MATH6112 - Abstract Algebra II

Ivo Terek Couto[*]

Lecture notes from the **Spring 2019 Abstract Algebra II** course taught by professor **David Anderson**. Everything here was written like a list of topics, following the pace of the lectures and trying to keep the main results bite-sized.

Disclaimer: I added a few comments and examples of my own here and there, so I take responsibility for any eventual mistakes you may find here.

[*] terekcouto.1@osu.edu

Contents

Category Theory

Jan 7$^{\text{th}}$

- **Historical context:** the notion of "category" was introduced in 1945 by Eilenberg and Maclane as a framework for studying "natural transformations".

- **Definition of a category:** a *category* C consists of

  (i) a collection (class) $\mathrm{Obj}(\mathsf{C})$ of *objects*;

  (ii) for each pair (A, B), a *set* $\mathrm{Mor}_{\mathsf{C}}(A, B)$ of *morphisms* (arrows) between A and B, such that if $(A, B) \neq (C, D)$, then $\mathrm{Mor}_{\mathsf{C}}(A, B) \cap \mathrm{Mor}_{\mathsf{C}}(C, D) = \varnothing$;

  (iii) *a composition law*

  $$\mathrm{Mor}_{\mathsf{C}}(A, B) \times \mathrm{Mor}_{\mathsf{C}}(B, C) \ni (f, g) \mapsto g \circ f \in \mathrm{Mor}_{\mathsf{C}}(A, C)$$

  which is associative and admits identity elements, that is, for every object A of C there is $\mathrm{Id}_A \in \mathrm{Mor}_{\mathsf{C}}(A, A)$ such that given any object B, we have $f \circ \mathrm{Id}_A = f$ for all $f \in \mathrm{Mor}_{\mathsf{C}}(A, B)$ and $\mathrm{Id}_A \circ g = g$ for all $g \in \mathrm{Mor}_{\mathsf{C}}(B, A)$. In terms of diagrams, we mean the following situations:

  $$\begin{tikzcd} A \arrow[r, "\mathrm{Id}_A"] \arrow[rr, bend right, "f"'] & A \arrow[r, "f"] & B \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} B \arrow[r, "g"] \arrow[rr, bend right, "g"'] & A \arrow[r, "\mathrm{Id}_A"] & A \end{tikzcd} .$$

- **Remark on notation:** In the above definition, condition (ii) says that $\mathrm{Mor}_{\mathsf{C}}(A, B)$ is completely specified by the *source* object A and the *target* object B. Another common notation for $\mathrm{Mor}_{\mathsf{C}}(A, B)$ is $\mathrm{Hom}_{\mathsf{C}}(A, B)$ ("hom" for "homomorphism").

- **Examples:**

  (1) Set is the *category of sets* (surprise?). It is defined by:
    - $\mathrm{Obj}(\mathsf{Set}) =$ all sets[1];
    - $\mathrm{Mor}_{\mathsf{Set}}(A, B) = \{$functions from A to $B\}$..

  (2) Grp is the *category of groups*. It is defined by:
    - $\mathrm{Obj}(\mathsf{Grp}) =$ all groups;
    - $\mathrm{Mor}_{\mathsf{Grp}}(G, H) = \{$group homomorphisms from G to $H\}$.

  (3) Ab is the *category of abelian groups*. It is defined by:
    - $\mathrm{Obj}(\mathsf{Ab}) =$ all abelian groups;
    - $\mathrm{Mor}_{\mathsf{Ab}}(G, H) = \{$group homomorphisms from G to $H\}$.

  (4) Top is the *category of topological spaces*. It is defined by:
    - $\mathrm{Obj}(\mathsf{Top}) =$ all topological spaces;

[1] Note that this is a proper class. This is the reason why in (i) of the definition of a category we do not require $\mathrm{Obj}(\mathsf{C})$ being a set.

  - $\mathrm{Mor}_{\mathsf{Top}}(X,Y) = \{$continuous maps from X to $Y\}$.

(5) Man is the *category of differentiable manifolds*. It is defined by:

  - $\mathrm{Obj}(\mathsf{Man})$ = all differentiable manifolds;
  - $\mathrm{Mor}_{\mathsf{Man}}(M,N) = \{$smooth maps from M to $N\}$.

(6) Rng is the *category of rings*. It is defined by:

  - $\mathrm{Obj}(\mathsf{Rng})$ = all rings;
  - $\mathrm{Mor}_{\mathsf{Rng}}(R,S) = \{$ring homomorphisms from R to $S\}$.

(7) Ring is the *category of rings with* 1. It is defined by:

  - $\mathrm{Obj}(\mathsf{Ring})$ = all rings with 1;
  - $\mathrm{Mor}_{\mathsf{Ring}}(R,S) = \{$ring homomorphisms from R to S with $1_R \mapsto 1_S\}$.

  From here on, whenever we say "ring", we mean "ring with identity".

(8) R-mod if the *category of left R-modules*. It is defined by:

  - $\mathrm{Obj}(R\text{-}\mathsf{mod})$ = all left R-modules;
  - $\mathrm{Mor}_{R\text{-}\mathsf{mod}}(M,N) = \{R$-module homomorphisms from M to $N\}$.

  Similarly, one has the category mod-R of right R-modules. When there is no ambiguity, one just writes $\mathrm{Hom}_R(M,N) = \mathrm{Mor}_{R\text{-}\mathsf{mod}}(M,N)$.

(9) $\mathsf{Vect}_{\Bbbk}$ is the *category of $\Bbbk$-vector spaces*. It is defined by:

  - $\mathrm{Obj}(\mathsf{Vect}_{\Bbbk})$ = all vector spaces over the field $\Bbbk$;
  - $\mathrm{Mor}_{\mathsf{Vect}_{\Bbbk}}(V,W) = \{$linear transformations from V to $W\}$.

With these examples in mind, it should be easier to recognize a category when you see one.

- **A less standard example:** let $(P,\leq)$ be a *poset*, that is, a set P equipped with a *partial order*[2]. The associated *poset-category* P is defined by

  - $\mathrm{Obj}(\mathsf{P}) = P$ = all elements of P.
  - there is precisely one morphism in $\mathrm{Mor}_{\mathsf{P}}(x,y)$ if and only if $x \leq y$, and $\mathrm{Mor}_{\mathsf{P}}(x,y) = \varnothing$ otherwise.

[2] That is, a relation $\leq$ satisfying

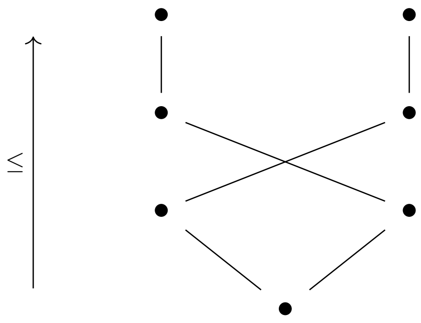
(i) $a \leq a$ for all $a \in P$;

(ii) $a \leq b$ and $b \leq c$ implies $a \leq c$ for all $a,b,c \in P$;

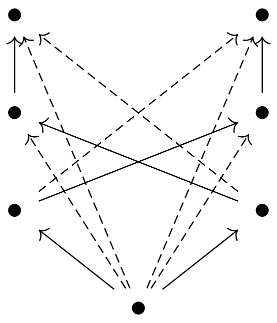
(iii) $a \leq b$ and $b \leq a$ implies $a = b$, for all $a,b \in P$.

Note that given any two elements of P, they might not be comparable, though.

The usual way to represent posets and poset-categories is via *Hasse diagrams*:



and



In the left we have the poset, where the order $\leq$ increases upwards. In the right, we have the poset-category, where the dashed arrows are the morphism compositions implied by the transitivity of $\leq$.

Jan 9th

- **Open category:** If X is a topological space, one may consider the topology of X partially ordered by inclusion. The corresponding poset-category is called the *open category of X*, and it is denoted by Open_X or $\mathsf{Op}(X)$.

- **Small categories:** A *small category* is a category C for which $\mathrm{Obj}(\mathsf{C})$ is a set. So, for example, Set is *not* a small category (again – because the collection of all sets is not a set, but a proper class).

- **Monoids and its associated categories:** Recall that a *monoid* is a set M equipped with an associative multiplications, with an identity[3]. For example, $(\mathbb{Z}, \cdot)$ is a monoid. A monoid M determines a category $\underline{M}$ with:

  - one object $\star$;
  - a morphism $\star \xrightarrow{m} \star$ for each element $m \in M$;
  - composition of morphisms given by multiplication in M:

  $$\begin{tikzcd} \star \arrow[r, "m"] \arrow[rr, bend right, "n\cdot m"'] & \star \arrow[r, "n"] & \star \end{tikzcd}$$

  In fact, a sort of converse holds: if a category C has only one object $\star$, then $\mathrm{Mor}_{\mathsf{C}}(\star,\star)$ is a monoid.

- **Isomorphisms:** an *isomorphism* between two objects in a category is a morphism which has a two-sided inverse with respect to morphism composition. An isomorphism from an object to itself is called an *automorphism*. With this terminology, one might say things like "an isomorphism of topological spaces is just an homeomorphism", etc..

[3] That is to say, the only difference between a monoid and a group is that elements in a monoid do not necessarily have inverses.

- **Groupoids:** Continuing the previous example, we can say that a group G is a monoid for which every element has an inverse. So, the corresponding category $\underline{G}$ has the property that all its morphisms are actually isomorphisms. Also, if a category C has only one object $\star$ and all morphisms are isomorphisms, then $\mathrm{Mor}_{\mathsf{C}}(\star,\star)$ is a group. In general, a category for which all morphisms are isomorphisms is called a *groupoid*. This in particular says that a group is nothing more than a groupoid with one object.

- **Core of a category:** If C is a category, we define its *core* to be the category $\mathrm{core}(\mathsf{C})$ with:

  - $\mathrm{Obj}(\mathrm{core}(\mathsf{C})) \doteq \mathrm{Obj}(\mathsf{C})$, and;
  - $\mathrm{Mor}_{\mathrm{core}(\mathsf{C})}(A,B) \doteq \{f \in \mathrm{Mor}_{\mathsf{C}}(A,B) \mid f \text{ is an isomorphism}\}$.

  Then, $\mathrm{core}(\mathsf{C})$ is always a groupoid.

- **Opposite categories:** Given a category C, its *opposite category* C^{op} is nothing more than C with its arrows reversed. To be more precise, we put $\mathrm{Obj}(\mathsf{C}^{\mathrm{op}}) \doteq \mathrm{Obj}(\mathsf{C})$, $\mathrm{Mor}_{\mathsf{C}^{\mathrm{op}}}(A,B) \doteq \mathrm{Mor}_{\mathsf{C}}(B,A)$, and the composition in C^{op} makes the diagram

$$\begin{tikzcd}
\mathrm{Mor}_{\mathsf{C}^{\mathrm{op}}}(A,B) \times \mathrm{Mor}_{\mathsf{C}^{\mathrm{op}}}(B,C) \arrow[r, "\text{comp. in } \mathsf{C}^{\mathrm{op}}"] \arrow[d, dash, "\cong"'] & \mathrm{Mor}_{\mathsf{C}^{\mathrm{op}}}(A,C) \arrow[d, dash, "="] \\
\mathrm{Mor}_{\mathsf{C}}(C,B) \times \mathrm{Mor}_{\mathsf{C}}(B,A) \arrow[r, "\text{comp. in } \mathsf{C}"] & \mathrm{Mor}_{\mathsf{C}}(C,A)
\end{tikzcd}$$

  commute, where the map $\cong$ indicated above is the obvious one, $(f,g) \mapsto (g,f)$.

- **Example:**

  (1) If $(G,\cdot)$ is a group, the *opposite group* $(G^{\mathrm{op}},*)$ is the same set $G^{\mathrm{op}} = G$ equipped with the operation defined by $g * h \doteq h \cdot g$. We then have the relation $\underline{(G^{\mathrm{op}})} = (\underline{G})^{\mathrm{op}}$ between the associated monoid-categories.

  (2) If $(P,\leq)$ is a poset, the *opposite order* $(P^{\mathrm{op}},\leq^{\mathrm{op}})$ is defined by $P^{\mathrm{op}} \doteq P$ and $x \leq^{\mathrm{op}} y$ if and only if $y \leq x$. Just like in the previous item, the poset-category associated to P^{op} is P^{op}.

  So the "op" notation is indeed adequate.

- **Subcategories:** A *subcategory* "$\mathsf{D} \subseteq \mathsf{C}$" is a category D where $\mathrm{Obj}(\mathsf{D}) \subseteq \mathrm{Obj}(\mathsf{C})$ is a subcolletion (subclass), and for all objects A and B of D, one has the inclusion $\mathrm{Mor}_{\mathsf{D}}(A,B) \subseteq \mathrm{Mor}_{\mathsf{C}}(A,B)$. We say that D is a *full subcategory* of C if actual equality $\mathrm{Mor}_{\mathsf{D}}(A,B) = \mathrm{Mor}_{\mathsf{C}}(A,B)$ holds. For example:

  (1) Ab is a full subcategory of Grp.

  (2) Grp is not a subcategory of Set, because there can be more than one group structure in a given set.

(3) Rng is not a subcategory of Set for the same reason given for Grp above, however Ring is a subcategory of Rng because if a multiplicative identity exists in a ring, then it is necessarily unique.

- **More geometric examples:** Man is not a subcategory of Top, because a given topological space can have more than one smooth structure. In fact, Man is not even a subcategory of the category TopMan of topological manifolds and continuous maps, for the same reason (e.g., consider exotic $\mathbb{R}^4$'s).

- **Products (and coproducts):** the idea is to generalize what we already know for some basic categories. Many familiar categories have a product. For example:

  (1) In Set, the *cartesian product* $A \times B = \{(a,b) \mid a \in A, b \in B\}$.

  (2) In Grp, the *product group* $G \times H$ with operation $(g,h)(g',h') \doteq (gg',hh')$.

  (3) In Top, the *product space* $X \times Y$ with the *product topology*[4].

  We want to axiomatize these notions using categorial terms. Say, in Grp, we have two projections $G_1 \times G_2 \xrightarrow{\mathrm{pr}_i} G_i$, $i = 1,2$ (which are homomorphisms, that is to say, arrows in Grp). Giving a morphism $H \xrightarrow{f} G_1 \times G_2$ is the same as giving two morphisms $H \xrightarrow{f_i} G_i$, $i = 1,2$, such that $f_i = \mathrm{pr}_i \circ f$. The idea is the following:

$$\begin{tikzcd}
 & & G_1 \\
H \arrow[r, "f"] \arrow[urr, bend left, "f_1"] \arrow[drr, bend right, "f_2"'] & G_1 \times G_2 \arrow[ur, "\mathrm{pr}_1"] \arrow[dr, "\mathrm{pr}_2"'] & \\
 & & G_2
\end{tikzcd}$$

  With this in mind, we have the following:

  Definition: in a category C, a *product* of two objects A_1 and A_2 is an object A together with "projection" morphisms $A \xrightarrow{\mathrm{pr}_i} A_i$, $i = 1,2$, such that given any object B and morphisms $B \xrightarrow{f_i} A_i$, $i = 1,2$, there is a unique morphism $B \xrightarrow{f} A$ commuting with projections:

$$\begin{tikzcd}
 & & A_1 \\
B \arrow[r, dotted, "\exists! f"] \arrow[urr, bend left, "f_1"] \arrow[drr, bend right, "f_2"'] & A \arrow[ur, "\mathrm{pr}_1"] \arrow[dr, "\mathrm{pr}_2"'] & \\
 & & A_2
\end{tikzcd}$$

[4] Some care should be takes with the product of infinite factors, since the *box topology* and the *product topology* are no longer the same.

It follows from this *universal property* that any two products of A_1 and A_2 (if they exists), are isomorphic, and the isomorphism is compatible with the projections in the sense that the following diagram commutes

$$\begin{tikzcd}
A \arrow[r, dash, "\exists!\cong"] \arrow[d, "\mathrm{pr}_1"'] \arrow[dr, bend right, "\mathrm{pr}_2" near start] & A' \arrow[d, "\mathrm{pr}_2'"] \arrow[dl, bend left, "\mathrm{pr}_1'" near end] \\
A_1 & A_2
\end{tikzcd}$$

We then say that products are *unique up to unique isomorphism* (where the isomorphism is the unique one compatible with projections). For example, in Set we have $\mathrm{Mor}_{\mathsf{C}}(B,A) \cong_{\text{bij.}} \mathrm{Mor}_{\mathsf{C}}(B,A_1) \times \mathrm{Mor}_{\mathsf{C}}(B,A_2)$. So, for this reason, we write $f = (f_1, f_2)$, according to the above notation.

- **Remark:** in the definition above, motivated by what happened in Grp, one could ask whether anything arises if instead of being given all the f_i, we were given just f instead. We can trivially define $f_i \doteq \mathrm{pr}_i \circ f$, so there is nothing else to discuss here.

Jan 11th

- **Definition for general products:** Let C be a category and $\{A_i\}_{i\in I}$ be an indexed set of objects (no restriction on the cardinality of I). A *product* of $\{A_i\}_{i\in I}$ is an object A together with morphisms $A \xrightarrow{\mathrm{pr}_i} A_i$, $i \in I$, such that given any object B with morphisms $B \xrightarrow{\mathrm{pr}_i} A_i$, there is a unique morphism $B \xrightarrow{f} A$ such that $f_i = \mathrm{pr}_i \circ f$.

$$\begin{tikzcd}
 & & \vdots \\
 & & A_i \\
B \arrow[r, dotted, "\exists! f"] \arrow[urr, bend left=40, "f_i"] \arrow[rr, bend left=40, "f_j"] \arrow[drr, bend right=40, "f_k"'] & A \arrow[ur, "\mathrm{pr}_i"] \arrow[r, "\mathrm{pr}_j"] \arrow[dr, "\mathrm{pr}_k"] & A_j \\
 & & A_k \\
 & & \vdots
\end{tikzcd}$$

Again, if such a product exists, it is unique up to unique isomorphism. So we may just write $A = \prod_{i\in I} A_i$.

- **Examples:** Arbitrary products exist in Set. One possible construction is to consider
$$A = \{\text{functions } \alpha\colon I \to \coprod_{i\in I} A_i \text{ with } \alpha(i) \in A_i\},$$
where $\coprod_{i\in I} A_i = \bigcup_{i\in I}\{i\} \times A_i$ denotes disjoint union, with the projection maps $\mathrm{pr}_i\colon A \to A_i$ given by $\mathrm{pr}_i(\alpha) \doteq \alpha(i)$. Arbitrary products also exist in Grp, Ab, Ring, etc.. Moreover, the notion of product reduces to the following situation in Set: $\mathrm{Mor}_{\mathsf{C}}\left(B, \prod_{i\in I} A_i\right) \cong \prod_{i\in I} \mathrm{Mor}_{\mathsf{C}}(B, A_i)$.

- **Maps between products:** In a category C with objects A, B, C and D for which the products $A \times B$ and $C \times D$ both exist, if we have morphisms $A \xrightarrow{f} C$ and $B \xrightarrow{g} D$, we may put them together in a single map $A \times B \xrightarrow{f\times g} C \times D$ in the following way: consider the compositions
$$A \times B \xrightarrow{\mathrm{pr}_A} A \xrightarrow{f} C \quad \text{and} \quad A \times B \xrightarrow{\mathrm{pr}_B} B \xrightarrow{g} D,$$
and apply the universal property of $C \times D$ to get a unique map $f \times g$ making the diagram
$$\begin{tikzcd}
 & A \arrow[rr, "f"] & & C \\
A \times B \arrow[ur, "\mathrm{pr}_A"] \arrow[rr, "f\times g"] \arrow[dr, "\mathrm{pr}_B"] & & C \times D \arrow[ur, "\mathrm{pr}_C"] \arrow[dr, "\mathrm{pr}_D"] & \\
 & B \arrow[rr, "g"] & & D
\end{tikzcd}$$
commute.

- **Dual notion to product:** Let C be a category and $\{A_i\}_{i\in I}$ be an indexed set of objects. A *coproduct* of $\{A_i\}_{i\in I}$ is an object A with morphisms $A_i \xrightarrow{\rho_i} A$, $i \in I$, such that for any object B with morphisms $A_i \xrightarrow{f_i} B$, $i \in I$, there is a unique morphism $A \xrightarrow{f} B$ such that $f_i = f \circ \rho_i$.

$$\begin{tikzcd}
 & & \vdots \\
 & & A_i \arrow[dl, "\rho_i"] \arrow[dll, bend right, "f_i"'] \\
B & A \arrow[l, dotted, "\exists! f"'] & A_j \arrow[l, "\rho_j"'] \arrow[ll, bend right, "f_j"'] \\
 & & A_k \arrow[ul, "\rho_k"'] \arrow[ull, bend left, "f_k"] \\
 & & \vdots
\end{tikzcd}$$

Again, coproducts are unique up to unique isomorphism, and so we may write $A = \coprod_{i\in I} A_i$. Note how the diagram describing the universal property for coproducts is the same as the one describing the universal property for products, but with the arrows reversed. This leads us to the conclusion: products in C are coproducts in C^{op}, and coproducts in C are products in C^{op}.

- **Example:** Arbitrary coproducts exist in Set: it is just the usual disjoint union. We then have, in an arbitrary category C that the notion of coproduct reduces again to Set: $\mathrm{Mor}_{\mathsf{C}}(\coprod_{i\in I} A_i, B) \cong \prod_{i\in I} \mathrm{Mor}_{\mathsf{C}}(A_i, B)$. Arbitrary coproducts also exist in Ring.

- **Direct sum is coproduct:** if R is a ring, consider the category R-mod of left R-modules and R-module homomorphisms. Assume that $\{M_i\}_{i\in I}$ is an indexed set of R-modules, and consider

$$M = \bigoplus_{i\in I} M_i \doteq \{(m_i)_{i\in I} \mid \text{all but finitely many of the } m_i\text{'s are zero}\}.$$

This is a submodule of the product module $\prod_{i\in I} M_i$. One may also use the notation $\bigoplus_{i\in I} M_i = \coprod_{i\in I} M_i$, meaning the categorical coproduct of $\{M_i\}_{i\in I}$, but this is rarely done and the notation does not refer to a disjoint union in this case. The "inclusions" are $\rho_i\colon M_i \to M$, $i \in I$, given by $\rho_i(m_i) = (\delta_{ij} m_i)_{j\in I}$ (to be more precise, let $m_j = m_i$ if $j = i$ and zero otherwise). To check that this satisfies the universal property for coproducts, let $f_i\colon M_i \to N$, $i \in I$, be a collection of R-module homomorphisms, and define $f\colon M \to N$ by $f((m_i)_{i\in I}) \doteq \sum_{i\in I} f_i(m_i)$. This is actually a finite sum (by the definition of M given above), and so this f is well-defined. And this such f is the unique possibility, since $f(\rho_i(m_i)) = f_i(m_i)$:

$$\begin{tikzcd} M_i \arrow[r, "\rho_i"] \arrow[rr, bend right, "f_i"'] & M \arrow[r, "f"] & N \end{tikzcd}$$

- **Graph morphism:** a morphism $A \xrightarrow{f} B$ between objects in a category C, for which the product $A \times B$ exists, determines a *graph morphism* $\Gamma_f\colon A \to A \times B$, induces by Id_A and f. That is, it is the unique morphism making the diagram

$$\begin{tikzcd} & & A \\ A \arrow[r, "\Gamma_f"] \arrow[urr, bend left, "\mathrm{Id}_A"] \arrow[drr, bend right, "f"'] & A \times B \arrow[ur, "\mathrm{pr}_1"] \arrow[dr, "\mathrm{pr}_2"] & \\ & & B \end{tikzcd}$$

commute. As a special case, $\Delta \doteq \Gamma_{\mathrm{Id}_A}$ is called the *diagonal morphism of A* (i.e., the graph of the identity).

- **Initial and terminal objects:** Let C be any category.
  - an object I is *initial* if it admits a unique morphism to every other object: $\mathrm{Mor}_{\mathsf{C}}(I,A)$ has only one element, for every object A.
  - an object T is *terminal* if it receives a unique morphism from every other object: $\mathrm{Mor}_{\mathsf{C}}(A,T)$ has only one element, for every object A.
  - an object is called a *zero object* if it is both initial and terminal.

  That is to say, initial objects are *universal sources* and terminal objects are *universal targets*. And if they exist, they are unique up to unique isomorphism.

- **Examples:** in Set, $\varnothing$ is initial and singletons are terminal, while in Grp the trivial group if both initial and terminal.

- **Group objects:** Assume C is a category with finite products and a terminal object $\star$. A *group object* in C is the data $(G,\cdot,\epsilon,\iota)$, where G is an object, and the others are morphisms

  (i) $G\times G\xrightarrow{\cdot} G$ (multiplication);

  (ii) $\epsilon\colon \star\to G$ (identity);

  (iii) $\iota\colon G\to G$ (inversion),

  satisfying the *group axioms in categorical form*:

  (a) Identity (both left and right):

$$\begin{tikzcd}
G \arrow[r] \arrow[rrd, "\mathrm{Id}_G"'] & \star\times G \arrow[r, "\epsilon\times\mathrm{Id}_G"] & G\times G \arrow[d, "\bullet"] \\
 & & G
\end{tikzcd}
\quad\text{and}\quad
\begin{tikzcd}
G \arrow[r] \arrow[rrd, "\mathrm{Id}_G"'] & G\times\star \arrow[r, "\mathrm{Id}_G\times\epsilon"] & G\times G \arrow[d, "\bullet"] \\
 & & G
\end{tikzcd}$$

  (b) Inverses (both left and right):

$$\begin{tikzcd}
G \arrow[r, "\Delta"] \arrow[d] & G\times G \arrow[r, "\iota\times\mathrm{Id}_G"] & G\times G \arrow[d, "\bullet"] \\
\star \arrow[rr, "\epsilon"] & & G
\end{tikzcd}
\quad\text{and}\quad
\begin{tikzcd}
G \arrow[r, "\Delta"] \arrow[d] & G\times G \arrow[r, "\mathrm{Id}_G\times\iota"] & G\times G \arrow[d, "\bullet"] \\
\star \arrow[rr, "\epsilon"] & & G
\end{tikzcd}$$

  (c) Associativity:

$$\begin{tikzcd}
G\times G\times G \arrow[r, "\mathrm{Id}_G\times\bullet"] \arrow[d, "\bullet\times\mathrm{Id}_G"'] & G\times G \arrow[d, "\bullet"] \\
G\times G \arrow[r, "\bullet"] & G
\end{tikzcd}$$

- **Remark on abuses of notation:** in the above definition there are some abuses of notation. For example, both morphisms $\mathrm{Id}_G \times \bullet$ and $\bullet \times \mathrm{Id}_G$ have $G \times G \times G$. In fact, all $(G \times G) \times G$, $G \times (G \times G)$ and $G \times G \times G$ are isomorphic, and to be completely precise, one should take into account these isomorphisms in the diagrams above. Also, the unnamed maps in (a) are the obvious ones, induced by the (unique) terminal map $G \to \star$ and Id_G via the universal property of $G \times G$.

Jan 14th

- **Examples:**

  (1) A group object in Set is a group.

  (2) A group object in Grp is an abelian group

  (3) A group object in Top is a topological group.

  (4) A group object in Man is a Lie group.

- **Functors:** They are basically "maps between categories". A *(covariant) functor* $F\colon \mathsf{C} \to \mathsf{D}$ from one category to another is:

  (i) an assignment $A \mapsto F(A)$ of an object of D for each object of C, and;

  (ii) for each morphism $A \xrightarrow{f} B$ in C, a morphism $F(A) \xrightarrow{F(f)} F(B)$ in D (that is, a map $\mathrm{Mor}_{\mathsf{C}}(A,B) \to \mathrm{Mor}_{\mathsf{D}}(F(A),F(B))$), also satisfying the conditions $F(g \circ f) = F(g) \circ F(f)$ for any $A \xrightarrow{f} B \xrightarrow{g} C$, and $F(\mathrm{Id}_A) = \mathrm{Id}_{F(A)}$.

  The definition of a *contravariant functor* is the same, but reversing the arrows in (ii), that is, $A \xrightarrow{f} B \xrightarrow{g} C$ goes into $F(A) \xleftarrow{F(f)} F(B) \xleftarrow{F(g)} F(C)$. So, a contravariant functor $\mathsf{C} \to \mathsf{D}$ is the same as a covariant function $\mathsf{C}^{\mathrm{op}} \to \mathsf{D}$. However, it is *not* the same as a covariant function $\mathsf{C} \to \mathsf{D}^{\mathrm{op}}$, as condition (ii) will fail.

- **Forgetful functors:**

  (1) $\mathsf{Grp} \to \mathsf{Mon}$[5] assigns to the group $(G,\cdot)$ the monoid $(G,\cdot)$, and assigns to the group homomorphism $f : G \to H$, the monoid homomorphism $f\colon G \to H$.

  (2) $\mathsf{Mon} \to \mathsf{Set}$, which forgets the monoid structure. That is, maps $(M,\cdot)$ to the set M, and any monoid homomorphism to its underlying set map.

  (3) $\mathsf{Man} \to \mathsf{Top}$, which forgets the smooth structure. That is, it maps a differentiable manifold to its underlying topological space, and any smooth map to its (underlying?) continuous map.

  (4) $\mathsf{Top} \to \mathsf{Set}$, which forgets the topology. And so on.

[5] Here, Mon denotes the category of monoids, with monoid homomorphisms.

- **Pre-sheaves:** Let X be a topological space. A *pre-sheaf of abelian groups* over X is a contravariant functor $F\colon \mathsf{Open}_X \to \mathsf{Ab}$ with $F(\varnothing) = \{0\}$. Similarly, one can define a *pre-sheaf of rings* as a contravariant functor $F\colon \mathsf{Open}_X \to \mathsf{Ring}$ with $F(\varnothing) = \{0\}$. Writing explicitly (in the abelian group case, say), this means that

  (i) for every open subset $U \subseteq X$ we assign an abelian group $F(U)$, and;

  (ii) for any given open sets $U \subseteq V \subseteq X$, we have a group homomorphism $\mathrm{Res}_{V,U}\colon F(V) \to F(U)$, suggestively called the *restriction*, which satisfies the conditions $\mathrm{Res}_{U,U} = \mathrm{Id}_{F(U)}$ and $\mathrm{Res}_{V,U} \circ \mathrm{Res}_{W,V} = \mathrm{Res}_{W,U}$, for all open sets $U \subseteq V \subseteq W \subseteq X$.

  A pre-sheaf is called a *sheaf* if it also satisfies the following *gluing axiom* (which ends up being similar to an universal property): for any given open cover $\{U_i\}_{i\in I}$ of X and any collection of elements $s_i \in F(U_i)$ satisfying the condition $\mathrm{Res}_{U_i,U_i\cap U_j}(s_i) = \mathrm{Res}_{U_j,U_i\cap U_j}(s_j)$ for all $i,j \in I$, there is a unique $s \in F(X)$ such that $\mathrm{Res}_{X,U_i}(s) = s_i$ for all $i \in I$.

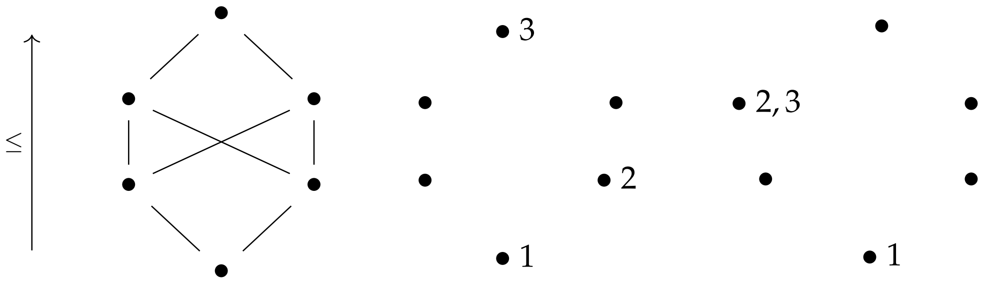
- **Definition:** A functor $F\colon \mathsf{C} \to \mathsf{D}$ is:

  - *faithful*, if for all objects A and B of C, the induced map
  $$\mathrm{Mor}_{\mathsf{C}}(A,B) \to \mathrm{Mor}_{\mathsf{D}}(F(A),F(B))$$
  is injective;
  - *full*, if for all objects A and B of C, the induced map
  $$\mathrm{Mor}_{\mathsf{C}}(A,B) \to \mathrm{Mor}_{\mathsf{D}}(F(A),F(B))$$
  is surjective;
  - *fully faithful* if it is full and faithful. That is, if it induces bijections on the hom-sets.

- **Examples:**

  (1) The inclusion of a subcategory is faithful; the inclusion of a full subcategory is fully faithful;

  (2) If $(P,\leq)$ is a poset and $n \in \mathbb{N}$ is a natural number, n can be seen as a poset $\{1 < 2 < \cdots < n\}$. Then a functor $F\colon \mathsf{n} \to \mathsf{P}$ between the corresponding poset-categories is a (possibly non-injective) n-chain in $(P,\leq)$ (it could have repeated elements). Fixing this subtlety is not as simple as requiring the functor to be faithful or even fully faithful. Consider the following situation:



In the left we have the Hasse diagram for a given poset $(P, \leq)$, and the other two figures depict two fully faithful functors $\mathsf{3} \to \mathsf{P}$.

(3) If R is a commutative ring and $S \subseteq R$ is multiplicatively closed subset of R, then $S^{-1}\colon R\text{-}\mathsf{mod} \to S^{-1}R\text{-}\mathsf{mod}$ is a functor taking M to the localized module $S^{-1}M$, and a R-module homomorphism $\varphi\colon M \to N$ to the unique $S^{-1}R$-linear map $S^{-1}(\varphi)\colon S^{-1}M \to S^{-1}N$ satisfying $S^{-1}(\varphi)(m/s) = \varphi(m)/s$, for all $m \in M$ and $s \in S$. This is not a faithful functor. Say $M = N \oplus R/(s)$ for some $s \in S$, and consider both maps

$$\begin{tikzcd} M \arrow[r] & N \arrow[r, hook] & M \\ (n,r) \arrow[r, mapsto] & n \arrow[r, mapsto] & (n,0) \end{tikzcd} \quad \text{and} \quad \mathrm{Id}_M\colon M \to M.$$

They have the same image in $\mathrm{Mor}_{S^{-1}R\text{-}\mathsf{mod}}(S^{-1}M, S^{-1}M)$.

(4) Let Top^* be the *category of pointed topological spaces*. The objects are pairs (X, x), where X is a topological space and $x \in X$ is a chosen point. A morphism $(X,x) \xrightarrow{f} (Y,y)$ is a continuous map $f\colon X \to Y$ satisfying also $f(x) = y$. Note that this condition can be expressed also in terms of the following commutative diagram:

$$\begin{tikzcd} X \arrow[r, "f"] & Y \\ \{x\} \arrow[u, hook] \arrow[r] & \{y\} \arrow[u, hook] \end{tikzcd}$$

Here, the vertical arrows are just inclusions. The *fundamental group* is a functor $\pi_1\colon \mathsf{Top}^* \to \mathsf{Grp}$, mapping (X,x) to $\pi_1(X,x)$ and a continuous map $(X,x) \xrightarrow{f} (Y,y)$ to a group homomorphism $f_*\colon \pi_1(X,x) \to \pi_1(Y,y)$. This functor happens to map terminal objects into terminal objects (indeed, the fundamental group of a one-point space is trivial), but this need not be the case even if the functor is fully faithful. This is because being fully faithful is a condition related mainly to morphisms, and one still could have objects in the target category which are not in the "image" of the functor).

- **Isomorphism of categories:** If C is a category, the *identity functor* is $\mathbf{1}_{\mathsf{C}}$ doing the obvious: $\mathbf{1}_{\mathsf{C}}(A) \doteq A$ and $\mathbf{1}_{\mathsf{C}}(f) \doteq f$. Functors can be composed in the obvious way (object-wise). So, a functor $F\colon \mathsf{C} \to \mathsf{D}$ is an *isomorphism of categories* if it has a two-sided inverse $G\colon \mathsf{D} \to \mathsf{C}$ (that is, satisfying $GF = \mathbf{1}_{\mathsf{C}}$ and $FG = \mathbf{1}_{\mathsf{D}}$). Note also that it follows that an isomorphism of categories actually induces bijections between $\mathrm{Obj}(\mathsf{C})$ and $\mathrm{Obj}(\mathsf{D})$, so in particular isomorphic categories must have the same number of objects. However, this almost never happens, and the best we get are uninteresting examples like $\mathsf{Ab} = \mathbb{Z}\text{-}\mathsf{mod}$ and $(\mathsf{C}^{\mathrm{op}})^{\mathrm{op}} = \mathsf{C}$.

Jan 16th

- **Natural transformations:** Let $F, G\colon \mathsf{C} \to \mathsf{D}$ be two (both covariant or both contravariant) functors between categories. A *natural transformation* $\eta\colon F \implies G$ is a morphism $\eta_A\colon F(A) \to G(A)$ in D, for each object A in C, such that given any morphism $A \xrightarrow{f} B$ in C, the diagram

$$\begin{tikzcd}
F(A) \arrow[r, "\eta_A"] \arrow[d, "F(f)"'] & G(A) \arrow[d, "G(f)"] \\
F(B) \arrow[r, "\eta_B"'] & G(B)
\end{tikzcd}$$

commutes.

- **Remark:** The definition above is uninteresting if one of the functors is covariant and the other contravariant. For example, switching $G(f)$ in the above diagram, one could try to define η_A as the composition $G(f) \circ \eta_B \circ F(f)$, which could be a circular definition also leading to compatibility problems.

- **Natural isomorphisms:** given a functor $F\colon \mathsf{C} \to \mathsf{C}$, the *identity transformation* $\mathbf{1}_F$ is the evident thing: $(\mathbf{1}_F)_A = \mathrm{Id}_{F(A)}$. Natural transformations can also be composed at the object level. Then, a natural transformation $\eta\colon F \implies G$ is a *natural isomorphism* if each η_A is an isomorphism. One can check that η is a natural isomorphism if and only if there exists an inverse natural transformation $\eta^{-1}\colon G \implies F$ such that $\eta^{-1}\eta = \mathbf{1}_F$ and $\eta\eta^{-1} = \mathbf{1}_G$.

- **Example:** Let $\Bbbk$ be a field and $\mathsf{Vect}_\Bbbk$ be the category of $\Bbbk$-vector spaces and linear transformations. The *duality functor* is $D\colon \mathsf{Vect}_\Bbbk \to \mathsf{Vect}_\Bbbk$ given by $D(V) \doteq V^*$ and sending $\varphi : V \to W$ to $D(\varphi) = \varphi^*\colon W^* \to V^*$ (defined by $\varphi^*(f) = f \circ \varphi$). Note that D is contravariant, so the composition (called the *double dual functor*) DD is covariant. We have a natural transformation $\eta\colon \mathbf{1}_{\mathsf{Vect}_\Bbbk} \implies DD$ defined by $\eta_V\colon V \to V^{**}$, $\eta_V(v) = v^{**} =$ evaluation at v. Then we can check naturality, which now has a precise meaning. That is to say, we must check that the diagram

$$\begin{tikzcd}
V \arrow[r, "\eta_V"] \arrow[d, "f"'] & V^{**} \arrow[d, "f^{**}"] \\
W \arrow[r, "\eta_W"] & W^{**}
\end{tikzcd}$$

commutes. This is done as follows: first recall that given $\xi \in V^{**}$ and $\psi \in W^*$, we have $f^{**}(\xi)(\psi) = \xi(f^*(\psi))$. With this in mind, we take $\xi = \eta_V(v)$ for some $v \in V$ and compute

$$f^{**}(\eta_V(v))(\psi) = \eta_V(v)(f^*(\psi)) = f^*(\psi)(v) = \psi(f(v)) = \eta_W(f(v))(\psi),$$

as wanted.

- **Equivalence of categories:** we would like to have a more "relaxed" (and more useful) notion of an isomorphism of categories. We say that a functor $F\colon \mathsf{C} \to \mathsf{D}$

is an *equivalence of categories* if there exist an "inverse" functor $G\colon \mathsf{D} \to \mathsf{C}$ and natural isomorphisms $GF \cong \mathbf{1}_{\mathsf{C}}$ and $FG \cong \mathbf{1}_{\mathsf{D}}$. In this case, we say that C and D are *equivalent categories*.

- **Remark:** Compare this with the situation in Top, where an homotopy equivalence is a continuous map which has an inverse up to homotopy. This ends up being a particular instance of the definition above.

- **Toy example:** Consider the category C associated to the multiplicative group $(\mathbb{Z}/2\mathbb{Z}, \cdot)$, and the category D depicted below:

$$\begin{tikzcd} A \arrow[r, bend left, leftrightarrow, "1"] \arrow[r, bend right, leftrightarrow, "-1"'] & A \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} A \arrow[r, bend left, leftrightarrow, "1"] \arrow[r, bend right, leftrightarrow, "-1"'] & A \arrow[r, bend left=50, "-a"] \arrow[r, bend left=15, "a"] \arrow[r, bend right=15, "a^{-1}"'] \arrow[r, bend right=50, "-a^{-1}"'] & A' \arrow[r, bend left, leftrightarrow, "1'"] \arrow[r, bend right, leftrightarrow, "-1'"'] & A' \end{tikzcd}$$

Note that C and D are not isomorphic (indeed, they do not even have the same number of objects), but we claim that they are equivalent. The "inclusion" functor $F\colon \mathsf{C} \to \mathsf{D}$ given by $F(A) = A$, $F(1) = 1$, $F(-1) = -1$ is an equivalence of categories. Indeed, the functor $G\colon \mathsf{D} \to \mathsf{C}$ given by

$$\begin{cases} G(A) & = G(A') = A \\ G(1) & = G(1') = 1 \\ G(-1) & = G(-1') = -1 \\ G(a) & = G(a^{-1}) = 1 \\ G(-a) & = G(-a^{-1}) = -1 \end{cases}$$

behaves like a deformation retract. We have that $GF = \mathbf{1}_{\mathsf{C}}$, and $FG \cong \mathbf{1}_{\mathsf{D}}$ via the natural isomorphism $\eta\colon \mathbf{1}_{\mathsf{D}} \implies FG$ given by $\eta_A = \mathrm{Id}_A$ and $\eta_{A'} = -a$.

Jan 18th

- **More definitions of equivalences:**
  - An equivalence $\mathsf{C}^{\mathrm{op}} \to \mathsf{D}$ is called an *anti-equivalence* between C and D (that is, it is given by a contravariant functor $\mathsf{C} \to \mathsf{D}$).
  - An equivalence $\mathsf{C} \to \mathsf{C}$ is called an *auto-equivalence*. For example, the double dual functor DD is an auto-equivalence of the full subcategory of finite-dimensional vector spaces over a fixed field $\Bbbk$.

- **Theorem:** A functor $F\colon \mathsf{C} \to \mathsf{D}$ is an equivalence of categories if and only if it is *fully faithful* and *essentially surjective* (that is, for every object D of D there is an object C of C and an isomorphism $F(C) \cong D$).

  This is generally a very useful criterion for checking whether a given functor is an equivalence of categories, just like one checks if a given function is bijective by checking that it is both injective and surjective (instead of always trying to exhibit an inverse function).

Half-proof: Suppose $G\colon \mathsf{D} \to \mathsf{C}$ is an inverse for F up to natural isomorphisms.

- F is faithful: assume given two morphisms $A \xrightarrow{f} B$ and $A \xrightarrow{g} B$ with $F(f) = F(g)$. By $GF \cong \mathbf{1}_{\mathsf{C}}$, we have that both diagrams

$$\begin{tikzcd} GF(A) \arrow[r, dash, "\cong"] \arrow[d, "GF(f)=GF(g)"'] & A \arrow[d, "f"] \\ GF(B) \arrow[r, "\cong"'] & B \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} GF(A) \arrow[r, dash, "\cong"] \arrow[d, "GF(f)=GF(g)"'] & A \arrow[d, "g"] \\ GF(B) \arrow[r, "\cong"'] & B \end{tikzcd}$$

  commute, and so $f = g$ (both are equal to the composition of the remaining three arrows on each diagram).

- F is essentially surjective: now we use the condition $FG \cong \mathbf{1}_{\mathsf{D}}$. Given an object D of D, we have that $G(D)$ is now an object in C. Then $F\big(G(D)\big) \cong D$, as wanted.

- F is full: given a morphism $F(A) \xrightarrow{h} F(B)$, we look for a morphism $A \xrightarrow{f} B$ such that $F(f) = h$. Define f as the composition:

$$\begin{tikzcd} A \arrow[r, dash, "\cong"] \arrow[rrr, bend right, "f"'] & GF(A) \arrow[r, "G(h)"] & GF(B) \arrow[r, dash, "\cong"] & B \end{tikzcd}$$

  To see that this indeed works, apply F to get

$$\begin{tikzcd} F(A) \arrow[r, dash, "\cong"] \arrow[rrr, bend left, dashed, "h"] \arrow[rrr, bend right, "F(f)"'] & FGF(A) \arrow[r, "FG(h)"] & FGF(B) \arrow[r, dash, "\cong"] & F(B) \end{tikzcd}$$

  as wanted.

- **Example:** If R is a ring, let $\operatorname{Mat}(n,R) \cong \operatorname{End}_R(R^{\oplus n})$ be the ring of $n \times n$ matrices with entries in R. The categories (of right modules) $\mathsf{mod}\text{-}R$ and $\mathsf{mod}\text{-}\operatorname{Mat}(n,R)$ are equivalent. To see this, consider the functor $F\colon \mathsf{mod}\text{-}R \to \mathsf{mod}\text{-}\operatorname{Mat}(n,R)$ given by $F(M) \doteq M^{\oplus n} = M \oplus \cdots \oplus M$ (n times) and $F(\varphi) = \varphi^{\oplus n} = \varphi \oplus \cdots \oplus \varphi$ (n times), for every R-module homomorphism $\varphi\colon M \to N$.

  We have that F is faithful, since if $\pi\colon N^{\oplus} \to N$ denotes projection in some fixed factor, then $\varphi^{\oplus} = \psi^{\oplus}$ readily implies that

$$\varphi = \pi \circ \varphi^{\oplus}\Big|_{M\oplus\{0\}^{\oplus(n-1)}} = \pi \circ \psi^{\oplus n}\Big|_{M\oplus\{0\}^{\oplus(n-1)}} = \psi,$$

as wanted.

The verification that F is full and essentially surjective is an exercise.

- **The Yoneda Embedding:** Fix an object X of C. There is a natural $h^X\colon \mathsf{C} \to \mathsf{Set}$ defined by

  - $h^X(A) \doteq \mathrm{Hom}_{\mathsf{C}}(X, A)$;
  - $h^X(f)\colon \mathrm{Hom}_{\mathsf{C}}(X, A) \to \mathrm{Hom}_{\mathsf{C}}(X, B)$, $h^X(f)(g) \doteq f \circ g$.

  This is called the *(covariant) Hom functor*. One may also define a contravariant version $h_X\colon \mathsf{C} \to \mathsf{Set}$ by

  - $h_X(A) \doteq \mathrm{Hom}_{\mathsf{C}}(A, X)$;
  - $h_X(f) \doteq \mathrm{Hom}_{\mathsf{C}}(B, X) \to \mathrm{Hom}_{\mathsf{C}}(A, X)$, $h_X(f)(g) \doteq g \circ f$.

  This is called the *(contravariant) Hom functor*. One can also see Hom as a "bifunctor" $\mathsf{C}^{\mathrm{op}} \times \mathsf{C} \to \mathsf{Grp}$ (here the definition of the *product category* is the obvious one, no subtleties).

- **Universality and representability are synonyms:**

  - A covariant functor $F\colon \mathsf{C} \to \mathsf{Set}$ is *representable (in* C*)* if there is an object X in C and a natural isomorphism $F \cong h^X = \mathrm{Hom}_{\mathsf{C}}(X, \_)$.
  - A contravariant functor $F\colon \mathsf{C} \to \mathsf{Set}$ is *representable (in* C*)* if there is an object X in C and a natural isomorphism $F \cong h_X = \mathrm{Hom}_{\mathsf{C}}(\_, X)$.

  In these cases, we say that F is representable by X.

- **Examples:** Universal properties are ultimately examples of the previous definitions. Let R be a ring, fix two left R-modules A_1 and A_2 and define a functor $F_{A_1,A_2}\colon R\text{-}\mathsf{mod} \to \mathsf{Set}$ by $F_{A_1,A_2}(M) = \mathrm{Hom}_R(A_1, M) \times \mathrm{Hom}_R(A_2, M)$, and taking a R-module homomorphism $f\colon M \to N$ to

$$\begin{tikzcd}
\mathrm{Hom}_R(A_1, M) \times \mathrm{Hom}_R(A_2, M) \arrow[r, "F_{A_1,A_2}(f)"] & \mathrm{Hom}_R(A_1, N) \times \mathrm{Hom}_R(A_2, N) \\
(\varphi, \psi) \arrow[r, mapsto] & (f \circ \varphi, f \circ \psi).
\end{tikzcd}$$

  This is covariant, and we have $F_{A_1,A_2} \cong h^{A_1 \oplus A_2}$ by the universal property of the direct sum in R-mod (coproduct). Similarly one may define a contravariant version F^{A_1,A_2} by $F^{A_1,A_2}(M) = \mathrm{Hom}_R(M, A_1) \times \mathrm{Hom}_R(M, A_2)$, with action on morphisms given by pre-composition this time, as to obtain $F^{A_1,A_2} \cong h_{A_1 \times A_2}$. Recall also that in this case we have $A_1 \oplus A_2 \cong A_1 \times A_2$.

Jan 23^{rd}

- **Yoneda Lemma:** For any functor $F\colon \mathsf{C} \to \mathsf{Set}$ any any object X of C, there is a natural bijection

$$\{\text{natural transformations } h^X = \mathrm{Hom}_{\mathsf{C}}(X, \_) \implies F\} \xrightarrow[\cong]{\eta} F(X)$$

  sending $h^X \overset{\alpha}{\implies} F$ to $\alpha_X(\mathrm{Id}_X)$.

- **Remarks:** Note that since both $\mathrm{Hom}_{\mathsf{C}}(X,X)$ and $F(X)$ are sets, we have that $\alpha_X\colon \mathrm{Hom}_{\mathsf{C}}(X,X) \to F(X)$ is a function, and so it makes sense to consider its value $\alpha_X(\mathrm{Id}_X)$ in some element of its domain. Moreover, naturality here means that given any morphism $X' \xrightarrow{f} X$, the diagram

$$\begin{tikzcd}
\{\text{natural transformations } \mathrm{Hom}_{\mathsf{C}}(X', \_) \implies F\} \arrow[r, "\eta_{X'}"] \arrow[d] & F(X') \arrow[d, "F(f)"] \\
\{\text{natural transformations } \mathrm{Hom}_{\mathsf{C}}(X, \_) \implies F\} \arrow[r, "\eta_X"] & F(X)
\end{tikzcd}$$

  commutes, where the unlabeled arrow maps $\mathrm{Hom}_{\mathsf{C}}(X', \_) \overset{\alpha'}{\implies} F$ to the transformation $\mathrm{Hom}_{\mathsf{C}}(X', \_) \overset{\alpha}{\implies} F$ given by $\alpha_Y(g) \doteq \alpha'_Y(g \circ f)$.

- **Proof of the Yoneda Lemma:** for each morphism $X \xrightarrow{f} A$ and each natural transformation $\mathrm{Hom}_{\mathsf{C}}(X, \_) \overset{\alpha}{\implies} F$, the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathsf{C}}(X,X) \arrow[r, "\alpha_X"] \arrow[d, "h^X(f)"'] & F(X) \arrow[d, "F(f)"] \\
\mathrm{Hom}_{\mathsf{C}}(X,A) \arrow[r, "\alpha_A"] & F(A)
\end{tikzcd}$$

  commutes. This allows us to construct the inverse η^{-1} in the following way: given $x \in F(X)$, we have to define a natural transformation $h^X \implies F$. So define $\alpha_X(\mathrm{Id}_X) = x$. This actually determines the entire natural map α_X, even though we have only defined its value on one element Id_X. For example, making $A = X$ and $f = \varphi$ in the above diagram and noting that $h^X(\varphi)(\mathrm{Id}_X) = \varphi$, it automatically follows that

$$\alpha_X(\varphi) = F(\varphi)\big(\alpha_X(\mathrm{Id}_X)\big) = F(\varphi)(x).$$

  In this sense, naturality "propagates", allowing us to define α_A also for $A \neq X$ in the same way, setting $\alpha_A(f) = F(f)(x)$.

- **Functor categories:** Another way to understand the naturality of the Yoneda bijection is via functor categories. Given categories C and D, there's a category

$\mathsf{Fun}(\mathsf{C},\mathsf{D})$ (also denoted D^{C} for clear reasons) with objects being functors $\mathsf{C} \to \mathsf{D}$ and morphisms being natural transformations $F \Longrightarrow G$. The Yoneda Lemma then says that there is a fully faithful "embedding" functor[6] $\mathscr{Y}\colon \mathsf{C}^{\mathrm{op}} \to \mathsf{Set}^{\mathsf{C}}$ defined on objects by $\mathscr{Y}(X) = h^X$ and mapping $X \to Y$ to $h^Y \Longrightarrow h^X$.

Similarly, there is a "dual" functor $\widetilde{\mathscr{Y}}\colon \mathsf{C} \to \mathsf{Set}^{\mathsf{C}}$ given by $\widetilde{\mathscr{Y}}(X) = h_X$, mapping $X \to Y$ to $h_X \Longrightarrow h_Y$.

- **Consequence:** Given a functor $F\colon \mathsf{C} \to \mathsf{Set}$, suppose X and X' are representing objects (in C) for F, with natural isomorphisms $h^X \overset{\eta}{\Longrightarrow} F$ and $h^{X'} \overset{\eta'}{\Longrightarrow} F$. There is a unique isomorphism $X \xrightarrow{\cong} X'$ which is compatible with these transformations. This is because in the hom-level, $\mathscr{Y}\colon \mathrm{Hom}_{\mathsf{C}}(X', X) \to \mathrm{Hom}_{\mathsf{Set}^{\mathsf{C}}}(h^X, h^{X'})$ is a bijection, and the composition $(\eta')^{-1} \circ \eta$ can be seen as a morphism $h^X \to h^{X'}$ in $\mathsf{Set}^{\mathsf{C}}$; consider $\mathscr{Y}^{-1}((\eta')^{-1} \circ \eta)^{-1}$.

- **Examples:**

  (1) In any category C with finite products, we have

  $$(A \times B) \times C) \cong A \times (B \times C) \cong A \times B \times C$$

  for any objects A, B and C. This is because all of them represent the same functor $F_{A,B,C}\colon \mathsf{C}^{\mathrm{op}} \to \mathsf{Set}$ given by

  $$F_{A,B,C}(D) \doteq \mathrm{Hom}_{\mathsf{C}}(D, A) \times \mathrm{Hom}_{\mathsf{C}}(D, B) \times \mathrm{Hom}_{\mathsf{C}}(D, C),$$

  acting on morphisms $D \to D'$ by a suitable composition. The moral of the history is that if some statement can be proven in Set, then it can be transferred to an arbitrary category C, if one can find convenient representations for a convenient functor.

  (2) Denote by CRing the category of commutative rings with 1 and ring homomorphisms which map $1 \mapsto 1$. Let A be a commutative ring, $S \subseteq A$ be a multiplicatively closed subset, and $I \lhd A$ an ideal. Then we have that

  $$\frac{S^{-1}A}{S^{-1}I} \cong \left(\frac{S}{I}\right)^{-1}\left(\frac{A}{I}\right),$$

  because they represent the same functor $F_{A,S,I}\colon \mathsf{CRing} \to \mathsf{Set}$ given by

  $$F_{A,S,I}(B) \doteq \{A \xrightarrow{g} B \mid g(s) \in B^{\times} \text{ for all } s \in S \text{ and } g(x) = 0 \text{ for all } x \in I\}$$

  and acting on morphisms via suitable compositions.

[6] The op here only says that $\mathscr{Y}$ will be a contravariant functor from C to $\mathsf{Set}^{\mathsf{C}}$.

Jan 25th

- **Adjoints:** Given a (covariant) functor $F\colon \mathsf{C} \to \mathsf{D}$, a *right adjoint* to F is a functor $G\colon \mathsf{D} \to \mathsf{C}$ with a bijection $\mathrm{Hom}_{\mathsf{D}}(F(A), B) \to \mathrm{Hom}_{\mathsf{C}}(A, G(B))$, for all objects A in C and B in D, which is natural in both variables. That is, given a morphism $B \to B'$ in D, the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathsf{D}}(F(A), B) \arrow[r, "\simeq"] \arrow[d] & \mathrm{Hom}_{\mathsf{C}}(A, G(B)) \arrow[d] \\
\mathrm{Hom}_{\mathsf{D}}(F(A), B') \arrow[r, "\simeq"] & \mathrm{Hom}_{\mathsf{C}}(A, G(B'))
\end{tikzcd}$$

commutes, and similarly for a given morphism $A' \to A$ in C. Or in other words, this means that there are natural isomorphisms

$$\mathrm{Hom}_{\mathsf{D}}(F(A), \_) \overset{\simeq}{\Longrightarrow} \mathrm{Hom}_{\mathsf{C}}(A, G(\_))$$

of functors $\mathsf{D} \to \mathsf{Set}$ and also

$$\mathrm{Hom}_{\mathsf{C}}(\_, G(B)) \overset{\simeq}{\Longrightarrow} \mathrm{Hom}_{\mathsf{D}}(F(\_), B)$$

of functors $\mathsf{C}^{\mathrm{op}} \to \mathsf{Set}$. In this setting, we also say that F is *left adjoint* to G, and that the pair (F, G) is an *adjunction*. Such an adjunction induces natural maps in the following way via the given bijections between hom-sets:

$$\begin{tikzcd}
\mathrm{Hom}_{\mathsf{D}}(F(A), F(A)) \arrow[r, "\simeq"] & \mathrm{Hom}_{\mathsf{C}}(A, GF(A)) \\
\mathrm{Id}_{F(A)} \arrow[r, mapsto] & \lambda_A
\end{tikzcd}$$

gives a morphism $A \xrightarrow{\lambda_A} GF(A)$ in C, while

$$\begin{tikzcd}
\mathrm{Hom}_{\mathsf{C}}(G(B), G(B)) \arrow[r, "\simeq"] & \mathrm{Hom}_{\mathsf{D}}(FG(B), B) \\
\mathrm{Id}_{G(B)} \arrow[r, mapsto] & \rho_B
\end{tikzcd}$$

gives a morphism $FG(B) \xrightarrow{\rho_B} B$ in D.

- **Examples:**

  (1) Consider the usual forgetful functor $G\colon \mathsf{Ab} \to \mathsf{Set}$. It has a left adjoint $F\colon \mathsf{Set} \to \mathsf{Ab}$ given by $F(S) \doteq$ free abelian group generated by S, and assigning to a set map the unique homomorphic extension between the corresponding free abelian groups. By the universal property of free groups, we indeed have $\mathrm{Hom}_{\mathsf{Ab}}(F(S), A) \simeq \mathrm{Hom}_{\mathsf{Set}}(S, G(A))$, for any set S and any abelian group A.

  (2) Consider now the forgetful functor $\mathsf{Top} \to \mathsf{Set}$. It has a left adjoint functor $\mathsf{Set} \to \mathsf{Top}$ which takes a set and equips it with the discrete topology. Any function between sets is then mapped to the (automatically) continuous function between the associated discrete spaces.

- **Limits (and colimits):** The idea is to generalize products and coproducts, respectively.
  - **Definition.** Let C be a category. An *inverse system* is a collection of objects $\{A_i\}_{i\in I}$ indexed by a poset I together with morphisms $A_i \xrightarrow{\varphi_{ij}} A_j$ whenever $i \geq j$, such that if $i \geq j \geq k$ we have $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$. That is, an inverse system is a functor $\underline{I}^{\mathrm{op}} \to \mathsf{C}$, sending $j \to i$ in I (when $j \leq i$) to $A_i \to A_j$. When regarding an inverse system as a functor like this, we set $\varphi_{ii} = \mathrm{Id}_{A_i}$ by convention.
  - **Definition.** An *(inverse) limit* of an inverse system (with the above notation) is an object $\varprojlim_I A_i$ (also denoted $\lim_I A_i$) together with morphisms $\mathrm{pr}_i \colon \varprojlim_I A_i \to A_i$ such that:

    (i) for all $i \geq j$, the diagram

$$\begin{tikzcd}
 & A_i \arrow[dd, "\varphi_{ij}"] \\
\varprojlim_I A_i \arrow[ur, "\mathrm{pr}_i"] \arrow[dr, "\mathrm{pr}_j"'] & \\
 & A_j
\end{tikzcd}$$

    commutes, and;

    (ii) $\varprojlim_I A_i$ is universal for condition (i), i.e., given an object B and morphisms $B \xrightarrow{f_i} A_i$ such that for $i \geq j$ the diagram

$$\begin{tikzcd}
 & A_i \arrow[dd, "\varphi_{ij}"] \\
B \arrow[ur, "f_i"] \arrow[dr, "f_j"'] & \\
 & A_j
\end{tikzcd}$$

    commutes, there is a unique morphism $B \xrightarrow{f} \varprojlim_I A_i$ making the following diagram commute:

$$\begin{tikzcd}
 & & A_i \arrow[dd, "\varphi_{ij}"] \\
B \arrow[r, dashed, "\exists!\, f"] \arrow[urr, bend left, "f_i"] \arrow[drr, bend right, "f_j"'] & \varprojlim_I A_i \arrow[ur, "\mathrm{pr}_i"] \arrow[dr, "\mathrm{pr}_j"'] & \\
 & & A_j
\end{tikzcd}$$

- **Examples:**

  (1) Products are indeed particular cases of limits, when $\{A_i\}_{i\in I}$ is indexed by the "anti-chain", that is, the only order relations are $i \leq i$ for all $i \in I$, and we have $\varphi_{ii} = \mathrm{Id}_{A_i}$. Moreover, when both $\varprojlim_I A_i$ and $\prod_{i\in I} A_i$ exist, there is a canonical morphism $\varprojlim_I A_i \to \prod_{i\in I} A_i$ given by the universal property of the product applied to the data $\varprojlim_I A_i \to A_i$, $i \in I$.

  (2) In Ring, consider $A_i = \mathbb{Z}/p^i\mathbb{Z}$, where p is a fixed prime and $i = 1, 2, \ldots$. We have maps $\mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ for $i \geq j$, and this is an inverse system whose limit is $\varprojlim_{\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z} = \mathbb{Z}_p$, the *ring of p-adic integers.*

- **Relation with limits from Calculus:** Consider in the real line $\mathbb{R}$ a decreasing sequence $(x_n)_{n\in\mathbb{N}}$, and assume that it is convergent, to $x \doteq \lim_{n\to+\infty} x_n$. The points in the sequence may be seen as objects in the poset-category $\underline{\mathbb{R}}$ associated to $(\mathbb{R}, \leq)$. Since for $n \geq m$ we have $x_n \leq x_m$, this says that we have a unique morphism $x_n \xrightarrow{\varphi_{nm}} x_m$ in $\underline{\mathbb{R}}$. The compatibility between said morphisms is nothing more than the transitivity of $\leq$ in $\mathbb{R}$, so we may see the sequence as an inverse system in $\underline{\mathbb{R}}$. Now we claim that $x = \varprojlim_{\mathbb{N}} x_n$. To wit, we have $x \leq x_n$ for all $n \in \mathbb{N}$ and this gives us the projection morphisms $x \xrightarrow{\mathrm{pr}_n} x_n$ in $\underline{\mathbb{R}}$. The diagram

$$\begin{tikzcd}
 & x_n \arrow[dd, "\varphi_{nm}"] \\
x \arrow[ur, "\mathrm{pr}_n"] \arrow[dr, "\mathrm{pr}_m"'] & \\
 & x_m
\end{tikzcd}$$

commutes in $\underline{\mathbb{R}}$ for $n \geq m$, again by transitivity of $\leq$ in $\mathbb{R}$. Now we only have to check universality. Assume we're given an object $y \in \mathbb{R}$ and morphisms $y \to x_n$, $n \in \mathbb{N}$. This just says that $y \leq x_n$ for all $n \in \mathbb{N}$, and in particular the diagram

$$\begin{tikzcd}
 & x_n \arrow[dd, "\varphi_{nm}"] \\
y \arrow[ur] \arrow[dr] & \\
 & x_m
\end{tikzcd}$$

automatically commutes for $n \geq m$. Since $y \leq x_n$ for all $n \in \mathbb{N}$, pass to the limit (in the usual Calculus sense) to conclude that $y \leq x$. This gives us a unique morphism $y \to x$ making the diagram

$$\begin{tikzcd}
& & x_n \arrow[dd, "\varphi_{nm}"] \\
y \arrow[r] \arrow[urr, bend left] \arrow[drr, bend right] & x \arrow[ur, "\mathrm{pr}_n"] \arrow[dr, "\mathrm{pr}_m"'] & \\
& & x_m
\end{tikzcd}$$

commute for $n \geq m$ (since then we have the three inequalities $y \leq x \leq x_n$, $y \leq x \leq x_m$ and $x \leq x_n \leq x_m$). We conclude that

$$\lim_{n \to +\infty} x_n = \varprojlim_{\mathbb{N}} x_n.$$

- **Colimits:** Now we state the definitions for the dual notion to inverse systems and limits.
  - **Definition.** Let C be a category. A *direct system* is a collection of objects $\{A_i\}_{i \in I}$ indexed by a poset I together with morphisms $A_i \xrightarrow{\psi_{ij}} A_j$ whenever $i \leq j$, such that if $i \leq j \leq k$ we have $\psi_{jk} \circ \psi_{ij} = \psi_{ik}$. Similar to before, a direct system is a functor $\underline{I} \to \mathsf{C}$, sending $i \to j$ in I (when $i \leq j$) to $A_i \to A_j$. Again, when regarding an inverse system as a functor like this, we set $\psi_{ii} = \mathrm{Id}_{A_i}$.
  - **Definition.** A *colimit* of a direct system (with the above notation) is an object $\varinjlim_I A_i$ (also denoted $\mathrm{colim}_I A_i$) together with morphisms $\rho_i \colon A_i \to \varinjlim_I A_i$ such that:

    (i) for all $i \leq j$, the diagram

$$\begin{tikzcd}
A_i \arrow[dd, "\psi_{ij}"'] \arrow[dr, "\rho_i"] & \\
& \varinjlim_I A_i \\
A_j \arrow[ur, "\rho_j"'] &
\end{tikzcd}$$

    commutes, and;

    (ii) $\varinjlim_I A_i$ is universal for condition (i), i.e., given an object B and morphisms $A_i \xrightarrow{f_i} B$ such that for $i \leq j$ the diagram

$$\begin{tikzcd}
A_i \arrow[dd, "\psi_{ij}"'] \arrow[dr, "f_i"] & \\
& B \\
A_j \arrow[ur, "f_j"'] &
\end{tikzcd}$$

commutes, there is a unique morphism $B \xrightarrow{f} \varinjlim_I A_i$ making the following diagram commute:

$$\begin{tikzcd}
A_i \arrow[dd, "\psi_{ij}"'] \arrow[dr, "\rho_i"] \arrow[drr, bend left, "f_i"] & & \\
 & \varinjlim_I A_i \arrow[r, dashed, "\exists! f"] & B \\
A_j \arrow[ur, "\rho_j"'] \arrow[urr, bend right, "f_j"'] & &
\end{tikzcd}$$

- **Remark:** Just like for limits, we have that coproducts are a particular case of colimits (indexed by an "anti-chain"), and we have a similar relation between colimits and increasing sequences in the real line, like previously.

Jan 28$^{\text{th}}$

- **Motivation for the projection formula (to be seen later):** If $f \colon X \to Y$ is just a function between sets, and we have two subsets $A \subseteq X$ and $B \subseteq Y$, there is only one way to compare A and B inside Y using f, since $f[A] \cap B = f[A \cap f^{-1}[B]]$. Later we will see certain functors inducing maps f^* and f_*, and they will satisfy the relation $f_*(A) \otimes B \cong f_*(A \otimes f^*(B))$.

- **Example:** Consider the following poset $(I, \leq)$:

$$\begin{tikzcd}
\overset{1}{\bullet} & & \overset{2}{\bullet} \\
 & * \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

(1) An inverse system in Ring indexed by I is a pair of morphisms $A_1 \xrightarrow{f_1} B$ and $A_2 \xrightarrow{f_2} B$ (more precisely, regarding the inverse system as a functor, it maps $1 \mapsto A_1$, $2 \mapsto A_2$ and $* \mapsto B$). The limit of this system is then the *fiber product* (pullback) ring

$$A_1 \times_B A_2 \doteq \{(a_1, a_2) \in A_1 \times A_2 \mid f_1(a_1) = f_2(a_2)\},$$

equipeed with the usual projections, which is a subring of $A_1 \times A_2$.

(2) In Top, a direct system indexed by I, mapping $*$ to a one-point space, is a pair of continuous maps ("inclusions") $* \xrightarrow{x} X$ and $* \xrightarrow{y} Y$. A colimit of this system is the identification space $X \cup_{x \sim y} Y \doteq (X \coprod Y)/(x \sim y)$:

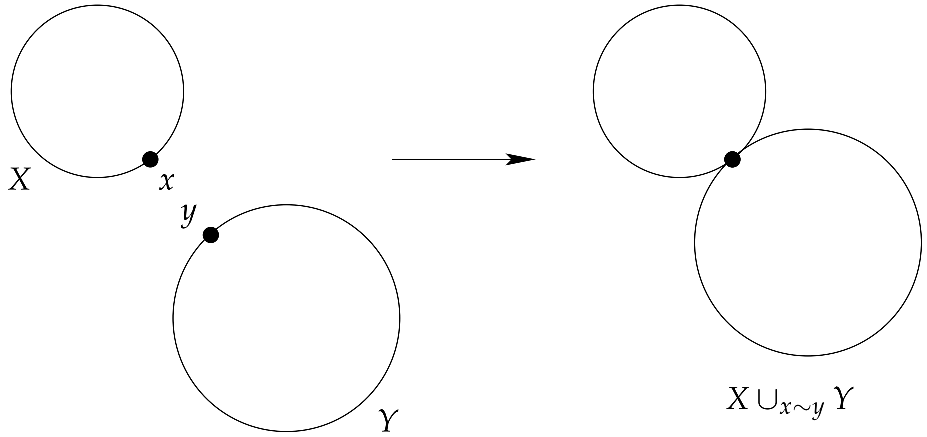


Figure 1: Gluing two spaces on a point.

Note that there is no need to restrict ourselves in this example to considering $*$ a one-point space (we could glue two spaces along subspaces).

- **Remark:** We often see the condition that a poset is *directed* (or filtered): for each $i, j \in I$ there is $k \in I$ with $i \leq k$ and $j \leq k$. This condition is not required to define limits and colimits, but it is useful if it holds. For example, if one replaces I with a subposet $J \subseteq I$ with the property that for every iI there is $j \in J$ with $i \leq j$, for every system $\{A_i\}_{i \in I}$ we have $\varprojlim_I A_i \cong \varprojlim_J A_j$ and $\varinjlim_I A_i \cong \varinjlim_J A_j$, when these exist.

- **Complete/cocomplete categories:** A category C is *complete* (resp. *cocomplete*) if all limits (resp. colimits) exist, for all posets I. Sometimes it is required in this definitions that the condition holds only for finite posets. In general, fixed a poset I for which all limits exist, a diagram indexed by I in C is a functor in $\mathsf{C}^{I^{\mathrm{op}}}$, and so we obtain a functor $\varprojlim_I : \mathsf{C}^{I^{\mathrm{op}}} \to \mathsf{C}$

- **Example:** Suppose that

$$A_1 \longleftarrow A_2 \longleftarrow \cdots \quad \text{and} \quad B_1 \longleftarrow B_2 \longleftarrow \cdots$$

are inverse systems of groups. Then $\varprojlim_{\mathbb{N}} A_n$ and $\varprojlim_{\mathbb{N}} B_n$ always exist. Giving morphisms $A_n \to B_n$, $n \in \mathbb{N}$, such that the diagram

$$\begin{tikzcd}
A_1 \arrow[d] & A_2 \arrow[l] \arrow[d] & \cdots \arrow[l] \\
B_1 & B_2 \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

commutes is the same as giving a morphism $\{A_n\}_{n \in \mathbb{N}} \to \{B_n\}_{n \in \mathbb{N}}$ in $\mathsf{Grp}^{\mathbb{N}^{\mathrm{op}}}$. We then obtain a morphism $\varprojlim_{\mathbb{N}} A_n \to \varprojlim_{\mathbb{N}} B_n$. As a subexample, when the systems are indexed by the antichain (meaning that we do not have the horizontal arrows), we obtain simply a morphism $\prod_{i \in I} A_i \to \prod_{i \in I} B_i$.

- **Monics and epis:** In a category C, a morphism $A \xrightarrow{f} B$ is called a:
  - *monomorphism* (monic) if it is left-cancellable:

$$\begin{tikzcd} T \arrow[r, bend left, "g_1"] \arrow[r, bend right, "g_2"'] & A \arrow[r, "f"] & B \end{tikzcd} \implies g_1 = g_2,$$

    or in other words, if $f \circ g_1 = f \circ g_2 \implies g_1 = g_2$ for every "test" object T.
  - *epimorphism* (epi) if it is right-cancellable:

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, bend left, "g_1"] \arrow[r, bend right, "g_2"'] & T \end{tikzcd} \implies g_1 = g_2,$$

    or in other words, if $g_1 \circ f = g_2 \circ f \implies g_1 = g_2$ for every "test" object T.

- **Example/Remark:** In Set, a map is a monomorphism (resp. epimorphism) if and only if it is injective (resp. surjective). But this need not be the case even for categories whose objects are sets with additional structure. For example, $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is epi in Ring, $\mathbb{Q} \hookrightarrow \mathbb{R}$ is epi in Top, etc..

- **Equalizers:** Let I be the poset $\begin{tikzcd} \bullet \arrow[r, bend left] \arrow[r, bend right] & \bullet \end{tikzcd}$. A limit over I in a category C is called an *equalizer*. More precisely, the *equalizer* of two morphisms $A \xrightarrow{f_1} B$ and $A \xrightarrow{f_2} B$ is an object K with a morphism $K \xrightarrow{\varepsilon} A$ such that $f_1 \circ \varepsilon = f_2 \circ \varepsilon$, which is universal among all the morphisms that equalize f and g, that is, for every morphism $T \xrightarrow{g} A$ such that $f_1 \circ g = f_2 \circ g$, there is a unique morphism $T \xrightarrow{u} K$ such that $\varepsilon \circ u = g$. Meaning that the following universal property is satisfied:

$$\begin{tikzcd} T \arrow[r, dashed, "\exists!"] \arrow[rr, bend left] & K \arrow[r, "\varepsilon"] & A \arrow[r, bend left, "f_1"] \arrow[r, bend right, "f_2"'] & B \end{tikzcd}$$

  Note that if an equalizer exists, it is automatically monic, in view of the uniqueness of u: to wit, if g_1 and g_2 are morphisms from T to K with $\varepsilon \circ g_1 = \varepsilon \circ g_2$, then the unique morphism completing the above diagram has to be g_1, and at the same time, g_2.

- **Remarks:**
  - Reversing the arrows, one may also define the *coequalizer* of two morphisms with same source and target. Coequalizers, when exist, are automatically epimorphisms (since coequalizers in C are the same as equalizers in C^{op}).
  - In the same fashion, one could also define what is the coequalizer of any family of morphisms in C with same source and target.

- **Example:** In Ab and Rng, equalizers always exist. Namely, ε will be the inclusion $\ker(f_1 - f_2) \hookrightarrow A$. This motivates the alternative name "difference kernel" for equalizers as well as the usual choice of letter K. Moreover, wanting to generalize this to categories where one cannot subtract morphisms motivates more general definitions of kernel, and the definition of an *abelian category*.

Homological Algebra (and more Category Theory)

Feb 1st

- **Additive categories:** The idea here is that an additive category is one whose hom-sets are abelian groups. An abelian category will satisfy additional conditions, modeled on Ab or R-mod. More precisely, we have the

  Definition: A category A is *additive* if:

  (i) all finite products exist (including the empty product – meaning that A has a terminal object);

  (ii) There is a zero object $\mathsf{0}$;

  (iii) $\mathrm{Hom}_{\mathsf{A}}(A,B)$ is an abelian group, for all objects A and B of A, and the compositions
  $$\mathrm{Hom}_{\mathsf{A}}(A,B)\times\mathrm{Hom}_{\mathsf{A}}(B,C)\to\mathrm{Hom}_{\mathsf{A}}(A,C)$$
  are bilinear.

- **Remark:** In the above definition, every $\mathrm{Hom}_{\mathsf{A}}(A,B)$ has a "0" morphism, namely, the only arrow making the diagram
  $$\begin{tikzcd} A \arrow[rr, dashed, "\exists!\,0"] \arrow[dr] & & B \\ & \mathsf{0} \arrow[ur] & \end{tikzcd}$$
  commute. This morphism must necessarily be the additive identity of $\mathrm{Hom}_{\mathsf{A}}(A,B)$, as the image of the bilinear map
  $$\mathrm{Hom}_{\mathsf{A}}(A,\mathsf{0})\times\mathrm{Hom}_{\mathsf{A}}(\mathsf{0},B)=\{(0,0)\}\to\mathrm{Hom}_{\mathsf{A}}(A,B)$$
  is just $\{0\}$.

- **Kernels and cokernels:** Let C be a category having a zero object (and hence zero morphisms between any give two objects of C – all denoted by 0). If $A\xrightarrow{f}B$ is a morphism, then:

  - a *kernel* of f is a morphism $K\xrightarrow{k}A$ such that $f\circ k=0$, and universal for this property:
  $$\begin{tikzcd} T \arrow[dr, "t"] \arrow[drr, bend left, "0"] \arrow[dd, dashed, "\exists!"'] & & \\ & A \arrow[r, "f"] & B \\ K \arrow[ur, "k"] \arrow[urr, bend right, "0"'] & & \end{tikzcd}$$

- a *cokernel* of f is a morphism $B \xrightarrow{c} C$ such that $c \circ f = 0$, and universal for this property:

$$\begin{tikzcd}
 & & T \\
A \arrow[r, "f"] \arrow[urr, bend left, "0"] \arrow[drr, bend right, "0"'] & B \arrow[ur, "t"] \arrow[dr, "c"'] & \\
 & & C \arrow[uu, dashed, "\exists!"']
\end{tikzcd}$$

- **Remark:** If kernels and cokernels exist, they're unique up to isomorphism, so one usually writes $K = \ker(f)$ and $C = \operatorname{coker}(f)$. Moreover, kernels and cokernels may be realized as certain limits and colimits, respectively.

- **Additive functors:** Let A and B be additive categories. A functor $F\colon \mathsf{A} \to \mathsf{B}$ is called *additive* if all the induced maps $\operatorname{Hom}_{\mathsf{A}}(A, B) \to \operatorname{Hom}_{\mathsf{B}}(F(A), F(B))$ are group homomorphisms.

- **Abelian categories:** An *abelian category* is an additive category satisfying the additional conditions:

  (iv) Every morphism has a kernel and a cokernel.

  (v) Every monic is the kernel of its cokernel; every epi is the cokernel of its kernel.

  (vi) Every morphism f factors as $f = m \circ e$, where m is monic and e is epic.

- **Understanding axiom (v):** In Ab, A is the kernel of $A \hookrightarrow B \twoheadrightarrow B/A$, and given $\ker(f) \hookrightarrow A \xrightarrow{f} B$, we have $B \cong A/\ker(f)$. Here, $\ker(f)$ measures how far f is from being injective, while $\operatorname{coker}(f) \cong B/\operatorname{Im}(f)$ measures for far f is from being surjective.

- **Propotype:** R-mod is an abelian category.

- **Counter-example:** The full subcategory FreeAb of Ab, of free abelian groups, is not abelian. For example, $\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}$ has no cokernel in FreeAb, since $\mathbb{Z}/2\mathbb{Z}$ has torsion (and it is not an object there).

- **Exactness:** A sequence $M \xrightarrow{f} N \xrightarrow{g} P$ in R-mod is *exact at N* if we have $\ker(f) = \operatorname{Im}(g)$ (as submodules of N). Categorically, the setup is

$$\begin{tikzcd}
M \arrow[rr, "f"] \arrow[dr, "e"'] & & N \arrow[rr, "g"] & & P \\
 & M' \arrow[ur, "m"] \arrow[rr, dashed, dash, "\simeq"] & & \ker(g) \arrow[ul, "k"'] &
\end{tikzcd},$$

which can be adapted to give a definition of exactness in abelian categories. Similarly, a sequence

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \cdots$$

is *exact* if it is exact at each M_i (i.e., $\ker(f_i) = \operatorname{Im}(f_{i-1})$ for all i). A *short exact sequence* is an exact sequence of the form

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0.$$

- **Remark:** In R-mod:
  - $0 \to M \xrightarrow{f} N$ is exact if and only if f is injective (monic).
  - $M \xrightarrow{f} N \to 0$ is exact if and only if f is surjective (epi).
  - There is a weaker notion of an "exact category" (due to Quillen), where exact sequences still make sense.

- **Exact functors:** Let $F\colon R\text{-mod} \to S\text{-mod}$ be an additive functor. Say that F is *exact* if it preserves all short exact sequences. More precisely, if for every short exact sequence

  $$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

  the image-sequence

  $$0 \longrightarrow F(M') \longrightarrow F(M) \longrightarrow F(M'') \longrightarrow 0$$

  is also exact. Also, F is *right-exact* (resp. *left-exact*) if only the sequence

  $$F(M') \longrightarrow F(M) \longrightarrow F(M'') \longrightarrow 0$$

  (resp. $0 \longrightarrow F(M') \longrightarrow F(M) \longrightarrow F(M'')$) is guaranteed to be exact. In other words, left-exact functors *produce* left-exact sequences and right-exact functors *produce* right-exact sequences.

Feb 4$^{\text{th}}$

- **Remark:** If A and B are abelian categories, a left-exact contravariant functor $\mathsf{A} \to \mathsf{B}$ is the same as a left-exact covariant functor $\mathsf{A}^{\mathsf{op}} \to \mathsf{B}$.

- **Example:** For any R-module M, we have that $\operatorname{Hom}_R(M, \_)$ is an additive functor $R\text{-mod} \to \mathsf{Ab}$, which is left-exact (but not right-exact, in general). The same holds for the contravariant version $\operatorname{Hom}_R(\_, M)$. Moreover, the same proof shows that if A is an abelian category and A is any object in A, then the functors $\operatorname{Hom}_{\mathsf{A}}(A, \_)$ and $\operatorname{Hom}_{\mathsf{A}}(\_, A)$ are left-exact. The modules P for which $\operatorname{Hom}_R(P, \_)$ is exact are called *projective*, while the modules Q for which $\operatorname{Hom}_R(\_, Q)$ is exact are called *injective*.

- **Tensor products:** Given vector spaces V and W, $V \otimes W$ is the space spanned by $\{v \otimes w \mid v \in V, w \in W\}$, and the elements in this spanning satisfy some algebraic relations. We want to generalize this idea for modules, giving a characterization in terms of universal properties. Denote a right R-module M simply by M_R and a left R-module N by ${}_RN$. This leads to the following formal definitions:

- a *balanced product* of M_R and ${}_RN$ is an abelian group A with a bi-additive map $f\colon M\times N\to A$ satisfying $f(mr,n)=f(m,rn)$ for all $m\in M$, $n\in N$ and $r\in R$.
- a *tensor product* of M_R and ${}_RN$ (over R) is a universal balanced product: in other words, it is an abelian group $M\otimes_R N$ with a map $(m,n)\mapsto m\otimes n$ such that

$$\begin{tikzcd} M\otimes_R N \arrow[dr, dashed, "\exists!\,\widetilde{f}"] & \\ M\times N \arrow[u] \arrow[r, "f"] & A \end{tikzcd}$$

for all balanced products $f\colon M\times N\to A$. All tensor products of M and N over R are isomorphic. Such a tensor product always exist (one possible construction is via a certain quotient of the free abelian group over $M\times N$).

- **$\otimes$ as a bifunctor:** Given $f\colon M\to M'$ and $g\colon N\to N'$ morphisms in mod-R and R-mod, respectively, we obtain a morphism $f\otimes g\colon M\otimes_R N\to M'\otimes_R N'$ in Ab. To see this, note that

$$M\times N\ni(m,n)\mapsto f(m)\otimes g(n)\in M'\otimes_R N'$$

is a balanced product, and universality gives us the desired map

$$\begin{tikzcd} M\otimes_N R \arrow[dr, dashed, "f\otimes g"] & \\ M\times N \arrow[u] \arrow[r] & M'\otimes_R N'. \end{tikzcd}$$

Also, one checks that this construction is compatible with compositions, in the sense that given $M\xrightarrow{f}M'\xrightarrow{f'}M''$ and $N\xrightarrow{g}N'\xrightarrow{g'}N''$ in mod-R and R-mod, we have from the uniqueness of linearizations of balanced products that $(f'\circ f)\otimes(g'\circ g)=(f'\otimes g')\circ(f\otimes g)$. This way, we have that the bifunctor $\_\otimes_R\_\colon \text{mod-}R\times R\text{-mod}\to\mathsf{Ab}$ specializes to one-variable, yielding two additive functors

$$M\otimes_R\_\colon R\text{-mod}\to\mathsf{Ab}\quad\text{and}\quad \_\otimes_R N\colon \text{mod-}R\to\mathsf{Ab},$$

acting on morphisms via $(f\colon N\to N')\rightsquigarrow(\mathrm{Id}_M\otimes f\colon M\otimes_R N\to M\otimes_R N')$, and similarly for the second functor. Formally, one could write $M\otimes_R f=\mathrm{Id}_M\otimes f$. We will not use this notation.

Feb 6th

- **$\otimes$ and $\oplus$ commute:** In general, additive functors preserves finite coproducts, which are the same as finite products in abelian categories. For modules, the situation is improved:

Proposition: Let $\{N_i\}_{i\in I}$ be any collection of left R-modules, and M be a right R-module. Then

$$M\otimes_R\left(\bigoplus_{i\in I}N_i\right)\cong\bigoplus_{i\in I}(M\otimes_R N_i).$$

Two proof ideas:

- Show that both objects in Ab represent a same functor $\mathsf{Ab} \to \mathsf{Set}$; conclude by applying the Yoneda Lemma.
- Combine the universal properties of tensor product and direct sum in different orders to obtain the isomorphism and its inverse. □

- **Right-exactness of $\otimes$:** The functors $M \otimes_R \_$ and $\_ \otimes_R N$ are right-exact (but not left-exact, in general).

  Proof: For $M \otimes_R \_$. Let $0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$ be a short exact sequence. We have to show that

  $$M \otimes_R N' \xrightarrow{\mathrm{Id}_M \otimes f} M \otimes_R N \xrightarrow{\mathrm{Id}_M \otimes g} M \otimes_R N'' \longrightarrow 0$$

  is exact, which we'll do in two steps:

  (i) $\ker(\mathrm{Id}_M \otimes g) = \mathrm{Im}(\mathrm{Id}_M \otimes f)$. By linearity, we may work with simple tensors. Since

  $$\begin{aligned}(\mathrm{Id}_M \otimes g) \circ (\mathrm{Id}_M \otimes f)(m \otimes n') &= (\mathrm{Id}_M \otimes g)(m \otimes f(n')) \\ &= m \otimes g(f(n')) = m \otimes 0 \\ &= 0,\end{aligned}$$

  we have one inclusion. Conversely, to prove the remaining inclusion $\ker(\mathrm{Id}_M \otimes g) \subseteq \mathrm{Im}(\mathrm{Id}_M \otimes f)$, it suffices to show that the map

  $$\frac{M \otimes_R N}{\mathrm{Im}(\mathrm{Id}_M \otimes f)} \xrightarrow{\overline{\mathrm{Id}_M \otimes g}} M \otimes_R N''$$

  induced by the previously proved inclusion, which is surjective (since g is), is actually an isomorphism. This will be done by exhibiting its inverse: let $\theta\colon M \times N'' \to (M \otimes_R N)/\mathrm{Im}(\mathrm{Id}_M \otimes f)$ be defined by $\theta(m, n'') = \overline{m \otimes n}$, where $n \in N$ is any element such that $g(n) = n''$. This is well-defined, since if $n_1, n_2 \in N$ are two elements such that $g(n_1) = g(n_2) = n''$, then $n_1 - n_2 \in \ker(g) = \mathrm{Im}(f)$ gives us $n' \in N'$ with $n_1 - n_2 = f(n')$, leading to

  $$m \otimes n_1 - m \otimes n_2 = m \otimes (n_1 - n_2) = m \otimes f(n') \in \mathrm{Im}(\mathrm{Id}_m \otimes f),$$

  hence $\overline{m \otimes n_1} = \overline{m \otimes n_2}$. That being established, it is easy to check that θ is a balanced product. The induced map $M \otimes_R N'' \to (M \otimes_R N)/\mathrm{Im}(\mathrm{Id}_M \otimes f)$ is the desired inverse (this can be checked only for simple tensors, again by linearity).

  (ii) $\mathrm{Id}_M \otimes g$ is surjective. Since tensor products are generated by simple tensors, it suffices to show that those are in the image of $\mathrm{Id}_M \otimes g$. Given any $m \otimes n'' \in M \otimes_R N''$, there is $n \in N$ with $g(n) = n''$, since g is assumed surjective. Thus $(\mathrm{Id}_M \otimes g)(m \otimes n) = \mathrm{Id}_M(m) \otimes g(n) = m \otimes n''$, as wanted.

□

- **Flat modules:** In a similar fashion that we mentioned the definition of projective and injective modules, we'll say that a right R-module M is *flat* if $M \otimes_R \_$ is exact. And a left R-module N is *flat* if $\_ \otimes_R N$ is exact.

- **Bimodules:** Let R and S be rings. A (R,S)-bimodule is a left R-module M, which is also a right S-module, such that the actions of R and S on M are compatible, in the sense that $(rm)s = r(ms)$ for all $r \in R$, $s \in S$ and $m \in M$. We may denote a (R,S)-bimodule simply by ${}_RM_S$. A map $f\colon M_1 \to M_2$ between (R,S)-bimodules is called a *(R,S)-bimodule homomorphism* if it is simultaneously a left R-module homomorphism and a right S-module homomorphism. The collection of (R,S)-bimodule homomorphisms from M_1 to M_2 is then denoted by $\mathrm{Hom}_{(R,S)}(M_1, M_2)$.

- **Structures induced by bimodules in $\otimes$:** Consider modules and bimodules M_R, ${}_RN_S$ and ${}_SP$. Then $M \otimes_R N$ has a natural right S-module structure (defined on simple tensors by $(m \otimes n)s = m \otimes (ns)$) and $N \otimes_S P$ has a natural left R-module structure (defined on simple tensors by $r(n \otimes p) = (rn) \otimes p$). In particular, if we're given ${}_RM$ and R is a subring of S, then S is an (R,R)-bimodule and $S \otimes_R M$ is said to be obtained from M by *extension of scalars*.

- **Associativity of $\otimes$ over bimodules:** Consider modules and bimodules M_R, ${}_RN_S$ and ${}_SP$. There is a canonical isomorphism $(M \otimes_R N) \otimes_S P \cong M \otimes_R (N \otimes_S P)$.

  Proof: Given $p \in P$, the map

  $$M \times N \ni (m,n) \mapsto m \otimes (n \otimes p) \in M \otimes_R (N \otimes_S P)$$

  is a balanced product of M and N over R, and so it induces a map acting on simple tensors by

  $$M \otimes_R N \ni m \otimes n \mapsto m \otimes (n \otimes p) \in M \otimes_R (N \otimes_S P).$$

  Now, letting p vary as well, we obtain a map

  $$(M \otimes_R N) \times P \to M \otimes_R (N \otimes_S P),$$

  that is a balanced product of $M \otimes_R N$ and P over S, and so induces yet another map

  $$(M \otimes_R N) \otimes_S P \to M \otimes_R (N \otimes_S P),$$

  which is finally the desired isomorphism. The inverse map is defined similarly.

  □

Feb 8th

- $\otimes$ **represents a functor:** By definition of tensor products, given M_R and ${}_RN$, we have a natural isomorphism $\mathrm{Bal}_R(M \times N, \_) \cong \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, \_)$ between functors $\mathsf{Ab} \to \mathsf{Set}$, where $\mathrm{Bal}_R(M \times N, \_)$ acts mapping
  - an abelian group A to $\mathrm{Bal}_R(M \times N, A) = \{\text{all balanced maps } M \times N \to A\}$, and;
  - a group homomorphism $\varphi\colon A \to A'$ to $\varphi_*(f) \doteq \varphi \circ f$ given by composition (i.e., if f is a balanced map with target A, then $\varphi \circ f$ is a balanced map with target A').

  Another proof of the associativity of $\otimes$ follows from the Yoneda Lemma, since both $M \otimes_R (N \otimes_S P)$ and $(M \otimes_R N) \otimes_S P$ both represent the "threefold functor" $\mathrm{Bal}_{R,S}(M \times N \times P, \_)$ similarly defined. When R is commutative (so that $M \otimes_R N$ is also a left R-module), this identification can be upgraded to a natural isomorphism $\mathrm{Bilin}_R(M \times N, \_) \cong \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, \_)$. We also conclude from this the so-called *hom-tensor adjointness*

  $$\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)),$$

  which in the categorial terms we have seen says nothing more than that the pair $(\_ \otimes_R N, \mathrm{Hom}_R(N, \_))$ is an adjunction. The induced maps induced by this adjunction are simply $\lambda_M\colon M \to \mathrm{Hom}_R(N, M \otimes_R N)$ given by $\lambda_M(m)(n) = m \otimes n$ and $\rho_P\colon \mathrm{Hom}_R(N, P) \otimes_R N \to P$ acting on simple tensors by $\rho_P(f \otimes n) = f(n)$.

- **Absorption:** Given modules M_R and ${}_RN$, then $M \otimes_R R$ and $R \otimes_R N$ are the underlying abelian groups of M and N. Namely, the multiplication

  $$M \times R \ni (m, r) \mapsto mr \in M$$

  is a balanced product which induces a map $M \otimes_R R \to M$, whose inverse is simply $M \ni m \mapsto m \otimes 1 \in M \otimes_R R$. The collection of such maps is actually a natural isomorphism $R \otimes_R \_ \cong \mathbf{1}_{\mathsf{mod}\text{-}R}$. Similarly we have $\_ \otimes_R R \cong \mathbf{1}_{R\text{-}\mathsf{mod}}$.

- **Dual modules:** Given a commutative ring R and a R-module R, the *dual module* to M is $M^\vee \doteq \mathrm{Hom}_R(M, R)$. The fact that R is commutative ensures that $\mathrm{Hom}_R(M, R)$ is an R-module, with multiplication defined by $(rf)(m) = rf(m)$ (if R is not commutative then $rf \notin M^\vee$). There is a natural homomorphism $M^\vee \otimes_R N \to \mathrm{Hom}_R(M, N)$, induced by $(f, n) \mapsto (m \mapsto f(m)n)$, which acts over simple tensors by $(f \otimes n)(m) = f(m)n$. If M and N are free with finite rank, this is an isomorphism. So...

- **Back to free modules:** Recall that given a set S, the free (left) R-module generated by S is $R^{(S)} \doteq \bigoplus_S R$. The "freeness" functor is the left-adjoint to the forgetful functor $R\text{-}\mathsf{mod} \to \mathsf{Set}$, and explicitly this just means that we have a bijection $\mathrm{Hom}_R(R^{(S)}, M) \cong \mathrm{Hom}_{\mathsf{Set}}(S, M)$, by the universal property of $\oplus$. Furthermore,

$R^{(S)}$ comes with a *distinguished* set of generators

$$\begin{tikzcd}
\mathrm{Hom}_S(R^{(S)}, R^{(S)}) \arrow[r] & \mathrm{Hom}_{\mathsf{Set}}(S, R^{(S)}) \\
\mathrm{Id}_{R^{(S)}} \arrow[r, mapsto] & (s \mapsto x_s),
\end{tikzcd}$$

where $x_s \in R^{(S)}$ has 1 in the s-th position and zeroes elsewhere. We say that $\{x_s \mid s \in S\}$ is a *basis* for $R^{(S)}$. In general, we say that a left R-module M is free if $M \cong R^{(S)}$ for some set S. Up to isomorphism, $R^{(S)}$ depends only on the cardinality $|S|$. Namely, if $|S_1| = |S_2|$, then $R^{(S_1)} \cong R^{(S_2)}$, but this does not discard the (admittedly bizarre) possibility of having $R^{(S_1)} \cong R^{(S_2)}$ even though $|S_1| \neq |S_2|$. For example, a ring is said to have *IBN (Invariant Basis Number)* if for all non-negative integers n and m, $R^n \cong R^m \implies n = m$ (e.g., non-trivial commutative rings and Noetherian rings have IBN). Whenever it makes sense, we may say that $\operatorname{rank}(M) = |S|$ is the *rank* of S.

- **Every module is a quotient of a free module.** That is, given any module M, there is an exact sequence $F \to M \to 0$ with F free.

  Proof: Identifying M with its image over $M \hookrightarrow R^{(M)}$, take the unique homomorphism $\varphi\colon R^{(M)} \to M$ such that $\varphi|_M = \mathrm{Id}_M$. □

  Note that the surjection is not, in general, unique.

Feb 11th

- **Theorem:** Every free R-module F is projective (i.e., $\mathrm{Hom}_R(F, \_)$ is exact).

  Proof: Since $\mathrm{Hom}_R(F, \_)$ is already left-exact (for any module), we just have to check that given $g\colon M \to M''$ surjective, we also have that the induced map $h^F(g)\colon \mathrm{Hom}_R(F, M) \to \mathrm{Hom}_R(F, M'')$ is also surjective. That is, every map $\varphi \in \mathrm{Hom}_R(F, M)$ lifts:

$$\begin{tikzcd}
 & F \arrow[dl, dashed, "\exists\,\psi"'] \arrow[d, "\varphi"] & \\
M \arrow[r, "g"] & M'' \arrow[r] & 0
\end{tikzcd}$$

  A morphism defined on a free module is (freely) determined by its values in a basis (we have seen that $\mathrm{Hom}_R(R^{(S)}, N) \cong \mathrm{Hom}_{\mathsf{Set}}(S, N)$). So choose a basis $\mathscr{B} = (x_i)_{i\in I}$ for F, define $\mathscr{B} \ni x_i \mapsto m_i \in M$, where m_i is any element in M such that $g(m_i) = \varphi(x_i)$, and consider the unique homomorphism $\psi\colon F \to M$ with $\psi(x_i) = m_i$ for all $i \in I$. □

- **Splitting:** If $0 \longrightarrow M' \longrightarrow M \xrightarrow{f} F \longrightarrow 0$ is exact with F free, then the sequence *splits*. In other words, there is a *section* $\sigma : F \to M$ with $f \circ \sigma = \mathrm{Id}_F$:

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] & M \arrow[r, "f"] & F \arrow[r] \arrow[l, dashed, bend left, "\sigma"] & 0
\end{tikzcd}$$

In particular, this implies that $M \cong F \oplus M'$.

Proof: This follows from the previous result:

$$\begin{tikzcd}
& F \arrow[dl, dashed, "\exists\sigma"'] \arrow[d, equal] & \\
M \arrow[r, "f"] & F \arrow[r] & 0
\end{tikzcd}$$

□

- **A list of equivalences:** For a R-module P, the following are equivalent:

  (i) P is projective (i.e., $\operatorname{Hom}_R(P, \_)$ is exact);

  (ii) every exact sequence $0 \to M' \to M \to P \to 0$ splits;

  (iii) P has the lifting property:

$$\begin{tikzcd}
& P \arrow[dl, dashed, "\exists"'] \arrow[d] & \\
M \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

  (iv) P is a direct summand of a free module.

- **Remark:** Conditions defined by the exactness of a functor are called *acyclic*. For example, flat modules are the ones acyclic for $\otimes$.

- **Proposition:** Any projective module is flat.

  Proof steps:

  (1) Free modules are flat, because R itself is flat and direct sums of flat modules are again flat, in view of the natural distributive isomorphism $M \otimes_R \bigoplus_{i \in I} N_i \cong \bigoplus_{i \in I}(M \otimes_R N_i)$.

  (2) Two modules are flat if and only if their direct sum is – this follows from the naturality of the isomorphism in (1).

  (3) Projective modules are direct summands of free modules – the conclusion follows from (2). □

- **Injective modules:** just like projective modules are related to freeness, injective modules are related to *divisibility* (a R-module M is divisible if for all $a \in R$, the multiplication map $M \xrightarrow{\cdot a} M$ is surjective). For a R-module Q, the following are equivalent:

  (i) Q is injective (i.e., $\operatorname{Hom}_R(\_, Q)$ is exact);

  (ii) every exact sequence $0 \to Q \to M \to M'' \to 0$ splits;

(iii) Q has the extension property:

$$\begin{tikzcd}
 & Q & \\
0 \arrow[r] & M' \arrow[u] \arrow[r] & M \arrow[ul, dashed, "\exists"']
\end{tikzcd}$$

- **Theorem**: Every R-module embeds in an injective module (just like every R-module is surjected by a projective module[7]).

  Proof steps for $R = \mathbb{Z}$: We have to show that every abelian group embeds in a divisible group.

  (1) A free abelian group $F \cong \mathbb{Z}^{(S)}$ embeds into the free $\mathbb{Q}$-vector space $F_{\mathbb{Q}}$ with the same basis.

  (2) Any abelian group is a quotient F/K, so it embeds in $F_{\mathbb{Q}}/K$, which is also divisible.

  (3) Every divisible abelian group is injective (proof uses Zorn's Lemma, and the converse is also true). $\square$

Feb 13$^{\text{th}}$

- **Proof for general R:** For any R-module M, $\mathrm{Hom}_R(R, M)$ becomes a R-module with operation $(r \cdot f)(x) \doteq f(xr)$, which is isomorphic to M itself via

  $$\mathrm{Hom}_R(R, M) \ni f \mapsto f(1) \in M, \text{ with inverse } M \ni m \mapsto (r \mapsto rm) \in \mathrm{Hom}_R(R, M).$$

  Also, we have $\mathrm{Hom}_R(R, M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, M)$. Now, since we have already verified the result for abelian groups, take Q an injective group with a $\mathbb{Z}$-linear embedding $\iota\colon M \hookrightarrow Q$. By left-exactness of $\mathrm{Hom}_{\mathbb{Z}}(R, \_)$, we get a $\mathbb{Z}$-linear embedding $h^R(\iota)\colon \mathrm{Hom}_{\mathbb{Z}}(R, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, Q)$. Now we claim that the composition of inclusions, $\mathrm{Hom}_R(R, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, Q)$, is actually R-linear and that $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module – this completes the proof.

  For R-linearity, let $r, x \in R$ and $f \in \mathrm{Hom}_R(R, M)$. On one hand, we have

  $$h^R(\iota)(r \cdot f)(x) = \iota \circ (r \cdot f)(x) = \iota((r \cdot f)(x)) = \iota(f(xr)),$$

  and on the other hand

  $$(r \cdot h^R(\iota)(f))(x) = h^R(\iota)(f)(xr) = (\iota \circ f)(xr) = \iota(f(xr)).$$

  Now, as for injectivity of $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$, take an exact sequence $0 \to N' \to N$. Then the first line in

  $$\begin{tikzcd}
  \mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(R, Q)) \arrow[r] \arrow[d, equal, "\cong"'] & \mathrm{Hom}_R(N', \mathrm{Hom}_{\mathbb{Z}}(R, Q)) \arrow[r] \arrow[d, equal, "\cong"'] & 0 \\
  \mathrm{Hom}_{\mathbb{Z}}(N \otimes_{\mathbb{Z}} R, Q) \arrow[r] & \mathrm{Hom}_{\mathbb{Z}}(N' \otimes_{\mathbb{Z}} R, Q) \arrow[r] & 0
  \end{tikzcd}$$

  is exact because the second line is, since Q is $\mathbb{Z}$-injective.

[7] Consider being "free" an improvement, which has no analogue in this new contravariant setting.

- **Modern version of Homological Algebra:** It was motivated by Algebraic Topology in the 1940's, with the Eilerberg-Steenrod axioms, influence by MacLane, etc.. Some precursors were Cayley ("Theory of Elimination", 1848) and Hilbert (syzygy theorem, 1890), leading to the notion of free resolutions. Also, we had the first results about homology and cohomology, such as Hilbert's theorem 90 (on cohomology of Galois groups) and Schur's theorem (1904) on $H^2(G, \mathbb{C}^*)$.

- **Complexes:** Can be defined in an arbitrary abelian category A. We will work on $\mathsf{A} = R\text{-}\mathsf{mod}$ for concreteness. So, a *complex of R-modules* is a sequence

$$\cdots \longrightarrow C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1} \longrightarrow \cdots$$

where each C_i is an R-module and $d_i \colon C_i \to C_{i-1}$ is a homomorphism of R-modules, such that $d_i \circ d_{i+1} = 0$ for all i. Such a complex is denoted simply by $C_\bullet$, or $(C_\bullet, d_\bullet)$ when we need to emphasize the *differentials*. A *morphism of complexes* $\varphi_\bullet \colon (C_\bullet, d_\bullet) \to (C'_\bullet, d'_\bullet)$ is a collection of homomorphism $\varphi_i \colon C_i \to C'_i$ such that

$$\begin{tikzcd}
\cdots \arrow[r] & C_{i+1} \arrow[r, "d_{i+1}"] \arrow[d, "\varphi_{i+1}"] & C_i \arrow[r, "d_i"] \arrow[d, "\varphi_i"] & C_{i-1} \arrow[r] \arrow[d, "\varphi_{i-1}"] & \cdots \\
\cdots \arrow[r] & C'_{i+1} \arrow[r, "d'_{i+1}"'] & C'_i \arrow[r, "d'_i"'] & C'_{i-1} \arrow[r] & \cdots
\end{tikzcd}$$

commutes. Composition of these morphisms is defined termwise, the identity morphism is the obvious one, and with this we have defined a category $\mathsf{Comp}(R\text{-}\mathsf{mod})$. In general, if A is an abelian category, $\mathsf{Comp}(\mathsf{A})$ is also an abelian category.

- **Prototypical example:** Let K be a simplicial complex, we have $C_\bullet$ defined by

$$C_i = \bigoplus_{\sigma \text{ is a } i\text{-simplex}} \mathbb{Z}\sigma,$$

with differential maps/boundary operators defined by

$$d_i(\sigma) = \sum_{j=0}^{i} (-1)^j \sigma(\hat{j})$$

extended linearly to C_i, where $\sigma(\hat{j})$ denotes the j-th face of σ.

- **Examples:**

  (1) An R-module M can be regarded as a "one-term" complex, with M placed in the 0-th degree:

$$\cdots \longrightarrow 0 \longrightarrow M \longrightarrow 0 \longrightarrow \cdots$$

(2) A short exact sequence $0 \to M' \to M \to M'' \to 0$ is a particular "three-term" complex

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots$$

(3) If $\varphi_\bullet \colon C_\bullet \to C'_\bullet$ is a morphism of complexes of R-modules, we may define a complex $\ker(\varphi_\bullet)$, whose terms are each $\ker(\varphi_i)$. The differentials of $C_\bullet$ may be restricted to $\ker(\varphi_\bullet)$ since the condition $\varphi_{i-1} \circ d_i = d'_i \circ \varphi_i$ says that d_i maps $\ker(\varphi_i)$ inside $\ker(\varphi_{i-1})$. Namely, we have

$$\cdots \longrightarrow \ker(\varphi_{i+1}) \xrightarrow{d_{i+1}} \ker(\varphi_i) \xrightarrow{d_i} \ker(\varphi_{i-1}) \longrightarrow \cdots$$

In a similar way, one may define a complex $\operatorname{coker}(\varphi_\bullet)$.

- **Constructions:**

(1) If $(C'_\bullet, d'_\bullet)$ and $(C''_\bullet, d''_\bullet)$ are two complexes of R-modules, we may define the sum $(C'_\bullet \oplus C''_\bullet, d_\bullet)$ by

$$\cdots \longrightarrow C'_{i+1} \oplus C''_{i+1} \xrightarrow{\quad d_{i+1} \quad} C'_i \oplus C''_i \xrightarrow{\quad d_i \quad} C'_{i-1} \oplus C''_{i-1} \longrightarrow \cdots$$

where $d_i(c'_i, c''_i) \doteq (d'_i(c'_i), d''_i(c''_i))$ for all i.

(2) If $(C_\bullet, d_\bullet)$ is a complex of right R-modules and M is a left R-module, we may define a complex of abelian groups $(C_\bullet \otimes_R M, d_\bullet \otimes \mathrm{Id}_M)$:

$$\cdots \longrightarrow C_{i+1} \otimes_R M \xrightarrow{d_{i+1} \otimes \mathrm{Id}_M} C_i \otimes_R M \xrightarrow{d_i \otimes \mathrm{Id}_M} C_{i-1} \otimes_R M \longrightarrow \cdots$$

Indeed, we have $(d_i \otimes \mathrm{Id}_M) \circ (d_{i+1} \otimes \mathrm{Id}_M) = (d_i \circ d_{i+1}) \otimes \mathrm{Id}_M = 0 \otimes \mathrm{Id}_M = 0$. Trying to define the tensor product of two complexes leads to *bicomplexes*, which are used in the study of spectral sequences. We will not pursue this further in details here.

Feb 15th

- **Free resolutions:** Since any R-module M is a quotient of a free module, we obtain an exact sequence $0 \longrightarrow M_1 \longrightarrow F_0 \xrightarrow{\varepsilon} M \longrightarrow 0$ with F_0 free, and some R-module M_1 (namely, $\ker(\varepsilon)$). Now, M_1 is also a quotient of a free-module, so we also obtain

$$\begin{tikzcd}
M_2 \arrow[dr, hook] & & & & & \\
& F_1 \arrow[rr, "d_1"] \arrow[dr, two heads] & & F_0 \arrow[r, "\varepsilon"] & M \arrow[r] & 0 \\
& & M_1 \arrow[ur, hook] & & &
\end{tikzcd}$$

with F_1 free. Continue proceeding this way and obtain an exact sequence

$$\begin{tikzcd}
\ddots \arrow[dr, hook] & & & & M_2 \arrow[dr, hook] & & & & & \\
\cdots \arrow[r] & F_3 \arrow[rr, "d_3"] \arrow[dr, two heads] & & F_2 \arrow[rr, "d_2"] \arrow[ur, two heads] & & F_1 \arrow[rr, "d_1"] \arrow[dr, two heads] & & F_0 \arrow[r, two heads, "\varepsilon"] & M \arrow[r] & 0 \\
& & M_3 \arrow[ur, hook] & & & & M_1 \arrow[ur, hook] & & &
\end{tikzcd}$$

Note that one could stop the process as soon as one of the M_i's is free, but there is no guarantee that this might happen – the process may go on forever. So, by construction, the complex

$$\cdots \longrightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} M \longrightarrow 0$$

is exact and consists of free modules F_i for $i \geq 0$. This is called a *free resolution* of M, and may be simply denoted by $F_\bullet \xrightarrow{\varepsilon} M$.

- **Remark:** Giving a free resolution $F_\bullet \xrightarrow{\varepsilon} M$ is the same as giving a morphism of complexes

$$\begin{tikzcd}
\cdots \arrow[r] & F_2 \arrow[r] \arrow[d] & F_1 \arrow[r] \arrow[d] & F_0 \arrow[r] \arrow[d, "\varepsilon"] & 0 \arrow[d] \\
\cdots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & M \arrow[r] & 0,
\end{tikzcd}$$

but here the complexes are no longer exact (for example, the first row is no longer exact at F_0). The notation $F_\bullet \xrightarrow{\varepsilon} M$ can be really understood as a morphism of complexes, if we denote again by M the one-term complex defined by M.

- **Examples:**

(1) If $R = \Bbbk[x,y]$ and $M = \Bbbk[x,y]/(x,y) \cong \Bbbk$, then

$$0 \longrightarrow R \xrightarrow{\begin{bmatrix} y \\ -x \end{bmatrix}} R \oplus R \xrightarrow{\begin{bmatrix} x & y \end{bmatrix}} M \longrightarrow 0$$

is a free resolution of M. The matrix notation here means that the first map is $r \mapsto (ry, -rx)$ and the second one is $(r_1, r_2) \mapsto r_1x + r_2y$.

(2) $R = \Bbbk[x]/(x^2)$ and $M = R/(x^2) \cong \Bbbk$. A free resolution of M is

$$\cdots \xrightarrow{\cdot x} R \xrightarrow{\cdot x} R \xrightarrow{\cdot x} R \longrightarrow M \longrightarrow 0,$$

which is not finite. In fact, one can show that there is no finite free resolution for M.

- **Projective resolutions:** Just like we did for free resolutions, a *projective resolution* of a R-module M is an exact complex of R-modules

$$\begin{tikzcd} \cdots \arrow[r] & P_2 \arrow[r, "d_2"] & P_1 \arrow[r, "d_1"] & P_0 \arrow[r, "\varepsilon"] & M \arrow[r] & 0, \end{tikzcd}$$

where each P_i is a projective module, for $i \geq 0$. We may denote a projective resolution of M by $P_\bullet \xrightarrow{\varepsilon} M$.

- **Homology functors:** Given a complex of R-modules $(C_\bullet, d_\bullet)$, its *i-th homology module* is defined by $H_i(C_\bullet) = Z_i(C_\bullet)/B_i(C_\bullet)$, where $Z_i(C_\bullet) = \ker(d_i)$ is the *module of i-cycles* and $B_i(C_\bullet) = \operatorname{Im}(d_{i+1})$ is the *module of i-boundaries*. Now, given a morphism of complexes $\varphi_\bullet\colon (C_\bullet, d_\bullet) \to (C'_\bullet, d'_\bullet)$

$$\begin{tikzcd} \cdots \arrow[r] & C_{i+1} \arrow[r, "d_{i+1}"] \arrow[d, "\varphi_{i+1}"] & C_i \arrow[r, "d_i"] \arrow[d, "\varphi_i"] & C_{i-1} \arrow[r] \arrow[d, "\varphi_{i-1}"] & \cdots \\ \cdots \arrow[r] & C'_{i+1} \arrow[r, "d'_{i+1}"'] & C'_i \arrow[r, "d'_i"'] & C'_{i-1} \arrow[r] & \cdots \end{tikzcd}$$

the commutativity of the squares implies that φ_i maps $Z_i(C_\bullet)$ inside $Z_i(C'_\bullet)$ and $B_i(C_\bullet)$ inside $B_i(C'_\bullet)$. Hence, it passes to the quotient as $H_i(\varphi)\colon H_i(C_\bullet) \to H_i(C'_\bullet)$. Once one checks the functoriality property

$$\begin{tikzcd} C_\bullet \arrow[rr] \arrow[dr] & & C'_\bullet \arrow[dl] & \Longrightarrow & H_i(C_\bullet) \arrow[rr] \arrow[dr] & & H_i(C'_\bullet) \arrow[dl] \\ & C''_\bullet & & & & H_i(C''_\bullet) & \end{tikzcd},$$

and so we obtain a functor $H_i\colon \mathsf{Comp}(R\text{-}\mathsf{mod}) \to R\text{-}\mathsf{mod}$, which also turns out to be additive (the addition of morphisms between complexes is done termwise). With this new terminology, we see that the homology of a complex measures how much it fails to be exact. Namely, a complex $(C_\bullet, d_\bullet)$ is exact if and only if $H_i(C_\bullet) = 0$ for all i.

- **Remark:** Homology functors may also be defined in arbitrary abelian categories, giving rise to *homology objects*. One needs to make sense of what a quotient means there, though.

- **Quasi-isomorphisms:** A morphism of complexes $\varphi_\bullet\colon C_\bullet \to C'_\bullet$ is called a *quasi-isomorphism* if all the induced maps $H_i(\varphi)\colon H_i(C_\bullet) \to H_i(C'_\bullet)$ are isomorphisms. Note that this is weaker than φ being an isomorphism of complexes, but it is stronger than the two complexes having all isomorphic homologies (because there is nothing to ensure that all the isomorphisms were induced by a single map). Here's a concrete example: if $F_\bullet \xrightarrow{\varepsilon} M$ is a free resolution, then it is a quasi-isomorphism when regarded as a morphism of complexes

$$\begin{tikzcd} \cdots \arrow[r] & F_2 \arrow[r] \arrow[d] & F_1 \arrow[r] \arrow[d] & F_0 \arrow[r] \arrow[d, "\varepsilon"] & 0 \arrow[d] \\ \cdots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & M \arrow[r] & 0. \end{tikzcd}$$

The reason is that all the i-th homologies of the two rows are trivial for $i \geq 1$ (hence any map induces isomorphisms), while $H_0(\varepsilon)$ is precisely the usual isomorphism $F_0/\ker(\varepsilon) \to M$ (remember here that $\mathrm{Im}(d_1) = \ker(\varepsilon)$) defined by $H_0(\varepsilon)(x + \ker\varepsilon) = \varepsilon(x)$. The same holds for projective (or any) resolutions. And the converse clearly holds: a quasi-isomorphism between the row complexes defines a resolution of M.

Feb 18th

- **Remark:** Quasi-isomorphisms need not have inverses, e.g.:

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & \mathbb{Z} \arrow[r, "\cdot 2"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d, two heads] & 0 \arrow[d] \\
0 \arrow[r] & 0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0.
\end{tikzcd}$$

- **Additivity:** Since $H_i \colon \mathsf{Comp}(R\text{-}\mathsf{mod}) \to R\text{-}\mathsf{mod}$ is an additive functor, it preserves direct sums. That is to say, $H_i(C'_\bullet \oplus C''_\bullet) \cong H_i(C'_\bullet) \oplus H_i(C''_\bullet)$.

- **"Dual" notation:** One can rename a complex as to obtain a *cochain* (ascending) complex $(C^\bullet, d^\bullet)$

$$\cdots \longrightarrow C^{i-1} \xrightarrow{d^{i-1}} C^i \xrightarrow{d^i} C^{i+1} \longrightarrow \cdots$$

with $d^i \circ d^{i-1} = 0$. We then have *cohomology* functors $H^i(C_\bullet) = Z^i(C^\bullet)/B^i(C^\bullet)$, where $Z^i(C^\bullet) = \ker(d^i)$ is the module of i-cocycles and $B^i(C^\bullet) = \mathrm{Im}(d^{i-1})$ is the module of i-coboundaries. We're not effectively dualzing anything here, but just changing notation, so that functoriality of H^i follows automatically from the functoriality of H_i. And H^i is also *covariant* (not contravariant).

- **Two general lemmas:** The following results hold in an arbitrary abelian category:

  (a) **Snake Lemma:** Given the following diagram with exact rows, there is a canonical homomorphism $\delta \colon \ker(f'') \to \mathrm{coker}(f')$ making it commute:

$$\begin{tikzcd}
 & & \ker(f'') \arrow[d, hook] \arrow[dddll, bend left, "\delta"] & \\
M' \arrow[r] \arrow[d, "f'"] & M \arrow[r] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
N' \arrow[r] \arrow[d, two heads] & N \arrow[r] & N'' & \\
\mathrm{coker}(f') & & &
\end{tikzcd}$$

(b) **Five-Lemma:** Consider the following commutative diagram with exact rows:

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & D \arrow[r] \arrow[d, "\delta"] & E \arrow[d, "\epsilon"] \\
A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & D' \arrow[r] & E'
\end{tikzcd}$$

If β and δ are isomorphism, α is epi and ϵ is monic, then γ is an isomorphism.

- **Sharpening the Five-Lemma:**
  - β, δ monic, α epi $\Longrightarrow$ γ monic;
  - β, δ epi, ϵ monic $\Longrightarrow$ γ epi.
- **Theorem (long exact sequence in homology):** Given a short exact sequence

$$0 \longrightarrow C'_\bullet \longrightarrow C_\bullet \longrightarrow C''_\bullet \longrightarrow 0$$

of complexes, there is a long exact sequence

$$\begin{tikzcd}
 & & \cdots \arrow[dll, "\delta_{i+1}"'] \\
H_i(C'_\bullet) \arrow[r] & H_i(C_\bullet) \arrow[r] & H_i(C''_\bullet) \arrow[dll, "\delta_i"'] \\
H_{i-1}(C'_\bullet) \arrow[r] & H_{i-1}(C_\bullet) \arrow[r] & H_{i-1}(C''_\bullet) \arrow[dll, "\delta_{i-1}"'] \\
\cdots & &
\end{tikzcd}$$

in homology. That is, there are natural homomorphisms δ_i making the above sequence exact.

Proof: Let's use the shorthands $Z''_i = Z_i(C''_\bullet)$, etc., and let α and β be the morphisms given in the short exact sequence of complexes. We first apply the Snake Lemma to obtain the diagram

$$\begin{tikzcd}
 & & & Z''_i \arrow[d, hook] \arrow[dddll, bend left] & \\
0 \arrow[r] & C'_i \arrow[r, "\alpha_i"] \arrow[d, "d'_i"'] & C_i \arrow[r, "\beta_i"] \arrow[d, "d_i"'] & C''_i \arrow[r] \arrow[d, "d''_i"'] & 0 \\
0 \arrow[r] & C'_{i-1} \arrow[r, "\alpha_{i-1}"] \arrow[d, two heads] & C_{i-1} \arrow[r, "\beta_{i-1}"] & C''_{i-1} \arrow[r] & 0 \\
 & C'_{i-1}/B'_{i-1} & & &
\end{tikzcd}$$

We claim that the "snake morphism" $Z_i'' \to C_{i-1}'/B_{i-1}'$ induces the desired map $\delta_i \colon H_i'' \to H_{i-1}'$. To see that this δ_i is well-defined, there are two things to check, using the definition of the snake morphism and some diagram chasing. Namely, that the snake morphism maps:

(i) $z_i'' \in Z_i''$ into $H_{i-1}' = Z_{i-1}'/B_{i-1}'$: there is $c_i \in C_i$ with $\beta_i(c_i) = z_i''$. Then

$$\beta_{i-1}(d_i(c_i)) = d_i''(\beta_i(c_i)) = d_i''(z_i'') = 0$$

says that $d_i(c_i) \in \ker(\beta_{i-1}) = \mathrm{Im}(\alpha_{i-1})$. Then take $c_{i-1}' \in C_{i-1}'$ with $\alpha_{i-1}(c_{i-1}') = d_i(c_i)$. It suffices now to check that $d_{i-1}'(c_{i-1}') = 0$. Here's how to do it: compute

$$\alpha_{i-2}(d_{i-1}'(c_{i-1}')) = d_{i-1}(\alpha_{i-1}(c_{i-1}')) = d_{i-1}(d_i(c_i)) = 0,$$

and conclude that $d_{i-1}'(c_{i-1}') = 0$ by injectivity of α_{i-2}, and then $c_{i-1}' \in Z_{i-1}'$. This step is done because the image of z_i'' under the snake morphism is the projection of c_{i-1}' in the quotient C_{i-1}'/B_{i-1}', which now lands inside $H_{i-1}' = Z_{i-1}'/B_{i-1}'$.

(ii) $b_i'' \in B_i''$ to zero in C_{i-1}'/B_{i-1}' (or in other words, that b_i'' is mapped inside B_{i-1}' before projecting): get $c_i \in C_i$ with $\beta_i(c_i) = b_i''$. Since $B_i'' \subseteq Z_i''$, the calculation done in the previous step gives $d_i(c_i) \in \ker(\beta_{i-1}) = \mathrm{Im}(\alpha_{i-1})$, and so we may take $c_{i-1}' \in C_{i-1}'$ with $\alpha_{i-1}(c_{i-1}') = d_i(c_i)$. We are done once we check that $c_{i-1}' \in B_{i-1}'$. Here's how to do it: take $c_{i+1}'' \in C_{i+1}''$ such that $d_{i+1}''(c_{i+1}'') = b_i''$, and use surjectivity of β_{i+1} to get $c_{i+1} \in C_{i+1}$ with $\beta_{i+1}(c_{i+1}) = c_{i+1}''$. We now have two elements in C_i, c_i and $d_{i+1}(c_{i+1})$. Then compute

$$\begin{aligned}\beta_i(c_i - d_{i+1}(c_{i+1})) &= \beta_i(c_i) - \beta_i(d_{i+1}(c_{i+1})) \\ &= b_i'' - d_{i+1}''(\beta_{i+1}(c_{i+1})) \\ &= b_i'' - d_{i+1}''(c_{i+1}'') \\ &= b_i'' - b_i'' = 0,\end{aligned}$$

so that $c_i - d_{i+1}(c_{i+1}) \in \ker(\beta_i) = \mathrm{Im}(\alpha_i)$, and we get an element $c_i' \in C_i'$ with $\alpha_i(c_i') = c_i - d_{i+1}(c_{i+1})$. Now, the only reasonable thing left to prove is that $d_i'(c_i') = c_{i-1}'$, and for that we use injectivity of α_{i-1} as follows:

$$\begin{aligned}\alpha_{i-1}(c_{i-1}' - d_i'(c_i')) &= \alpha_{i-1}(c_{i-1}') - \alpha_{i-1}(d_i'(c_i')) \\ &= d_i(c_i) - d_i(\alpha_i(c_i')) \\ &= d_i(c_i - \alpha_i(c_i')) \\ &= d_i(d_{i+1}(c_{i+1})) \\ &= 0.\end{aligned}$$

Exactness of the long exact sequence in homology comes directly from the Snake Lemma itself. □

- **"Dual" notion again:** The same argument says that if

$$\begin{tikzcd} 0 \arrow[r] & C'^{\bullet} \arrow[r] & C^{\bullet} \arrow[r] & C''^{\bullet} \arrow[r] & 0 \end{tikzcd}$$

  is a short exact sequence of (ascending) complexes, then we have a long exact sequence in cohomology:

$$\begin{tikzcd} & & \cdots \arrow[dll, "\delta^{i-1}" description] \\ H^i(C'_\bullet) \arrow[r] & H^i(C_\bullet) \arrow[r] & H^i(C''_\bullet) \arrow[dll, "\delta^{i}" description] \\ H^{i+1}(C'_\bullet) \arrow[r] & H^{i+1}(C_\bullet) \arrow[r] & H^{i+1}(C''_\bullet) \arrow[dll, "\delta^{i+1}" description] \\ \cdots & & \end{tikzcd}$$

- **Naturality:** The naturality of the δ-morphisms in those long exact sequences means that if we're given a morphism

$$\begin{tikzcd} 0 \arrow[r] & C'_\bullet \arrow[r] \arrow[d] & C_\bullet \arrow[r] \arrow[d] & C''_\bullet \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \widetilde{C}'_\bullet \arrow[r] & \widetilde{C}_\bullet \arrow[r] & \widetilde{C}''_\bullet \arrow[r] & 0 \end{tikzcd}$$

  between two exact sequences of complexes, then the diagram

$$\begin{tikzcd} \cdots \arrow[r] & H_i(C_\bullet) \arrow[r] \arrow[d] & \mathbf{H_i(C''_\bullet)} \arrow[r, "\delta_i"] \arrow[d] & \mathbf{H_{i-1}(C'_\bullet)} \arrow[r] \arrow[d] & H_{i-1}(C_\bullet) \arrow[r] \arrow[d] & \cdots \\ \cdots \arrow[r] & H_i(\widetilde{C}_\bullet) \arrow[r] & \mathbf{H_i(\widetilde{C}''_\bullet)} \arrow[r, "\widetilde{\delta}_i"] & \mathbf{H_{i-1}(\widetilde{C}'_\bullet)} \arrow[r] & H_{i-1}(\widetilde{C}_\bullet) \arrow[r] & \cdots \end{tikzcd}$$

  commutes. The only square whose commutativity does not follow from functoriality of H_i is the one indicated in bold – naturality means that this particular square does, in fact, commute as well. In other words, $H_\bullet$ is a *δ-functor* (that is, a collection of functors that transforms a morphism between short exact sequences of complexes into a natural morphism between the associated long exact sequences).

- **Homotopy of complexes:** When do two homomorphisms of complexes φ and ψ induce the same homomorphisms in homology, $\overline{\varphi}_i = \overline{\psi}_i$, for all i? Obviously if, for example, $\varphi = \psi$, or equivalently if $\varphi - \psi = 0$ (subtraction of morphisms is allowed because we are working in an abelian category). Here's an idea: a morphism $C_\bullet \to C'_\bullet$ induces the zero map between homologies when for each i,

z_i is mapped to $b'_i = d_{i+1}(\text{something})$. Writing the dependence of this something on z_i as $h_i(z_i)$, we see that we're actually looking for lifts:

$$\begin{tikzcd}
\cdots \arrow[r] & C_{i+1} \arrow[r, "d_{i+1}"] \arrow[d] & C_i \arrow[r, "d_i"] \arrow[d] \arrow[dl, dashed, "h_i"'] & C_{i-1} \arrow[r] \arrow[d] \arrow[dl, dashed, "h_{i-1}"'] & \cdots \\
\cdots \arrow[r] & C'_{i+1} \arrow[r, "d'_{i+1}"'] & C'_i \arrow[r, "d'_i"'] & C'_{i-1} \arrow[r] & \cdots
\end{tikzcd}$$

Then the composition $d'_{i+1} \circ h_i$ would map Z_i inside B'_i, but we have a problem: this does not define a morphism of complexes. To correct it (to obtain something commuting with differentials), we consider instead the *splitting maps*

$$s_i = d'_{i+1} \circ h_i + h_{i-1} \circ d_i,$$

which gives a bona fide morphism $s\colon C_\bullet \to C'_\bullet$. We have reverse-engineered the following result: if $\varphi, \psi\colon C_\bullet \to C'_\bullet$ are two morphisms of complexes and there are morphisms $h_i\colon C_i \to C_{i+1}$ such that $\varphi_i - \psi_i = d'_{i+1} \circ h_i + h_{i-1} \circ d_i$ for all i, then φ and ψ induce the same maps between homologies.

Feb 22nd

- **Left-derived functors:** Let $F\colon R\text{-mod} \to S\text{-mod}$ (for concreteness) be a functor. The *left-derived functors* $L_iF\colon R\text{-mod} \to S\text{-mod}$ are computed as follows:

  (i) Choose a projective resolution $P_\bullet \xrightarrow{\varepsilon} M$;

  (ii) Apply F to $P_\bullet$, obtaining a complex $F(P_\bullet)$;

  (iii) Take the homology $(L_iF)(M) = H_i(F(P_\bullet))$.

  It can be proved that this does not depend on the choice of projective resolution, and the action of L_iF on morphisms uses the fact that every morphism between modules can be lifted to a morphism between projective resolutions, and that the maps induced on the homologies are unique up to chain homotopy. So L_iF is well-defined.

- **Long exact sequences (1):** If $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ is a short exact sequence of R-modules, we will obtain a long exact sequence in homology:

$$\begin{tikzcd}
 & & \cdots \arrow[dll] \\
(L_1F)(M') \arrow[r] & (L_1F)(M) \arrow[r] & (L_1F)(M'') \arrow[dll] \\
(L_0F)(M') \arrow[r] & (L_0F)(M) \arrow[r] & (L_0F)(M'') \arrow[r] & 0
\end{tikzcd}$$

  If F is right-exact, then $L_0F \cong F$, so the above becomes

$$\cdots \to (L_1F)(M') \to (L_1F)(M) \to (L_1F)(M'') \to F(M') \to F(M) \to F(M'') \to 0$$

and we conclude that the left-derived functors are the answer to the problem of continuing the image of the initial short exact sequence to the left. We need to understand exactly how this long exact sequence is induced.

The first step is to obtain a short exact sequence of projective resolutions of M', M and M''. To compute the functors L_iF, we know that any choice of projective resolution can be made, but to obtain the desired short exact sequence of resolutions, we'll need to make a good choice of resolution for M (*Horseshoe Lemma*).

Namely, start choosing projective resolutions $P'_\bullet \xrightarrow{\varepsilon'} M'$ and $P''_\bullet \xrightarrow{\varepsilon''} M''$. Let $P_i \doteq P'_i \oplus P''_i$, for all $i \geq 0$. This indeed defines a projective complex with differential $(d'_\bullet, d''_\bullet)$, but to produce a resolution of M, we'll also need the augmentation map $\varepsilon\colon P_0 \to M$. To wit, since β is onto, we may use that P''_0 is projective to obtain a map $\sigma\colon P''_0 \to M$, and then the universal property of the direct sum $P'_0 \oplus P''_0$ applied to $\alpha \circ \varepsilon'$ and σ yields the desired ε, according to the following diagram:

$$\begin{tikzcd}
0 \arrow[d] & \\
M' \arrow[d, "\alpha"'] & P'_0 \arrow[l, "\varepsilon'"'] \arrow[ld, "\alpha\circ\varepsilon'"'] \arrow[d, hook] \\
M \arrow[d, "\beta"'] & P'_0 \oplus P''_0 \arrow[l, dashed, "\varepsilon"'] \arrow[d, two heads] \\
M'' \arrow[d] & P''_0 \arrow[l, "\varepsilon''"'] \arrow[lu, dashed, "\sigma"] \\
0 &
\end{tikzcd}$$

The problem now is that there is no reason whatsoever for the map ε given by this procedure to be compatible with $(d'_\bullet, d''_\bullet)$. So we need to produce the correct differential for $P_\bullet$ to obtain a bona fide projective resolution $P_\bullet \xrightarrow{\varepsilon} M$. We'll look for $d_1\colon P'_1 \oplus P''_1 \to P'_0 \oplus P''_0$ of the form $d_1(x'_1, x''_1) = (d'_1(x'_1) + \theta_1(x''_1), d''_1(x''_1))$, for some $\theta_1\colon P''_1 \to P'_0$ to be determined. Computing

$$\begin{aligned}
\varepsilon \circ d_1(x'_1, x''_1) &= \varepsilon(d'_1(x'_1) + \theta_1(x''_1), d''_1(x''_1)) \\
&= \varepsilon(d'_1(x'_1) + \theta_1(x''_1), 0) + \varepsilon(0, d''_1(x''_1)) \\
&= \alpha \circ \varepsilon'(d'_1(x'_1) + \theta_1(x''_1)) + \sigma(d''_1(x''_1)) \\
&= \alpha(\varepsilon'(\theta_1(x''_1))) + \sigma(d''_1(x''_1)) \\
&= (\alpha \circ \varepsilon' \circ \theta_1 + \sigma \circ d''_1)(x''_1)
\end{aligned}$$

we see that $\varepsilon \circ d_1 = 0$ is equivalent to $\alpha \circ \varepsilon' \circ \theta_1 = -\sigma \circ d''_1$. And P''_1 being projective will give us θ_1 such that

$$\begin{tikzcd}
P'_0 \arrow[d, "\alpha\circ\varepsilon'"'] & \\
M \arrow[d, "\beta"'] & P''_1 \arrow[l, "-\sigma\circ d''_1"'] \arrow[ul, dashed, "\theta_1"'] \\
M'' &
\end{tikzcd}$$

commutes, once we check that the image of $-\sigma \circ d''_1$ lands inside the image of $\alpha \circ \varepsilon'$. This is a simple diagram chasing: $\beta(\sigma(d''_1(x''_1))) = \varepsilon'(d''_1(x''_1)) = 0$ says that $\sigma(d''_1(x''_1)) \in \ker(\beta) = \operatorname{Im}(\alpha)$, and we obtain $m \in M$ with $\sigma(d_1(x''_1)) = \alpha(m)$ – now ε' being surjective gives $x'_0 \in P'_0$ with $m = \varepsilon'(x'_0)$, and we conclude that $\sigma(d''_1(x''_1)) = \alpha(\varepsilon'(x'_0))$ as wanted.

We proceed inductively to define differentials $d_i\colon P'_i \oplus P''_i \to P'_{i-1} \oplus P''_{i-1}$ of the form $d_i(x'_i, x''_i) = (d'_i(x'_i) + \theta_i(x''_i), d''_i(x''_i))$ for convenient maps $\theta_i\colon P''_i \to P'_{i-1}$ fitting the diagram

$$\begin{tikzcd}
P'_i \arrow[d, "d'_i"'] & \\
P'_{i-1} \arrow[d, "d'_{i-1}"'] & P''_{i+1} \arrow[l, "-\theta_i\circ d''_{i+1}"'] \arrow[ul, dashed, "\theta_{i+1}"'] \\
P'_{i-2} &
\end{tikzcd}$$

for all i. This is because $d_i \circ d_{i+1} = 0$ is equivalent to $d'_i \circ \theta_{i+1} + \theta_i \circ d''_{i+1} = 0$. So, to complete the induction, it suffices to check that the image of $\theta_i \circ d''_{i+1}$ lands inside the image of d'_i – this way P''_{i+1} being projective gives us θ_{i+1}. Again, we repeat the previous diagram chasing: compute

$$d'_{i-1}(\theta_i(d''_{i+1}(x''_{i+1}))) = -\theta_{i-1}(d''_i(d''_{i+1}(x''_{i+1}))) = 0,$$

so that $\theta_i(d''_{i+1}(x''_{i+1})) \in \ker(d'_{i-1}) = \operatorname{Im}(d'_i)$, as wanted. The situation is described in the following summarized diagram (commutative up to a sign):

$$\begin{tikzcd}
P'_{i-2} & P'_{i-1} \arrow[l, "d'_{i-1}"'] & P'_i \arrow[l, "d'_i"'] & \\
& P''_{i-1} \arrow[ul, "\theta_{i-1}"] & P''_i \arrow[l, "d''_i"] \arrow[ul, "\theta_i"] & P''_{i+1} \arrow[l, "d''_{i+1}"]
\end{tikzcd}$$

To see that with these new differentials we obtain a resolution $P_\bullet \xrightarrow{\varepsilon} M$, we use the long exact sequence in homology induced by the first row in

$$\begin{tikzcd}
0 \arrow[r] & P'_\bullet \arrow[r] \arrow[d] & P_\bullet \arrow[r] \arrow[d] & P''_\bullet \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

to obtain $\cdots \longrightarrow \cancelto{0}{H_i(P'_\bullet)} \longrightarrow H_i(P_\bullet) \longrightarrow \cancelto{0}{H_i(P''_\bullet)} \longrightarrow \cdots$ for all $i > 0$ – exactness obviously then gives $H_i(P_\bullet) = 0$ as well. Finally, for $i = 0$, the conclusion $H_0(P_\bullet) \cong M$ follows from the Five-Lemma applied to the diagram

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, equal] & H_0(P'_\bullet) \arrow[r] \arrow[d, "\cong"] & H_0(P_\bullet) \arrow[r] \arrow[d] & H_0(P''_\bullet) \arrow[r] \arrow[d, "\cong"] & 0 \arrow[d, equal] \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0.
\end{tikzcd}$$

Feb 25th

- **Long exact sequences (2):** Continuing from where we left off, the next step would be to check that $0 \longrightarrow F(P'_\bullet) \longrightarrow F(P_\bullet) \longrightarrow F(P''_\bullet) \longrightarrow 0$ is exact. By construction, each step sequence $0 \longrightarrow P'_i \longrightarrow P_i \longrightarrow P''_i \longrightarrow 0$ is split exact. Then the conclusion follows from the general fact that every additive functor preserves short split-exact sequences: the image

  $$0 \longrightarrow F(P'_i) \longrightarrow F(P_i) \longrightarrow F(P''_i) \longrightarrow 0$$

  is also split-exact. Thus, we obtain the long exact sequence for $L_\bullet F$.

- **Right-derived functors:** Those are defined in a similar way to left-derived functors. Assume (for concreteness) that $F\colon R\text{-mod} \to S\text{-mod}$ is a functor. The right-derived functors of F are defined/computed in the following way:

  (i) Choose an injective resolution $M \xrightarrow{\eta} Q^\bullet$, that is an exact (ascending) complex of R-modules

  $$0 \longrightarrow M \xrightarrow{\eta} Q^0 \xrightarrow{d^0} Q^1 \xrightarrow{d^1} Q^2 \xrightarrow{d^2} \cdots$$

  where each Q^i is an injective module, for $i \geq 0$.

  (ii) Apply F to $Q^\bullet$, obtaining a complex $F(Q^\bullet)$;

  (iii) Take the cohomology $(R^iF)(M) \doteq H^i(F(Q^\bullet))$.

  We have the same results as the ones for left-derived functors, such as independence of choice of resolution, long exact sequences, etc.. In particular, this is useful when F is left-exact, so that $R^0F \cong F$.

- **Remark:** If F is *contravariant* instead, the roles projective/injective are reversed. Namely, we use:
  - *projective* resolutions to define and compute R^iF, and;
  - *injective* resolutions to define and compute L_iF.

- **Ext & Tor:** They are the derived functors of $\mathrm{Hom}_R(\_, N)$ and $M \otimes_R \_$, respectively. We will focus on the Ext functor first, and come back to Tor later. Note that there is a certain initial ambiguity regarding Ext, as it could be computed in two different ways:

  (1) Consider the contravariant functor $\mathrm{Hom}_R(\_, N)$ and then compute $\mathrm{Ext}^i_R(M, N) = R^i(\mathrm{Hom}_R(\_, N))(M)$ using a projective resolution of M, or;

  (2) Consider the covariant functor $\mathrm{Hom}_R(M, \_)$ and then compute $\mathrm{Ext}^i_R(M, N) = R^i(\mathrm{Hom}_R(M, \_))(N)$ using an injective resolution of N.

  It is a non-trivial fact that both procedures give the same result. Usually, working with (1) is easier, so we'll take this as the definition and denote by $\widetilde{\mathrm{Ext}}$ the functors produced by (2). There is a natural isomorphism $\mathrm{Ext} \cong \widetilde{\mathrm{Ext}}$, since both are δ-functors satisfying a certain universal property related to Hom. Note that since the hom-functor is left-exact, we automatically have $\mathrm{Ext}^0_R(M, N) = \mathrm{Hom}_R(M, N)$.

- **Ext for projective modules:** Given a R-module P, the following are equivalent:

  (i) P is projective.

  (ii) $\mathrm{Ext}^i_R(P, N) = 0$ for all $i > 0$ and all R-modules N.

  (iii) $\mathrm{Ext}^1_R(P, N) = 0$ for all R-modules N.

  Proof:

  (i) $\Longrightarrow$ (ii) : Assume that P is projective. Then

  $$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow P \longrightarrow P \longrightarrow 0$$

  is a projective resolution of P. Apply the contravariant functor $\mathrm{Hom}_R(\_, N)$ to the projective complex

  $$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow P$$

  to get the ascending complex

  $$\mathrm{Hom}_R(P, N) \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots$$

  Now it is obvious that the cohomologies of this complex are $\mathrm{Ext}^i_R(P, N) = 0$ for all $i > 0$.

  (ii) $\Longrightarrow$ (iii) : Trivial.

(iii) $\Longrightarrow$ (i) : Our goal is to prove that $\operatorname{Hom}_R(P,\_)$ is exact. If one already has established the natural isomorphism $\operatorname{Ext} \cong \widetilde{\operatorname{Ext}}$, one easy proof follows from just taking a short exact sequence

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

and using the long exact sequence for $\widetilde{\operatorname{Ext}}$, which yields

$$0 \longrightarrow \operatorname{Ext}^0_R(P,N') \longrightarrow \operatorname{Ext}^0_R(P,N) \longrightarrow \operatorname{Ext}^0_R(P,N'') \longrightarrow \operatorname{Ext}^1_R(P,N') \longrightarrow \cdots$$

Then $\operatorname{Ext}^i_R(P,\_) = 0$ for $i \geq 1$ and $\operatorname{Ext}^0_R(P,\_) \cong \operatorname{Hom}_R(P,\_)$ give us that

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

is exact, as wanted. An alternative proof of this implication without using the isomorphism $\operatorname{Ext} \cong \widetilde{\operatorname{Ext}}$ is as follows: take a *free presentation*

$$0 \longrightarrow N \longrightarrow F \longrightarrow P \longrightarrow 0$$

of P (i.e., the sequence is exact and F is free). We are done if we prove that the sequence splits, so P is a direct summand of a free module, hence projective. Apply $\operatorname{Hom}_R(\_,N)$ and use the given hypothesis $\operatorname{Ext}^1_R(P,N) = 0$ to get the exact sequence

$$0 \longrightarrow \operatorname{Hom}_R(P,N) \longrightarrow \operatorname{Hom}_R(F,N) \longrightarrow \operatorname{Hom}_R(N,N) \longrightarrow 0$$

Since $\operatorname{Hom}_R(F,N) \to \operatorname{Hom}_R(N,N)$, there is $\rho\colon F \to N$ which gets mapped to Id_N. This ρ is a splitting map.

□

- **Ext and extensions:** An *extension* of an R-module M by another R-module N is an exact sequence $0 \to N \to E \to M \to 0$, for some R-module E. Two extensions of M by N are called *isomorphic* if there is a isomorphism $E \xrightarrow{\simeq} E'$ such that

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d, "\simeq"] & M \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & N \arrow[r] & E' \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

commutes. Let $\operatorname{E}(M,N)$ be the collection of isomorphism classes of extensions of M by N. This is natural in both variables. For example, given $f\colon N \to N'$, there is $\operatorname{E}(M,N) \to \operatorname{E}(M,N')$ given by

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] \arrow[d, "f"'] & E \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & N' \arrow[r] & E' \arrow[r] & M \arrow[r] & 0, \end{tikzcd}$$

where $\iota\colon N \hookrightarrow N' \oplus E$ is given by $\iota(n) = (f(n), -n)$ and $E' = (N' \oplus E)/\iota(N)$ is the pushout of the diagram

$$\begin{tikzcd} N \arrow[r] \arrow[d, "f"'] & E \\ N' & \end{tikzcd}$$

Here, of course, we may regard N as a submodule of E. It has to be shown that the bottom row is indeed exact. To wit, let ψ be the arrow $E \to M$, so that we're effectively setting $N = \ker\psi$, and also let ψ' be the arrow $E' \to M$. The map ψ' is well-defined since

$$(n', e) \mapsto \psi(e) \quad \text{and} \quad (n' + f(n), e - n) \mapsto \psi(e - n) = \psi(e).$$

Also, we clearly have $\psi'((n, 0) + \iota(N)) = \psi(n) = 0$. On the other hand, if $\psi'((n, e) + \iota(N)) = 0$, then $\psi(e) = 0$ says that $e \in N$, allowing:

$$(n', e) + \iota(N) = (n' + f(e), e - e) + \iota(N) = (n' + f(e), 0) + \iota(N),$$

which then lies in the image of $N' \to E'$.

Feb 27th

- **The name "extension":** There is a natural isomorphism $\mathrm{E}(M, N) \cong \mathrm{Ext}^1_R(M, N)$.

  Proof: Let a class $[E] \in \mathrm{E}(M, N)$ be represented by the extension

  $$0 \longrightarrow N \longrightarrow E \longrightarrow M \longrightarrow 0,$$

  and apply the covariant functor $\mathrm{Hom}_R(\_, N)$ to get the long exact sequence

  $$0 \longrightarrow \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(E, N) \longrightarrow \mathrm{Hom}_R(N, N) \longrightarrow \mathrm{Ext}^1_R(M, N) \longrightarrow \cdots$$

  Then we can define $\alpha_{M,N}\colon \mathrm{E}(M, N) \to \mathrm{Ext}^1_R(M, N)$ by sending $[E]$ to the image of Id_N via the arrow $\mathrm{Hom}_R(N, N) \to \mathrm{Ext}^1_R(M, N)$ in the above sequence. This is indeed well-defined by the naturality of the long exact sequence in cohomology.

  Let's understand this transformation $\alpha_{M,N}$ more concretely. For this, consider a projective presentation $0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0$ of M. Apply $\mathrm{Hom}_R(\_, N)$ to get (the piece of) the sequence

  $$\mathrm{Hom}_R(P, N) \longrightarrow \mathrm{Hom}_R(K, N) \longrightarrow \mathrm{Ext}^1_R(M, N) \longrightarrow 0,$$

  by using that P is projective (and hence $\mathrm{Ext}^i_R(P, \_) = 0$ for $i \geq 1$). We obtain that

  $$\mathrm{Ext}^1_R(M, N) \cong \frac{\mathrm{Hom}_R(K, N)}{\mathrm{Im}(\mathrm{Hom}_R(P, N) \to \mathrm{Hom}_R(K, N))}.$$

And in the following diagram, lifts $f\colon P \to E$ restrict to maps $g\colon K \to N$:

$$\begin{tikzcd}
 & & & 0 & \\
0 \arrow[r] & N \arrow[r] & E \arrow[r] & M \arrow[r] \arrow[u] & 0 \\
 & & & P \arrow[u] \arrow[ul, "f"] & \\
 & & & K \arrow[u] \arrow[uull, "g"] & \\
 & & & 0 \arrow[u] &
\end{tikzcd}$$

Thus we have obtained an element of $\mathrm{Hom}_R(K,N)$. To eliminate the dependence on the choice of lift, assume that $f'\colon P \to E$ restricts to $g'\colon K \to N$. Then the difference $f - f'$ has image in $\ker(E \to M) = N$, i.e., $f - f' \in \mathrm{Hom}_R(P,N)$. This means $[f - f'] = 0$ in the quotient, and we get a well-defined map

$$\mathrm{E}(M,N) \ni [E] \mapsto [g] \in \frac{\mathrm{Hom}_R(K,N)}{\mathrm{Im}(\mathrm{Hom}_R(P,N) \to \mathrm{Hom}_R(K,N))} \cong \mathrm{Ext}^1_R(M,N).$$

Up to the last identification $\cong$, this is $\alpha_{M,N}$.

- Surjectivity: given $K \to N$, consider the same projective presentation of M previously given. Let E be the pushout of N and P over K:

$$\begin{tikzcd}
 & N \arrow[dr, dashed] & \\
K \arrow[ur, "g"] \arrow[dr] & & E \\
 & P \arrow[ur, dashed, "f"'] &
\end{tikzcd}$$

  This produces a class $[E] \in \mathrm{E}(M,N)$, to be mapped back to $[g]$.
- Injectivity: every extension which maps to the same $[g]$ will actually be isomorphic to the above pushout.

Checking for naturality is left as an exercise. □

- **Remarks:**
  - The extension set $\mathrm{E}(M,N)$ is sometimes called the *Yoneda-Ext*.
  - The same idea works for higher order ext's: define $\mathrm{E}^n(M,N)$ as the collection of the equivalence classes of n-extensions of M by N, i.e., exact sequences

$$0 \longrightarrow N \longrightarrow E_1 \longrightarrow \cdots \longrightarrow E_n \longrightarrow M \longrightarrow 0$$

    We have a natural isomorphism $\mathrm{E}^n(M,N) \cong \mathrm{Ext}^n_R(M,N)$.

- Ext^1 appears in algebraic topology: the *universal coefficients theorem* related $H^\bullet(X)$ and the dual $H_\bullet(X)^\vee$. In general, for every abelian group A we have the exact sequences

$$0 \longrightarrow \operatorname{Ext}^1_{\mathbb{Z}}(H_{i-1}(X;\mathbb{Z}),A) \longrightarrow H^i(X;A) \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(H_i(X;\mathbb{Z}),A) \longrightarrow 0.$$

If $A=\mathbb{Z}$ and $H_{i-1}(X;\mathbb{Z})$ is free (or more generally, projective), the above sequence gives an isomorphism $H^i(X;\mathbb{Z}) \cong H_i(X;\mathbb{Z})^\vee \doteq \operatorname{Hom}_{\mathbb{Z}}(H_i(X;\mathbb{Z}),\mathbb{Z})$.

- **Group cohomology:** Fix a ring R (usually $\mathbb{Z}$ or a field $\Bbbk$) and a group G. We have the group ring $R[G]$ and the *fixed point functor* $(\_)^G\colon R[G]\text{-mod} \to R\text{-mod}$, sending:

  - an $R[G]$-module A to $A^G = \{a\in A \mid ga = a \text{ for all } g\in G\}$, which is isomorphic to $\operatorname{Hom}_{R[G]}(R,A)$, where we regard R as an $R[G]$-module with trivial action by elements of G (i.e., $gr \doteq r$ for all $g\in G$)[8];
  - an $R[G]$-linear map $f\colon A\to B$ to the restriction $f^G\colon A^G\to B^G$ (indeed, the codomain is correct, since for all $a\in A^G$ and $g\in G$ we have

$$gf^G(a) = gf(a) = f(ga) = f(a) = f^G(a)$$

and hence $f^G(a)\in B^G$).

Functoriality over morphisms is clear from properties of restrictions. This functor is covariant and additive. Let's also see that it is left-exact. For this, consider a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\varphi"] & B \arrow[r, "\psi"] & C \arrow[r] & 0 \end{tikzcd}$$

in $R[G]$-mod. Our goal is to prove that

$$\begin{tikzcd} 0 \arrow[r] & A^G \arrow[r, "\varphi^G"] & B^G \arrow[r, "\psi^G"] & C^G \end{tikzcd}$$

is exact in R-mod. Clearly the restriction of an injective map is injective and $\psi^G\circ\varphi^G = (\psi\circ\varphi)^G = 0^G = 0$, so that the only non-trivial thing to check here is one remaining inclusion for exactness at B^G. For this, take an element $b\in\ker(\psi^G)\subseteq\ker(\psi)=\operatorname{Im}(\varphi)$, and take $a\in A$ such that $b=\varphi(a)$. We claim that actually $a\in A^G$: to wit, given any $g\in G$ we have

$$\varphi(a-ga) = \varphi(a)-\varphi(ga) = \varphi(a)-g\varphi(a) = b-gb = b-b = 0,$$

and since φ is injective it follows that $a=ga$. Now $g\in G$ was arbitrary, and thus $a\in A^G$. Note that the same argument fails to prove that ψ^G is surjective if

[8] The natural isomorphism here is $\eta\colon(\_)^G \Longrightarrow \operatorname{Hom}_{R[G]}(R,\_)$ defined by $\eta_A(a)(r) = ra$, for all $R[G]$-modules A. We have that $\eta_A(a)$ is $R[G]$-linear precisely because $a\in A^G$. The naturality of η is trivial. The inverse is defined as follows: if $\varphi\colon R\to A$ is $R[G]$-linear, put $a=\varphi(1)$. Then we actually have $a\in A^G$, since for all $g\in G$ we have $ga = g\varphi(1) = \varphi(g1) = \varphi(1) = a$, and so we may compute $\eta_A(a)(r) = ra = r\varphi(1) = \varphi(r)$ for all $r\in R$.

ψ is, since given $c \in C^G$ we may obtain $b \in B$ such that $\psi(b) = c$, but we cannot prove that $b \in B^G$ – the best we can do here is obtain, for every $g \in G$, an element $a_g \in A$ such that $b - gb = \varphi(a_g)$. This leads to the:

Definition: Let G be a group and R be a ring. The *group cohomologies of G over R* are the right-derived functors of $(\_)^G$. Since $(\_)^G \cong \mathrm{Hom}_{R[G]}(R, \_)$, the i-th group cohomology of G with coefficients in a given $R[G]$-module A is then $H^i(G; A) \cong \mathrm{Ext}^i_{R[G]}(R, A)$.

Mar 1$^{\text{st}}$

- **An explicit description for the case $R = \mathbb{Z}$ using complexes:** Build a cochain complex $(C^\bullet(G; A), d^\bullet)$ as follows:
  - For all $n \geq 0$, put $C^n(G; A) \doteq \{\text{functions } G^n = G \times \cdots \times G \to A\}$. Since A is a $\mathbb{Z}[G]$-module, it is an abelian group, and $C^n(G; A)$ inherits this structure. Note that $C^0(G; A) = A$.
  - For all $n \geq 0$, define $d^n \colon C^n(G; A) \to C^{n+1}(G; A)$ by

    $$(d^n\varphi)(g_0, \ldots, g_n) = g_0\varphi(g_1, \ldots, g_n) + \\ + \sum_{i=0}^{n-1} (-1)^{i+1}\varphi(g_0, \ldots, g_{i-1}, g_i g_{i+1}, \ldots, g_n) + (-1)^n \varphi(g_0, \ldots, g_{n-1}).$$

    A standard counting argument gives that $d^{n+1} \circ d^n = 0$.

  In particular, we have that the zeroth differential $d^0 \colon A \to C^1(G; A)$ is given by $(d^0 a)(g) = ga - a$, so that $\ker(d^0) = A^G$, while the first differential $d^1 \colon C^1(G; A) \to C^2(G; A)$ is given by $(d^1\varphi)(g_0, g_1) = g_0\varphi(g_1) - \varphi(g_0 g_1) + \varphi(g_0)$. **Claim:** $H^n(G; A) \cong H^n(C^\bullet(G; A))$.

- **Twisted homomorphism:** Let G be a group and A be a $\mathbb{Z}[G]$-module. A map $\varphi \colon G \to A$ is called a *twisted homomorphism* if $\varphi(gh) = g\varphi(h) + \varphi(g)$ for all $g, h \in G$. By definition, we have $\ker(d^1)$ is precisely the collection of twisted homomorphism from G to A. Moreover, if the action of G on A is trivial (i.e., $A = A^G$), then twisted homomorphism are just usual homomorphisms.

- **Examples:**
  (1) $A = \mathbb{Z}$ is a $\mathbb{Z}[\mathbb{Z}_2]$-module, with $G = \mathbb{Z}_2$ acting trivially. Then we may consider the group cohomologies $H^0(\mathbb{Z}_2; \mathbb{Z})$ and $H^1(\mathbb{Z}_2; \mathbb{Z})$. To compute them, just note since the entire $\mathbb{Z}$ is fixed we have $d^0 = 0$, from which follows that

  $$H^0(\mathbb{Z}_2; \mathbb{Z}) = \mathbb{Z} \quad \text{and} \quad H^1(\mathbb{Z}_2; \mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2; \mathbb{Z}) = 0,$$

  by using again that since the action is trivial, twisted homomorphisms are just homomorphisms.

(2) Now let $G = \{1, -1\}$ act multiplicatively on $A = \mathbb{Z}$. Since no element of $\mathbb{Z} \setminus \{0\}$ is fixed by G, we have $\mathbb{Z}^G = 0$ and so $H^0(G; \mathbb{Z}) = 0$. To compute $H^1(G; \mathbb{Z})$, we have to understand what are the twisted homomorphisms $\varphi\colon \{1, -1\} \to \mathbb{Z}$. We have that $\varphi(1) = \varphi(1 \cdot 1) = 1\varphi(1) + \varphi(1) = 2\varphi(1)$, and so $\varphi(1) = 0$. However, the choice of value for $\varphi(-1)$ is arbitrary, since

$$\begin{aligned} \varphi(-1) = \varphi(-1 \cdot 1) &= -\varphi(1) + \varphi(-1) = \varphi(-1) \quad \text{and} \\ 0 = \varphi(1) &= \varphi((-1)(-1)) = -\varphi(-1) + \varphi(-1) = 0 \end{aligned}$$

give us no new information whatsoever. Thus $\ker(d^1) \cong \mathbb{Z}$, and for all $n \in \mathbb{Z}$ we have $(d^0 n)(1) = 0$ and $(d^0 n)(-1) = -2n$, so that $\mathrm{Im}(d^0) \cong 2\mathbb{Z}$ (both isomorphisms induced by $\varphi \mapsto \varphi(-1)$). So $H^1(G; \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$.

- **Remark:** This is also related to other types of cohomology. For example, f G is a finite group acting trivially on $A = \mathbb{Z}$, then $H^1(G; Z) = H^1(\mathbb{B}G) = H^n_G(\mathrm{pt})$, where the latter are the topological cohomology of the classifying space $\mathbb{B}G$ (*equivariant cohomology*). Or if $G = \mathrm{Gal}(E/F)$ and A is a G-module, then $H^n(G; A)$ is the so-called *Galois cohomology*.

- **Tor:** Recall that given any right R-module M, the functor $M \otimes_R \_\colon R\text{-}\mathsf{mod} \to \mathsf{Ab}$ is right-exact, and its left-derived functors are $\mathrm{Tor}_i^R(M, \_)$. To compute it, we follow the standard procedure: take a left R-module N, choose a projective resolution $P_\bullet \to N$, form the complex $M \otimes_R P_\bullet$ by

$$\cdots \longrightarrow M \otimes_R P_2 \longrightarrow M \otimes_R P_1 \longrightarrow M \otimes_R P_0 \longrightarrow 0,$$

and take the homology $\mathrm{Tor}_i^R(M, N) = H_i(M \otimes_R P_\bullet)$. Again by right-exactness of the tensor functor, we in particular have $\mathrm{Tor}_0^R(M, N) = M \otimes_R N$. And if we have a short exact sequence

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

we obtain the long exact sequence

$$\begin{tikzcd}
 & \cdots \arrow[r] & \mathrm{Tor}_2^R(M, N'') \arrow[dll] & \\
\mathrm{Tor}_1^R(M, N') \arrow[r] & \mathrm{Tor}_1^R(M, N) \arrow[r] & \mathrm{Tor}_1^R(M, N'') \arrow[dll] & \\
M \otimes_R N' \arrow[r] & M \otimes_R N \arrow[r] & M \otimes_R N'' \arrow[r] & 0
\end{tikzcd}$$

- **Tor for flat modules:** Given a right R-module M, the following are equivalent:

  (i) M is flat.

  (ii) $\mathrm{Tor}_i^R(M, N) = 0$ for all $i > 0$ and all left R-modules N.

(iii) $\operatorname{Tor}_1^R(M, N) = 0$ for all left R-modules N.

Proof:

(i) $\Longrightarrow$ (ii) : If M is flat, then $M \otimes_R \_$ is exact. This means that for every left R-module N and any projective resolution $P_\bullet \to N$, the complex

$$\cdots \longrightarrow M \otimes_R P_1 \longrightarrow M \otimes_R P_0 \longrightarrow M \otimes_R N \longrightarrow 0$$

is exact, and it follows that $\operatorname{Tor}_i^R(M, N) = 0$ for all $i > 0$.

(ii) $\Longrightarrow$ (iii) : Trivial.

(iii) $\Longrightarrow$ (i) : Consider a short exact sequence

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0.$$

Our goal is to prove that

$$0 \longrightarrow M \otimes_R N' \longrightarrow M \otimes_R N \longrightarrow M \otimes_R N'' \longrightarrow 0$$

is exact. This is precisely the end of the long exact sequence for Tor, since $\operatorname{Tor}_1^R(M, N) = 0$. We are done.

□

- **Bifunctoriality of Tor:** For a left R-module N, one could also define $\widetilde{\operatorname{Tor}}_i^R(\_, N)$ as the left-derived functors of $\_ \otimes_R N$. We again have natural isomorphisms $\operatorname{Tor}_i^R(M, N) \cong \widetilde{\operatorname{Tor}}_i^R(M, N)$.

Galois Theory

Mar 20th

- **Theme and History:** A natural goal to pursue is to solve polynomial equations. For degree 2 polynomials we have the quadratic formula, while for degree 3 polynomials $x^3 + ax^2 + bx + c$, which can always be depressed to the simpler form $x^3 + px + q$, we have Cardano's formula (actually due to Tartaglia, ∼1540's). There is also Ferrari's formula for the degree 4 case. But not for degree 5: Abel (1827) and Ruffini (1813) proved that the general quintic *cannot* be solved for radicals. Galois (1832) gave an analysis of this face via *symmetries*. Why care about radicals? Again one possible answer is because these illustrate symmetries of the equation (e.g., complex roots of polynomials with real coefficients come in conjugate pairs).

  The idea to discuss this efficiently is to explore correspondences:

  $$\begin{aligned} \text{field theory} &\longleftrightarrow \text{group theory} \\ \text{extension fields } E/F &\longleftrightarrow \text{Galois groups } \mathrm{Gal}(E/F) \\ \text{towers of extensions } E \supseteq K \supseteq F &\longleftrightarrow \mathrm{Gal}(E/K) \subseteq \mathrm{Gal}(E/F) \text{ (reverse inclusions)} \end{aligned}$$

  and more. There is a strong analogy between Galois groups for extension fields and fundamental groups (as deck transformations of covering spaces) in Algebraic Topology.

- **Basic Field Theory:** We start with some terminology and conventions.
  - A *field* is always commutative.
  - The degree of the zero polynomial is $-\infty$.
  - A ring where every nonzero element has an inverse is a *division ring* (or *skew-field*).
  - If E and F are fields with $F \subseteq E$, we say that F is a *subfield* of E or, equivalently, that E is an *extension field* of F. We write E/F (since we will never consider quotients of fields, this notation won't cause confusion). Still in this setup, given elements $\alpha_1, \alpha_2, \ldots \in E$, the field obtained from F by *adjoining* these elements if $F(\alpha_1, \alpha_2, \ldots) \subseteq E$, the smallest subfield of E containing F and all the α's. Do note that the set of adjoined elements need not be countable.
  - The *degree* of a field extension E/F, denoted by $[E : F]$ (to echo the index of a subgroup, in group theory), is defined to be $\dim_F E$ (the dimension of E as a vector space over F). When $[E : F] < +\infty$, we say that E/F is a *finite* extension.

- **Example:** $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Then $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ because $\{1, \sqrt{2}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2})$.

- **Tower Law:** Suppose $F \subseteq K \subseteq E$ are fields. Then $[E : F] = [E : K][K : F]$.

Proof: Choose bases $\{u_i\}_{i\in I}$ and $\{v_j\}_{j\in J}$ for K/F and E/K, respectively. We will show that $\{u_iv_j\}_{(i,j)\in I\times J}$ is a basis for E/F. That is spans E over F is clear. So we only have to check that it is linearly independent. Indeed, if $(a_{ij})_{(i,j)\in I\times J}$ is a family of elements in F, all but finitely many of them zero, then

$$\sum_{(i,j)\in I\times J} a_{ij}u_iv_j = 0 \implies \sum_{j\in J}\left(\sum_{i\in I} a_{ij}u_i\right)v_j = 0 \implies \sum_{i\in I} a_{ij}u_i = 0 \implies a_{ij} = 0,$$

for all $(i,j) \in I\times J$. □

- **Algebraic elements:** Given a field extension E/F, we say that an element $\alpha \in E$ is *algebraic over F* is there is a polynomial $f(x) \in F[x]$ with $f(\alpha) = 0$. If all elements of E are algebraic over F, the extension E/F is called *algebraic*.

- **Minimal polynomials:** Given a field extension E/F and $\alpha \in E$ algebraic over F, its *minimal polynomial (over F)* is the monic polynomial $f(x) \in F[x]$ with $f(\alpha) = 0$, having minimal degree.

  Claim: the minimal polynomial is completely determined by these conditions, and it is also irreducible in $F[x]$.

  Proof: Suppose $g(x) \in F[x]$ is another polynomial with $g(\alpha) = 0$. Then we have $\deg g \geq \deg f$, and so we may write $g(x) = f(x)q(x) + r(x)$ with polynomials $q(x), r(x) \in F[x]$ and $\deg r < \deg f$. If $r(x) \neq 0$, evaluating at α gives $r(\alpha) = 0$, contradicting the minimality of $\deg f$. Hence $r(x) = 0$ and $f(x) \mid g(x)$. Irreducibility follows from $0 = f(\alpha) = f_1(\alpha)f_2(\alpha)$ implying $f_1(\alpha) = 0$ or $f_2(\alpha) = 0$, with $\deg f_i < \deg f$, $i = 1, 2$. □

- **Example:** Consider the extension $\mathbb{R}/\mathbb{Q}$ and $\alpha = \sqrt{3-\sqrt{6}}$. Since

  $$\alpha^2 = 3-\sqrt{6} \implies \alpha^2 - 3 = -\sqrt{6} \implies \alpha^4 - 6\alpha^2 + 9 = 6 \implies \alpha^4 - 6\alpha^2 + 3 = 0,$$

  we consider $f(x) \in \mathbb{Q}[x]$ given by $f(x) = x^4 - 6x^2 + 3$. From Eisenstein's criterion ($p = 3$), $f(x)$ is irreducible over $\mathbb{Q}$. Thus $f(x)$ is the minimal polynomial of α over $\mathbb{Q}$.

- **Splitting fields:** Conversely, given a monic polynomial $f(x) \in F[x]$ of degree n, a *splitting field* of $f(x)$ is an extension E/F so that

  $$f(x) = (x-\alpha_1)\cdots(x-\alpha_n),$$

  with $\alpha_1, \ldots, \alpha_n \in E$, and minimal for this property (so that $E = F(\alpha_1, \ldots, \alpha_n)$).

- **Remark:** Above, note that it only makes sense to talk about $F(\alpha_1, \ldots, \alpha_n)$ once we already have E, as $\alpha_1, \ldots, \alpha_n \in E$. Any possible dependence on E is implicit in the notation.

- **Example:** A splitting field for $x^2 - 2 \in \mathbb{Q}[x]$ is $\mathbb{Q}(\sqrt{2})$, since there we have the factorization $x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2}) \in \mathbb{Q}(\sqrt{2})[x]$.

- **Lemma (Kronecker):** Given a field F and $f(x) \in F[x]$, there is an extension E/F so that $f(x)$ has a root in E.

  Proof: We may assume that $f(x)$ is irreducible (a root of any factor of $f(x)$ is a root of $f(x)$), so that $(f(x)) \subseteq F[x]$ is a maximal ideal, since $F[x]$ is a PID. Then $E = F[x]/(f(x))$ is a field, and $\alpha \doteq \overline{x} \in E$ satisfies $f(\alpha) = 0$ by construction. □

- **Remark:** In the setup of the above Lemma, $E = F[\alpha] = \{g(\alpha) \mid g(x) \in F[x]\}$, that is, ring-adjunction is the same as field-adjunction. Also, note here that we have $F[\alpha] \cong F[x]/(m(x))$, where $m(x)$ is the (monic) minimal polynomial of α.

- **Existence of splitting fields:** Given any field F, every monic polynomial $f(x) \in F[x]$ has a splitting field.

  Proof: Write $f(x) = f_1(x)\cdots f_r(x) \in F[x]$ as a product of irreducible monic factors. If all these factors are linear, we are done. Else, assume (reordering if necessary) that $\deg f_1 > 1$, and let F_1/F be a field extension where $f_1(x)$ has a root (by Kronecker). Now, factor $f_1(x), \ldots, f_r(x)$ over $F_1[x]$. The degrees of the new irreducible factors have decreased at least by one, since we may write $f_1(x) = (x - \alpha_1)\widetilde{f_1}(x)$, for some $\alpha_1 \in F_1$ and $\widetilde{f_1}(x) \in F_1[x]$. This means we may proceed by induction until stopping at a field extension F_k/F for which

  $$f(x) = (x - \alpha_1)\cdots(x - \alpha_n),$$

  with $\alpha_1, \ldots, \alpha_n \in F_k$. This F_k is not necessarily a splitting field for $f(x)$, as it might be too big: take $E = F(\alpha_1, \ldots, \alpha_n) \subseteq F_k$ instead. □

- **Splitting fields are unique up to isomorphism:** Let F and F' be fields and $\sigma\colon F \to F'$ be a field isomorphism. If $f(x) \in F[x]$ and $f'(x) \in F'[x]$ are polynomials with splitting fields E/F and E'/F' such that the extension of σ to a homomorphism $F[x] \to F'[x]$ maps $f(x)$ to $f'(x)$, then σ further extends to an isomorphism $\hat{\sigma}\colon E \to E'$:

  $$\begin{tikzcd} E \arrow[r, dashed, "\hat{\sigma}"] \arrow[d, dash] & E' \arrow[d, dash] \\ F \arrow[r, "\sigma"] & F' \end{tikzcd}$$

  Observe that such extension need not be unique.

Mar 22nd

- **Lemma:** Let E/F be a field extension and $\alpha \in E$ be algebraic over F, with minimal polynomial $f(x) \in F[x]$. If E'/F is any field extension, then a field isomorphism $\sigma\colon F \to F'$ extends to an embedding $F(\alpha) \hookrightarrow E'$ if and only if the image $g'(x)$ of $g(x)$ has a root in E'. In such case, there are #{distinct roots of $g'(x)$ in E'} such embeddings.

Proof: If σ extends to $\hat{\sigma}\colon F(\alpha) \hookrightarrow E'$, then $\hat{\sigma}$ still maps 0 to 0 and so we obtain $g'(\hat{\sigma}(\alpha)) = \hat{\sigma}(g(\alpha)) = \hat{\sigma}(0) = 0$. Conversely, assume that $g'(x)$ has a root $\alpha' \in E'$. This determines an embedding $F(\alpha) \hookrightarrow E'$, via composition with the induced isomorphism that maps $\alpha \mapsto \alpha'$:

$$F(\alpha) = \frac{F[x]}{(g(x))} \xrightarrow{\ \simeq\ } \frac{F'[x]}{(g'(x))} = F'[\alpha'] \hookrightarrow E'.$$

Since distinct roots of $g'(x)$ in E' produce distinct embeddings, we have at least such many embeddings. "At most" such embeddings actually follows from the start of the argument (any embedding produces a root of $g'(x)$). This concludes the count.

$$\begin{tikzcd}
E & E' \\
F(\alpha) \arrow[u, dash] \arrow[ur, hook] & \\
F \arrow[u, dash] \arrow[r, "\sigma"] & F' \arrow[uu, dash]
\end{tikzcd}$$

□

- **Proof of "uniqueness" of splitting fields:** We'll proceed by induction on the number n of roots of $f(x)$ *not* in F. The base of the induction is the when where all the roots of $f(x)$ lie on F, in which case $E = F$ and $E' = F'$. For the induction step, factor $f(x) = f_1(x)\cdots f_r(x)$ as a product of irreducible polynomials in $F[x]$. Then we also have (by applying σ) that $f'(x) = f_1'(x)\cdots f_r'(x)$, where $f_1'(x),\ldots,f_r'(x) \in F'[x]$ are irreducible. Reordering if needed, assume $\deg f_1 > 1$, and let $\alpha_1 \in E$ be a root of $f_1(x)$. The previous lemma extends σ to an isomorphism $\sigma_1\colon F(\alpha_1) \xrightarrow{\simeq} F'(\alpha_1') \subseteq E'$ (since $\alpha_1' \doteq \sigma(\alpha_1)$ is a root of $f_1'(x)$ in E'). With this, the number of roots of $f(x)$ not in $F(\alpha_1)$ is less than n, and the induction hypothesis kicks in to give us an extension $\hat{\sigma}\colon E \xrightarrow{\simeq} E'$ of σ_1 (which is automatically an isomorphism).

$$\begin{tikzcd}
E \arrow[r, dashed, "\sigma"] & E' \\
F(\alpha_1) \arrow[u, dash] \arrow[ur, hook] \arrow[r, "\sigma_1"] & F'(\alpha_1') \arrow[u, dash] \\
F \arrow[u, dash] \arrow[r, "\sigma"] & F' \arrow[u, dash]
\end{tikzcd}$$

□

- **Linear independence of characters:** If G is a group and F is a field, a *character* of G with values in F is a group homomorphism $\sigma\colon G \to F^\times$. Characters $\sigma_1,\ldots,\sigma_n$ are *linearly dependent* if there are $a_1,\ldots,a_n \in F$, not all of them zero, such that

$$a_1\sigma_1 + \cdots + a_n\sigma_n = 0 \qquad (\text{as maps } G \to F^\times)$$

The characters are *linearly independent* otherwise.

Claim: If $\sigma_1,\ldots,\sigma_n\colon G\to F^\times$ are *distinct* characters, they are automatically linearly independent.

Proof: If $n=1$, a single character is linearly independent (to wit, $a_1\sigma_1=0$, so choose any $g\in G$ and compute $a_1\sigma_1(g)=0$; since $\sigma_1(g)\neq 0$ we have $a_1=0$).

Now assume $n>1$, that every set with less than n characters of G is linearly independent and, by contradiction, that $\sigma_1,\ldots,\sigma_n$ are linearly dependent. Take $a_1,\ldots,a_n\in F$, not all of them zero, such that

$$a_1\sigma_1+\cdots+a_n\sigma_n=0.$$

The induction hypothesis actually ensures that *none* of the coefficients a_i is zero, so we can rescale the above by dividing by $1/a_n$, obtaining

$$b_1\sigma_1+\cdots+b_{n-1}\sigma_{n-1}+\sigma_n=0,$$

where $b_i=a_i/a_n$ for $i=1,\ldots,n-1$. Also, we may take an element $x\in G$ with $\sigma_1(x)\neq\sigma_n(x)$ (such x exists because σ_1 and σ_n are distinct). Take arbitrary $g\in G$, evaluate the above expression at xg (using that all the σ_i's are multiplicative) and divide through by $\sigma_n(x)$ to obtain

$$\begin{aligned}0&=\sigma_n(x)^{-1}\big(b_1\sigma_1(xg)+\cdots+b_{n-1}\sigma_{n-1}(xg)+\sigma_n(xg)\big)\\&=b_1\frac{\sigma_1(x)}{\sigma_n(x)}\sigma_1(g)+\cdots+b_{n-1}\frac{\sigma_{n-1}(x)}{\sigma_n(x)}\sigma_{n-1}(g)+\sigma_n(g)\end{aligned}$$

We can use this and the previous expression to eliminate σ_n, leading to

$$0=b_1\left(1-\frac{\sigma_1(x)}{\sigma_n(x)}\right)\sigma_1+\cdots+b_{n-1}\left(1-\frac{\sigma_{n-1}(x)}{\sigma_n(x)}\right)\sigma_{n-1}.$$

This $b_i(1-\sigma_i(x)/\sigma_n(x))=0$ for $i=1,\ldots,n-1$. Since each a_i does not vanish, the same holds for b_i. Then $\sigma_i(x)=\sigma_n(x)$ for all $i=1,\ldots,n-1$, and the particular equality $\sigma_1(x)=\sigma_n(x)$ contradicts our choice of x. We are done. □

- **Corollary:** If E and E' are fields, and $\sigma_1,\ldots,\sigma_n$ are given distinct embeddings $E\hookrightarrow E'$, then $\sigma_1,\ldots,\sigma_n$ are linearly independent when regarded as characters $E^\times\to(E')^\times$.

- **Fixed points and subfields:** Let E and E' be fields, and $\{\sigma_1,\ldots,\sigma_n\}$ a collection of embeddings $E\hookrightarrow E'$. A *fixed point* for this set is a point $a\in E$ such that $\sigma_1(a)=\cdots=\sigma_n(a)$. The *fixed field* is the collection of the fixed points[9].

- **Main example:** If $E=E'$ and all the σ_i's are automorphisms, with $\sigma_1=\mathrm{Id}_E$, then $a\in E$ is a fixed point if $\sigma_i(a)=a$ for all i.

[9] This is indeed a field: the only non-trivial verification is that if a is fixed, then so is a^{-1}. If we start with $\sigma_1(a)=\cdots=\sigma_n(a)$, inverting everything gives $\sigma_1(a)^{-1}=\cdots=\sigma_n(a)^{-1}$. Since all the σ_i's are multiplicative, it follows that $\sigma_1(a^{-1})=\cdots=\sigma_n(a^{-1})$, as wanted.

- **Theorem:** If $\sigma_1, \ldots, \sigma_n \colon E \hookrightarrow E'$ are *distinct* embeddings and $F \subseteq E$ is the fixed subfield of $\{\sigma_1, \ldots, \sigma_n\}$, then $[E : F] \geq n$.

  Proof: If $[E : F] = +\infty$, done. Else, assume by contradiction that $\{\alpha_1, \ldots, \alpha_r\}$ is a basis for E/F with $r < n$. Consider the system of equations

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_1)x_n = 0 \\ \vdots \\ \sigma_1(\alpha_r)x_1 + \cdots + \sigma_n(\alpha_r)x_n = 0. \end{cases}$$

  Since $r < n$, this has a non-trivial solution $(a_1, \ldots, a_n) \in F^n$. We will use this to produce a non-trivial dependence relation between the given embeddings, which will gives us the desired contradiction (using that the embeddings are distinct to apply the last corollary). Let $\alpha \in E$ be any element, and write $\alpha = c_1\alpha_1 + \cdots + c_r\alpha_r$, with $c_1, \ldots, c_r \in F$. Since each c_i is a fixed point of $\{\sigma_1, \ldots, \sigma_n\}$, we may multiply the i-th equation of the system above by c_i and obtain

$$\begin{cases} \sigma_1(c_1\alpha_1)a_1 + \cdots + \sigma_n(c_1\alpha_1)a_n = 0 \\ \vdots \\ \sigma_1(c_r\alpha_r)a_1 + \cdots + \sigma_n(c_r\alpha_r)a_n = 0. \end{cases}$$

  Adding these equations yield

$$a_1\sigma_1(\alpha) + \cdots + a_n\sigma_n(\alpha) = 0,$$

  and we are done since $\alpha \in E$ was arbitrary. □

- **Corollary/definition:** Let E/F be a field extension, and G be the group of automorphisms of E fixing F. Then $[E : F] \geq |G|$. The group G is called the *Galois group* of E/F, and it is denoted by $\mathrm{Gal}(E/F)$.

- **Remark:** In the above definition, note that the fixed field of $\mathrm{Gal}(E/F)$ might be *strictly* bigger than F. This is an important point, and we will come back to that later.

- **Examples:**

  (1) Consider the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. If $\varphi \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, then

$$\varphi(a + b\sqrt{2}) = \varphi(a) + \varphi(b)\varphi(\sqrt{2}) = a + b\varphi(\sqrt{2}),$$

  so that φ is determined by $\varphi(\sqrt{2})$. Since $2 = \varphi(2) = \varphi(\sqrt{2}^2) = \varphi(\sqrt{2})^2$ gives $\varphi(\sqrt{2}) = \pm 2$ and both the identity and

$$\mathbb{Q}(\sqrt{2}) \ni a + b\sqrt{2} \mapsto a - b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

  are automorphisms of $\mathbb{Q}(\sqrt{2})$ fixing $\mathbb{Q}$, we may conclude that the Galois group of this extension is $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}_2$. Similarly one can prove that $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}_2$.

(2) Consider now the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Since the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is x^3-2, we conclude that $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$ and that $\{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$ is a basis for $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Now, if $\varphi \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, like before we obtain

$$\varphi(a+b\sqrt[3]{2}+c\sqrt[3]{2^2}) = a + b\varphi(\sqrt[3]{2}) + c\varphi(\sqrt[3]{2})^2,$$

so that φ is determined by the value $\varphi(\sqrt[3]{2})$. Now, φ should permute the roots of x^3-2 in $\mathbb{Q}(\sqrt[3]{2})$. But $\sqrt[3]{2}$ is the only such root (namely, the other ones are complex roots), so we conclude that φ also fixes $\sqrt[3]{2}$ and hence φ is the identity. Thus $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is trivial.

Mar 25th

- **Normal and separable extensions:**
  - A field extension E/F is *normal* whenever any given irreducible polynomial $f(x) \in F[x]$ has a root in E, it splits over E. In other words, if there is $\alpha_1 \in E$ such that $f(\alpha_1) = 0$, then $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ for $\alpha_1, \ldots, \alpha_n \in E$ (and c necessarily in F, at is is the leading coefficient of a polynomial in $F[x]$).
  - A polynomial $f(x) \in F[x]$ is *separable* if it splits into distinct linear factors over its splitting field E/F. That is, in $E[x]$ we may completely factor $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in E$ pairwise distinct. In other words, there exists an extension E/F such that $f(x)$ has $n = \deg f$ distinct roots in E.
  - Given a field extension E/F, an element $\alpha \in E$ is *separable* (over F) if its minimal polynomial is separable over F.
  - A field extension E/F is separable if every element in E is separable over F.

- **Examples:**

  (1) If p is a prime number, the polynomial $x^p - a \in \mathbb{F}_p[x]$ is not separable if a is not a p-th power in $\mathbb{F}_p$, since if $a = b^p$, then $x^p - a = x^p - b^p = (x-b)^p$ (by the Freshman's Dream).

  (2) The polynomial $x^p - t \in \mathbb{F}_p(t)[x]$ is not separable. Thus, the extension $\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$ is not separable.

- **Galois extensions:** An algebraic extension E/F is a *Galois extension* if it is both normal and separable.

- **Theorem (Artin):** Suppose that E/F is a finite extension. The following are equivalent:

  (i) E/F is Galois.

  (ii) The fixed field of $\mathrm{Gal}(E/F)$ is precisely F.

  (iii) E is the splitting field of a separable polynomial in $F[x]$.

In what follows, we will work towards a proof of this theorem.

- **Lemma:** Let $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ be a finite groups of automorphisms of a field E, and let E^G be its fixed field. Then $[E : E^G] = |G|$.

  Proof: Assume by contradiction that $[E : E^G] > n$ and let $\alpha_1, \ldots, \alpha_{n+1} \in E$ be linearly independent over E^G. Consider the homogeneous linear system

$$\begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_{n+1}) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_{n+1}) \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_{n+1} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

  Take a non-trivial solution $(x_1, \ldots, x_{n+1}) \in E^{n+1}$ of this system. Note that we cannot have all the x_i's in E^G, as the equation of the above system corresponding to the identity would read $\alpha_1 x_1 + \cdots + \alpha_{n+1} x_{n+1} = 0$, contradicting the linear independence of the α_i's over E^G.

  With this, be rescaling the solution (the system is homogeneous) and further permuting $\sigma_1, \ldots, \sigma_n$, we may assume that

$$(x_1, \ldots, x_{n+1}) = (a_1, \ldots, a_{r-1}, 1, 0, \ldots, 0)$$

  with $a_1, \ldots, a_{r-1} \neq 0$ and $a_1 \in E \setminus E^G$, for some r minimal for these properties. Do note that we could have $r = n+1$ here (i.e., the solution we chose could have no zeros whatsoever). We will conclude the contradiction argument by producing another non-trivial solution for the system with less that r non-zero elements. Our solution satisfies

$$a_1 \sigma_i(\alpha_1) + \cdots + a_{r-1} \sigma_i(\alpha_{r-1}) \sigma_i(a_r) = 0$$

  for all $i = 1, \ldots, n$. Now, there is k such that $\sigma_k(a_1) \neq a_1$ (else, $a_1 \in E^G$). Applying this particular σ_k on the above relation and reindexing all the elements in G (for $\sigma_k \circ \sigma_i \mapsto \sigma_i$ is a bijection), we conclude that

$$\sigma_k(a_1)\sigma_1(\alpha_1) + \cdots + \sigma_k(a_{r-1})\sigma_i(\alpha_{r-1}) + \sigma_i(\alpha_r) = 0$$

  for all $i = 1, \ldots, n$. Subtraction yields

$$(a_1 - \sigma_k(a_1))\sigma_i(\alpha_1) + \cdots + (a_{r-1} - \sigma_k(a_{r-1}))\sigma_i(\alpha_{r-1}) = 0,$$

  and $(a_1 - \sigma_k(a_1), \ldots, a_{r-1} - \sigma_k(a_{r-1}), 0, \ldots, 0) \neq \mathbf{0}$ has less than r non-zero entries. We are done. □

- **Corollary:** If G is a finite group of automorphisms of E, then $G = \mathrm{Gal}(E/E^G)$.

  Proof: By definition, $G \subseteq \mathrm{Gal}(E/E^G)$. The above result says that $[E : E^G] = |G|$, but we also have seen that $[E : F] \geq |\mathrm{Gal}(E/E^G)|$. Thus $|G| \geq |\mathrm{Gal}(E/E^G)|$ gives us the remaining inclusion, and we conclude that $G = \mathrm{Gal}(E/E^G)$ as wanted. □

- **Corollary:** If G_1 and G_2 are distinct finite groups of automorphisms of a field E, then $E^{G_1} \neq E^{G_2}$.

  Proof: If $E^{G_1} = E^{G_2}$, the previous corollary would give $G_1 = G_2 = \mathrm{Gal}(E/E^{G_1})$. □

Mar 27th

- **Proof of Artin's Theorem:** We'll verify the following three implications:

  (i) $\Longrightarrow$ (iii) : Take a basis $\{\alpha_1, \ldots, \alpha_t\}$ for E/F, and let $f_i(x) = \min(\alpha_i, F)(x)$. Note that each $f_i(x)$ is separable, since E/F is a separable extension (indeed, each α_i is a root of a separable polynomial in $E[x]$, which is then divided by $f_i(x)$, showing that the latter is also separable). Now, eliminate the repetitions and consider $\{f_1(x), \ldots, f_r(x)\} = \{f_1(x), \ldots, f_t(x)\}$, with $f_1(x), \ldots, f_r(x)$ pairwise distinct, and consider E' the splitting field of the separable polynomial $f_1(x) \cdots f_r(x)$ over F (separability here follows from the linear independence of the α's). Since E/F is normal, we have $E' \subseteq E$. But since E' contains the basis $\{\alpha_1, \ldots, \alpha_t\}$, we also have $E \subseteq E'$. Thus $E = E'$ and we are done.

  (iii) $\Longrightarrow$ (ii) : Assume that E is the splitting field of a separable polynomial $f(x) \in F[x]$. If all the roots of $f(x)$ already lie in F, then $E = F$ and we have that $\mathrm{Gal}(E/F) = \{\mathrm{Id}_E\}$. Else, we proceed by induction on the number $n \geq 1$ of roots of $f(x)$ outside F, assuming that result is true for all extensions and polynomials with less than n roots outside the base field F. Factor $f(x) = f_1(x) \ldots f_r(x)$ as a product of irreducible factors in $F[x]$. Let $s = \deg f_1 > 1$ (by reordering the factors if needed) and $\alpha_1 \in E$ be a root of $f_1(x)$, so that $[F(\alpha_1) : F] = \deg f_1$ (since $f_1(x) = \min(\alpha_1, F)(x)$). Now, $E/F(\alpha_1)$ is a splitting field for $f(x) \in F(\alpha_1)[x]$, but $f(x)$ has less than n roots outside $F(\alpha_1)$. The induction hypothesis gives that the fixed field of $\mathrm{Gal}(E/F(\alpha_1))$ is precisely $F(\alpha_1)$.

  To proceed, recall that the roots $\alpha_1, \ldots, \alpha_s \in E$ of $f_1(x)$ are pairwise distinct, and so we obtain automorphisms $\sigma_1, \ldots, \sigma_s \in \mathrm{Gal}(E/F)$ with $\sigma_i(\alpha_1) = \alpha_i$, for all i (indeed, we have maps $F(\alpha_1) \to F(\alpha_i)$ which extend to the splitting fields, $E \to E$). Since the fixed field of $\mathrm{Gal}(E/F)$ always contains F, we will conclude the proof of this implication by verifying the remaining inclusing directly: let $\beta \in E$ be fixed by all of $\mathrm{Gal}(E/F)$. Our goal is to prove that $\beta \in F$. Since $\mathrm{Gal}(E/F) \supseteq \mathrm{Gal}(E/F(\alpha_1))$, we automatically get that

$$\beta \in E^{\mathrm{Gal}(E/F)} \subseteq E^{\mathrm{Gal}(E/F(\alpha_1))} = F(\alpha_1),$$

  which allows us to write $\beta = c_0 + c_1\alpha_1 + \cdots + c_{s-1}\alpha_1^{s-1}$, for certain coefficients $c_0, \ldots, c_{s-1} \in F$. Applying all of the σ_i previously considered gives that

$$\beta = \sigma_i(\beta) = c_0 + c_1\alpha_i + \cdots + c_{s-1}\alpha_i^{s-1}, \qquad \text{for all } i.$$

This says that the degree $s-1$ polynomial

$$g(x) = (c_0 - \beta) + c_1 x + \cdots + c_{s-1}x^{s-1} \in F(\alpha_1)[x]$$

has s distinct roots $\alpha_1, \ldots, \alpha_s$. This forces $g(x) = 0$, so that $\beta = c_0 \in F$, as wanted.

(ii) $\Longrightarrow$ (i) : Assume that the fixed field of $\mathrm{Gal}(E/F)$ is precisely F, and write $\mathrm{Gal}(E/F) = \{\sigma_1 = \mathrm{Id}_E, \sigma_2, \ldots, \sigma_s\}$ (note that $\mathrm{Gal}(E/F)$ is indeed finite, since $|\mathrm{Gal}(E/F)| \leq [E:F] < +\infty$, by assumption). We will prove first that E/F is separable. Take $\alpha = \alpha_1 \in E$, and consider $\alpha_1, \ldots, \alpha_r$ the distinct *Galois conjugates* of α, defined by $\alpha_1 = \sigma_1(\alpha), \ldots, \alpha_s = \sigma_s(\alpha)$ (i.e., we eliminate repetitions and consider the $\mathrm{Gal}(E/F)$-orbit of α). The separable polynomial

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_r)$$

actually has coefficients in F, since it is invariant under $\mathrm{Gal}(E/F)$ (whose fixed field is F, by assumption). If $g(x) \in F[x]$ is any polynomial having $g(\alpha_1) = 0$ also satisfies $g(\alpha_i) = 0$ (apply σ_i), and so $f(x) \mid g(x)$. This shows that $f(x) = \min(\alpha, F)(x)$, and we conclude that E/F is separable, since the element $\alpha \in E$ was arbitrary. A similar reasoning as above starting with irreducible $g(x)$ and a root $\alpha_1 \in E$ shows that E/F is separable, as E contains the splitting field of $f(x)$.

□

- **Corollary:** Let E/F be a finite and Galois extension. Then for every *intermediate field* $F \subseteq K \subseteq E$, the extension E/K is also Galois.

  Proof: By the tower law, E/K is a finite extension, so that Artin's Theorem applies: E is the splitting field of a separable polynomial in $F[x]$, which is also in $K[x]$. Then E/K is Galois. □

- **Galois Theory slogan:** If E/F is a finite and Galois extension, then subgroups of $\mathrm{Gal}(E/F)$ correspond to intermediate fields $F \subseteq K \subseteq E$.

- **Fundamental Theorem of Galois Theory (finite case):** Let E/F be a finite and Galois field extension. Then:

  (i) Every intermediate field $F \subseteq K \subseteq E$ is the fixed field of a unique subgroup $G_K \subseteq \mathrm{Gal}(E/F)$. In other words, the *Galois correspondence* is a bijection

  $$\{\text{subgroups of } \mathrm{Gal}(E/F)\} \ni G_K \leftrightarrow E^{G_K} = K \in \{\text{intermediate fields of } E/F\}.$$

  (ii) The following are equivalent:

  (a) K/F is Galois.

  (b) K/F is normal.

  (c) $G_K \lhd \mathrm{Gal}(E/F)$ (in this case, $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/G_K$).

  (iii) For every intermediate field $F \subseteq K \subseteq E$, we have

  $$[K:F] = [\mathrm{Gal}(E/F) : G_K] = |\mathrm{Gal}(E/F)/G_K| \quad \text{and} \quad [E:K] = |G_K|.$$

- **Remark:** The Galois correspondence is *inclusion reversing*.

Mar 29th

- **Proof of Fundamental Theorem:**

  (i) Since distinct subgroups of $\mathrm{Gal}(E/F)$ have distinct fixed fields (here we use that E/F is finite), the map that takes a subgroup H of $\mathrm{Gal}(E/F)$ to the fixed subfield E^H of E is injective. Said map is also surjective since E/F is Galois: given an intermediate field $F \subseteq K \subseteq E$, E/K is also Galois and so $\mathrm{Gal}(E/K) \mapsto K$.

  (ii) That (a) is equivalent to (b) is clear (since separability of an extension is an elementwise property). So we'll show that (b) is equivalent to (c). Start noting that embeddings $K \hookrightarrow E$ which fix F correspond to cosets $\mathrm{Gal}(E/K)/G_K$ (for any $\sigma \in \mathrm{Gal}(E/K)$ and $\tau \in G_K$, we have $[\sigma\tau] = [\sigma]$ and so $\sigma\tau(K) = \sigma(K)$).

  Also, note that $\sigma(K) = E^{\sigma G_K \sigma^{-1}}$. Indeed, if $x \in K$, we directly compute that $\sigma\tau\sigma^{-1}(\sigma(x)) = \sigma\tau(x) = \sigma(x)$ for all $\tau \in G_K$, which shows the inclusion $\sigma(K) \subseteq E^{\sigma G_K \sigma^{-1}}$. On the other hand, if $x \in E^{\sigma G_K \sigma^{-1}}$, we take $\tau \in G_K$ and write $x = \sigma(\tau(\sigma^{-1}(x)))$, noting that $\sigma^{-1}(x) \in K$ because $\tau \in G_K$. This proves the remaining inclusion.

  Thus $G_K \lhd \mathrm{Gal}(E/F)$ if and only if $K = \sigma(K)$ for all $\sigma \in \mathrm{Gal}(E/F)$. The proof is concluded once we check that on the other hand, K/F is Galois (hence normal, by (a)) if and only if $\sigma(K) = K$ for all $\sigma \in \mathrm{Gal}(E/F)$. Indeed:

  - If a separable polynomial $f(x) \in F[x]$ has K as a splitting field, then $f(x)$ also splits over E, and $\sigma \in \mathrm{Gal}(E/F)$ permutes the roots of $f(x)$. So $\sigma(K) = K$, because the the roots of $f(x)$ generate K.
  - Suppose K/F is not normal and take $\alpha \in K$ for which $\min(\alpha, F)(x)$ has a root $\alpha' \notin K$. There is $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(\alpha) = \alpha'$, and so $\sigma(K) \neq K$.

  (iii) We have seen that $[E : F] = |\mathrm{Gal}(E/F)|$ for finite extensions, and in fact $[E : K] = |G_K|$ whenever $K = E^{G_K}$, for any subgroup G_K of $\mathrm{Gal}(E/F)$. The first formula in the statement follows from the first one by applying the tower law: $[E : F] = [E : K][K : F]$ implies that

  $$[K : F] = \frac{[E : F]}{[E : K]} = \frac{|\mathrm{Gal}(E/F)|}{|G_K|} = \left|\frac{\mathrm{Gal}(E/F)}{G_K}\right| = [\mathrm{Gal}(E/F) : G_K],$$

  as wanted.

- **Terminology:** Given subfields K, L of a given field E, their *intersection* is the subfield $K \cap L$, and their *compositum* is the smallest subfield $K \cdot L$ containing both K and L. Note that the compositum is well-defined, since arbitrary intersections of subfields of E is again a subfield of E.

$$\begin{tikzcd}
 & K \cdot L \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & L \arrow[dl, dash] \\
 & K \cap L &
\end{tikzcd}$$

Similarly, if H, K are subgroups of a group G, we have their intersection $H \cap K$ and their compositum $H \cdot K$ – the smalles subgroup of G containing both H and K (do not confuse this with $HK = \{hk \mid h \in H, k \in K\}$, which is only a subgroup of G if H or K is normal in G). These operations of intersection and compositum turn both the collection of subfields of E and subgroups of G into lattices, ordered by inclusion.

- **Corollary:** Let E/F be a finite and Galois field extension. If Λ and Λ' are, respectively, the lattices of intermediate subfields of E/F and subgroups of $\mathrm{Gal}(E/F)$, then Λ and Λ' are dual under $(F \subseteq K \subseteq E) \mapsto (\mathrm{Gal}(E/F) \supseteq G_K \supseteq \{e\})$. In particular, we have $G_{K \cdot K'} = G_K \cap G_{K'}$ and $G_{K \cap K'} = G_K \cdot G_{K'}$.

- **Quadratic extensions:** Let F be a field with $\operatorname{char} F \neq 2$, and $f(x) = x^2 - a \in F[x]$. If a is not a square in F, then $f(x)$ is irreducible. The splitting field E/F of $f(x)$ is Galois, $E = F(\beta)$ with $\beta \in E$ satisfying $\beta^2 = a$, and $\mathrm{Gal}(E/F) \cong \mathbb{Z}/2\mathbb{Z}$ is generated by $\beta \mapsto -\beta$.

  Conversely, any degree 2 extension of F (again assumed with $\operatorname{char} F \neq 2$) comes by adjoining a square root of β of some element $a \in F$. Indeed, given any element $\alpha \in E \setminus F$, $\{1, \alpha\}$ is a basis for E/F and we consider $f(x) = \min(\alpha, F)(x)$. Completing the square gives $x^2 - a$.

Apr 1st

- **Remark:** If E/F is a finite and Galois extension, and E is the splitting field of a polynomial $f(x) \in F[x]$ written as $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ in $E[x]$, then the Galois group $\mathrm{Gal}(E/F)$ permutes the roots of $f(x)$, which gives us an embedding $\mathrm{Gal}(E/F) \hookrightarrow S_n$.

- **Cubic extensions:** Let F be a field with $\operatorname{char} F$ not equal to 2 or 3 and take a polynomial $f(x) = x^3 + px + q \in F[x]$ (any degree 3 monic polynomial can be *depressed*[10] to this form). Assume that $f(x)$ has no roots in F, so that it is irreducible over F. Thus if E/F is the splitting field of $f(x)$, E/F is Galois, since

[10] If $ax^3 + bx^2 + cx + d$ is a degree 3 polynomial, $\operatorname{char} F \neq 3$ allows us to substitute x by $x + \frac{b}{3a}$. We are translating the polynomial to bring the average of the roots to 0. One can think of

$$\operatorname{avg}\left(x + \frac{b}{3a}\right) = \operatorname{avg}(x) + \operatorname{avg}\left(\frac{b}{3a}\right) = -\frac{b}{3a} + \frac{b}{3a} = 0.$$

$f(x)$ is separable ($f'(x) = 3x^2 + p$ is not the zero polynomial, by $\operatorname{char} F \neq 3$). Now, if $\alpha \in E$ is a root of $f(x)$, then $F(\alpha)/F$ is a separable extension of degree 3. But is it normal? Since $\operatorname{Gal}(E/F) \hookrightarrow S_3$ and $|S_3| = 6$, we have that $[E : F] = 3$ or 6.

- If $[E : F] = 3$, then $F(\alpha)/F = E/F$ is Galois and so we have that $\operatorname{Gal}(F(\alpha)/F) \cong \mathbb{Z}/3\mathbb{Z} \cong A_3 \subseteq S_3$;
- If $[E : F] = 6$, $F(\alpha)/F$ is not normal and $\operatorname{Gal}(E/F) \cong S_3$.

In general, the *discriminant* of $f(x)$ distinguishes the two cases. This is a universal polynomial Δ in the coefficients of $f(x)$, and it vanishes precisely when $f(x)$ has multiple roots. In degrees 2 and 3 we have

- $f(x) = ax^2 + bx + c \implies \Delta = b^2 - 4ac$;
- $f(x) = x^3 + px + q \implies \Delta = -4p^3 - 27q^2$.

If $\alpha_1, \alpha_2, \alpha_3 \in E$ are the roots of $f(x)$, then $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ satisfies $\Delta = \delta^2$ up to a scalar multiple. Moreover $\sigma(\Delta) = \Delta$ and $\sigma(\delta) = \pm\delta$ for all $\sigma \in \operatorname{Gal}(E/F)$. The ± sign gives us information about the extension, according to the:

Proposition: Let F be a field and E be the splitting field of a separable polynomial $f(x) \in F[x]$, so that E/F is Galois and $\operatorname{Gal}(E/F) \hookrightarrow S_n$. The following are equivalent:

(i) $\operatorname{Gal}(E/F) \subseteq A_n$.

(ii) $\sigma(\delta) = \delta$ for all $\sigma \in \operatorname{Gal}(E/F)$.

(iii) $\delta \in F$.

(iv) Δ is a square in F.

- **Examples:**

  (1) Consider $x^3 - a \in \mathbb{Q}[x]$, where a is not a cube, so that $f(x)$ is irreducible. Since $\Delta = -27a^2$ is not a square in $\mathbb{Q}$, if we let E be the splitting field of $x^3 - a$ over $\mathbb{Q}$, then $\operatorname{Gal}(E/\mathbb{Q}) = S_3$. We conclude that if $\sqrt[3]{a} \notin \mathbb{Q}$, then $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$ is not normal.

  (2) $x^3 - 3x - 1 \in \mathbb{Q}[x]$ is irreducible and $\Delta = 81 = 9^2$, so $G \cong A_3$.

- **Finite fields:** We will start the discussion with the:

  Lemma: Let F be any field, and $S \subseteq F^\times$ a finite subset which is a multiplicative group. Then S is cyclic.

  Proof: Let $n = |S|$ and r be the largest order of any element in S. So $s^r - 1 = 0$ for all $s \in S$. Since S is abelian, by the structure theorem for finitely generated abelian groups, we may write $S \cong C_{r_1} \times \cdots \times C_{r_k = r}$ with $r_1 \mid r_2 \mid \cdots \mid r_k = r$. But then $r \geq n$, since $x^r - 1$ has at most r distinct roots. On the other hand, $r \leq n$ leads us to $r = n$. □

Corollary: If F is a finite field, $F^\times$ is cyclic.

- **Prime field:** Let F be a field and consider the canonical homomorphism

$$\mathbb{Z} \ni n \overset{\varphi}{\longmapsto} \begin{cases} \underbrace{1+\cdots+1}_{n \text{ times}}, \text{ if } n \geq 0 \\ -(\underbrace{1+\cdots+1}_{|n| \text{ times}}), \text{ if } n < 0 \end{cases} \in F.$$

This φ is always a ring homomorphism, which may or may not be injective.

  - If φ is injective, the universal property of localizations gives us an embedding $\mathbb{Q} \hookrightarrow F$.
  - If φ is not injective, $\mathbb{Z}$ being a PID says that $\ker\varphi = n\mathbb{Z}$ for some n and we get an embedding $\mathbb{Z}/n\mathbb{Z} \hookrightarrow F$. Since F is a field, $\mathbb{Z}/n\mathbb{Z}$ is a domain, and so $n = p$ is a prime number.

The *prime field* of F is the smallest subfield of F containing the image of φ. By the above, it is always isomorphic to $\mathbb{Q}$ ($\operatorname{char} F = 0$) or to $\mathbb{Z}/p\mathbb{Z}$ for some prime p ($\operatorname{char} F = p$).

- **Remark:** The prime field of a finite field is $\mathbb{F}_p$ for some prime p. Now suppose that $|F| = q$ and E/F is an extension of degree n. So $|E| = q^n$, because $E \cong F^n$ as F-vector spaces. Since $E^\times$ is cyclic, it is generated by a single element α, so $E = F(\alpha)$.

- **Corollary:** Any finite field F has $q = p^n$ elements, for some prime p and $n > 0$.

Proof: Apply the previous remark for the extension $F/\mathbb{F}_p$. □

Apr 3rd

- **Corollary:** Let F be a field with $|F| = q = p^n$ elements, where $p, n > 0$ and p is prime. Then F is the splitting field of $x^q - x \in \mathbb{F}_p[x]$.

Proof: Since $F^\times$ is cyclic of order $q-1$, every nonzero element of F is a root of $x^{q-1} - 1$. Together with 0, the elements of F are the q distinct roots of $x^q - x$. □

- **Theorem:** Given integers $p, n > 0$ with p prime, there is a unique field with p^n elements, up to isomorphism. It is denoted by $\mathbb{F}_{p^n}$ (effectively extending the notation $\mathbb{F}_p$ for prime order fields).

Proof: For existance, split $x^{p^n} - x$. Uniqueness follows because two such fields are splitting fields of the same polynomial in $\mathbb{F}_p$. □

- **Roots of unity:** Let F be a field with $\operatorname{char} F = p \geq 0$, $n > 0$ be such that $p \nmid n$, and $f(x) = x^n - 1$. So $f(x)$ is separable over F (since $\gcd(f, f') = 1$). Let E/F be the splitting field of $f(x)$, obtained by adjoining the *nth roots of unity* to F (E/F is then called the *nth cyclotomic extension of* F). Since $f(x)$ is separable, E/F is Galois. Moreover, the roots $\{\zeta_1, \ldots, \zeta_n\}$ of $f(x)$ form a subgroup of $E^\times$, which is then cyclic. Say that ζ_n is a generator of such subgroup. Then ζ_n is called a *primitive nth root of unity*, and $E = F(\zeta_n)$. With this setting, we have the:

  Proposition: $\mathrm{Gal}(F(\zeta_n)/F)$ is abelian, and if n is also prime, it is cyclic.

  Proof: If $\zeta = \zeta_n$ is primitive, any $\sigma \in \mathrm{Gal}(F(\zeta)/F)$ sends ζ to $\sigma(\zeta) = \zeta^k$ for some k. Since $\{1, \zeta, \ldots, \zeta^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$, we get an embedding

$$\begin{tikzcd} \mathrm{Gal}(F(\zeta)/F) \arrow[r, hook] & \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ (\zeta \mapsto \zeta^k) \arrow[r, mapsto] & (1 \mapsto k). \end{tikzcd}$$

  Now, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, and so is $\mathrm{Gal}(F(\zeta)/F)$. If n is also prime, then $(\mathbb{Z}/n\mathbb{Z})^\times \cong C_{n-1}$ is cyclic, and the conclusion follows since subgroups of cyclic groups are cyclic themselves. □

- **Remark:** The above proof also shows that $[F(\zeta) : F] = |\mathrm{Gal}(F(\zeta)/F)| \leq \varphi(n)$, where φ is the Euler totient function, given by

$$\varphi(n) = |\{1 \leq k \leq n \mid \gcd(k, n) = 1\}|.$$

  Moreover, since $\varphi(n) = |\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})|$ and $\mathrm{Gal}(F(\zeta)/F)$ is a subgroup of $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, we have that $|\mathrm{Gal}(F(\zeta)/F)|$ actually divides $\varphi(n)$.

- **Noether's equations:** Let E be a field and G a finite group of automorphisms of E. Write a set map $G \ni \sigma \xmapsto{\chi} \alpha_\sigma \in E^\times$. The elements $\{\alpha_\sigma\}_{\sigma \in G}$ are said to *satisfy Noether's equations* if $\alpha_\sigma \sigma(\alpha_\tau) = \alpha_{\sigma\tau}$, for all $\sigma, \tau \in G$. These equations mean that χ is a 1-cocycle for the G-module $E^\times$, that is, $d^1\colon C^1(G, E^\times) \to C^2(G, E^\times)$ maps χ to 0. Indeed, the additive expression

$$(d^1\chi)(\sigma, \tau) = \sigma(\chi(\tau)) - \chi(\sigma\tau) + \chi(\sigma) = 0$$

  writes multiplicatively as

$$(d^1\chi)(\sigma, \tau) = \frac{\sigma(\alpha_\tau)\alpha_\sigma}{\alpha_{\sigma\tau}} = 1.$$

  The next natural thing to wonder is whether χ vanishes in cohomology. The answer is yes.

- **Theorem (Speiser):** Let E be a field and G a finite group of automorphisms of E. Then $\{\alpha_\sigma\}_{\sigma \in G}$ is a solution to Noether's equations if and only if there is $\beta \in E^\times$ such that $\alpha_\sigma = \beta/\sigma(\beta)$, for all $\sigma \in G$.

- **Remark:** Speiser's theorem actually says that every solution to Noether's equations is a coboundary, with the element β defining the 0-cochain. In other words, the content of this result is that $H^1(G, E^\times)$ is trivial.

Apr 5th

- **Proof of Speiser's theorem:** If the 0-cochain $\beta \in E^\times$ exists, then we compute
$$\alpha_\sigma\sigma(\alpha_\tau) = \frac{\beta}{\sigma(\beta)}\sigma\left(\frac{\beta}{\tau(\beta)}\right) = \frac{\beta}{\sigma(\beta)}\frac{\sigma(\beta)}{\sigma(\tau(\beta))} = \frac{\beta}{\sigma(\tau(\beta))} = \alpha_{\sigma\tau}.$$
This is nothing more than the statement that every coboundary is a cocycle. Conversely, assume that $\{\alpha_\sigma\}_{\sigma\in G}$ solves Noether's equations. By linear independence of the characters, we may fix $x \in E$ such that $\beta \doteq \sum_{\tau\in G}\alpha_\tau\tau(x) \neq 0$. Then
$$\sigma(\beta) = \sigma\left(\sum_{\tau\in G}\alpha_\tau\tau(x)\right) = \sum_{\tau\in G}\sigma(\alpha_\tau)\sigma(\tau(x)),$$
and so
$$\alpha_\sigma\sigma(\beta) = \sum_{\tau\in G}\alpha_\sigma\sigma(\alpha_\tau)\sigma(\tau(x)) = \sum_{\tau\in G}\alpha_{\sigma\tau}\sigma(\tau(x)) = \beta,$$
using that $\tau \mapsto \sigma\tau$ is a bijection of G. □

- **Equivalent formulation:** Keeping the above notation, regard again a collection $\{\alpha_\sigma\}_{\sigma\in G}$ as a map $\chi\colon G \to E$. If $\alpha_\sigma \in E^G$ for all $\sigma \in G$, then χ is a character of G with values in $(E^G)^\times$. And conversely, any $\chi\colon G \to (E^G)^\times$ solves Noether's equations. The next two corollaries summarize this remark.

- **Corollary:** Let E/F be a finite and Galois field extension, and $\chi\colon \mathrm{Gal}(E/F) \to F^\times$ a character. Then, there is $\beta \in E^\times$ such that $\chi(\sigma) = \beta/\sigma(\beta)$, for all $\sigma \in \mathrm{Gal}(E/F)$. Conversely, any $\beta \in E^\times$ defines such a character, provided $\beta/\sigma(\beta) \in F$ for all $\sigma \in \mathrm{Gal}(E/F)$.

- **Corollary:** Let E/F be a finite and Galois field extension, and r be the least common multiple of the orders of all elements in $\mathrm{Gal}(E/F)$. Then $\beta^r \in F$ for all $\beta \in E^\times$ such that $\beta/\sigma(\beta) \in F$ (for all $\sigma \in \mathrm{Gal}(E/F)$).

  Proof: Since E/F is Galois, it suffices to show that $\sigma(\beta^r) = \beta^r$ for all $\sigma \in \mathrm{Gal}(E/F)$. But
$$\frac{\beta^r}{\sigma(\beta^r)} = \left(\frac{\beta}{\sigma(\beta)}\right)^r = \chi(\sigma)^r = \chi(\sigma^r) = \chi(\mathrm{Id}_E) = 1,$$
as wanted. □

- **Norm and trace:** Let E/F be a finite extension, $[E:F] = n$. Any $\alpha \in E$ defines a F-linear map $m_\alpha\colon E \to E$ by $m_\alpha(x) = \alpha x$. The *norm* of α and the *trace* of α are defined as
$$N_{E/F}(\alpha) = \det(m_\alpha) \quad \text{and} \quad \mathrm{tr}_{E/F}(\alpha) = \mathrm{tr}(m_\alpha).$$

- **Examples:** These quantities indeed depend on the extension E/F, not only on the element α.

  - $N_{\mathbb{Q}/\mathbb{Q}}(2) = 2$, $\mathrm{tr}_{\mathbb{Q}/\mathbb{Q}}(2) = 2$;

  - $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(2) = 2 \cdot 2 = 4$, $\mathrm{tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(2) = 2 + 2 = 4$;
  - $N_{\mathbb{C}/\mathbb{R}}(a+bi) = a^2 + b^2$, $\mathrm{tr}_{\mathbb{C}/\mathbb{R}}(a+bi) = 2a$.

- **Theorem (alternate definition):** Let E/F be a finite extension, $[E : F] = n$. There is a unique function $N = N_{E/F} \colon E \to F$, called the *norm on E/F*, satisfying:

  (i) character: $N(\alpha\beta) = N(\alpha)N(\beta)$, for all $\alpha, \beta \in E$.

  (ii) homogeneity: $N(\alpha) = \alpha^n$ for all $\alpha \in F$.

  (iii) simple extensions: if $E = F(\alpha)$ and $\min(\alpha, F)(x) = x^n + c_1x^{n-1} + \cdots + c_n$, then $N(\alpha) = (-1)^n c_n$.

  (iv) transitive: for a tower $E \supseteq K \supseteq F$, $N_{E/F} = N_{K/F} \circ N_{E/K}$, as functions $E \to F$.

Apr 8th

- **Proof:** First let's show that there is at most one norm function with properties (i)-(iv). We will do this by taking an arbitrary $\alpha \in E$, and computing $N_{E/F}(\alpha)$ explicitly by using (i)-(iv). Here's how: consider the tower $E \supseteq F(\alpha) \supseteq F$ and write $[E : F(\alpha)] = m$ and $[F(\alpha) : F] = k$, so that

$$N_{E/F}(\alpha) \overset{(iv)}{=} N_{F(\alpha)/F} \circ N_{E/F(\alpha)}(\alpha) \overset{(ii)}{=} N_{F(\alpha)/F}(\alpha^m) \overset{(i)}{=} (N_{F(\alpha)/F}(\alpha))^m \overset{(iii)}{=} ((-1)^k c_k)^m,$$

  where $\min(\alpha, F)(x) = x^k + c_1x^{k-1} + \cdots + c_k$. With this, we only have to show that there is at least one norm function with properties (i)-(iv). Of course the map we're looking for is just $E \ni \alpha \overset{N}{\longmapsto} \det(m_\alpha) \in F$. We check:

  (i) $N(\alpha\beta) = \det(m_{\alpha\beta}) = \det(m_\alpha \circ m_\beta) = \det(m_\alpha)\det(m_\beta) = N(\alpha)N(\beta)$.

  (ii) If $\alpha \in F$, the matrix representing m_α (with respect to *any* basis of E/F) is $\alpha\mathrm{Id}_n$. Thus $N(\alpha) = \det(\alpha\mathrm{Id}_n) = \alpha^n$.

  (iii) If $\min(\alpha, F)(x) = x^n + c_1x^{n-1} + \cdots + c_n$, we consider the basis $(1, \alpha, \cdots, \alpha^{n-1})$ of E/F and compute

$$[m_\alpha]_{\mathscr{B}} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_n \\ 1 & 0 & \cdots & 0 & -c_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -c_2 \\ 0 & 0 & \cdots & 1 & -c_1 \end{pmatrix} \implies N(\alpha) = \det(m_\alpha) = (-1)^n c_n.$$

  The matrix above is called the *companion matrix* of $\min(\alpha, F)(x)$, and the last equality may be obtained by noting that in the (possible) definition $\det(A) = \sum_{\sigma \in S_n} \prod_{i=1}^n a_{i,\sigma(i)}$ of a $n \times n$ matrix $A = (a_{ij})_{i,j=1}^n$ applied for $A = [m_\alpha]_{\mathscr{B}}$, only one term survives: $1 \cdot 1 \cdots 1 \cdot (-c_n)$, with the overall sign $(-1)^n$ in the final result coming from the sign of a suitable permutation.

(iv) We'll outline the proof strategy, focusing in two special cases. Consider a tower $E \supseteq K \supseteq F$ and take $\alpha \in E$. Then either $\alpha \in K$ or $\alpha \notin K$.

- If $\alpha \in K$, assume that our tower is $F(\alpha, \beta) \supseteq F(\alpha) \supseteq F$, with degrees $[F(\alpha,\beta) : F(\alpha)] = m$ and $[F(\alpha) : F] = n$. Then consider the ordered basis

$$\mathscr{B} = (1, \alpha, \ldots, \alpha^{n-1}, \beta, \beta\alpha, \ldots, \beta\alpha^{n-1}, \ldots, \beta^{m-1}, \beta^{m-1}\alpha, \ldots, \beta^{m-1}\alpha^{n-1})$$

of $F(\alpha,\beta)/F$. So we have the $m \times m$ block matrix (whose entries are $n \times n$ matrices)

$$[m_\alpha]_{\mathscr{B}} = \left(\begin{array}{c|c|c|c} C_{f(x)} & 0 & \cdots & 0 \\ \hline 0 & C_{f(x)} & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & C_{f(x)} \end{array}\right),$$

where $C_{f(x)}$ is the companion matrix of $f(x) = \min(\alpha, F)(x)$. So, by the already verified properties (i)-(iii) we have

$$\begin{aligned} N_{F(\alpha,\beta)/F}(\alpha) &= \det(C_{f(x)})^m = N_{F(\alpha)/F}(\alpha)^m \\ &= N_{F(\alpha)/F}(\alpha^m) = N_{F(\alpha)/F} \circ N_{F(\alpha,\beta)/F(\alpha)}(\alpha), \end{aligned}$$

as wanted.

- If $\alpha \notin K$, we consider the tower $F(\alpha,\beta) \supseteq F(\beta) \supseteq F$ instead, and the same ordered basis $\mathscr{B}$ for $F(\alpha,\beta)/F$ given above. Then

$$[m_\alpha]_{\mathscr{B}} = \left(\begin{array}{c|c|c|c} 0 & 0 & \cdots & -m_{c_n} \\ \hline \mathrm{Id}_m & 0 & \ddots & \vdots \\ \hline \vdots & \ddots & \ddots & -m_{c_2} \\ \hline 0 & \cdots & \mathrm{Id}_m & -m_{c_n} \end{array}\right),$$

where $\min(\alpha, F(\beta))(x) = x^n + c_1 x^{n-1} + \cdots + x_n$ and m_{c_i} is the matrix representation of the multiplication by $c_i \in F(\beta)$. Now, we already know that $N_{F(\alpha,\beta)/F(\beta)}(\alpha) = (-1)^n c_n$, and so

$$\begin{aligned} N_{F(\alpha,\beta)/F}(\alpha) &= \det(m_\alpha) \overset{(*)}{=} (-1)^{nm} \det(m_{c_n}) \\ &= (-1)^{nm} N_{F(\beta)/F}(c_n) = N_{F(\beta)/F}((-1)^n c_n) \\ &= N_{F(\beta)/F}(N_{F(\alpha,\beta)/F(\beta)}(\alpha)), \end{aligned}$$

as wanted (where the equality in $(*)$ boils down to linear algebra). □

- **Corollary:** Suppose that E/F is a finite and Galois field extension. Then we have that $N_{E/F}(\alpha) = \prod_{\sigma\in\mathrm{Gal}(E/F)} \sigma(\alpha)$.

  Proof: Take $\alpha \in E$ and consider the tower $E \supseteq F(\alpha) \supseteq F$, where $[E : F(\alpha)] = m$. On one hand, we have that

  $$N_{E/F}(\alpha) = (N_{F(\alpha)/F}(\alpha))^m = \left(\prod \text{roots of } \min(\alpha, F)\right)^m.$$

  On the other hand, since E/F is Galois we may write

  $$\prod_{\sigma\in\mathrm{Gal}(E/F)} \sigma(\alpha) = \prod_{[\sigma]\in\mathrm{Gal}(E/F)/G_{F(\alpha)}} \prod_{\tau\in[\sigma]} \tau(\alpha) = \prod \sigma\tau(\alpha) = \prod_{\sigma\in\mathrm{Gal}(E/F)/G_{F(\alpha)}} \sigma(\alpha)^m,$$

  where the unlabeled product is taken over $\tau \in G_{F(\alpha)}$ and *distinct cosets* $[\sigma]$, and the last one is taken by choosing one representative σ for each distinct cosets of $\mathrm{Gal}(E/F)/G_{F(\alpha)}$. Since the $\sigma(\alpha)$ are precisely the roots of $\min(\alpha, F)(x)$, we are done. □

Apr 10th

- **Remark:** We conclude from the previous result that if E/F is a finite and Galois extension, then $N_{E/F}(\sigma(\alpha)) = N_{E/F}(\alpha)$ for all $\sigma \in \mathrm{Gal}(E/F)$ (although this holds even under weaker assumptions than being Galois).

- **Theorem (Hilbert 90):** Suppose that E/F is a cyclic[11] extension of degree n. Let $\alpha \in E$ and σ be a generator of $\mathrm{Gal}(E/F)$. Then $N_{E/F}(\alpha) = 1$ if and only if there is $\beta \in E^\times$ such that $\alpha = \beta/\sigma(\beta)$.

  Proof: If such β exists, then

  $$N_{E/F}(\alpha) = N_{E/F}\left(\frac{\beta}{\sigma(\beta)}\right) = \frac{N_{E/F}(\beta)}{N_{E/F}(\sigma(\beta))} = 1,$$

  by the previous remark. Conversely, assume that $N_{E/F}(\alpha) = 1$, and let's find β. For every $i = 1, \ldots, n$, define $\alpha_i = \alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{i-1}(\alpha)$. Then $\alpha_i\sigma^j(\alpha) = \alpha_{i+j}$, provided $i + j \leq n$. Else, we have

  $$\begin{aligned} \alpha_i\sigma^i(\alpha_j) &= \alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha)\sigma^i(\alpha)\cdots\sigma^{i+j-1}(\alpha) \\ &= \alpha\sigma(\alpha)\cdots\alpha^{n-1}(\alpha)\alpha\sigma(\alpha)\cdots\sigma^{i+j-1 \pmod n}(\alpha) \\ &= N_{E/F}(\alpha)\alpha_{i+j-1 \pmod n} \\ &= \alpha_{i+j-1 \pmod n}. \end{aligned}$$

  Thus, $\sigma^i \mapsto \alpha_i$ is a set of elements satisfying Noether's equations. The sought element β is then given by Speiser's theorem. □

[11] Usually, E/F is an adjective-of-a-group extension means that E/F is Galois and $\mathrm{Gal}(E/F)$ is adjective. For example, one may talk about abelian extensions, solvable extensions, nilpotent extensions...

- **Primitive Element Theorem:** Let E/F be a finite extension. Then:

  (i) $E = F(\alpha)$ for some $\alpha \in E$ (called a *primitive element*) if and only if E/F has only finitely many intermediate extensions.

  (ii) If E/F is separable, then $E = F(\alpha)$ for some $\alpha \in E$.

  Proof:

  (i) If F is finite, so is E, then $E^\times$ is cyclic and $E = F(\alpha)$ for some generator α of $E^\times$. So, we only have to prove the result when F is infinite. Assume that E/F has only finitely many intermediate extensions. Fix $\alpha, \beta \in E$ and consider the family of intermediate fields $\{F(\alpha + c\beta) \mid c \in F\}$. The assumption says that there are distinct $c_1, c_2 \in F$ such that $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$. Let $\theta_i = \alpha + c_i\beta$, for $i = 1, 2$. Then we have that (in order):

  $$\theta_2 \in F(\theta_1) \implies \beta = \frac{\theta_1 - \theta_2}{c_1 - c_2} \in F(\theta_1) \implies \alpha = \theta_1 - c_1\beta \in F(\theta_1).$$

  Thus $F(\alpha, \beta) = F(\theta_1)$. The conclusion follows from induction (more precisely, E is obtained by adjoining finitely many elements to F, and we keep exchanging two of those elements by a single one, until we obtain $E = F(\theta)$ for some $\theta \in E$)

  Conversely, assume given $E = F(\alpha)$ for some $\alpha \in E$. We will construct an injection

  $$\{\text{intermediate fields } E \supseteq K \supseteq F\} \hookrightarrow \{\text{divisors } g(x) \text{ of } \min(\alpha, F)(x) \text{ in } F[x]\},$$

  which will conclude the proof. So, consider a tower $E \supseteq K \supseteq F$. We have that $\min(\alpha, K)(x) \mid \min(\alpha, F)(x)$ in $K[x]$, and hence in $E[x]$. Furthermore, $\deg \min(\alpha, K) = [K(\alpha) : K] = [E : K]$ (since $E = K(\alpha)$). Finally, consider K' to be $K(\text{coeffs. of } \min(\alpha, K)(x))$. Then $K' \subseteq K$. Also, $E = K'(\alpha) = K(\alpha)$ and $\min(\alpha, K)(x)$ is irreducible over K', but $[E : K] = [E : K'] = \deg \min(\alpha, F)$. Hence $K = K'$. We are done.

  (ii) If E/F is finite and separable, write $E = F(\alpha_1, \ldots, \alpha_r)$, where $\alpha_1, \ldots, \alpha_r \in E$ are separable over F. Let E' be the splitting field of all the minimal polynomials $\min(\alpha_1, F)(x), \ldots, \min(\alpha_r, F)(x)$ over F. Then E'/F is finite and Galois, and so it has only finitely many intermediate fields (namely, in Galois correspondence with the finitely many subgroups of $\mathrm{Gal}(E'/F)$). A fortiori, E/F will also have finitely many intermediate extensions, and the conclusion follows from (i).

  □

Apr 12th

- **Kummer Theory:** Suppose F is a field that contains a primitive nth root of unity ζ_n, where $\operatorname{char} F \nmid n$ (in other words, $F = F(\zeta_n)$). A *Kummer field* (or *Kummer extension*) os a splitting field of a polynomial of the form $(x^n - a_1) \cdots (x^n - a_r)$, where $a_1, \ldots, a_r \in F$.

- **Remark:** If $F = F(\zeta_n)$, then we automatically have $p = \operatorname{char} F \nmid n$. Else, write that $p = nm$ for some integer m and then $x^n - 1 = (x^m - 1)^p$ will not have n distinct roots. Also, it follows that Kummer extensions are Galois: the splitting field of $(x^n - a_1)\cdots(x^n - a_r)$ is the same for the polynomial $(x^n - b_1)\cdots(x^n - b_s)$, where $b_1, \ldots, b_s \in F$ are pairwise distinct and $\{b_1, \ldots, b_s\} = \{a_1, \ldots, a_r\}$ (i.e., remove repetitions) – but the latter is separable.

- **Example:** $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Kummer (because it is not Galois), but the extension $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}(\zeta_3)$ is Kummer.

- **Theorem:** Let $F = F(\zeta_n)$ be a field containing a primitive nth root of unity ζ_n, with $\operatorname{char} F \nmid n$.

  (i) If E/F is a cyclic extension of degree n, then there is $\alpha \in E$ such that $E = F(\alpha)$ and $\min(\alpha, F)(x) = x^n - a$ for some $a \in F$.

  (ii) Conversely, given $a \in F$ and a root α of $x^n - a$ (in its splitting field), then the extension $F(\alpha)/F$ is cyclic of degree d for some divisor $d \mid n$ and $\alpha^d \in F$. In this case, $F(\alpha)$ is the splitting field of $x^d - \alpha^d$.

Proof: Let $\zeta = \zeta_n$ be the given primitive nth root of unity.

(i) Assume that $\operatorname{Gal}(E/F) \cong C_n$ is cyclic with a generator σ. We know that $N_{E/F}(\zeta) = N_{E/F}(\zeta^{-1}) = \zeta^n = 1$. Hilbert 90 gives an element $\beta \in E^\times$ such that $\zeta^{-1} = \beta/\sigma(\beta)$, so that $\sigma(\beta) = \zeta\beta$. Since E/F is Galois and $\zeta \in F$, σ fixes ζ and it follows that $\sigma^i(\beta) = \zeta^i\beta$ for $i = 1, \ldots, n$. This means that $\beta, \zeta\beta, \ldots, \zeta^{n-1}\beta$ are the distinct Galois conjugates of β, and so $[F(\beta) : F] = n$. It follows that $E = F(\beta)$. Moreover, $\sigma(\beta^n) = \sigma(\beta)^n = (\zeta\beta)^n = \zeta^n\beta^n = \beta^n$ says that $a \doteq \beta^n \in F$.

(ii) Suppose that $a \in F$ and let α be a root of $f(x) = x^n - a$ in some splitting field E of $f(x)$ over F. Certainly $\zeta^i\alpha$ is also a root of $f(x)$ for $i = 1, \ldots, n$. Then
$$f(x) = (x - \alpha)(x - \zeta\alpha)\cdots(x - \zeta^{n-1}\alpha)$$
splits over $F(\alpha)$, so $E = F(\alpha)$ and $F(\alpha)/F$ is Galois. Let $\sigma \in \operatorname{Gal}(F(\alpha)/F)$. Then $\sigma(\alpha) = \zeta^i\alpha$ for some i, since σ permutes the roots of $f(x)$. This gives us an embedding
$$\begin{tikzcd}\operatorname{Gal}(F(\alpha)/F) \arrow[r, hook] & \{n\text{th roots of unity}\} \cong C_n \\ \sigma \arrow[r, mapsto] & \zeta^i\end{tikzcd}$$
Since subgroups of cyclic groups are again cyclic, we conclude that $\operatorname{Gal}(F(\alpha)/F) \cong C_d$ for some divisor $d \mid n$, and the generator σ is mapped to a dth root of unity ω. So $\sigma(\alpha^d) = \sigma(\alpha)^d = (\omega\alpha)^d = \omega^d\alpha^d = \alpha^d$ says that $\alpha^d \in F$.

□

- **Theorem:** A finite extension E/F is Kummer if and only if all of the following conditions hold:

  (i) E/F is Galois.

  (ii) $\mathrm{Gal}(E/F)$ is abelian (hence isomorphic to a product $C_{d_1} \times \cdots \times C_{d_r}$, where $d_1 \mid \cdots \mid d_r$).

  (iii) F contains a primitive dth root of unity, where $d = d_r$ is also the least common multiple of the orders of the elements in $\mathrm{Gal}(E/F)$.

Apr 15th

- **Proof:** Let's work on the two implications separately:

  $\Longrightarrow$**:** Assume that E/F is Kummer. Let's check that the stated conditions are satisfied.

  (i) Done before.

  (ii) Assume that $F = F(\zeta_n)$ contains nth roots of unity, and that E splits $(x^n - a_1)\cdots(x^n - a_r)$, for $a_1, \ldots, a_r \in F$ pairwise distinct. Call those factors $f_i(x)$, and proceed by induction: if E_1 splits $f_1(x)$ and E_2 splits $f_2(x), \ldots, f_r(x)$, then $E = E_1 \cdot E_2$, $E_1 \cap E_2 = F$, and both E_1/F and E_2/F are normal. So $\mathrm{Gal}(E/F) = \mathrm{Gal}(E/E_1) \times \mathrm{Gal}(E/E_2)$. By induction, $\mathrm{Gal}(E/E_1) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/E_2) \cong \mathrm{Gal}(E_2/F)$ is a product of cyclic groups, while $\mathrm{Gal}(E/E_2) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/E_1) \cong \mathrm{Gal}(E_1/F)$ is cyclic.

  (iii) By (ii), $\mathrm{Gal}(E/F) \cong C_{d_1} \times \cdots \times C_{d_r}$, with $d_1 \mid \cdots \mid d_r$. Now take $d = \mathrm{lcm}(d_1, \ldots, d_r) = d_r$. By the cyclic case and induction, we have that $d_i \mid n$ for all i. Hence $d \mid n$, so $\zeta_n \in F$ implies $\zeta_d \in F$.

  $\Longleftarrow$**:** We start with a general remark about groups and fields: if G is any group of the form $C_{d_1} \times \cdots \times C_{d_r}$, $d_1 \mid \cdots \mid d_r$, with $d = d_r = \mathrm{lcm}(d_1, \ldots, d_r)$ and F if any field such that $\mu_d \subseteq F^\times$ (here μ_d denotes the dth roots of unity), then $G \cong \mathbb{X}$, where $\mathbb{X} = \{\text{characters}\, \chi\colon G \to \mu_d \subseteq F^\times\}$. Indeed, pick a generator σ_i for each factor C_{d_i} and $\zeta_{d_i} \in \mu_d$ a d_i-th root of unity. Then define $\chi_i\colon G \to F^\times$ by $\chi_i(\sigma_i) = \zeta_{d_i}$ and $\chi_i(\sigma_j) = 1$ if $i \neq j$. This defines the desired isomorphism[12] $G \ni \sigma_i \longmapsto \chi_i \in \mathbb{X}$. With this, we assume again the conditions of the theorem, and set $G = \mathrm{Gal}(E/F)$. What we need to proceed is the following:

  Lemma. *Consider $A = \{\alpha \in E^\times \mid \alpha^d \in F^\times\}$. Then*

$$\frac{A}{F^\times} \xrightarrow{\simeq} \frac{A^d}{(F^\times)^d} \cong \mathrm{Gal}(E/F) \cong \mathbb{X}.$$

  Note that A is a subgroup of $E^\times$.

[12] One should think of $\mathbb{X}$ as the dual space to G, with the χ_i being the dual basis to σ_i

Proof: The map $A/F^\times \ni [\alpha] \mapsto [\alpha^d] \in A^d/(F^\times)^d$ is well-defined and surjective. As for injectivity, assume that $[\alpha^d] = [1]$. Our goal is to show that $\alpha \in F^\times$. Note that $\alpha^d = a^d$ for some $a \in F$. In other words, α solves $x^d - a^d = 0$. This means that the other solutions of this equation are $\zeta_d\alpha$, $\zeta_d^2\alpha, \ldots, \zeta_d^{d-1}\alpha$. But since a is also a solution, this means that $a = \zeta_d^k\alpha$ for some $0 \leq k \leq d-1$. Then $\alpha = \zeta_d^{d-k}a \in F$. This establishes the first isomorphism stated above. As the next step, we check that $A/F^\times \cong \mathbb{X}$: for any $\alpha \in A$ we have

$$\left(\frac{\alpha}{\sigma(\alpha)}\right)^d = \frac{\alpha^d}{\sigma(\alpha^d)} = \frac{\alpha^d}{\alpha^d} = 1,$$

so by Speiser's theorem and Hilbert 90, $\sigma \mapsto \alpha/\sigma(\alpha)$ defines a character $G \to \mu_d \subseteq F^\times$ and, conversely, any character $G \to \mu_d$ arises this way. Moreover, such a character is trivial precisely when $\alpha/\sigma(\alpha) = 1$ for all σ, which is the same as saying that $\alpha \in F^\times$. That is, $A^G = F^\times$. Thus $A/F^\times \cong \mathbb{X}$, as wanted. □

With this lemma in place, write $A/F^\times = \{\alpha_1 F^\times, \ldots, \alpha_t F^\times\}$, where each $\alpha_i \in A$ is a root of $x^d - a_i$ for some $a_i \in F^\times$. Then $\zeta_d a_i, \ldots, \zeta_d^{d-1}a_i$ are also roots of $x^d - a_i$, and we see that $x^d - a_i$ and $x^d - a_j$ have distinct roots if $i \neq j$, which means that $(x^d - a_1)\cdots(x^d - a_t)$ splits over E. The conclusion will follow once we check that $E = F(\alpha_1, \ldots, \alpha_t)$. So assume not, take a non-trivial $\sigma \in \mathrm{Gal}(E/F)$ fixing $F(\alpha_1, \ldots, \alpha_t)$, and also take $\chi \in \mathbb{X}$ such that $\chi(\sigma) \neq 1$. Write $\chi(\sigma) = \alpha/\sigma(\alpha) \neq 1$ for some α. Then $\alpha^d \in F$ says that $\alpha \in A$, hence $\alpha \in F(\alpha_1, \ldots, \alpha_t)$. But σ fixes $F(\alpha_1, \ldots, \alpha_t)$ and $\sigma(\alpha) \neq \alpha$, a contradiction.

□

Apr 17th

- **Lemma (transitivity):** Let $E \supseteq K \supseteq F$ be a tower of fields such that K/F and E/K are algebraic extensions. Then so is E/F.

  Proof: Let $\alpha \in E$, and take $p(x) \in K[x]$ with $p(\alpha) = 0$. Each coefficient $c_i \in K$ of $p(x)$ is algebraic over F. So α is algebraic over the finite extension $F(\{c_i\}, \alpha)/F$. Since every finite extension is algebraic[13], we are done. □

- **Corollary:** Let E/F be any field extension. If $\alpha, \beta \in E$ are algebraic (resp. separable), then so are $\alpha + \beta, \alpha\beta$ and $\alpha - \beta$.

  Proof: Take $\alpha, \beta \in E$, and consider the tower $F(\alpha, \beta) \supseteq F(\alpha) \supseteq F$. Since β is algebraic over F, it is algebraic over $F(\alpha)$, and so $F(\alpha, \beta)/F(\alpha)$ is algebraic. Similarly, since α is algebraic over F, $F(\alpha)/F$ is algebraic. By transitivity, $F(\alpha, \beta)/F$ is algebraic, and the conclusion follows since $\alpha + \beta, \alpha - \beta, \alpha\beta \in F(\alpha, \beta)$.

[13] Every element of a finite extension is a root of its own minimal polynomial over the base field.

Now, for the separable analogue, one can reason as follows: if α and β are separable, then $F(\alpha)/F$ and $F(\beta)/F$ are separable. So $F(\alpha, \beta)$ is separable. □

- **Algebraic and separable closures:** Let $K \subseteq E$ be fields. The *algebraic closure* (resp. *separable closure*) of K in E is the set of elements in E which are algebraic (resp. separable) over K. These closures are fields, by the previous corollary.

- **Algebraically closed fields:** A field $\mathsf{k} \subseteq E$ is *algebraically closed in E* (resp. *separably closed in E*) if it equals its own algebraic (resp. separable) closure in E. We say that k is *algebraically closed* (resp. *separably closed*) if it is algebraically (resp. separably) closed in every extension.

  Equivalently, k is algebraically (resp. separably) closed if and only if every (separable) nonconstant polynomial in $\mathsf{k}[x]$ has a root in k.

- **Theorem:** Let k be a field. There exists an algebraically closed extension K/k (i.e., K is algebraically closed).

  Proof: Let $S = \{x_f \mid f(x) \in \mathsf{k}[x], \deg f \geq 1\}$ and consider the (very big) polynomial ring $\mathsf{k}[S]$. Take also the ideal $\mathfrak{a} = \{f(x_f) \mid f(x) \in \mathsf{k}[x], \deg f \geq 1\}$. Modding out $\mathfrak{a}$ would ensure that all polynomials $f(x)$ will gain a root x_f, but $\mathsf{k}[S]/\mathfrak{a}$ might not be a field (if $\mathfrak{a}$ is not maximal). We know that every non-trivial ideal is contained in a maximal ideal. So we need to verify the:

  Claim: $\mathfrak{a} \subsetneq \mathsf{k}[S]$. Indeed, if $1 \in \mathfrak{a}$, write $1 = \sum_i g_i(x) f_i(x_{f_i})$, for some coefficients $g_i(x) \in \mathsf{k}[S]$ (finite combination). Since we have only finitely many $g_i(x)$'s, there are only finitely many variables $x_1, \ldots, x_N$ of S (corresponding to $f_1(x), \ldots, f_N(x)$) appearing in the last combination. This means that for all i we have $g_i(x) \in \mathsf{k}[x_1, \ldots, x_N]$. Now find a finite extension F/k where $f_1(x), \ldots, f_N(x)$ have roots $\alpha_1, \ldots, \alpha_N \in F$, and consider the homomorphism $\mathsf{k}[S] \to F$ fixing k and sending $x_i = x_{f_i}$ to α_i, and the remaining x_f's to zero. Then we have that $f_i(x_i) \mapsto f_i(\alpha_i) = 0$, and these relations applied to the expression given for 1 become $1 = 0$, a contradiction.

  With this set in place, we may consider the maximal ideal $\mathfrak{m} \subseteq \mathsf{k}[S]$ containing $\mathfrak{a}$. Now the quotient $E_1 = \mathsf{k}[S]/\mathfrak{m}$ is a field, having roots $\overline{x_f} \in E_1$ for every nonconstant polynomial in $\mathsf{k}[x]$. But this might not be algebraically closed. So we repeat the process and find another extension E_2/E_1 for which every nonconstant polynomial in $E_1[x]$ has a root in E_2. Proceed and get an ascending chain of fields $\mathsf{k} \subseteq E_1 \subseteq E_2 \subseteq \cdots$. Put $K = \bigcup_{n \geq 1} E_n$. This is clearly a field, and it is algebraically closed: any $f(x) \in K[x]$ is in $E_n[x]$ for large enough n, and so it has a root in $E_{n+1} \subseteq K$. □

- **Corollary:** Let k be a field. There is an *algebraic* extension $\overline{\mathsf{k}}/\mathsf{k}$ which is algebraically closed. Such an extension is called an *algebraic closure* of k.

  Proof: Let K/k be an algebraically closed extension of k and $\overline{\mathsf{k}} \subseteq K$ be the algebraic closure of k in K. Then $\overline{\mathsf{k}}$ is algebraically closed: any element of K which is algebraic over $\overline{\mathsf{k}}$ already lies in $\overline{\mathsf{k}}$, since it is algebraic over k (by transitivity). □

- **Remark:** Algebraic closures are unique up to isomorphism (but there are uncountable many isomorphisms). Assume $\overline{\mathsf{k}}$ and $\overline{\mathsf{k}}'$ are algebraic closures of a field k. By Zorn's Lemma, we get an embedding $\overline{\mathsf{k}} \hookrightarrow \overline{\mathsf{k}}'$ (by extending embeddings of finite extensions F/k into $\overline{\mathsf{k}}'$ further and further). So $\mathsf{k} \subseteq \overline{\mathsf{k}} \subseteq \overline{\mathsf{k}}'$, but $\overline{\mathsf{k}}$ contains all elements of $\overline{\mathsf{k}}'$ which are algebraic over k, so $\overline{\mathsf{k}} = \overline{\mathsf{k}}'$.

- **Separable closure:** Let k be a field and $\overline{\mathsf{k}}/\mathsf{k}$ an algebraic closure of k. Let $\mathsf{k}^{\mathrm{sep}} \subseteq \overline{\mathsf{k}}$ be the separable closure of k in $\overline{\mathsf{k}}$. Then $\mathsf{k}^{\mathrm{sep}}$ is separably closed, and it is called a *separable closure* of k.

- **Galois extensions (infinite case):** A field extension K/k is *Galois* if it is normal, separable, and *algebraic*. By transitivity, it follows also in this setup that if we have a tower $\mathsf{k} \subseteq L \subseteq K$ and K/k is Galois, then so is K/L.

- **Lemma:** Let K/k be a Galois extension, and consider a tower $K \supseteq L \supseteq \mathsf{k}$. Then every embedding $L \hookrightarrow K$ which restricts to the identity on k extends to an isomorphism $K \xrightarrow{\simeq} K$.

Apr 19th

- **Proof of lemma:** Use the finite extension lemma and Zorn's Lemma to produce an embedding $K \overset{\widetilde{\sigma}}{\hookrightarrow} K$ extending $L \overset{\sigma}{\hookrightarrow} K$. Surjectivity of such extension is not automatic as in the finite case. So, take an element $\alpha \in K$ with minimal polynomial $f(x) \in \mathsf{k}[x]$. Since $f(x)$ splits into distinct factors in K, it also splits in $\widetilde{\sigma}(K)$. Now α is one of the $\deg f$ roots of $\widetilde{\sigma}(f) = f$. Thus $\alpha \in \widetilde{\sigma}(K)$, as wanted. □

- **Corollary:** Let K/k be a Galois extension, and consider a tower $K \supseteq L \supseteq \mathsf{k}$. If $\sigma(L) = L$ for every $\sigma \in \mathrm{Gal}(K/\mathsf{k})$, then L/k is Galois.

  Proof: It suffices to show that L/k is normal, as algebraicity and separability are elementwise conditions. Let $f(x) \in \mathsf{k}[x]$ be irreducible, with a root $\alpha \in L$. Then $f(x)$ has $n = \deg f$ distinct roots in K, say $\alpha_1 = \alpha, \ldots, \alpha_n$, and for each one we have the diagram

$$\begin{tikzcd}
K \arrow[rr, "\sigma"] \arrow[d, dash] & & K \arrow[d, dash] \\
\mathsf{k}(\alpha) \arrow[rr, "\simeq"] \arrow[dr, dash] & & \mathsf{k}(\alpha_i) \arrow[dl, dash] \\
& \mathsf{k} &
\end{tikzcd}$$

  showing that $\alpha_i \in L$ for all i. □

- **A quick review on point-set topology:** Let X be a topological space. A *basis* for X is a collection $\mathscr{B}$ of subsets of X such that:

  (i) $\bigcup \mathscr{B} = X$;

(ii) Given $B, B' \in \mathscr{B}$ and $x \in B \cap B'$, there is $B'' \in \mathscr{B}$ with $x \in B'' \subseteq B \cap B'$.

(iii) Every open subset of X is the union of elements in $\mathscr{B}$.

Conversely, given a set X and a collection $\mathscr{B}$ of subsets of X, one can define a topology on X by taking the open sets to be unions of elements in $\mathscr{B}$.

Lemma. *Let G be a topological group and $\mathscr{B}_e$ a local basis of open neighborhoods of the identity (that is, every neighborhood of the identity contains some element of $\mathscr{B}_e$). Then:*

(i) For $B, B' \in \mathscr{B}_e$, there is $B'' \in \mathscr{B}_e$ such that $B'' \subseteq B \cap B'$.

(ii) For $B \in \mathscr{B}_e$, there is $B' \in \mathscr{B}_e$ such that $B'B' \subseteq B$.

(iii) For $B \in \mathscr{B}_e$, there is $B' \in \mathscr{B}_e$ such that $B' \subseteq B^{-1}$.

(iv) For $B \in \mathscr{B}_e$ and $g \in G$, there is $B' \in \mathscr{B}_e$ such that $B' \subseteq gBg^{-1}$

(v) For any $g \in G$, $\mathscr{B}_g = g\mathscr{B}_e$ is a local basis of open neighborhoods of g.

And conversely, given $\mathscr{B}_e$ satisfying (i) to (iv), there is a unique topology on G satisfying also (v).

Proof: Condition (i) is trivial. Conditions (ii), (iii) and (iv) follow from the continuity of the multiplication, inversion and conjugation. Condition (v) follows from translations being homeomorphisms. The converse follows from declaring $\{g \cdot \mathscr{B}_e \mid g \in G\}$ as a basis for the topology. □

- **Theorem:** Let K/k be any field extension. For any finite subset $S \subseteq K$, consider $G_S = \{\sigma \in \mathrm{Gal}(K/\mathsf{k}) \mid \sigma(s) = s \text{ for all } s \in S\}$. Then $\mathrm{Gal}(K/\mathsf{k})$ has a unique structure of topological group for which $\{G_S \mid S \subseteq K \text{ is finite}\}$ is a local basis of open neighborhood of the identity. Furthermore, in this topology, $\mathscr{N}_e = \{G_S \mid S \subseteq K \text{ is finite and } G \cdot S = S\}$ is a base of open *normal* neighborhoods of the identity. This is called the *Krull topology* on $\mathrm{Gal}(K/\mathsf{k})$, and when $K = \mathsf{k}^{\mathrm{sep}}$, $\mathrm{Gal}(\mathsf{k}^{\mathrm{sep}}/\mathsf{k})$ is called the *absolute Galois group* of k.

  Proof: It suffices to show that $\{G_S \mid S \subseteq K \text{ is finite}\}$ satisfies conditions (i) to (iv) from the above lemma. Indeed, given finite subsets S and S' of K and any $\sigma \in \mathrm{Gal}(K/\mathsf{k})$, we have:

  (i) $G_{S\cup S'} = G_S \cap G_{S'}$.

  (ii) $G_S G_S = G_S$.

  (iii) $G_S^{-1} = G_S$.

  (iv) $\sigma G_S \sigma^{-1} = G_{\sigma \cdot S}$ (which implies that if $\sigma \cdot S = S$ for all $\sigma \in \mathrm{Gal}(K/\mathsf{k})$, then G_S is normal in $\mathrm{Gal}(K/\mathsf{k})$).

  □

- **Remark:** In the previous theorem, one could also replace G_S for the set $G_L = \{\sigma \in \mathrm{Gal}(K/\mathsf{k}) \mid \sigma(x) = x \text{ for all } x \in L\}$, where $K \supseteq L \supseteq \mathsf{k}$ and L/k is a finite extension.

- **Facts:**
  1. (i) $\mathsf{k}^{\mathrm{sep}}/\mathsf{k}$ is the largest algebraic Galois extension of k, i.e., if K/k is any Galois extension, there is an embedding $K \hookrightarrow \mathsf{k}^{\mathrm{sep}}$ which restricts to the identity on k.
  2. (ii) For finite extensions, the Krull topology in the Galois group is the discrete topology.

- **Proposition:** Let $K \supseteq E \supseteq \mathsf{k}$ be a tower of fields with K/k Galois and E/k finite and Galois. Then the map

$$\mathrm{Gal}(K/\mathsf{k}) \ni \sigma \mapsto \sigma\big|_E \in \mathrm{Gal}(E/\mathsf{k}),$$

  which is well-defined by normality of E/k, is a continuous surjection.

  Proof: Denote by π the above map. Any $\sigma \in \mathrm{Gal}(E/\mathsf{k})$ is an embedding $E \hookrightarrow K$ which restricts to the identity on k, and so it extends to an isomorphism $K \to K$. This shows that π is surjective. As for continuity, since the topology on $\mathrm{Gal}(E/\mathsf{k})$ is discrete, it suffice to show that the fibers of π are surjective. But since we're dealing with topological groups, it suffices to show that the kernel of π (the fiber of the identity) is open. Consider the finite set $S \subseteq E$ generating E over k (i.e., $E = \mathsf{k}(S)$). Then $\mathrm{Gal}(K/E) = G_S$ is open and normal. □

Apr 22th

- **Profinite groups:** We'll say that a group G is *profinite* if it is isomorphic to an inverse limit $\varprojlim_I G_i$ of finite groups.

- **Profinite topology:** Let G be a profinite group. Then G has a natural topological group structure which makes it compact, Hausdorff and totally disconnected (that is, the connected subspaces of G are precisely the singletons).

  Proof: Applying the universal property of inverse limits, we get an embedding $G \cong \varprojlim_I G_i \hookrightarrow \prod_{i \in I}$. Each G_i has the discrete topology, so $\prod_{i \in I} G_i$ is Hausdorff, and compact (Tychonoff theorem). So G, equipped with the subspace topology, is Hausdorff. Since the embedding is closed, G is closed and hence compact. As for G being totally disconnected, we recall two general properties of topological groups[14]:

  1. (i) any open subgroup is closed;
  2. (ii) any closed subgroup of finite index is open.

[14] **Proof:**

(i) Let $H \leq G$ be open, and take $g \in G \setminus H$. There is a neighborhood U of e with $U \subseteq H$. Then $gU \subseteq G \setminus H$, and H is closed.

(ii) If $[G : H] = n < +\infty$, write $G/H = \{H, g_2H, \ldots, g_nH\}$ and a disjoint union $G = H \cup \bigcup_{i=2}^n g_iH$. Then $G \setminus H = \bigcup_{i=2}^n g_iH$ is a finite union of closed sets (by (i)), hence closed. Thus H is open.

Then let $N_i = p_i^{-1}(e)$ be the kernel of the projection $p_i\colon G \to G_i$. Then by the above facts, each N_i is clopen and $\bigcap_{i\in I} N_i = \{e\}$, which says that the largest connected subspace of G containing $e \in G$ is $\{e\}$ itself. By homogeneity, the same holds for all points in G (since translations are homeomorphisms). $\square$

- **Proposition:** Let K/k be a Galois extension. Then $\mathrm{Gal}(K/\mathsf{k}) \cong \varprojlim \mathrm{Gal}(E/\mathsf{k})$, where the inverse limit is taken over all finite Galois extensions E/k with $E \subseteq K$. It follows that the Krull topology on $\mathrm{Gal}(K/\mathsf{k})$ is compact, Hausdorff and totally disconnected.

  Proof: Let's show, in fact, that $\mathrm{Gal}(K/\mathsf{k}) \cong \varprojlim_S \mathrm{Gal}(K/\mathsf{k})/G_S$, where the inverse limit is taken over all $\mathrm{Gal}(K/\mathsf{k})$-stable finite subsets S of K (this is clearly isomorphic to the original inverse limit in the statement of the proposition). So, let's organize the argument in steps:

  - For a $\mathrm{Gal}(K/\mathsf{k})$-stable finite subset S of K, the stabilizer G_S is the kernel of the action map $\mathrm{Gal}(K/\mathsf{k}) \to \mathrm{Sym}(S)$. So G_S is a finite index open normal subgroup of $\mathrm{Gal}(K/\mathsf{k})$.
  - Every finite subset S of K is contained in a $\mathrm{Gal}(K/\mathsf{k})$-stable finite subset S' of K: since every $\alpha \in K$ is algebraic, the $\mathrm{Gal}(K/\mathsf{k})$-orbit of α is finite, consisting precisely of the roots of $\min(\alpha, \mathsf{k})(x)$. Thus if we take S' to be the union of the orbits of the elements in S, S' is finite and $\mathrm{Gal}(K/\mathsf{k})$-stable.
  - The map $\mathrm{Gal}(K/\mathsf{k}) \to \prod_S \mathrm{Gal}(K/\mathsf{k})/G_S$ (where the product is taken over all $\mathrm{Gal}(K/\mathsf{k})$-stable finite subsets S of K) is injective: if $\sigma \in \mathrm{Gal}(K/\mathsf{k})$ is not the identity, it moves some $\alpha \in K \setminus \mathsf{k}$. This means that if S is a $\mathrm{Gal}(K/\mathsf{k})$-stable finite subset of K containing α, then σ is not mapped to the trivial element in this particular factor $\mathrm{Gal}(K/\mathsf{k})/G_S$. So the kernel of the map in question is trivial.
  - Since $S' \subseteq S$ implies $G_S \subseteq G_{S'}$ for any two finite subsets of K, we obtain maps $\mathrm{Gal}(K/\mathsf{k})/G_S \to \mathrm{Gal}(K/\mathsf{k})/G_{S'}$. Thus, ordering the collection of $\mathrm{Gal}(K/\mathsf{k})$-stable finite subsets of K by inclusion, we turn $\{\mathrm{Gal}(K/\mathsf{k})/G_S\}_S$ into an inverse system, whose limit is $\mathrm{Gal}(K/\mathsf{k})$.

  The conclusion now follows because the Krull topology (generated by the stabilizers G_S) *is* the profinite topology, as it is the coarsest (homogeneous) topology making all the projections $\mathrm{Gal}(K/\mathsf{k}) \to \mathrm{Gal}(K/\mathsf{k})/G_S$ continuous. $\square$

- **Lemma:** Let K/k be a Galois extension. Then $K^{\mathrm{Gal}(K/\mathsf{k})} = \mathsf{k}$.

  Proof: Any $\alpha \in K$ lies in some finite Galois intermediate extension E/k of K/k, so the conclusion follows from the finite version of this result. Namely, take some finite set S spanning E, so that $\mathrm{Gal}(K/\mathsf{k}) \to \mathrm{Gal}(K/\mathsf{k})/G_E = \mathrm{Gal}(K/\mathsf{k})/G_S$ and $E^{\mathrm{Gal}(E/\mathsf{k})} = \mathsf{k}$. $\square$

- **Lemma:** Let K/k be a Galois extension. Then:

(i) For any intermediate $K \supseteq L \supseteq \mathsf{k}$, we have that K/L is Galois, $\mathrm{Gal}(K/L)$ is closed in $\mathrm{Gal}(K/\mathsf{k})$, and $K^{\mathrm{Gal}(K/L)} = L$.

(ii) For any subgroup $H \leq \mathrm{Gal}(K/\mathsf{k})$, $\mathrm{Gal}(K/K^H) = \overline{H}$ is the *closure* of H in $\mathrm{Gal}(K/\mathsf{k})$.

Proof:

(i) We had already seen that K/L is Galois. Now, for any finite subset S of L, G_S is an open subgroup of $\mathrm{Gal}(K/\mathsf{k})$. Hence it is also closed, and with this $\mathrm{Gal}(K/L) = \bigcap\{G_S \mid S \subseteq L \text{ is finite}\}$ is closed. Also, $K^{\mathrm{Gal}(K/L)} = L$ by the previous lemma.

(ii) We have that $\mathrm{Gal}(K/K^H) \supseteq H$ and $\mathrm{Gal}(K/K^H)$ is closed, so we necessarily have that $\mathrm{Gal}(K/K^H) \supseteq \overline{H}$. For the reverse inclusion, we argue as follows: take $\sigma \in G \setminus \overline{H}$. Then $\{\sigma \cdot G_S \mid S \text{ is finite and } \mathrm{Gal}(K/\mathsf{k})\text{-stable}\}$ is a local basis of open neighborhoods of σ, meaning that for some such S, we have $\sigma \cdot G_S \subseteq G \setminus \overline{H}$. In other words, we obtain a finite $\mathrm{Gal}(K/\mathsf{k})$-stable set S such that $(\sigma \cdot G_S) \cap H = \varnothing$.

Thus S corresponds to some finite Galois extension E/k (e.g., $E = \mathsf{k}(S)$). Now, the restriction map $\mathrm{Gal}(K/\mathsf{k}) \to \mathrm{Gal}(K/\mathsf{k})/G_S$ itself restricts to a map $H \to H/(H \cap G_S)$. So $\sigma\big|_E \notin H/(H \cap G_S)$, meaning that $\sigma\big|_E$ moves some element in the fixed field of $H/(H \cap G_S)$. Hence σ moves some element of K^H, showing that $\sigma \notin \mathrm{Gal}(K/K^H)$.

□

- **Fundamental Theorem of Galois Theory (infinite case):** Let K/k be a Galois extension. Then:

(i) There is an inclusion-reversing bijection

$$\{\text{closed subgroups } H \leq G\} \leftrightarrow \{\text{intermediate fields } \mathsf{k} \subseteq K^H \subseteq K\}.$$

(ii) A closed subgroup $H \leq \mathrm{Gal}(K/\mathsf{k})$ is open if and only if $[K^H : K]$ is finite, in which case we have $[K^H : K] = [\mathrm{Gal}(K/\mathsf{k}) : H]$.

(iii) If $H \leq \mathrm{Gal}(K/\mathsf{k})$ is a closed subgroup corresponding to an intermediate field $K \supseteq L \supseteq \mathsf{k}$, the conjugate $\sigma H \sigma^{-1}$ corresponds to $\sigma(L) \subseteq K$.

(iv) A subgroup $H \leq \mathrm{Gal}(K/\mathsf{k})$ is normal if and only if the corresponding intermediate field $\mathsf{k} \subseteq L \subseteq K$ has L/k Galois. In this case, we have the isomorphism $\mathrm{Gal}(K/\mathsf{k})/H \cong \mathrm{Gal}(L/\mathsf{k})$.

References

[1] Artin, E., *Galois Theory*, Notre Dame Mathematica Lectures Number 2, 1942.

[2] Jacobson, N., *Basic Algebra II*, Dover Books on Mathematics, 2012.

[3] Lang, S., *Algebra*, Springer-Verlag (Graduate Texts in Mathematics), 2002.

[4] Weibel, C. A., *An introduction to homological algebra*, Cambridge University Press, 1994.