a_2}{s_2}$ are in $\mathfrak{p}^e$. □

Proposition 5.59

More generally, we have a bijection

$$\left\{\begin{array}{c}\text{ideals}\\ \text{of } R[S^{-1}]\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{ideals } I \subseteq R \text{ such that}\\ sa \in I, s \in S' \implies a \in I\end{array}\right\}.$$

Corollary 5.60

More specifically, we have a bijection

$$\left\{\begin{array}{c}\text{maximal ideals}\\ \text{of } R[S^{-1}]\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{prime ideals } \mathfrak{p} \subseteq R \text{ such that } \mathfrak{p} \cap S = \varnothing\\ \text{that are maximal amongst such ideals}\end{array}\right\}.$$

5.16.1. Localization at a prime

If $\mathfrak{p} \subseteq R$ is a prime ideal, then $R - \mathfrak{p}$ is a multiplicative set. Let

$$R_\mathfrak{p} := R[(R-\mathfrak{p})^{-1}].$$

Then prime ideals in $R_\mathfrak{p}$ are in bijection with prime ideals of $\mathfrak{q} \subseteq R$ with $\mathfrak{q} \subseteq \mathfrak{p}$. There is a single ideal that has this property: $\mathfrak{p}$. Therefore, $R_\mathfrak{p}$ is local with maximal ideal $R_\mathfrak{p}\mathfrak{p}$.

Example 5.42 – The prime ideals of $\mathbb{Z}$ are (p) for p prime.

- In $\mathbb{Z}[2^{-1}]$, we have all the same ideals except (2) (e.g., $(3) \subseteq \mathbb{Z}[2^{-1}]$ is generated by fractions of the form $\frac{3}{2^k}$, where $k \geq 0$).
- In $\mathbb{Z}_{(2)}$, the only non-trivial ideal is (2) (e.g., 9 is a unit with inverse $\frac{1}{9}$, but 4 is not an inverse because $\frac{1}{4} \notin \mathbb{Z}_{(2)}$).
- $\mathbb{Z}_{(0)} = \mathbb{Q}$.

5.17. Localization of modules

π March 14, 2025

Definition 5.36

Let R be a ring, $S \subseteq R$ a multiplicative set, and M an R-module. The **localization of M with respect to S** is set of pairs $(m, s) \in M \times S$, often written $\frac{m}{s}$ modulo the equivalence relation $\frac{m_1}{s_1} = \frac{m_2}{s_2}$ if there exists $s \in S$ such that $ss_2m_1 = sm_2s_1$. Denote this module as $M[S^{-1}]$.

Notice that $M[S^{-1}]$ is an $R[S^{-1}]$-module.

Moreover, the localization of modules is an extension of scalars: $M[S^{-1}] = R[S^{-1}] \otimes_R M$. Therefore, the functor $M \mapsto M[S^{-1}]$ sending the morphism $f\colon M \to N$ to $S^{-1}f\colon M[S^{-1}] \to N[S^{-1}]\colon \frac{m}{s} \mapsto \frac{f(m)}{s}$ is right exact.

Proposition 5.61

$M \mapsto M[S^{-1}]$ is an exact functor. Equivalently, $R[S^{-1}]$ is a flat R-module.

Proof. It suffices to show the functor preserves injections. Let $f\colon M' \hookrightarrow N$. Let $\frac{m'}{s} \in M'[S^{-1}]$ and suppose $\frac{f(m')}{s} = 0$. Then there exists $s' \in S$ such that $f(m')s' = f(m's') = 0$. Therefore, $s'm' = 0$, so $\frac{m'}{s} = 0$. □

Remark 5.62. What are $R[S^{-1}]$-modules? Using a characterization from before, it is the same an abelian group M together with a ring homomorphism $R[S^{-1}] \to \mathrm{End}_\mathbb{Z}(M)$. By the universal mapping property, this is the same as ring homomorphisms $R \to \mathrm{End}_\mathbb{Z}(M)$ such that the image of S is contained within the units of $\mathrm{End}_{\mathbb{Z}}(M)$. This exactly means that M is an R-module with any action of $s \in S$ being bijective.

To be extra careful, we notice that $\mathrm{End}_{\mathbb{Z}}(M)$ need not be commutative. To fix this, we need to show that if $a, b \in \mathrm{End}_{\mathbb{Z}}(M)$ commute and a is invertible, then a^{-1} and b commute.

5.18. Determinants and the Cayley-Hamilton theorem

March 17, 2025 If we use the standard definition of the determinant in linear algebra (e.g., $\sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$), we can extend it to $A \in \mathrm{Mat}_{n\times n}(R)$ to get $\det(A) \in R$.

Proposition 5.63

The following are equivalent:

1. A is invertible.
2. $\det(A) \in R^\times$.
3. The columns of A form a basis for R^n.
4. The rows of A form a basis for R^n.

Proof. ((1) $\iff$ (3)) follows from properties of the basis.

((1) $\implies$ (2)) Determinants are multiplicative, so $\det(A)\det(A^{-1}) = \det(I) = 1$.

((2) $\implies$ (1)) A^{-1} can be written explicitly using the formula for the inverse of a determinant from linear algebra.

((1) $\iff$ (4)) $\det(A) = \det(A^\top)$. □

Remark 5.64. The gist for some of the above proofs was to reduce to the case over fields, where we already know how linear algebra works. If R is a domain, then we may embed it into its field of fractions, but what about more generally?

Example 5.43 – The formula $\det(AB) = \det(A)\det(B)$ is checking that some polynomial equation holds. The claim is that it suffices to check in the "universal ring" $S = \mathbb{Z}[a_{11}, \dots, a_{nn}, b_{11}, \dots, b_{nn}]$. Then we map into any ring R. To reduce to a field, we use the field of fractions of S: $\mathbb{Q}(a_{11}, \dots, a_{nn}, b_{11}, \dots, b_{nn})$, where we know it holds.

In summary, $\det(AB) = \det(A)\det(B)$ holds in $\mathrm{Frac}(S)$, so it holds in S. Then under the natural map $S \to R$, the formula also holds.

Similarly, for any polynomial identity in some number of variables, we can follow the same process. There's another trick if we want to include inverses.

Example 5.44 – Consider the formula $A^{-1} = \det(A)^{-1}\mathrm{adj}(A)$ if $\det(A) \in R^\times$. We need to check that

$$\det(A)^{-1}\mathrm{adj}(A)A = A\det(A)^{-1}\mathrm{adj}(A) = I,$$

which gives a polynomial system in R. Our "universal ring" now needs the inverse of $\det(A)$ for it to make sense. We can do this precisely with localization:

$$S := \mathbb{Z}[a_{11}, \dots, a_{nn}][\det(A)^{-1}],$$

which is a domain that we can embed into its field of fractions and repeat the same reasoning as the last problem.

Recall that we defined the determinant of $\varphi\colon M \to M$, where M are free modules of rank n, as the scalar that represents multiplication for the map $\bigwedge^n \varphi\colon \bigwedge^n M \to \bigwedge^n M$.

Remark 5.65. If M and M' are free modules of the same finite rank, then it's a little misleading to talk about the determinant of a map $\varphi\colon M \to M'$, since it isn't invariant under changes of bases: $\det(A) \neq \det(CA(C')^{-1})$ generally. However, one can still consider $\det(\varphi)$ under the identification $\bigwedge^n M \cong R$, $\bigwedge^n M' \cong R$.

Warning: Eigenvalues/vectors don't work as nicely. The characteristic polynomial $\chi_A(t) \coloneqq \det(t \cdot I - A) \in R[t]$ exists, but

1. The polynomial may not have roots.
2. A root λ of $\chi(t)$ means $\det(\lambda I - A) = 0$, but we have that $\lambda I - A$ is invertible if and only if $\det(\lambda I - A)$ is a unit, so we don't have enough information.
3. Even if $Av = \lambda v$ for some v, we may not even by able to use it in some basis of R^n.

However, not all is lost.

Theorem 5.66 (Cayley-Hamilton for rings)
Let $A \in \mathrm{Mat}_{n\times n}(R)$. Then $\chi_A(A) = 0$.

There are two ways to prove this: repeat the proof from fields and be slightly careful, or use the "universal ring" trick from the above remark. We won't cover either.

5.19. PID structure theorem

March 19, 2025 We'll cover the PID structure theorem, which tells us what finitely generated modules over a PID R look like. A corollary is the classification of finitely generated abelian groups (with $R = \mathbb{Z}$).

Recall the following definition from UFD theory:

Definition 5.37
Let R be an integral domain.

1. Let $r \in R - \{0\}$ be a non-unit. Then r is **irreducible** if, whenever $r = ab$ for $a, b \in R$, at least one of a, b is a unit. Otherwise, r is **reducible**.
2. $p \in R - \{0\}$ is **prime** if (p) is a prime ideal. In other words, a nonzero element p is prime if it is not a unit, and whenever $p \mid ab$ for any $a, b \in R$, then either $p \mid a$ or $p \mid b$.
3. Two elements $a, b \in R$ are said to be **associate** if there exists a unit $u \in R$ such that $a = ub$.

Proposition 5.67
In a PID, a nonzero element is prime $\iff$ it is irreducible.

Theorem 5.68 (PID structure theorem)
Let R be a PID, M a finitely generated R-module. Then we can decompose

$$M \cong R \oplus \cdots \oplus R \oplus R/(a_1) \oplus \cdots \oplus R/(a_n)$$

for $a_1, \dots, a_n \in R$. There are two well-known decompositions that have uniqueness properties.

1. (*Elementary divisors*):
$$M \cong R^n \oplus \bigoplus_{i=1}^{k} R/(p_i^{m_i}),$$
where p_i is irreducible and $m_i \geq 1$. The **rank** n is unique and $p_i^{m_i}$ are unique up to permutation and multiplication by an associate.
2. (*Invariant factors*):
$$M \cong R^n \oplus \bigoplus_{i=1}^{m} R/(a_i),$$
where $a_1 \mid a_2 \mid \cdots \mid a_m$.

5.19.1. Application: structure of polynomial rings via rational normal form

Let F be a field and let $R = F[x]$. Then R is a PID. There is a correspondence

$$\{\text{R-modules}\} \longleftrightarrow \left\{ \begin{array}{c} \text{vector spaces } V/F \text{ together with} \\ \text{an endomorphism } A \colon V \to V \end{array} \right\}. \tag{5.4}$$

We may wonder what the finitely generated modules are. If $\dim_F V < \infty$, then V is finitely generated as a F-module, so it is finitely generated as an R-module.

Remark 5.69. V is finitely generated as an R-module $\iff$ there exist $v_1, \dots, v_m \in V$ such that $V = \operatorname{span}\{A^i v_k : i \geq 0, 1 \leq k \leq m\}$.

Note that R is infinite-dimensional over F, but $R/(p)$ is finite-dimensional over F for any nonzero $p \in R$.

If we use the PID structure theorem (5.68) for finite dimensional V/F, then the rank is zero.

Let $p(t) = a_0 + \cdots + t^m \in R[t]$ (we may assume p is monic). Then $F[t]/(p)$ is a finitely-generated F[t]-module. In the correspondence (5.4), the vector space is $F[t]/(p)$ and A represents multiplication by t. We'll now explicitly write what multiplication by t looks like with the basis $\{1, t, \dots, t^{m-1}\}$:

$$\begin{bmatrix} & & & & -a_0 \\ 1 & & & & -a_1 \\ & 1 & & & -a_2 \\ & & \ddots & & \vdots \\ & & & 1 & -a_{m-1} \end{bmatrix} \tag{5.5}$$

Theorem 5.70 (Rational normal form)
Let V be a finite-dimensional over F and $A \colon V \to V$ is an endomorphism. Then there exists a decomposition $V = \bigoplus_{i=1}^m V_i$, such that on some basis of each V_i, $A|_{V_i}$ takes the form (5.5) (so A is a block matrix with blocks of this form), and the associated polynomials $p_1, \dots, p_m$ satisfy $p_1 \mid \cdots \mid p_m$.

Notice that the characteristic polynomial of each block is the associated polynomial.

5.19.2. Structure of polynomials rings via Jordan normal form

March 21, 2025 Suppose the elementary divisors of an operator $A\colon V \to V$ over a finite dimensional vector space V/F are of the form $(x-\lambda)^m$. Equivalently, assume that the characteristic polynomial of A splits completely over F. In particular, this always holds if F is algebraically closed.

For $F[x]/(x-\lambda)^m$, a good basis to choose is $\left\{1, (x-\lambda), \dots, (x-\lambda)^{m-1}\right\}$. Then multiplication by x corresponds to the matrix

$$\begin{bmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \end{bmatrix}.$$

Traditionally, we reverse the order of the basis so that the above matrix is upper triangular.

Theorem 5.71 (Jordan normal form)

Let V be a vector space over F and $A\colon V \to V$ an endomorphism whose characteristic polynomial splits completely over F. Then there exists a basis of V for which A is a block diagonal matrix with blocks as above (each block may have different values for λ).

The so-called "Jordan basis" generalizes an eigenbasis; each block has an eigenvector with eigenvalue λ and each other basis vector is an eigenvector modulo the previous eigenvector.

6. Field theory and Galois theory

March 31, 2025 Let F be a field. Fields are examples of rings. We'll investiage some properties by looking a ring homomorphisms to F. The only ideals of a field F are F and (0). If

$$\varphi\colon F \to E$$

is a nonzero ring homomorphism, then $\ker(\varphi) = (0)$, so it is injective. We say that F is a **subfield** of E and E is an **extension** of F.

6.1. Characteristic

Since $\mathbb{Z}$ is initial in Ring, there exists a unique morphism $\varphi\colon \mathbb{Z} \to F$ (what is it?). Moreover, $\ker(\varphi)$ is prime ($\varphi(\mathbb{Z})$ is contained in a field, so it is an integral domain, now use the fact that $\mathbb{Z}/\ker(\varphi) \cong \varphi(\mathbb{Z})$''). We have two cases:

- Case 1: $\ker(\varphi) = (p)$. Then F is an extension of $\mathbb{F}_p$. We say that $\mathbb{F}_p$ is the **prime field** of F and that F has **characteristic p**.
- Case 2: $\ker(\varphi) = (0)$. Then the following diagram commutes by the universal mapping property of localization

$$\begin{tikzcd}
\mathbb{Z} \arrow[r] \arrow[rd] & \mathbb{Z}[(\mathbb{Z}-\{0\})^{-1}] = \mathbb{Q} \arrow[d, dashed, "\exists!"'] \\
& F
\end{tikzcd}$$

Since $\mathbb{Q} \to F$ is nonzero, $\mathbb{Q}$ embeds into F. We say $\mathbb{Q}$ is the prime field of F and that F has **characteristic 0**.

Fact 6.1. If F and E have different characteristics, then there are no nonzero homomorphisms from F to E.

6.2. Extensions generated by a set

Let $F \subseteq E$ be a subfield and $S \subseteq E$ a subset. Then the **ring extension (F-algebra) of F generated by S**, denoted $F[S]$, is the smallest subring of E containing F and S. The **field extension of F generated by S**, denoted $F(S)$, is the smallest subfield of E containing F and S.

Proposition 6.2

If $F \subseteq R$ is a field contained in a ring, and R is a domain and finite-dimensional over F, then R is a field.

Proof. Let $\alpha \in R$ be nonzero. Consider the linear map μ defined by multiplication by α. Then α is not a zero-divisor $\iff$ μ is injective $\iff$ μ is surjective. Thus, $\mu(x) = 1$ for some x. □

Corollary 6.3

If $F[S]$ is finite-dimensional over F, then $F[S] = F(S)$.

Example 6.1 (Multiplying by conjugates) – Concretely, in high school algebra you learned that $\frac{1}{\sqrt{2}} = \frac{1}{2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

6.2.1. Simple extensions

A **simple extension** if an extension of the form $F(\alpha) \supseteq F$. We say that α is **primitive**. Given $\alpha \in E \supseteq F$, consider the map

$$\varphi \colon F[x] \to E \colon p(x) \mapsto p(\alpha).$$

Then $\ker(\varphi)$ is a prime ideal. There are two cases:

- Case 1: $\ker(\varphi) = (m)$ for an irreducible polynomial $m(x) \in F[x]$. Then

$$\varphi(F[x]) = F[\alpha] = F[x]/(m)$$

  is finite-dimensional over F, so $F[\alpha] = F(\alpha)$. We say α is **algebraic (over F)**, i.e. φ is not injective, i.e. α is a root of some polynomial over F. In this case, we say that $m(x)$ is the **minimal polynomial of α**.

- Case 2: $\ker(\varphi) = (0)$. Then $F[x]$ is isomorphic to $F[\alpha]$, so $F[\alpha]$ is only a ring. To get a field, we need to consider its field of fractions, which corresponds to the field of rational functions of one variable, $F(x)$. In this case, we say that α is **transcendental (over F)**.

Remark 6.4. We will use the shorthand notation "α/F is algebraic," for some α in a field extension of F, and "E/F is finite," for some field extension E of F (and other such combinations) often. These should not be read as quotients, rather they should be read as the word "over."

April 2, 2025

Example 6.2 – $\mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[x]/(x^2+1)$ is a simple extension. In fact, $\mathbb{C} = \mathbb{R}(z)$ for any $z = a + bi$, $b \neq 0$, e.g., $\mathbb{C} = \mathbb{R}(3+2i) \cong \mathbb{R}[x]/((x-3)^2+4)$.

Remark 6.5. Given an irreducible $m \in F[x]$, $E \coloneqq F[x]/(m)$ is a field. Then $E = F[\alpha]$, where α is the image of x in E. We have that the minimal polynomial of α over F is m.

6.3. Degrees of extensions

Definition 6.1

If $F \hookrightarrow E$, then E is naturally a F-vector space. We say E/F is **finite** if $\dim_F(E) < \infty$. If so, let the **degree of extension** be denoted $[E : F] \coloneqq \dim_F(E)$.

Example 6.3 (Degree of simple extension) – $F(\alpha)/F$ is finite $\iff$ α is algebraic. Note that

$$[F(\alpha) : F] = \deg(m_{\alpha,F}(x)).$$

We call the above quantity the **degree of α over F**, denoted $\deg_F(\alpha)$. The basis for $F(\alpha)/F$ is $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{\deg_F(\alpha)-1}\right\}$.

For other extensions, e.g.,

$$\begin{tikzcd}
F(\alpha, \beta) \arrow[d, dash] \\
F(\alpha) \arrow[d, dash] \\
F
\end{tikzcd}$$

we have the issue that, e.g., $F[x, y]$ is not a PID, unlike $F[x]$, so it is more challenging to describe $F(\alpha, \beta)$. Instead, we can consider $F(\alpha, \beta) = (F(\alpha))(\beta)$. We have a nice fact about such towers of simple extensions.

Proposition 6.6

Let $K \supseteq E \supseteq F$ be fields.

1. K/F is finite $\iff$ F/E and E/F are finite.
2. $[K : F] = [K : E] \cdot [E : F]$.

Proof. $K \cong E^{[K:E]}$ as an E-vector space, and $E \cong F^{[E:F]}$ as an F-vector space, so $K \cong F^{[K:E]\cdot[E:F]}$ as an F-vector space. □

Written explicitly, if K/E has basis $\{\alpha_1, \ldots, \alpha_n\}$ and E/F has basis $\{\beta_1, \ldots, \beta_m\}$, then K/F has basis $\left\{\alpha_i \beta_j : 1 \leq i \leq n, 1 \leq j \leq m\right\}$.

Corollary 6.7

1. If $K \supseteq E \supseteq F$ are fields, then $[E : F] \mid [K : F]$.
2. If $E = F(\alpha)$, then $\deg_F(\alpha) \mid [K : F]$ for any $\alpha \in K$, where K/F is a finite extension. In particular, α is algebraic.

Example 6.4 – $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's criterion ($p = 2$). Therefore, $x^3 - 2 = m_{\sqrt[3]{2},\mathbb{Q}}(x)$. By Example 6.3,

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3,$$

with basis $\left\{1, \sqrt[3]{2}, \sqrt[3]{4}\right\}$. Let $\beta \in \mathbb{Q}(\sqrt[3]{2})$. Then $\deg_F(\beta) \mid 3$. If $\deg_F(\beta) = 1$, then $\beta \in \mathbb{Q}$. If $\deg_F(\beta) = 3$, then $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt[3]{2})$, i.e., β is **primitive** (it generates the extension).

Corollary 6.8

Let $\alpha_1, \ldots, \alpha_k \in E \supseteq F$. $F(\alpha_1, \ldots, \alpha_k)/F$ is finite if $\alpha_1, \ldots, \alpha_k$ are algebraic over F.

Proof. Construct a tower

$$\begin{tikzcd}
F(\alpha_1,\dots,\alpha_k) = (F(\alpha_1,\dots,\alpha_{k-1}))(\alpha_k) \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
F(\alpha_1,\alpha_2) = (F(\alpha_1))(\alpha_2) \arrow[d, dash] \\
F(\alpha_1) \arrow[d, dash] \\
F
\end{tikzcd}$$

each extension is finite, since it is a simple extension with an algebraic generator. □

Remark 6.9. This gives us a way to explicitly get information about $[F(\alpha_1,\dots,\alpha_k) : F]$. For example, if $k = 2$, then

$$[F(\alpha_1,\alpha_2) : F] = [F(\alpha_1,\alpha_2) : F(\alpha_1)][F(\alpha_1) : F] = \deg_{F(\alpha_1)}(\alpha_2) \cdot \deg_F(\alpha_1).$$

The first term may be challenging to compute, but we have that

$$\deg_{F(\alpha_1)}(\alpha_2) \leq \deg_F(\alpha_2),$$

since the minimal polynomial in $F(\alpha_1)$ of α_2 certainly has $\leq$ degree to the minimal polynomial in F of α_2. So

$$[F(\alpha_1,\alpha_2) : F] \leq \deg_F(\alpha_2) \cdot \deg_F(\alpha_1).$$

It's clear how to extend this to show

$$[F(\alpha_1,\dots,\alpha_k) : F] \leq \prod_{i=1}^{k} \deg_F(\alpha_i).$$

Definition 6.2

E/F is an **algebraic extension** if every $\alpha \in E$ is algebraic over F. E/F is a **transcendental extension** if there exists a transcendental element $\alpha \in E$ over F.

Proposition 6.10

1. Finite extensions are algebraic.

2. $F(\alpha_1,\dots,\alpha_k)/F$ finite implies $\alpha_1,\dots,\alpha_k$ are algebraic.

   Fact 6.11. E/F is finite $\iff$ E/F is algebraic and finitely generated.[1]

3. Let $S \subseteq E$ be a subset where all $\alpha \in S$ are algebraic over F. Then $F(S)/F$ is algebraic.

4. If K/E is algebraic and E/F is algebraic, then K/F is algebraic.

[1] Recall finitely generated means $F(s_1,\dots,s_\ell) = E$, which may create a much larger field than the vector space generated by $s_1,\dots,s_\ell$ over F

Proof of (4). We have another explicit construction. Let $\alpha \in K$. Then it satisfies a polynomial equation in E

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0.$$

The extension $F(a_0, \dots, a_{n-1})/F$ is finite, and $F(\alpha, a_0, \dots, a_{n-1})/F(a_0, \dots, a_{n-1})$ is finite (we wrote a finite polynomial with α as a root above), so $F(\alpha, a_0, \dots, a_{n-1})/F$ is finite and α is algebraic. □

April 4, 2025

Example 6.5 ($\mathbb{Q}(\sqrt[3]{2}, i)$) – The number $\alpha = \sqrt[3]{2} + i \in \mathbb{Q}(\sqrt[3]{2}, i)$, so it is algebraic. Suppose we want to know $\deg_{\mathbb{Q}}(\alpha)$. The tower

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[3]{2}, i) & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[ur, dash] & & \mathbb{Q}(i) \arrow[ul, dash] \\
 & \mathbb{Q} \arrow[ul, dash, "3"] \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

implies that $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}] = 6$ (alternatively, $i \notin \mathbb{Q}(\sqrt[3]{2})$, so $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[3]{2})] = 2$). This gives us an explicit basis for $\mathbb{Q}(\sqrt[3]{2}, i)/\mathbb{Q}$:

$$\left\{1, \sqrt[3]{2}, \sqrt[3]{4}, i, i\sqrt[3]{2}, i\sqrt[3]{4}\right\}.$$

Now checking the degree of α is the same as writing powers of α: $\left\{1, \alpha, \dots, \alpha^5\right\}$ in terms of the basis above and "waiting for linear dependence." A direct computation verifies that its degree is 6.

6.4. Algebraic closure

Given $E \supseteq F$, let $K := \{\alpha \in E : \alpha \text{ is algebraic}/F\}$. Then K is a field called the **algebraic closure of F in E**, denoted $\overline{F}_E$. K is a the largest subfield of E that is algebraic over F.

This construction is a "relative algebraic closure" (to E). Our goal now is to construct an "absolute algebraic closure."

Proposition 6.12

Let F be a field. The following are equivalent:

1. Every non-constant polynomial $p(x) \in F[x] - F$ has a root in F.

1′. $p(x) \in F[x] - F$ splits completely in F. That is, $p(x) = c(x - \alpha_1)\cdots(x - \alpha_n)$.

2. $p(x)$ is irreducible $\iff$ $p(x)$ is linear.

3. If E/F is finite, $E = F$.

3′. If E/F is algebraic, $E = F$.

3″. If $E \supseteq F$, $\alpha \in E$ algebraic $/F$, then $\alpha \in F$.

Proof (sketch). ((1) $\iff$ (1′)) ($\impliedby$) is clear. ($\implies$) is by polynomial long division. (1′) and (2) are clearly equivalent.

((3) $\implies$ (3′)) is immediate. [1]

((3) $\implies$ (3″)) $F(\alpha)/F$ is finite, therefore $F(\alpha) = F$, so $\alpha \in F$.

((3″) $\implies$ (3′))

((3) $\implies$ (2)) If $p(x)$ is irreducible, then $[F[x]/(p) : F] < \infty$ □

[1] Student question: Shouldn't it be the other way, since finite $\implies$ algebraic? Answer: We're showing that, given $A \implies B$, $(B \implies C) \implies (A \implies C)$. So it's something like a contravariant functor...

Definition 6.3

F is called **algebraically closed** if any of the properties in Proposition 6.12 hold.

$E \supseteq F$ is an **algebraic closure of F** if E/F is algebraic and E is algebraically closed (we think of E as a maximal algebraic extension of F).

Proposition 6.13

E if an algebraic closure of $F \iff E/F$ is algebraic and all $p(x) \in F[x] - F$ split in E.[1]

[1] This is an "easier" thing to prove. The definition above asks us to show all polynomials in $E[x] - E$ split completely.

Proof. ($\implies$) Obvious (see footnote). ($\impliedby$) Let $\alpha \in K \supseteq E \supseteq F$ be algebraic over E. Since E/F is algebraic, α is algebraic over F, so $m_{\alpha,F}$ splits completely in E, so $\alpha \in E$. □

Remark 6.14.

- This proposition actually holds if we replace "all $p(x) \in F[x] - F$ split" with "all $p(x) \in F[x] - F$ have a root," but proving this fact is harder.
- We will later prove that (1) any field has an algebraic closure and (2) any two algebraic closures of F are isomorphic. Therefore, we will write $\overline{F}$ as *the* algebraic closure of F.
- In particular, $F = \overline{F}$ means F is algebraically closed.

Example 6.6 – By the fundamental theorem of algebra, $\mathbb{C} = \overline{\mathbb{C}}$. Embarassingly, the proof of the fundamental theorem of algebra doesn't purely use algebra, and need to divert to analysis. But we should expect that because $\mathbb{R}$ is *constructed* with analytical techniques. Since $\mathbb{C}/\mathbb{R}$ is finite, $\overline{\mathbb{R}} = \mathbb{C}$ as well.

Example 6.7 – $\mathbb{C} \neq \overline{\mathbb{Q}}$, but since $\mathbb{C} \supseteq \mathbb{Q}$, we can actually just take the relative algebraic closure to get

$$\overline{\mathbb{Q}} = \overline{\mathbb{Q}}_{\mathbb{C}} = \{\alpha \in \mathbb{C} : \alpha \text{ algebraic } /\mathbb{Q}\}.$$

6.5. Morphisms of extension

April 7, 2025 Let $F(\alpha)/F$ be a simple extension. Suppose E/F is some other extension. To describe a **morphism of extensions** $\varphi\colon F(\alpha) \to E$, we want F to be fixed. In other words, with the natural structure maps $F \to F(\alpha)$, $F \to E$, a morphism of extensions is an F-algebra homomorphism $F(\alpha) \to E$.

- Case 1: α is algebraic. Let $F(\alpha) = F[x]/(m)$, where $m(x) = m_{\alpha,F}(x)$. Then φ is determined by the image of α. Call it β. Then β must satisfy $m(\beta) = 0$ (i.e., $m_{\beta,F}(x) = m(x)$).
  Categorical interpretation: $\mathrm{Hom}_F(F(\alpha), E) = \{\beta \in E : m(\beta) = 0\}$.
- Case 2: α is transcendental. It's easy to show that $\varphi(\alpha)$ must also be transcendental (one way: φ is injective).
  Categorical interpretation: $\mathrm{Hom}_F(F(\alpha), E) = \{\beta \in E : \beta \text{ is transcendental}/F\}$.

Example 6.8 – Consider a morphism of extensions/$\mathbb{Q}$ from $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$. Then $\sqrt[3]{2}$ can map to $\beta_1, \beta_2, \beta_3$, where $\beta_k = e^{2\pi k i/3}\sqrt[3]{2}$ are the roots of $x^3 - 2$ in $\mathbb{C}$.

More generally, suppose $F(\alpha)/F$ is algebraic and E is some field. For any $\varphi_0 \colon F \to E$, there exists a bijection

$$\left\{\varphi \colon F(\alpha) \to E : \varphi\big|_F = \varphi_0\right\} \longleftrightarrow \{\beta \in E : \widetilde{m}(\beta) = 0\},$$

where $\widetilde{m} \in E[x]$ is the image of $m_{\alpha,F} \in F[x]$ under φ_0.

6.6. Splitting fields

Motivation. *We want to add all the roots of a certain polynomial to a field.*

Definition 6.4

E/F is a **splitting field of** $p(x) \in F[x]$ if

1. $p(x)$ splits completely in E.
2. E/F is generated by p's roots. That is, $E = F(\alpha_1, \ldots, \alpha_m)$, where $p(x) = (x - \alpha_1)\cdots(x - \alpha_m) \in E[x]$.

We assume p is monic here.

Proposition 6.15 (Existence)

For any $p(x) \in F[x]$, a splitting field E/F of p exists. Moreover, $[E : F] \leq m!$, where $\deg(p) = m$.

Proof. Choose an irreducible $m_1(x) \mid p(x)$ and let $E_1 := F[x]/(m_1)$. Then $E_1 = F(\alpha_1)$ and $p(\alpha_1) = 0$. Repeat the previous construction with $p_2(x)$, where $p(x) = (x - \alpha_1)p_2(x)$ to create $E_2 = E_1(\alpha_2) = E_1[x]/(m_2)$, where $p_2(\alpha_2) = 0$, $m_2(x) \mid p_2(x)$ is irreducible over E_1.

By construction, $[E_{j+1} : E_j] \leq m - j$ (where $E_0 = F$) for $0 \leq j \leq m - 1$. □

Proposition 6.16

Let $E, \widetilde{E}$ be two splitting fields/F of $p(x) \in F[x]$. Then there are isomorphic/F.

Proof. Recall that $E = F(\alpha_1, \ldots, \alpha_m)$, so it belongs to a tower adjoining roots.

- On $F(\alpha_1)$, find roots of $m_{\alpha_1,F}(x) \mid p(x)$ in E. $p(x)$ splits in $\widetilde{E}$, and so does $m_{\alpha_1,F}$. Find $\beta_1 \in \widetilde{E}$ such that $m_{\alpha_1,F}(\beta_1) = 0$. This gives an isomorphism $\varphi_1 \colon F(\alpha_1) \to F(\beta_1)$.

- Let $m_{\alpha_2,F(\alpha_1)} \in F(\alpha_1)[x]$ and apply φ_1:

  $$\varphi_1(m_{\alpha_2,F(\alpha_1)})\widetilde{m}_2 \in F(\beta_1)[x].$$

  Then $\widetilde{m}_2(x) \mid p(x)$, which splits in E. Therefore, we get an isomorphism

  $$\varphi_2 \colon F(\alpha_1, \alpha_2) \xrightarrow{\sim} F(\beta_1, \beta_2).$$

- Repeat this process. □

We also proved that if E/F is generated by roots of $p(x)$ which splits in $\widetilde{E}/F$, there exists a morphism of extensions of F

$$\varphi \colon E \to \widetilde{E}.$$

April 9, 2025

Definition 6.5

Let $S \subseteq F[x] - F$ be a family of polynomials. E/F is a **splitting field of S** if

1. Every $p \in S$ splits completely$/E$.
2. E/F is generated by the roots of all $p \in S$.

Example 6.9 –

1. If $S = \{p\}$, then E is the splitting field of p.
2. If $S = \{p_1, \ldots, p_n\}$, then E is the splitting field of $p_1, \ldots, p_n$.
3. (The most important) If $S = F[x] - F$, then $E = \overline{F}$.

Theorem 6.17

For any F, S, a splitting field E/F of S exists. If E/F and $\widetilde{E}/F$ are splitting fields of S, then they are isomorphic extensions.

Corollary 6.18

$\overline{F}$ exists and is unique up to isomorphic extensions.

Proof of Theorem 6.17. Uniqueness. Consider the following poset:

$$\left\{(K, \varphi) : F \subseteq K \subseteq E \text{ is a field}, \varphi \colon K \to \widetilde{E} \text{ a homomorphism}/F\right\},$$

where the partial order $\preceq$ is given by

$$(K_1, \varphi_1) \preceq (K_2, \varphi_2) \iff K_2 \supseteq K_1, \varphi_2|_{K_1} = \varphi_1.$$

Let $(K_\alpha, \varphi_\alpha)_\alpha$ be a chain. Define $K = \bigcup_\alpha K_\alpha$ (this is a subfield of E) and $\varphi \colon K \to \widetilde{E}$, where $\varphi(x) = \varphi_\alpha(x)$ if $x \in K_\alpha$. Therefore, by Zorn's lemma, there exists a maximal (K, φ). We claim this is E. To prove this, we show by contradiction that (K, φ) can be extended, making it not maximal. Let $K \subset E$, so there exists $p \in S$ and $\alpha \in E - K$ with $p(\alpha) = 0$. We have that $m_{\alpha,K}(x) \mid p(x)$ in $K[x]$. There is a natural map $\varphi\colon K[x] \to \varphi(K)[x]$, so $\varphi(m_{\alpha,K}) \in \varphi(K)[x]$ is a polynomial that divides $p(x)$, which splits in $\widetilde{E}$, so there exists $\beta \in \widetilde{E}$ with $\varphi(m_{\alpha,K})(\beta) = 0$. This defines a morphism $\widehat{\varphi}\colon K(\alpha) \to \varphi(K)(\beta)$ that extends φ. Therefore, $(K, \varphi) \prec (K(\alpha), \widehat{\varphi})$, which is a contradiction.

Since E and $\widetilde{E}$ are generated by all roots of $p \in S$, φ defined on E induces an isomorphism.

Existence. Set $\Omega \supseteq F$ and consider extensions $K \subseteq \Omega$. Consider the poset

$$\{(K, +, \cdot) : K \text{ is an extension of } F \text{ generated by some roots of } p(x) \in F[x]\},$$

where the partial order $\preceq$ is given by

$$(K_1, +_1, \cdot_1) \preceq (K_2, +_2, \cdot_2) \iff K_1 \text{ is a subfield of } K_2.$$

Similar to the uniqueness proof, Zorn's lemma implies there exists a maximal element $(K, +, \cdot)$. We claim $(K, +, \cdot)$ is a splitting field. Suppose not. Then some $p(x) \in F[x]$ does not split completely in K. Then there exists an irreducible, degree ≥ 2 polynomial $\widehat{p}(x) \in K[x]$ that divides $p(x)$. But then

$$(K[x]/(\widehat{p}), +, \cdot) \succ (K, +, \cdot),$$

contradiction. We still need to show that $K[x]/(\widehat{p}) \hookrightarrow \Omega$. It suffices to choose Ω with cardinality

$$|\Omega| > |F[x] \times \mathbb{Z}|.$$

Let $\Omega = K$. □

Example 6.10 – We know that $\mathbb{C} \supset \overline{\mathbb{Q}}$ because there are countably many algebraic numbers. Choose some $\alpha_1 \in \mathbb{C} - \overline{\mathbb{Q}}$. Further there exists $\alpha_2 \in \mathbb{C} - \overline{\mathbb{Q}(\alpha_1)}$. This process can be continued infinitely by the axiom of choice to give a subfield

$$\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots) \subseteq \mathbb{C}.$$

But it can be shown this field is isomorphic to $\mathbb{Q}(\alpha_2, \ldots, \alpha_n, \ldots)$. This induces an isomorphism from $\mathbb{C}$ to a subfield of itself. This is completely non-constructive because we applied the axiom of choice.

6.7. Separability

April 11, 2025 Let E/F be a finite extension, i.e., $E = (\alpha_1, \ldots, \alpha_k)$ where α_i is algebraic/F. Suppose K/F is any extension. Consider the set $\mathrm{Hom}_F(E, K)$ of morphisms of F-extensions.

Example 6.11 ($\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{C})$) – Suppose we want a morphism of $\mathbb{Q}$-extensions from $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ to $\mathbb{C}$. We first describe where the map φ sends $\sqrt{2}$. There are two options, corresponding to the two roots of $m_{\sqrt{2},\mathbb{Q}}(x)$:

$$\sqrt{2} \mapsto \sqrt{2}, \qquad \sqrt{2} \mapsto -\sqrt{2}.$$

Notice that we have constructed morphisms

$$\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}, \qquad \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}.$$

Now we decide where to send $\sqrt{3}$ given either of the maps $\mathbb{Q}(\sqrt{2}) \to \mathbb{C}$. We have $m_{\sqrt{3},\mathbb{Q}(\sqrt{2})} = x^2 - 3$ [Exercise], so $\varphi(\sqrt{3})^2 - 3 = 0$, hence $\varphi(\sqrt{3})$ is a root of $m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x)$. Again, there are two options:

$$\sqrt{3} \mapsto \sqrt{3}, \quad \sqrt{3} \mapsto -\sqrt{3}.$$

This gives us a map $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{C}$. In the process, notice that at most 4 maps are formed.

The maps were constructed iteratively through a tower of simple extensions (orange first, then red).

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[r, "\varphi"'] \arrow[d, dash] & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[r] \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, "\mathrm{id}"'] & \mathbb{Q}
\end{tikzcd}$$

Remark 6.19. Two things in this construction don't happen in general:

- $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$. That is, adjoining a root single root may result in a different field, depending on the root. Consider $\mathrm{Hom}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})$.
- The irreducible polynomial of $\sqrt{3}/\mathbb{Q}$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Consider $\mathrm{Hom}(\mathbb{Q}(\sqrt{2}, \sqrt[4]{8}), \mathbb{C})$ (notice that $(\sqrt[4]{8})^2 = 2\sqrt{2}$, so $\mathbb{Q}(\sqrt[4]{8}) \supseteq \mathbb{Q}(\sqrt{2})$).

A similar process as described in the example works for $\mathrm{Hom}_F(E, K)$. The number of choices at step i will be at most $m_{\alpha_i, F(\alpha_1, \ldots, \alpha_{i-1})}$. Therefore, we have

Proposition 6.20

$$\begin{aligned}
\#\mathrm{Hom}_F(E,K) &\le \prod_{i=1}^{k} \deg(m_{\alpha_i, F(\alpha_1,\ldots,\alpha_{i-1})}) \\
&= \prod_{i=1}^{k} \deg_{F(\alpha_1,\ldots,\alpha_{i-1})}(\alpha_i) \\
&= \prod_{i=1}^{k} [F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})] \\
&= [E : F].
\end{aligned}$$

This inequality is strict if at least one of the polynomials $m_{\alpha_i, F(\alpha_1,\ldots,\alpha_{i-1})}$ has fewer roots than its degree. This happens in two cases:

- Case 1: $m_{\alpha_i, F(\alpha_1,\ldots,\alpha_{i-1})}$ does not split completely in K. In this case, K was too small! To resolve this, let K contain the splitting field of $m_{\alpha_i, F}$ for all i (this works because $m_{\alpha_i, F(\alpha_1,\ldots,\alpha_{i-1})}(x) \mid m_{\alpha_i F}(x)$). E.g. let $K = \overline{F}$.
- Case 2: $m_{\alpha_i, F(\alpha_1,\ldots,\alpha_{i-1})}$ has multiple roots. This issue is harder to resolve...

Definition 6.6

Let $p(x) \in F[x]$ be a nonzero polynomial. We say p is **separable** if all of its roots are **simple** (have multiplicity 1) in some extension where p splits completely.

Lemma 6.21

α_i is a multiple root of $p \iff p(\alpha) = p'(\alpha) = 0$.

Remark 6.22. We are using a formal derivative $\frac{d}{dx} \colon F[x] \to F[x]$, where is defined purely algebraically. It's a F-linear map that satisfies the *Leibniz rule*: $(p(x)q(x))' = p'(x)q(x) + p(x)q'(x)$. In fact, any F-linear map $F[x] \to F[x]$ satisfying the Leibniz rule is called a *derivation*.

Corollary 6.23

$p(x)$ is separable $\iff \gcd(p(x), p'(x)) = 1$.

Remark 6.24. To prove this, first note that if $f, g \in F[x]$ and E/F is an extension, then $\gcd(f, g)$ is equal over both polynomial rings. Therefore, if f, g are coprime over F, they are coprime over E. Since $F[x]$ is a PID, there exist polynomials α, β with $\alpha f + \beta g = 1$.

6.7.1. Perfect fields

Notice that an irreducible polynomial $f(x)$ is separable $\iff f(x) \nmid f'(x) \iff f'(x) = 0$. This does *not* imply that $f(x)$ is a constant. For example, if F has characteristic p, then $(x^p)' = px^{p-1} = 0$. This actually characterizes the polynomials with derivative zero: $f'(x) = 0 \iff f(x) \in F[x^p]$.

Therefore, if $\text{char}(F) = 0$, then all irreducible polynomials are separable.

Definition 6.7

A field F is **perfect** if either

1. $\text{char}(F) = 0$,
2. $\text{char}(F) = p$ and $F^p = \{x^p : x \in F\} = F$.

Remark 6.25. (2) is an important condition because in characteristic p, $(x + y)^p = x^p + y^p$. Therefore, we can reduce any polynomial in $F[x^p]$ as follows:

$$a_k x^{kp} + \cdots + a_1 x^p + a_0 = (a_k^{1/p} x^k + \cdots + a_1^{1/p} x + a_0^{1/p})^p,$$

provided that $a_i^{1/p}$ exists. This is precisely the condition for a perfect field. Therefore, we avoid the issues above in characteristic p given that the field is perfect.

April 14, 2025

Proposition 6.26

If F is a perfect field, then every irreducible polynomial is separable.

Definition 6.8

Let α be algebraic$/F$. We say that α is **separable** if $m_{\alpha,F}(x)$ is separable.

Corollary 6.27

If F is perfect, then α algebraic $\implies$ α separable.

Remark 6.28. Conversely, if F is not perfect, there exists $a \in F - F^p$. A problem on the homework is to show that $x^p - a$ is irreducible.

Non-Example 6.1 (Imperfect fields) – Let's try to find an imperfect field.

1. $\text{char}(F) = 0$ implies perfect, so we need to assume positive characteristic.
2. $\mathbb{F}_p = \mathbb{Z}/p$ is perfect by Fermat's little theorem.
3. On the homework we showed that a finite (and algebraic) extension of a perfect field is perfect, so $\mathbb{F}_{p^n}$ is perfect as well.
4. Therefore, we must add a transcendental element. Consider $\mathbb{F}_p(t)$. The element t is not the pth power of some rational function. By the previous remark, the polynomial $x^p - t \in (\mathbb{F}_p(t))[x]$ is irreducible, but has formal derivative 0, so it is inseparable.

6.7.2. Separable extensions

Theorem 6.29

Let $E = F(\alpha_1, \dots, \alpha_k)/F$ be a finite extension. Let K/F be an extension such that $m_{\alpha_i,F}$ split$/K$. The following a equivalent:

1. $\#(\text{Hom}_F(E, K)) = [E : F]$.
2. $m_{\alpha_1,F}, m_{\alpha_2,F(\alpha_1)}, \dots, m_{\alpha_k,F(\alpha_1,\dots,\alpha_{k-1})}$ are separable.
3. All $\alpha \in E$ are separable$/F$.

Proof. ((1) $\iff$ (2)) is given by counting maps from looking at the tower

$$\begin{tikzcd}
F(\alpha_1, \dots, \alpha_k) \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
F(\alpha_1) \arrow[d, dash] \\
F
\end{tikzcd}$$

(we did this computation already).

((1) $\implies$ (3)) Consider $E(\alpha, \alpha_1, \dots, \alpha_k)$. We construct a map $E \to K$ by first considering a map $F(\alpha) \to K$, then extending it further to a map $E \to K$.

((3) $\implies$ (2)) If $m_{\alpha_i,F}$ is separable, then $m_{\alpha_i,F(\alpha_1,\dots,\alpha_{i-1})} \mid m_{\alpha_i,F}$ is also separable (all roots are simple). □

Definition 6.9

An extension E/F is **separable** if it satisfies any of the above conditions (6.29).

Remark 6.30. Let F have characteristic p. Let E/F be algebraic (or finite). The **separable closure**, $E^{\mathrm{sep}} := \{\alpha \in E : \alpha \text{ separable}/F\}$ is a subfield of E, which is the maximal separable subextension of F.

A homework problem is that $m_{\alpha,F}(x)$ can be expressed in the form $g(x^{p^k})$ for some $k \geq 0$, and g is irreducible and separable/F. In other words, E/E^{sep} has the following property: for all $\alpha \in E$, there exists $k \geq 0$ such that $\alpha^{p^k} \in E^{\mathrm{sep}}$. Another way to say this is that E/E^{sep} is **purely inseparable**.

Notice that this remark is only interesting for imperfect fields.

6.7.3. Normal extensions and the start of Galois theory

Theorem 6.31

Let $E = F(\alpha_1, \dots, \alpha_k)/F$ be a finite extension. Let K/F be an extension such that $m_{\alpha_i,F}$ split/K. Embed $E \hookrightarrow K$. The following are equivalent:

1. $m_{\alpha_i,F}$ split in E.
2. For any $\varphi \colon E \to K$ (such that $\varphi|_F = \mathrm{id}_F$), $\varphi(E) \subseteq E$.
3. For any $\alpha \in E$, $m_{\alpha,F}$ splits/E.

This is another homework problem, with some simplifying assumptions (e.g., $K = \overline{F}$).

Remark 6.32. The above statements are equivalent to E/F being the splitting field of some polynomial $q(x) \in F[x]$.

Definition 6.10

We say an extension E/F is **normal** if it satisfies any of the above conditions (6.31), (6.32).

Definition 6.11

A finite (or algebraic) extension E/F is **Galois** if it is normal and separable.

Remark 6.33. If F is perfect, a finite (or algebraic) extension E/F is Galois $\iff$ it is normal. The most important case for the rest of the course is $F = \mathbb{Q}$.

Theorem 6.34
For a finite extension E/F, the following are equivalent:

1. E/F is Galois.
2. $\#\mathrm{Hom}_F(E, E) = \#\mathrm{Aut}_F(E) = [E : F]$.
3. E/F is a splitting field of a *separable* polynomial $q(x) \in F[x]$.

Galois theory is the study of Galois extensions, which is what we will study for the rest of the course. The idea with the definition of a Galois extension is that

- Separability gives us that $\#(\mathrm{Hom}_F(E, K))$ is as big as possible.
- Normality gives us that $\varphi \in \mathrm{Hom}_F(E, K)$ is actually an automorphism, so we can form a group of automorphisms of E/F.

6.8. Galois correspondence

The group of automorphisms of a Galois extension is so important that it gets its own name.

April 16, 2025

Definition 6.12
The **Galois** group of E/F is defined as $\mathrm{Gal}(E/F) := \mathrm{Aut}_F(E)$ when E/F is Galois.

Here's the big theorem:

Theorem 6.35 (Fundamental theorem of Galois theory)
Let E/F be a finite Galois extension. There is a bijection between the intermediate fields K and the subgroups of the Galois group $\mathrm{Gal}(E/F)$, where we send intermediate fields K to the Galois group of E over K, and send subgroups to the fixed field by that subgroup:

$$\begin{array}{ccc}
\left\{ \begin{array}{c} \text{intermediate fields } K \\ E \supseteq K \supseteq F \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{subgroups} \\ H \leq \mathrm{Gal}(E/F) \end{array} \right\} \\
K & \mapsto & \mathrm{Gal}(E/K) = \{\sigma \in \mathrm{Gal}(E/F) : \sigma|_K = \mathrm{id}_K\} \\
E^H := \{\alpha \in E : H \cdot \alpha = \alpha\} & \leftarrow\!\shortmid & H
\end{array}$$

The correspondence is inclusion-reversing (that is, larger intermediate fields correspond to smaller subgroups).

Example 6.12 $(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ – The field $E = \mathbb{Q}(\sqrt{2}, i)$ is the splitting field of the polynomial $(x^2-2)(x^2+1)$, so $E/\mathbb{Q}$ is Galois. Consider the tower

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2}, i) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Since $m_{\sqrt{2},\mathbb{Q}}(x) = x^2-2$, $m_{i,\mathbb{Q}(\sqrt{2})}(x) = x^2+1$, the extension has degree 4. Therefore,

$$\#\operatorname{Gal}(E/\mathbb{Q}) = [E:\mathbb{Q}] = 4.$$

The automorphisms of $E/\mathbb{Q}$ are as follows:

Automorphism	$\sqrt{2}\mapsto$	$i\mapsto$
id	$\sqrt{2}$	i
σ_1	$-\sqrt{2}$	i
σ_2	$\sqrt{2}$	$-i$
σ_3	$-\sqrt{2}$	$-i$

Now consider $\operatorname{Gal}(E/\mathbb{Q}(\sqrt{2}))$. It has two elements: id, σ_2, and it naturally is a subgroup of $\operatorname{Gal}(E/\mathbb{Q})$. Similarly, $\operatorname{Gal}(E/\mathbb{Q}(i)) = \{\mathrm{id}, \sigma_1\}$. We are missing the subgroup $\{\mathrm{id}, \sigma_3\}$. To figure out what intermediate field this corresponds to, write out an element of $\mathbb{Q}(\sqrt{2}, i)$ as $a + b\sqrt{2} + ci + di\sqrt{2}$, $a, b, c, d \in \mathbb{Q}$. Then

$$\begin{aligned}
\mathrm{id}(a + b\sqrt{2} + ci + d\sqrt{2}i) &= a + b\sqrt{2} + ci + di\sqrt{2} \\
\sigma_3(a + b\sqrt{2} + ci + d\sqrt{2}i) &= a - b\sqrt{2} - ci + di\sqrt{2}.
\end{aligned}$$

It follows that the fixed subfield is $\mathbb{Q}(i\sqrt{2})$, so $\operatorname{Gal}(E/\mathbb{Q}(i\sqrt{2})) = \{\mathrm{id}, \sigma_3\}$. In summary, we've constructed a correspondence

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2}, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \{\mathrm{id}\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{\mathrm{id}, \sigma_2\} \arrow[dr, dash] & \{\mathrm{id}, \sigma_1\} \arrow[d, dash] & \{\mathrm{id}, \sigma_3\} \arrow[dl, dash] \\
& \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\} &
\end{tikzcd}$$

Example 6.13 (Non-Galois extension) – Consider $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. This is not a Galois extension, but we can consider the Galois extension $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)/\mathbb{Q}$, where $\alpha_j = \sqrt[3]{2}\zeta_3^j$ are roots of x^3-2.

Any $\varphi \in \operatorname{Gal}(E/\mathbb{Q})$ permutes the roots $\alpha_1, \alpha_2, \alpha_3$, so $\operatorname{Gal}(E/\mathbb{Q}) \cong S_3$. Since $\varphi \in \operatorname{Gal}(E/\mathbb{Q}(\sqrt[3]{2}))$ fixes $\sqrt[3]{2}$, the only possible maps are $\alpha_1 \mapsto \alpha_1$, $\alpha_2 \mapsto \alpha_2$, and $\alpha_1 \mapsto \alpha_2$, $\alpha_2 \mapsto \alpha_1$. Similar calculations give us $\operatorname{Gal}(E/\mathbb{Q}(\alpha_1)), \operatorname{Gal}(E/\mathbb{Q}(\alpha_2))$.

But there's one more subgroup of S_3 we haven't covered: A_3. One can realize (with some cleverness) that $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$. The corresponding intermediate field turns out to be $\mathbb{Q}(\sqrt{-3})$.

April 18, 2025

Proof of Theorem 6.35. Let $G = \mathrm{Gal}(E/K)$. The following are easy to show:

1. E/K is Galois, $\{\sigma \in G : \sigma|_K = \mathrm{id}_K\} = \mathrm{Gal}(E/K)$, so $\#\mathrm{Gal}(E/K) = [E : K] = \frac{[E:F]}{[K:F]}$.
2. Order-reversing: $K_1 \subseteq K_2$ implies $\mathrm{Gal}(E/K_1) \supseteq \mathrm{Gal}(E/K_2)$ (an automorphism fixing K_2 certainly fixes K_1), and $H_1 \leq H_2$ implies $E^{H_1} \supseteq E^{H_2}$ (this is a basic fact about fixed points a group action).
3. $K \subseteq E^{\mathrm{Gal}(E/K)}$ and $H \subseteq \mathrm{Gal}(E/E^H)$ are clear.

We want to show that the inclusions in (3) are equality. We'll use a counting argument. For the first equality,

1. For all $H \leq G$, $[E : E^H] = \#\mathrm{Gal}(E/E^H) \geq \#H$.
2. For all $K \supseteq F$, $[E : E^{\mathrm{Gal}(E/K)}] \geq \#\mathrm{Gal}(E/K) = [E : K]$. But since $E^{\mathrm{Gal}(E/K)} \supseteq K$, $K = E^{\mathrm{Gal}(E/K)}$, as desired.

The other equality is more challenging. We use (and prove!) the following theorem.

Theorem 6.36 (Artin's theorem)
Let E be any field, and let $H \leq \mathrm{Aut}(E)$ be a finite subgroup. Let $F = E^H$. Then

$$[E : F] \leq \#H.$$

Proof. Since we are concerned with the degree, this argument is linear-algebra-flavored. Let $H = \{\sigma_1, \dots, \sigma_m\}$. Let $\alpha_1, \dots, \alpha_n \in E$ be linearly independent over F. We claim $n \leq m$. Consider the system of linear equations

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_n)x_n = 0, \\ \sigma_2(\alpha_1)x_1 + \cdots + \sigma_2(\alpha_n)x_n = 0, \\ \vdots \\ \sigma_m(\alpha_1)x_1 + \cdots + \sigma_m(\alpha_n)x_n = 0, \end{cases}$$

where $(x_1, \dots, x_n) \in E^n$. We claim the only solution is the trivial $x_1 = \cdots = x_n = 0$ (which implies $m \geq n$). Suppose $(x_1, \dots, x_n) \neq 0$ is a solution. WLOG, $x_1 \neq 0$. Since the system is homogeneous, we may divide by x_1 to get $x_1 = 1$. Notice that $\mathrm{id} \in H$, so let $\sigma_1 = \mathrm{id}$. Then we get

$$\alpha_1 x_1 + \cdots + \alpha_n x_n = 0.$$

But since $\alpha_1, \dots, \alpha_n$ are independent/F, one of the x_i's, say, x_2 is not in F, i.e., $\sigma_i(x_2) \neq x_2$ for some i. For $\sigma_j \in H$, we have

$$\begin{aligned} 0 &= \sigma_i(\sigma_j(\alpha_1)x_1 + \cdots + \sigma_j(\alpha_n)x_n) \\ &= (\sigma_i \circ \sigma_j)(\alpha_1) \cdot \sigma_i(x_1) + \cdots + (\sigma_i \circ \sigma_j)(\alpha_n) \cdot \sigma_i(x_n). \end{aligned}$$

It follows that $(\sigma_i(x_1), \dots, \sigma_i(x_n)) = (1, \dots, \sigma_i(x_n))$ is also a solution (since $(\sigma_i \circ \sigma_j)_j$ is just a permutation of $(\sigma_j)_j$). But subtracting from the original solution $(x_1, \dots, x_n)$, we get $(0, \sigma_i(x_2) - x_2, \dots, \sigma_i(x_n) - x_n)$ is also a solution.

We prove that the only solution is trivial by a "descent" argument. Suppose $(x_1, \dots, x_n) \in E^n$ is a nonzero solution with the largest number of nonzero entries. If $n - 1$ entries are nonzero, then all entries are zero because E is a field. Otherwise, the above procedure creates a solution at least one more zero and a nonzero term, yielding a contradiction. ■

Since $[E : E^H] \leq \#H$ and $H \subseteq \mathrm{Gal}(E/E^H)$, we have $H = \mathrm{Gal}(E/E^H)$. □

Remark 6.37. The proof of Artin's theorem (6.36) seems somewhat magical. However, it's well-motivated. Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for E/F. Consider the extension of scalars $E \otimes_F E$. The elements look like $\alpha_1 \otimes x_1 + \cdots + \alpha_n \otimes x_n$ for $x_i \in E$. Define a map

$$\begin{aligned} E \otimes_F E &\to E^{\mathrm{Aut}_F(E)} \\ \alpha_1 \otimes x_1 + \cdots + \alpha_n \otimes x_n &\mapsto \left(\sum_{j=1}^{n} x_j \sigma_i(\alpha_j) \right)_{\sigma_i \in \mathrm{Aut}_F(E)}. \end{aligned}$$

Then Artin's theorem says that this map is injective ($n = \dim_E(E \otimes_F E) \leq \dim(E^m) = m$).

Example 6.14 – If E/F is a finite Galois extension with $[E : F] = \#\mathrm{Gal}(E/F) = n$, then the above map is

$$\begin{aligned} E \otimes_F E &\to E^n \\ \alpha \otimes x &\mapsto (\sigma_1(\alpha) \cdot x, \dots, \sigma_n(\alpha) \cdot x). \end{aligned}$$

Since the dimensions are equal, this map is bijective.

On the homework, we showed that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$. Notice that this is a special case of the above statement, because $\mathbb{C}/\mathbb{R}$ is a degree 2 Galois extension.

Exercise 6.1. Prove that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$ as $\mathbb{R}$-algebras, by describing a map.

Remark 6.38. Artin's theorem shows that if $F = E^H$ is the field fixed by $H \leq \operatorname{Aut}_F(E)$, then $[E : F] \leq \#H$. But combining the facts

$$H \subseteq \operatorname{Aut}_F(E), \qquad \#\operatorname{Aut}_F(E) \leq [E : F],$$

we get that

$$H = \operatorname{Aut}_F(E) \iff [E : F] = \#H \iff E/F \text{ is Galois.}$$

This gives an easier way to show a field extension is Galois.

An easy consequence of the correspondence (6.35): if $K_1, K_2 \subseteq E$ are two intermediate fields, then $K_1 \cap K_2$ and K_1K_2 are also intermediate fields, which correspond to $\langle H_1, H_2 \rangle$ and $H_1 \cap H_2$, respectively.

April 21, 2025

Example 6.15 (Cyclotomic extension) – Let $\zeta = e^{\frac{2\pi i}{17}}$ and consider the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Since ζ is the splitting field of $x^{17} - 1$ (which actually factors as $(x-1)(x^{16} + \cdots + x + 1)$), the extension is Galois.

Fact 6.39. $\Phi_p(x) := \frac{x^p - 1}{x - 1} \in \mathbb{Q}[x]$ is irreducible.

Proof (sketch). Do the Eisenstein criterion on $\Phi_p(x+1) = \frac{(x+1)^p - 1}{x}$. □

Remark 6.40. In fact, for any $n \geq 1$,

$$\Phi_n(x) = \frac{x^n - 1}{\operatorname{lcm}_{\substack{d \mid n \\ d < n}} x^d - 1} \in \mathbb{Z}[x]$$

is irreducible over $\mathbb{Q}$.

Therefore, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 16$. Every $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is determined by where it sends ζ. ζ can only be mapped to ζ^k for $1 \leq k \leq 16$. Looking at how composition works, it's not hard to prove an isomorphism

$$\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/17)^\times.$$

Since 17 is prime, $(\mathbb{Z}/17)^\times \cong \mathbb{Z}/16$. We know the subgroup lattice of $\mathbb{Z}/16$ well:

$$\begin{tikzcd}
\{e\} \arrow[d, dash] \\
8\mathbb{Z}/16 \arrow[d, dash] \\
4\mathbb{Z}/16 \arrow[d, dash] \\
2\mathbb{Z}/16 \arrow[d, dash] \\
\mathbb{Z}/16
\end{tikzcd}$$

so we have a corresponding tower of fields

$$\begin{tikzcd}
\mathbb{Q}(e^{\frac{2\pi i}{n}}) \arrow[d, dash, "2"'] \\
E_3 \arrow[d, dash, "2"'] \\
E_2 \arrow[d, dash, "2"'] \\
E_1 \arrow[d, dash, "2"'] \\
\mathbb{Q}
\end{tikzcd}$$

where each extension is *quadratic* (i.e., degree 2). Computing E_3 is done by noting that $8\mathbb{Z}/16$ corresponds to the two element subgroup $\{\mathrm{id}, \sigma\} \leq \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, where σ is complex conjugation. Therefore,

$$E_3 = \mathbb{R} \cap \mathbb{Q}(e^{\frac{2\pi i}{n}}) = \mathbb{Q}\left(\frac{\zeta + \zeta^{-1}}{2}\right) = \mathbb{Q}\left(\cos\left(\frac{2\pi}{17}\right)\right)$$

(showing the second equality may take some work).

Fact 6.41. Any quadratic extension E/F is of the form $F(\sqrt{a})$ for some $a \in F$ (assuming that $\mathrm{char}(F) \neq 2$).

As a corollary, $\cos\left(\frac{2\pi}{17}\right)$ can be written with the operations $+, -, \cdot, /, \sqrt{\ }$ on $\mathbb{Q}$, since all extensions are quadratic.

Exercise 6.2 (Challenging)**.** Find this expression.

Remark 6.42. In general, $\mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}) \cong (\mathbb{Z}/n)^{\times}$ by a similar argument.

If F is an arbitrary field, and we let E be the splitting field of $x^n - 1$, then

$$\mathrm{Gal}(E/F) \subseteq (\mathbb{Z}/n)^{\times},$$

provided that $\mathrm{char}(F) \nmid n$.

6.8.1. Constructible numbers

$\alpha > 0$ is **constructible** if a segment of length α can be constructed using a ruler and compass, starting from a unit length. Algebraically, α is constructible if there exists a formula for it in terms of the operations $+, -, \cdot, /, \sqrt{\ }$ on $\mathbb{Q}$.

As a corollary of the last example, a regular 17-gon is constructible.

Fact 6.43 (By MATH 741...)**.** Let $E/\mathbb{Q}$ be a finite Galois extension. If $[E : \mathbb{Q}] = 2^k$, then $\mathrm{Gal}(E/\mathbb{Q})$ is a 2-group (it's order is a power of 2). By MATH 741 Corollary 2.13, we get a chain of groups

$$\mathrm{Gal}(E/\mathbb{Q}) \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_k = \{e\},$$

where $\#H_i = 2^{k-i}$ (i.e., we halve the subgroup size at each step).

By Galois theory, this corresponds to a tower

$$\begin{tikzcd}
E = E^{H_k} \arrow[d, dash, "2"'] \\
E^{H_{k-1}} \arrow[d, dash, "2"'] \\
\vdots \arrow[d, dash, "2"'] \\
E^{H_1} \arrow[d, dash, "2"'] \\
\mathbb{Q}
\end{tikzcd}$$

of quadratic extensions. Then every $\alpha \in E$ is “constructible” (we now allow α to be complex).

Corollary 6.44

If $E/\mathbb{Q}$ is not an extension of degree 2^k for some k, then there does not exist a tower of quadratic extensions

$$E_k \supseteq \cdots E_2 \supseteq E_1 \supseteq \mathbb{Q},$$

where $E \subseteq E_k$.

Example 6.16 – A regular n-gon is constructible $\iff$ $(\mathbb{Z}/n\mathbb{Z})^\times$ is a 2-group $\iff$ $\varphi(n)$ is a power of 2.

Example 6.17 – Suppose $\deg_{\mathbb{Q}}(\alpha) = 2^k$ for some algebraic α. This condition is necessary, but not sufficient for α to be constructible, since $\mathbb{Q}(\alpha)/\mathbb{Q}$ (a degree 2^k extension) may not be Galois. Let $\alpha_2, \ldots, \alpha_n$ be the other roots of $m_{\mathbb{Q},\alpha}(x)$. If

$$[\mathbb{Q}(\alpha, \alpha_2, \ldots, \alpha_n) : \mathbb{Q}]$$

is not a power of 2, then α is *not* constructible (the proof idea is as follows: suppose there is a tower $\mathbb{Q} \subseteq E_1 \subseteq \cdots E_{k-1} \subseteq E_k \subseteq \mathbb{Q}(\alpha, \alpha_2, \ldots, \alpha_n)$. Then there exists an automorphism of $\mathbb{Q}(\alpha, \alpha_2, \ldots, \alpha_n)$ switching α and any other α_i. We can show the degree of each extension in the tower is still the same, so all α_i are constructible, contradicting the extension not being a power of 2).

6.8.2. Conjugates

Definition 6.13

April 23, 2025

Let $\alpha, \beta \in E/F$ be algebraic. We say that α and β are **conjugate**/F if $m_{\alpha,F} = m_{\beta,F}$ ($\iff$ there exists an isomorphism of F-extensions $F(\alpha) \xrightarrow{\sim} F(\beta)$).

Proposition 6.45

If E/F is Galois with $G = \mathrm{Gal}(E/F)$, then $\alpha, \beta \in E$ are conjugate $\iff$ $\beta \in G \cdot \alpha = \{\sigma(\alpha) : \sigma \in G\}$.

Proof. ($\implies$) Extend the F-map $F(\alpha) \xrightarrow{\sim} F(\beta)$ to a map $E \to E$, which is possible precisely because E/F is Galois.

($\impliedby$) This is true even if E/F is not Galois. □

Moreover, since α is separable/F (because E/F is Galois), $m_{\alpha,F}(x) = \prod_{\sigma \in G}(x - \sigma(\alpha))$. In other words, $\deg_F(\alpha) = |G \cdot \alpha|$.

Example 6.18 – Let $\alpha = \sqrt{2} + i \in \mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$. Then its conjugates are $\left\{\pm\sqrt{2} \pm i\right\}$, so $\deg_{\mathbb{Q}}(\alpha) = 4$, and the minimal polynomial is $\prod(x \pm \sqrt{2} \pm i)$.

6.8.3. Normal extensions and normal subgroups

If E/F is Galois and K is an intermediate field, then we know E/K is Galois:

$$G = \mathrm{Gal}(E/F) \geq H = \left\{\sigma : \sigma|_K = \mathrm{id}_K\right\} = \mathrm{Gal}(E/K).$$

When is K/F Galois? We know that the extension is automatically separable, so it suffices to check then K/F is normal. This happens $\iff$ for all $\alpha \in K$, all conjugates are in K, i.e., $G \cdot K \subseteq K$. For all $\sigma \in G$, $\sigma(K)$ is another intermediate field, so we want to check when $\sigma(K) = K$. By Galois theory, we have a correspondence

$$\begin{aligned} K &\leftrightarrow H = \left\{\tau : \tau|_K = \mathrm{id}_K\right\}, \\ \sigma(K) &\leftrightarrow H' = \left\{\tau : \tau|_{\sigma(K)} = \mathrm{id}_{\sigma(K)}\right\}. \end{aligned}$$

So

$$\begin{aligned} \sigma^{-1}\tau\sigma \in H &\iff \text{for all } \alpha \in K, \tau \circ \sigma(\alpha) = \sigma(\alpha) \\ &\iff \text{for all } \alpha \in K, \sigma^{-1} \circ \tau \circ \sigma(\alpha) = \alpha. \end{aligned}$$

So $H = \sigma^{-1}H'\sigma$. Hence, normal extensions coincide with normal subgroups.

Proposition 6.46

Let E/F be a finite Galois extension and K an intermediate field. Let $G = \mathrm{Gal}(E/F)$, $H = \mathrm{Gal}(E/K)$. Then

1. K is a Galois extension of F $\iff$ H is a normal subgroup of G.
2. If (1) holds, then $\mathrm{Gal}(K/F) \cong G/H$.

Proof. (1) was proved above.

(2) For all $\sigma \in G$, $\sigma|_K : K \to K$, so we have a map

$$\begin{aligned} G &\to \mathrm{Gal}(K/F) \\ \sigma &\mapsto \sigma|_K. \end{aligned}$$

The kernel of this map is H by definition. This map is surjective either by a counting argument or by extending automorphisms. □

Example 6.19 – Let E be the splitting field of $x^{17}-2$ over $\mathbb{Q}$. In other words,

$$E=\mathbb{Q}(\sqrt[17]{2},\ \sqrt[17]{2}\zeta,\dots,\ \sqrt[17]{2}\zeta^{16}),$$

where $\zeta=e^{\frac{2\pi i}{17}}$. Let $\alpha=\sqrt[17]{2}$. We can consider E in the tower

$$\begin{tikzcd}
\mathbb{Q}(\alpha,\zeta) \arrow[d, dash] \\
\mathbb{Q}(\zeta) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

We already know that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})=(\mathbb{Z}/17)^{\times}$. We can now consider $\mathrm{Aut}_{\mathbb{Q}(\zeta)}(\mathbb{Q}(\alpha,\zeta))$. The automorphisms are given by

$$\alpha\mapsto\alpha\zeta^{m}$$

for $0\le m\le 16$, which identifies group of automorphisms with $\mathbb{Z}/17$.

Exercise 6.3. Show that $\deg_{\mathbb{Q}(\zeta)}(\alpha)=17$.

So $\mathbb{Q}(\alpha,\zeta)/\mathbb{Q}(\zeta)$ is Galois. If we let $G=\mathrm{Gal}(\mathbb{Q}(\alpha,\zeta)/\mathbb{Q})$, then we have some facts:

$$G\ge H\cong\mathbb{Z}/17,\qquad G/H\cong(\mathbb{Z}/17)^{\times}.$$

In fact, with some effort, we get that

$$G\cong\mathbb{Z}/17\rtimes(\mathbb{Z}/17)^{\times}.$$

A more enlightening way to describe this group is as linear automorphisms of $\mathbb{Z}/17$:

$$\left\{f\colon\mathbb{Z}/17\to\mathbb{Z}/17\colon x\mapsto kx+m : k\in(\mathbb{Z}/17)^{\times}, m\in\mathbb{Z}/17\right\},$$

from which the isomorphism becomes more clear.

Question. What is the meaning of G being a semidirect product?

Exercise 6.4. Let F be a field with $\mathrm{char}(F)\nmid n$. Then a primitive nth root of unity exists.

Here's the generalization.

Proposition 6.47

Let F be any field and $a \in F - \{0\}$. Let E be the splitting field of $f(x) = x^n - a$ over F, assuming $\mathrm{char}(F) \nmid n$ so that f is separable. Let α be a root of f and let ζ be a primitive nth root of unity. Then

- $\mathrm{Gal}(F(\zeta)/F) \leq (\mathbb{Z}/n)^\times$,
- $\mathrm{Gal}(F(\alpha, \zeta)/F(\zeta)) \leq \mathbb{Z}/n$,

and so

- $\mathrm{Gal}(F(\alpha, \zeta), F) \leq \mathbb{Z}/n \rtimes (\mathbb{Z}/n)^\times$.

6.9. Solvability

April 25, 2025 Recall the following from MATH 741:

Definition 6.14

Let G be a finite group. G is **solvable** if $G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_k = \{e\}$ such that G_i/G_{i+1} is abelain for all i. In other words, G is successively constructed from abelian groups.

Fact 6.48. G is solvable $\iff$ H is solvable and G/H is solvable.

Example 6.20 – Let F be a field, $a \in F$, and $n \in \mathbb{N}$ such that $\mathrm{char}(F) \nmid n$. Let E be the splitting field of $x^n - a$. Then $\mathrm{Gal}(E/F)$ is solvable.

On the field theoretic side:

Definition 6.15

Let E/F be a finite field extension. E/F is **solvable** if we have a tower

$$\begin{tikzcd}
E \subseteq K = K_m \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
K_2 \arrow[d, dash] \\
K_1 \arrow[d, dash] \\
F
\end{tikzcd}$$

such that each K_i/K_{i-1} is a splitting field of $x^k - a$ for some k and $a \in K_{i-1}$ (dependent on i) (and $\mathrm{char}(F) \nmid k$).

In other words, we want every element of E to be expressed using $+, -, /, \cdot$, and $\sqrt[k]{}$ (possibly nested).

Corollary 6.49

If E/F is solvable, then $\mathrm{Gal}(E/F)$ is solvable.

Proof (sketch). $\mathrm{Gal}(E/F)$ is a quotient of $\mathrm{Gal}(K/F)$, which is an extension of $\mathrm{Gal}(K_i/K_{i-1})$'s. □

Exercise 6.5. Suppose E/F is a Galois extension of prime degree p, and $\sigma\colon E \to E$ is a non-trivial element of its Galois group. Suppose that σ is diagonalizable (that is, there exists a basis of E as a vector space over F such that σ is diagonal in this basis). Show that E is the splitting field of a polynomial $x^p - a$ for some $a \in F$.

Proposition 6.50

Conversely, if $\mathrm{Gal}(E/F)$ is solvable, then E/F is solvable (assuming $\mathrm{char}(F) \nmid [E : F]$).

Proof (sketch).

1. Replace F with $F(\zeta)$, where ζ is a primitive nth root of unity where $n = [E : F]$.

$$\begin{tikzcd}
 & E(\zeta) \arrow[d, dash] \\
E \arrow[ur, dash] \arrow[d, dash] & F(\zeta) \\
F \arrow[ur, dash] &
\end{tikzcd}$$

   Since $\mathrm{Gal}(E/F)$ is solvable and $\mathrm{Gal}(E(\zeta)/E)$ is abelian, $\mathrm{Gal}(E(\zeta)/F)$ is solvable. This implies $\mathrm{Gal}(E(\zeta)/F(\zeta))$ is solvable. Therefore, it suffices to show $E(\zeta)/F(\zeta)$ is solvable.

2. By induction, we may assume $\mathrm{Gal}(E/F) \cong \mathbb{Z}/q$ for some prime q.

3. We claim the following:

   Claim 6.1. $E = F(\sqrt[q]{a})$ for some $a \in E$.

   To prove this claim, let $\sigma \in \mathrm{Gal}(E/F)$ generate the Galois group. Since $\sigma^q = \mathrm{id}_E$, and σ may be viewed as an F-linear map from $E \to E$, σ is diagonalizable. By Exercise 6.5, E is a splitting field of some $x^q - a \in F[x]$. □

6.9.1. Solvability of algebraic equations

Let F be a field, and $f \in F[x]$ be separable. Let E be the splitting field of f over F. For simplicity, we will define

$$G_f \coloneqq \mathrm{Gal}(E/F).$$

We just proved that E/F is solvable $\iff$ G_f is solvable. Suppose $f(x) = (x - \alpha_1)\cdots(x - \alpha_n)$. Since automorphisms of G_f is uniquely determined by the image of each α_i, which is some element in $\{\alpha_1, \dots, \alpha_n\}$, there is an inclusion

$$G_f \hookrightarrow S_n.$$

G_f acts transitively on $S_n \iff f$ is irreducible.

f (that is, E/F) is **solvable** $\iff G_f$ is solvable. It now seems more realistic that some quintics (and above) will be not solvable, since $S_5, S_6, \ldots$ are not solvable (because $A_n \trianglelefteq S_n$ and A_n is simple for $n \geq 5$). We'll show that there are actually polynomials f with $G_f \cong S_5$.

Example 6.21 – We'll construct an $f \in \mathbb{Q}[x]$ with $G_f \cong S_5$.

Lemma 6.51

If $G \leq S_n$ such that (1) G acts transitively on $\{1, \ldots, n\}$ (2) G contains a transposition, then $G = S_n$. [1]

[1] Lecture correction: this only holds if n is prime. In general, instead of G acting transitively, you need G to be a *primitive permutation group*.

Therefore, we need f to be irreducible (e.g. by Eisenstein), and have 3 real roots, and 2 complex roots, so the complex conjugation automorphism transposes the two complex roots. Now look up what polynomials work.

6.9.2. General formula for roots

April 28, 2025 Consider a "general polynomial:"

$$x^n + a_{n-1}x^{n-1} + \cdots a_0,$$

where $a_0, \ldots, a_{n-1}$ are variables, so we view it as a polynomial in $F(a_0, \ldots, a_{n-1})$. If $x_1, \ldots, x_n$ are the roots of this polynomial, then $(x - x_1) \cdots (x - x_n)$ expands to $x^n + a_{n-1}x^{n-1} + \cdots a_0$. Therefore, the extension $F(a_0, \ldots, a_{n-1}, x_1, \ldots, x_n)/F(a_0, \ldots, a_{n-1})$ satisfies

$$F(a_0, \ldots, a_{n-1}, x_1, \ldots, x_n) = F(x_1, \ldots, x_n).$$

On the other hand, we can view $F(a_0, \ldots, a_{n-1}) \subseteq F(x_1, \ldots, x_n)$ as the field

$$F(\sigma_1, \ldots, \sigma_n),$$

where σ_i are the elementary symmetric polynomials:

$$\begin{aligned} \sigma_1 &= x_1 + \cdots + x_n \\ \sigma_2 &= x_1^2 + x_1x_2 + \cdots + x_n^2 \\ &\vdots \\ \sigma_n &= x_1 \cdots x_n, \end{aligned}$$

which follows by expanding $(x - x_1) \cdots (x - x_n)$. Consider the actions of S_n on $F(x_1, \ldots, x_n)$ by permuting the elements x_i accordingly. By the theory of symmetric functions, the fixed elements of $F(x_1, \ldots, x_n)$ under the symmetric group S_n are precisely $a_0, \ldots, a_{n-1}$:

$$F(x_1, \ldots, x_n)^{S_n} = F(a_{n-1}, \ldots, a_0).$$

By Artin's theorem (6.36),

$$S_n \cong \mathrm{Gal}(F(x_1, \ldots, x_n)/F(a_0, \ldots, a_{n-1})).$$

This also suggests to us that finding a general formula for the x_i's would mean dealing with an extension with Galois group S_n.

6.10. Finite fields

We deduce what finite fields could exist: let F be a field with $\#F < \infty$.

- Then $\operatorname{char}(F) = p$, so $F \supseteq \mathbb{F}_p$.
- $[F : \mathbb{F}_p] < \infty$, so the order of F must be a prime power: $\#F = p^{[F:\mathbb{F}_p]} =: q$.
- From group theory, $|F^\times| = q - 1$, which implies (from Fermat's little theorem), for all $\alpha \in F^\times$, $\alpha^{q-1} = 1$. Equivalently, all $\alpha \in F$ are roots of $x^q - x$.

Therefore, F, defined as the splitting field of $x^q - x$ over $\mathbb{F}_p$, is unique (up to isomorphism). Conversely, given $q = p^n$, take $\mathbb{F}_p \subseteq \overline{\mathbb{F}_p}$.

Claim 6.2. The set $\{\alpha : \alpha^q = \alpha\} \subseteq \overline{\mathbb{F}_p}$ is a field of size q.

Proof. We use the special property of characteristic p: $(\alpha \pm \beta)^p = \alpha^p \pm \beta^p$. Otherwise, showing this is a field is clear. Since $(x^q - x)' = -1$, which is coprime with $x^q - x$, $x^q - x$ is separable and has q roots. ■

Hence, for every $q = p^n$, there exists a unique (up to isomorphism) field with q elements, which we denote $\mathbb{F}_q$, satisfying $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \overline{\mathbb{F}_p}$.

Question. What does the poset $\{\mathbb{F}_q : q = p^n\}$ look like (ordered by inclusions $\mathbb{F}_{q_1} \hookrightarrow \mathbb{F}_{q_2}$)? Some necessary conditions:

- $\operatorname{char}(\mathbb{F}_{q_1}) = \operatorname{char}(\mathbb{F}_{q_2})$, so let $q_1 = p^n$, $q_2 = p^m$.
- If $[\mathbb{F}_{q_2} : \mathbb{F}_{q_1}] = k$, then $q_2 = p^m = p^{nk} = p_1^k$.

We claim these conditions are sufficient. Indeed, if $\alpha \in \overline{\mathbb{F}_p}$ satisfies $x^{p^n} = x$, then it also satisfies $x^{p^{nk}} = x$.

Example 6.22 – The proper subfields of $\mathbb{F}_{p^6}$ are $\left\{\mathbb{F}_p, \mathbb{F}_{p^2}, \mathbb{F}_{p^3}, \mathbb{F}_{p^6}\right\}$ with inclusions as follows:

$$\begin{tikzcd}
 & \mathbb{F}_{p^6} & \\
\mathbb{F}_{p^2} \arrow[ur, dash] & & \mathbb{F}_{p^3} \arrow[ul, dash] \\
 & \mathbb{F}_p \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

Suppose we wanted to find $|\mathbb{F}_{p^6} - (\mathbb{F}_{p^3} \cup \mathbb{F}_{p^2})|$. Then it has precisely

$$p^6 - p^3 - p^2 + p$$

elements by inclusion-exclusion. This gives the number of primitive elements of $\mathbb{F}_{p^6}/\mathbb{F}_p$. Similarly, we can calculate the number of elements of degree 1, 2, and 3: p, $p^2 - p$, and $p^3 - p$ elements respectively.

Moreover, the $p^6 - p^3 - p^2 + p$ primitive elements come in groups of 6, where each group has an element and its 5 other conjugates. In fact, $\frac{p^6-p^3-p^2+p}{6}$ is the number of irreducible polynomials of degree 6.

A similar exclusion-exclusion applies to the polynomials $x^{p^n} - x$ associated with the intermediate fields $\mathbb{F}_{p^n}$:

$$\prod_{\substack{p\in\mathbb{F}_p[x]\\ \deg p=6\\ p \text{ irreducible, monic}}} p(x) = \frac{(x^{p^6}-x)(x^p-x)}{(x^{p^3}-x)(x^{p^2}-x)}.$$

April 30, 2025

Yesterday's discussion was the same as looking at the **Frobenius homomorphism**

$$\begin{aligned} \mathrm{Fr}\colon \overline{\mathbb{F}_p} &\to \overline{\mathbb{F}_p} \\ x &\mapsto x^p. \end{aligned}$$

For any $q = p^n$, define $\mathbb{F}_q \coloneqq \left\{x \in \overline{\mathbb{F}_p} : \mathrm{Fr}^n(x) = x\right\}$. This embeds all finite fields in $\overline{\mathbb{F}_p}$ and all finite subfields of $\overline{\mathbb{F}_p}$ are $\mathbb{F}_{p^n}$ for $n \geq 1$.

Corollary 6.52

$$\overline{\mathbb{F}_p} = \bigcup_{n\geq 1} \mathbb{F}_{p^n}.$$

6.10.1. Galois theory perspective

$\mathbb{F}_{p^n}/\mathbb{F}_p$ is a finite Galois extension (indeed, it is the splitting field of $x^{p^n} - x$ (or, more economically, any of its irreducible degree n factors)).

Proposition 6.53

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \mathrm{Fr} \rangle = \left\{\mathrm{id}, \mathrm{Fr}, \ldots, \mathrm{Fr}^{n-1}\right\}.$$

It would be more accurate to write $\mathrm{Fr}|_{\mathbb{F}_{p^n}}$ here.

Proof (sketch).

- It is clear that these are all automorphisms.
- In fact, these are all distinct, because if $\mathrm{Fr}^k = \mathrm{id}$ for some $k < n$, then $x^{p^k} = x$ for all $x \in \mathbb{F}_{p^n}$, which contradicts the supposed size of $\mathbb{F}_{p^n}$.
- Therefore, these are all automorphisms, since $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. □

For $m \mid n$, Galois theory tells us that

$$(\mathbb{F}_{p^n})^{\mathrm{Fr}^m} = \mathbb{F}_{p^m}.$$

Remark 6.54. We can write $\mathbb{F}_{p^n}$ as the quotient $\mathbb{F}_p[x]/(f)$, where $f \in \mathbb{F}_p[x]$ is irreducible. This is analogous to quotienting $\mathbb{Z}$ by the ideal (ℓ), where ℓ is prime to get $\mathbb{Z}/\ell$. One could argue that the former is easier to work with, since, as a group, $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p^n$.

Example 6.23 (RSA) – RSA encryption uses the following facts:

1. We can find large primes:
   a) The prime number theorem gives us the probability that a number $\leq N$ is prime.

b) We have fast primality tests.

2. By the Chinese remainder theorem,

$$\mathbb{Z}/pq \cong \mathbb{Z}/p \times \mathbb{Z}/q.$$

3. We have no fast factorization algorithm (i.e., to get from pq to p, q).

Here are the analogous questions for finite fields. To solve the questions, it's helpful to note the Galois theory structure (that is, the Frobenius map) Fix a prime p.

1. We want to find large degree irreducibles $f(x) \in \mathbb{F}_p[x]$.
   a) **Question.** What is the probability a random f is irreducible?
   b) **Question (harder).** Are there fast "irreducibility tests"?

2. By the Chinese remainder theorem, if f, g are distinct irreducibles,

$$\mathbb{F}_p[x]/(fg) \cong \mathbb{F}_p[x]/(f) \times \mathbb{F}_p[x]/(g).$$

3. **Question.** Is there a fast factorization algorithm (i.e., to get from $f(x)g(x)$ to $f(x), g(x)$)?

Spoiler: there are fast factorization algorithms for polynomials over $\mathbb{F}_p[x]$, so working over finite fields is, indeed, "nicer" than over $\mathbb{Z}/\ell$ in this case.

Last time (6.22) we showed that there exist degree 6 irreducible polynomials in $\mathbb{F}_p[x]$, essentially by counting the size of $\mathbb{F}_{p^6}$ and comparing it to the size of $\mathbb{F}_{p^3} \cup \mathbb{F}_{p^2} \cup \mathbb{F}_p$. In general, there exists a degree n irreducible polynomial because

$$\mathbb{F}_{p^n} \supset \bigcup_{\substack{m|n \\ m<n}} \mathbb{F}_{p^m}.$$

It follows that for all n, there exists an element $\alpha \in \overline{\mathbb{F}_p}$ such that $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$. This statement holds more generally.

Theorem 6.55 (Primitive element theorem)
Any finite separable extension E/F is simple: $E = F(\alpha)$ for some algebraic α/F.

Notice that we have gone very far without invoking this theorem.

6.11. Infinite Galois theory

Suppose $K \supseteq F$ is an infinite Galois extension. In other words, K is the splitting field of (an infinite) collection of separable polynomials.

Example 6.24 – $\overline{\mathbb{Q}}/\mathbb{Q}$ is an infinite Galois extension, since $\overline{\mathbb{Q}}$ is the splitting field of *all* polynomials in $\mathbb{Q}[x]$.

Hence, we can consider K as the union of finite Galois extensions, where each is the splitting field of finitely many separable polynomials. The Galois groups are not completely unrelated. Indeed, consider

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) \supseteq \mathbb{Q}(\sqrt{-3}) \supseteq \mathbb{Q}.$$

Then

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})/\mathbb{Q}) \cong S_3,$$

and more importantly,

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}) \cong S_3/A_3 \cong \mathbb{Z}/2.$$

More generally,

Proposition 6.56

If E_1, E_2 are Galois extensions/F satisfying $E_1 \subseteq E_2$, then $\mathrm{Gal}(E_1/F)$ is a quotient of $\mathrm{Gal}(E_2/F)$ with quotient map

$$\begin{aligned} \mathrm{Gal}(E_2/F) &\twoheadrightarrow \mathrm{Gal}(E_1/F), \\ \sigma &\mapsto \sigma|_{E_1}. \end{aligned}$$

May 2, 2025 If intermediate fields are unrelated, then we can construct the field E_1E_2 containing both. This extension is Galois because

$$\mathrm{Gal}(K/E_1E_2) = \mathrm{Gal}(K/E_1) \cap \mathrm{Gal}(K/E_2),$$

and the latter Galois groups are normal.

Proposition 6.57

Let $\mathrm{Gal}(K/F) := \mathrm{Aut}_F(K)$. Then

$$\mathrm{Gal}(K/F) = \varprojlim_{E} \mathrm{Gal}(E/F),$$

where $\varprojlim$ is the **projective limit/inverse limit/limit** over all finite Galois extensions E/F.

Example 6.25 – Consider $\overline{\mathbb{F}_p}/\mathbb{F}_p$. The only finite extension intermediate fields are $\mathbb{F}_{p^n}$, and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \left\{\mathrm{id}, \mathrm{Fr}, \dots, \mathrm{Fr}^{n-1}\right\} \cong \mathbb{Z}/n$. If $m \mid n$, we have a map (in fact, a quotient map)

$$\mathbb{Z}/n \to \mathbb{Z}/m.$$

Then

$$\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim_{n} \mathbb{Z}/n = \{(\alpha_n : \alpha_n \in \mathbb{Z}/n) : m \mid n \implies \alpha_n \equiv \alpha_m \pmod{m}\}.$$

Note that $\varprojlim_n \mathbb{Z}/n$ also contains the information of the quotient maps.

We'll now try to understand the group $\varprojlim_n \mathbb{Z}/n$ is. If we fix a prime p, then $\varprojlim_k \mathbb{Z}/p^k$ consists of infinite tuples $(\cdots, a_2, a_1, a_0)$ such that if $n \geq m$, $a_n \equiv a_m \pmod{p^m}$. This is precisely the definition of the **p-adic numbers**, $\mathbb{Z}_p$. The Chinese remainder theorem essentially gives us that

$$\hat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p.$$

To add more structure, we can define a topology on $\varprojlim_E \mathrm{Gal}(E/F)$ as follows: let $(\sigma_E) = \sigma \in \varprojlim_E \mathrm{Gal}(E/F)$. Fix some finite Galois extension E/F. Then define open sets as

$$\left\{(\tau_E) \in \varprojlim_{E} \mathrm{Gal}(E/F) : \sigma_E = \tau_E\right\}.$$

Theorem 6.58 (Fundamental theorem of Galois theory for infinite extensions)
Let K/F be a Galois extension.

1. (*Finite extensions*) We have an order-reversing bijection

$$\left\{\begin{array}{c}\text{intermediate fields } E\\ \text{with } [E:F]<\infty\\ K\supseteq E\supseteq F\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{open}\text{ subgroups}\\ H\le \mathrm{Gal}(K/F)\end{array}\right\}$$

$$E \mapsto \mathrm{Gal}(K/E)=\{\sigma\in\mathrm{Gal}(K/F):\sigma|_E=\mathrm{id}_E\}$$

$$K^H:=\{\alpha\in K: H\cdot\alpha=\alpha\} \leftarrow\!\shortmid H$$

2. (*Infinite extensions*) We have an order-reversing bijection

$$\left\{\begin{array}{c}\text{intermediate fields } E\\ \text{with } [E:F]\text{ infinite}\\ K\supseteq E\supseteq F\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{closed}\text{ subgroups}\\ H\le \mathrm{Gal}(K/F)\end{array}\right\}$$

$$E \mapsto \mathrm{Gal}(K/E)=\{\sigma\in\mathrm{Gal}(K/F):\sigma|_E=\mathrm{id}_E\}$$

$$K^H:=\{\alpha\in K: H\cdot\alpha=\alpha\} \leftarrow\!\shortmid H$$

The punchline is that understanding separable algebraic extensions of F is the same as understanding the group

$$\mathrm{Gal}(\overline{F}/F),$$

(or the separable closure if F is not perfect).

One can think of number theory as trying to understand the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

References

[AK12] A. Altman and S. Kleiman. *A Term of Commutative Algebra*. Worldwide Center of Mathematics, 2012.

[Art18] M. Artin. *Algebra*. Pearson Modern Classics for Advanced Mathematics Series. Pearson, 2018.

[Hun12] T.W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2012.

[Mil22] J. S. Milne. *Fields and Galois Theory*. Kea Books, Ann Arbor, MI, 2022.